



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

TRABAJO DE TITULACIÓN

Previa a la obtención del título de:

INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA.

TEMA:

“Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013.”

AUTORA:

JENNY MARGARITA VELOZ CHUNATA

Riobamba-Ecuador

2015

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de investigación sobre el tema “AUDITORÍA INFORMÁTICA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE, PROVINCIA DE CHIMBORAZO, PERÍODO 2013.” previo a la obtención del título de Ingeniera en Contabilidad y Auditoría CPA., ha sido desarrollado por la Srta. Jenny Margarita Veloz Chunata, ha cumplido con las normas de investigación científica y una vez analizado su contenido, se autoriza su presentación.

Ing. Edison Cristóbal Erazo Robalino
DIRECTOR DEL TRIBUNAL

Ing. Carlos Alfredo Ebla Olmedo
MIEMBRO DEL TRIBUNAL

CERTIFICADO DE RESPONSABILIDAD

Yo, JENNY MARGARITA VELOZ CHUNATA, estudiante de la Escuela de Ingeniería en Contabilidad y Auditoría de la Facultad de Administración de Empresas, declaro que el Trabajo de Titulación que presento es auténtico y original. Soy responsable de las ideas expuestas y los derechos de autoría corresponden a la Escuela Superior Politécnica de Chimborazo.

Jenny Margarita Veloz Chunata

DEDICATORIA

A Dios por llenarme de bendiciones y ser mi fortaleza cada día, dándome oportunidades para lograr mis sueños.

A mi familia por ser el pilar fundamental en mi vida, quienes me han inculcado valores y principios guiando mi camino para ser una persona de bien y una profesional exitosa.

A mis profesores que han compartido sus conocimientos y experiencias dentro y fuera del aula de clase.

A mis compañeros y amigos por el apoyo y confianza que depositaron en mí a lo largo de la carrera.

Jenny Margarita Veloz Chunata

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, y a sus docentes por brindarme conocimientos y experiencias durante toda la carrera ayudando a mi formación profesional.

Al Alcalde del GAD Municipal del Cantón Penipe y al personal que labora en el mismo por darme apertura para realizar la presente investigación.

Al Ing. Cristóbal Erazo R. y al Ing. Carlos Ebla O. por el apoyo, dedicación y experiencia transmitida para realizar el presente trabajo de investigación.

A mis compañeros, amigos y familiares por brindarme su amistad y apoyo durante toda esta etapa de enseñanza.

Jenny Margarita Veloz Chunata

ÍNDICE DE CONTENIDO

Portada.....	i
Certificación del tribunal.....	ii
Certificado de responsabilidad.....	iii
Dedicatoria	iv
Agradecimiento	v
Índice de contenido	vi
Índice de tablas.....	x
Índice de cuadros.....	xi
Índice de gráficos	xi
Índice de anexos	xii
Resumen ejecutivo	xiii
Summary	xiv
Introducción	1
CAPÍTULO I: EL PROBLEMA.....	2
1.1. PLANTEAMIENTO DEL PROBLEMA	2
1.2. Formulación del Problema	4
1.3. Delimitación del Problema.....	6
1.4. JUSTIFICACIÓN	6
1.5. OBJETIVOS	7
1.6. Objetivo General	7
1.7. Objetivos Específicos.....	7
CAPÍTULO II: MARCO TEÓRICO	9
2.1. ANTECEDENTES INVESTIGATIVOS.....	9
2.2.1. Antecedentes históricos.....	9
2.2. FUNDAMENTACIÓN TEÓRICA.....	11
2.2.1. Auditoría	11
2.2.1.1. Concepto.....	11
2.2.1.2. Alcance	12

2.2.1.3.	Objetivo	12
2.2.1.4.	Tipos de Auditoría	12
2.2.1.5.	Riesgo en Auditoría	15
2.2.2.	Auditoría informática	16
2.2.2.1.	Concepto	16
2.2.2.2.	Auditor Informático	17
2.2.2.3.	Importancia	17
2.2.2.4.	Alcance	17
2.2.2.5.	Objetivos.....	18
2.2.2.6.	Riesgo en Informática.....	18
2.2.2.7.	Tipos de Riesgos en Informática	18
2.2.3.	Control interno	19
2.2.3.1.	Concepto	19
2.2.3.2.	Objetivos.....	20
2.2.3.3.	Importancia del Control Interno	21
2.2.4.	Coso II o ERM	21
2.2.4.1.	Concepto.....	21
2.2.4.2.	Componentes	22
2.2.5.	Control interno informático.....	24
2.2.5.1.	Concepto.....	24
2.2.5.2.	Clases de Control Interno Informático	24
2.2.6.	Fases de la auditoría informática.....	25
2.2.6.1.	FASE I. Planificación	25
2.2.6.2.	FASE II. Ejecución.....	29
2.2.6.3.	FASE III. Informe	30
2.2.7.	Papeles de trabajo.....	31
2.2.7.1.	Concepto.....	31
2.2.7.2.	Documentación.....	32
2.2.7.3.	Referencias y marcas	32
2.2.7.4.	Archivo Permanente	33
2.2.7.5.	Archivo Corriente	34
2.2.8.	Evidencia.....	34
2.2.8.1.	Requisitos de la Evidencia.....	35

2.2.8.2.	Clasificación de la Evidencia	35
2.2.9.	Hallazgo	36
2.2.9.1.	Concepto.....	36
2.2.9.2.	Atributos	37
2.2.10.	Indicadores o parámetros.....	37
2.2.10.1.	Concepto.....	37
2.2.10.2.	Cualidades	37
2.2.10.3.	Tipos	38
2.3.	HIPÓTESIS	39
2.3.1.	Hipótesis General	39
2.3.2.	Hipótesis Específicas	39
2.4.	VARIABLES	39
2.4.1.	Variable Independiente	39
2.4.2.	Variable Dependiente.....	39
2.5.	MARCO CONCEPTUAL	40
2.5.1.	Conceptos.....	40
CAPÍTULO III: MARCO METODOLÓGICO		44
3.1.	MODALIDAD DE LA INVESTIGACIÓN	44
3.1.1.	Tipos de estudios de investigación.....	44
3.1.2.	Diseño de la investigación	45
3.2.	POBLACIÓN Y MUESTRA	45
3.3.	MÉTODOS, TÉCNICAS E INSTRUMENTOS	45
3.3.1.	Métodos.....	45
3.3.2.	Técnicas.....	46
3.3.3.	Instrumentos	46
3.4.	RESULTADOS	47
3.5.	VERIFICACIÓN DE LA HIPÓTESIS	57
CAPÍTULO IV: MARCO PROPOSITIVO		60
4.1.	TÍTULO	60
4.1.1	Metodología de la auditoría informática	60
4.2.	CONTENIDO DE LA PROPUESTA	61
4.2.1.	Archivo permanente	61
4.2.1.1.	Información General.....	62

4.2.1.2.	Ubicación.....	65
4.2.1.3.	Base Legal	67
4.2.1.4.	Funciones del GAD Municipal.....	68
4.2.1.5.	Estructura Organizacional	70
4.2.1.6.	Principales Funcionarios	71
4.2.2.	Archivo de planificación	72
4.2.2.1.	Orden de trabajo N° 001	73
4.2.2.2.	Carta de Aceptación de Auditoría	74
4.2.2.3.	Contrato de Auditoria Informática	75
4.2.2.4.	Notificación de inicio de examen	78
4.2.2.5.	Equipo de Trabajo	79
4.2.2.6.	Índice de Auditoría	80
4.2.2.7.	Marcas de Auditoría	82
4.2.3.	Archivo corriente	83
4.2.3.1.	Fase I: Planificación	84
4.2.3.2.	Fase II: Evaluación del Control Interno	96
4.2.3.3.	Fase III: Análisis de Áreas Críticas	131
4.2.3.4.	Fase IV: Informe.....	149
	CONCLUSIONES	165
	RECOMENDACIONES	166
	BIBLIOGRAFÍA.....	167
	ANEXOS.....	169

ÍNDICE DE TABLAS

Tabla 1. Marcas de Auditoría	33
Tabla 2. Pregunta N°1. Realización de una Auditoría Informática	47
Tabla 3. Pregunta N°2. Existencia de una Unidad Informática	48
Tabla 4. Pregunta N°3. Necesidad de una Auditoría Informática	49
Tabla 5. Pregunta N°4. Existencia de un Plan de Contingencias	50
Tabla 6. Pregunta N°5. Manejo de la información y los equipos informáticos	51
Tabla 7. Pregunta N°6. Seguridad de los equipos informáticos	52
Tabla 8. Pregunta N°7. Existencia de un Plan de Capacitación Informática	53
Tabla 9. Pregunta N°8. Uso de firmas electrónicas	54
Tabla 10. Pregunta N°9. Restricción de páginas web	55
Tabla 11. Pregunta N°10. Informe de Auditoría Informática	56
Tabla 12. Cálculo del Grado de libertad	57
Tabla 13. Grados de libertad - Chi Cuadrado	58
Tabla 14. Cálculo del Chi-cuadrado	58
Tabla 15. Frecuencia observada y esperada	59
Tabla 16. Funcionarios del GAD de Penipe	71
Tabla 17. Equipo de Trabajo	79

ÍNDICE DE CUADROS

Cuadro 1. Árbol de Problemas.....	5
Cuadro 2. Hilo Conductor.....	9
Cuadro 3. Tipos de Auditoría	12
Cuadro 4. Fases de la Auditoría Informática	25
Cuadro 5. Clasificación de la Evidencia	35

ÍNDICE DE GRÁFICOS

Gráfico 1. Componentes COSO II.....	22
Gráfico 2. Pregunta N°1. Realización de una Auditoría Informática	47
Gráfico 3. Pregunta N°2. Existencia de una Unidad Informática.....	48
Gráfico 4. Pregunta N°3. Necesidad de una Auditoría Informática	49
Gráfico 5. Pregunta N°4. Existencia de un Plan de Contingencias	50
Gráfico 6. Pregunta N°5. Manejo de la información y los equipos informáticos.....	51
Gráfico 7. Pregunta N°6. Seguridad de los equipos informáticos	52
Gráfico 8. Pregunta N°7. Existencia de un Plan de Capacitación Informática.....	53
Gráfico 9. Pregunta N°8. Uso de firmas electrónicas	54
Gráfico 10. Pregunta N°9. Restricción de páginas web.....	55
Gráfico 11. Pregunta N°10. Informe de Auditoría Informática	56
Gráfico 12. Metodología de la Auditoría Informática	60
Gráfico 13. Ubicación del Cantón Penipe	65
Gráfico 14. Ubicación del GAD Municipal del Cantón Penipe	66
Gráfico 15. Estructura Organizacional	70

ÍNDICE DE ANEXOS

Anexo 1. Solicitud dirigida al Alcalde para recabar información	169
Anexo 2. Certificado de Partida Presupuestaria para Equipos Informáticos	170
Anexo 3. Informe Técnico de Petición de Token (Firma Electrónica) al BCE	171
Anexo 4. Acta de Entrega de Recepción de Bienes para Activos Informáticos.	172
Anexo 5. Ingreso al Sistema Operativo sin contraseña	174
Anexo 6. Ingreso al Sistema Operativo con contraseña	174
Anexo 7. Registro de Entrada de usuarios externos al Municipio	174
Anexo 8. Secretaria General del Municipio.....	175
Anexo 9. Oficina del Técnico de Informática.....	175
Anexo 10. Departamento de Higiene Ambiental y Salud Pública	175
Anexo 11. Concejala del Municipio	176

RESUMEN EJECUTIVO

En el presente trabajo investigativo se realizó una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013, con el objetivo de medir el grado de eficiencia, eficacia y seguridad con la cual el personal maneja la información y los equipos informáticos.

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 Alcalde, visita previa a las instalaciones, marco jurídico al que se rige la entidad y el memorándum de planificación.

Se realizó la evaluación del sistema de control interno informático aplicando los ocho componentes del COSO II con la finalidad de analizar el nivel de riesgo y confianza resultante de los cuestionarios realizados.

En el análisis de áreas críticas se elaboró indicadores de eficiencia, eficacia y seguridad del área informática, y se identificó los principales hallazgos, el más importante fue que el Municipio de Penipe no cumple con las Normas de Control Interno de la CGE, poniendo en riesgo la integridad, seguridad y disponibilidad de los activos informáticos.

A lo que se recomienda a los Directivos del Municipio cumplir y hacer cumplir las Normas de Control de la CGE, específicamente la sección 410 que trata sobre las Tecnologías de la Información, además de instalar dispositivos de seguridad para la protección de los sistemas informáticos.

Ing. Edison Cristóbal Erazo Robalino

DIRECTOR

SUMMARY

In the present research work, an Informatics Auditor ship to the Autonomous Decentralized Municipal Government of the Penipe Canton, Chimborazo Province, 2013 period to measure the efficiency, effectiveness and security degree with which the staff handles the information and the informatics equipment.

The methodology used for the development of the informatics auditor ship has four phases; in planning, the work program, the major interview, a previous visit to the installations, the juridical framework of the entity and the planning memorandum, are detailed.

The informatics internal control system evaluation was carried out applying the eight of the COSO II to analyze the trust level from the questionnaires.

In the analysis of critical areas, efficiency, effectiveness and security indicators of the informatics area were elaborated, and the main findings were identified; the most important was that the Penipe Municipality does not accomplish the CGE Internal Control Norms risking the integrity, security and availability of the informatics assets.

The Municipality Directives are recommended to accomplish and make accomplish the CGE Control Norms, specifically the 410 section which deals with Information Technologies, installing, at the same time, the security devices for the protection of the informatics systems.

INTRODUCCIÓN

La evolución de las nuevas tecnologías ha causado preocupaciones y cambios en la forma de entender y resolver problemas dentro de una entidad, generando a su vez una gran incertidumbre por conocer el funcionamiento y la seguridad de los sistemas 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 mala utilización de los recursos tecnológicos, por ello se desarrolla cuatro capítulos detallados a continuación.

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

CAPITULO II: denominado Marco Teórico donde se desarrolla la fundamentación teórica realizada mediante conceptos, magnitudes, variables, leyes y modelos que ayudan al análisis y solución del problema encontrado, además se formula las hipótesis y variables encontradas.

CAPITULO III: denominado Marco Metodológico donde se identificaron los métodos, técnicas e instrumentos que se utilizó para recolectar información y la población a la cual se aplicó encuestas para verificar la hipótesis mediante el método del Chi-cuadrado.

CAPITULO IV: denominado Marco Propositivo que consta de tres archivos: Permanente, Planificación y Corriente que a su vez se subdivide en cuatro fases: Planificación, Evaluación del Control Interno, Análisis de Áreas Críticas e Informe.

CAPÍTULO I: EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

El avance y la necesidad de tecnología a nivel mundial hacen que los países busquen mejorar su desempeño y competitividad a través de investigaciones y capacitaciones, los mismos se dividen en desarrollados, en vías de desarrollo y subdesarrollados por la inversión tecnológica que realiza cada uno de ellos.

Según los Indicadores del desarrollo mundial (IDM) basados en datos del Banco Mundial establecen que el porcentaje del PIB asignado para la innovación tecnológica a nivel mundial es del 2,13% en el 2011, para América Latina es del 0,84% y para el Ecuador no existe ningún porcentaje en esta base de datos puesto que es un país en vías de desarrollo.

A diferencia de datos mundiales, fuentes ecuatorianas de la SENESCYT y el INEC indican que antes del gobierno de la Revolución Ciudadana la inversión en Ciencia y Tecnología era del 0,06% del PIB, pero en el 2013 el gobierno asignó 782 millones de dólares que equivale al 0,55% del PIB para dicha causa, pero aun no es suficiente puesto que la UNESCO recomienda que llegue como mínimo al 1%.

El Plan Estratégico de la Secretaría Nacional de Planificación y Desarrollo indica que del Presupuesto General del Estado para el 2013 la inversión para el sector público fue del 14% del PIB, de los cuales el 28% es asignado para la tecnología en sectores estratégicos y un 9% para la Investigación, Desarrollo e Innovación del Talento Humano, valores que han incrementado en referencia a los años anteriores.

Según el Ministerio de Finanzas el 67% del Presupuesto General del Estado del 2013 se designó para los GAD Municipales y Distritos Metropolitanos, de este porcentaje le corresponde al GAD Municipal del Cantón Penipe el 0,09% que equivale a USD 1,679.755, de los cuales se distribuye para las diferentes necesidades que tienen las comunidades del cantón y gastos del municipio en sus diferentes áreas.

En el portal de Compras Públicas no se registra ninguna compra de equipos informáticos, contratación de seguros para respaldar los mismos o algún tipo de capacitación referente a la seguridad de la información y al uso de los activos informáticos para los empleados del municipio en el período 2013.

Dado a que el presupuesto que recibe el Municipio es del Estado, el mismo debe cumplir con las funciones establecidas en el Código Orgánico de Organización Territorial, Autonomía y Descentralización, el cual no incluye el aporte hacia el ámbito tecnológico sino a cubrir las necesidades y procurar el bienestar de los habitantes del cantón por medio de obras municipales.

Por otro lado también debe cumplir con las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos, en el numeral **410** se especifica sobre la **Tecnología de la Información**, las mismas que deben ser aplicadas en su totalidad.

Después de analizar los indicadores mundiales, nacionales y locales se puede concluir que actualmente las entidades públicas del Ecuador no invierten los recursos suficientes para el desarrollo tecnológico, lo cual impide que sean eficientes, eficaces y seguros en el manejo de la información y el uso de los equipos informáticos, siendo necesario realizar una Auditoría Informática para mejorar el desempeño de las actividades del GAD Municipal del Cantón Penipe motivo de la presente investigación.

Definición del Problema

Los principales problemas encontrados en el GAD Municipal del Cantón Penipe, en el área informática, se enumeran a continuación:

- Inexistencia de una Unidad Informática dentro del organigrama institucional.
- Carencia de un Plan de Contingencias para prevenir riesgos en la información y en los equipos informáticos.
- No cuenta con un Plan de Capacitación informático para los usuarios de la información y de los equipos informáticos.

- Inseguridad de la información y de los equipos informáticos.

Problema Central de la Investigación

Manejo inadecuado de la información y los equipos informáticos del GAD Municipal del Cantón Penipe.

1.2. Formulación del Problema

¿Cómo influye una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013, en la eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos?

Causas y Efectos de los principales problemas encontrados durante la investigación

1. Inexistencia de una unidad informática dentro del organigrama institucional.

Causa: No se aplica las normas de control interno de la CGE, específicamente el numeral **410-01** donde se define sobre la organización informática, la cual se encarga de regular y controlar todos los temas y proyectos tecnológicos y al mismo tiempo de dar asesoría y apoyo a los usuarios de la información y de los equipos informáticos.

Efecto: Los usuarios de la información y de los equipos informáticos no tienen un lugar donde recibir asesoría y apoyo para resolver problemas, y no se realizan cambios ni mejoras tecnológicas acordes a las necesidades de la entidad.

2. Carencia de un plan de contingencias para prevenir riesgos en la información y en los equipos informáticos.

Causa: Por la inexistencia de una unidad informática no hay personal autorizado que redacte el plan de contingencias, incumpliendo con el numeral **410-11** de las normas de control interno de la CGE.

Efecto: Al no tener un documento que detalle los procedimientos a seguir en caso de alguna emergencia los empleados no saben qué hacer antes, durante o después de un desastre perdiendo tiempo y recursos innecesarios.

3. No cuenta con un Plan de Capacitación informático para los usuarios de la información y de los equipos informáticos.

Causa: Por falta de presupuesto no se realiza capacitación informática a los empleados como está dispuesto en el numeral **410-15** de las normas de control interno de la CGE, puesto que los recursos son destinados para otros fines.

Efecto: Al no existir un plan de capacitación los empleados carecen de habilidades, conocimientos y la preparación necesaria para manejar la información y los equipos informáticos de manera eficiente, eficaz y segura.

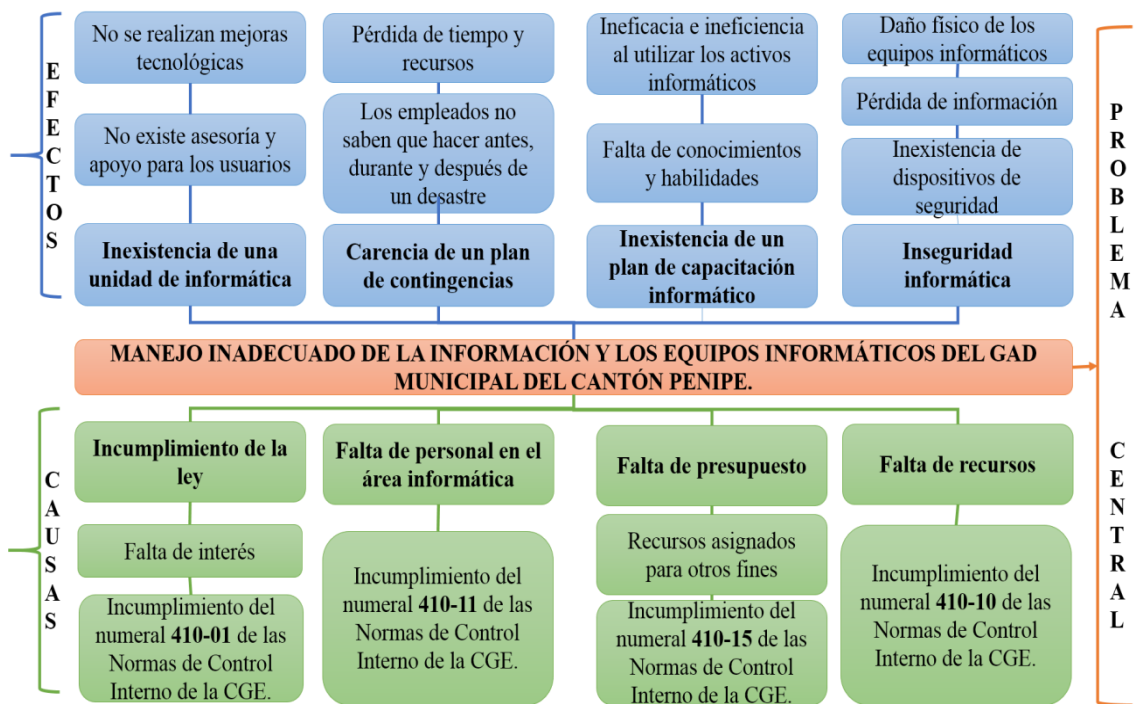
4. Inseguridad de la información y de los equipos informáticos.

Causa: Falta de recursos para implementar un sistema de protección para la seguridad física y lógica de los recursos informáticos, incumpliendo con el numeral **410-10** de las normas de control interno de la CGE, que trata sobre la seguridad informática.

Efecto: La inseguridad provoca pérdida de información y daño físico de los equipos informáticos provocado por desastres naturales, tecnológicos o por terceras personas, ya que no cuenta con dispositivos de seguridad instalados en la entidad para prevenir desastres.

Árbol de Problemas

Cuadro 1. Árbol de Problemas



Fuente: GAD Municipal del Cantón Penipe
Elaborado por: Veloz, J. (2015)

1.3.Delimitación del Problema

Campo: Auditoría

Área: Auditoría Informática

Temporal: Período 2013

Espacial: Gobierno Autónomo Descentralizado Municipal del Cantón Penipe,
Provincia de Chimborazo

1.4.JUSTIFICACIÓN

En el GAD Municipal del Cantón Penipe se ha detectado que el manejo de la información y de los equipos informáticos no es eficiente, eficaz y seguro, debido a la falta de interés por parte del nivel directivo en cumplir y hacer cumplir las **Normas de Control Interno de la CGE**, la sección **410** que se refiere a las **Tecnologías de la Información**.

Dado a los problemas detectados y a que no se ha realizado una Auditoría Informática hasta la actualidad, es necesario realizar la presente investigación con la finalidad de poner en práctica los conocimientos adquiridos en la carrera y dar soluciones a las falencias encontradas en el Municipio de Penipe.

La importancia de realizar la presente investigación es porque permite evaluar el uso, control y seguridad de la Infraestructura Tecnológica permitiendo adoptar medidas de control: detectivas, preventivas y correctivas, con la finalidad de asegurar la confidencialidad y disponibilidad de los equipos informáticos y la información almacenada en los mismos.

El impacto que causa el presente trabajo para el Municipio es positivo ya que el manejo de los activos informáticos será eficiente, eficaz y seguro, así como el servicio que brinda a la comunidad, puesto que la información entregada será confiable y siempre estará disponible para los usuarios internos y externos que tengan acceso autorizado a la misma.

Los beneficiarios directos son el Alcalde, los Concejales y empleados que laboran en el Municipio de Penipe, ya que utilizan la Infraestructura Tecnológica como principal herramienta de trabajo, los beneficiarios indirectos son las personas de la comunidad que reciben el servicio que brinda la entidad y finalmente el investigador que mediante la aplicación de conocimientos adquiridos en las aulas de clase durante el transcurso de la carrera cumple con uno de los requisitos para obtener el título de Ingeniera en Contabilidad y Auditoría CPA.

Es factible realizar la presente Auditoría al Municipio de Penipe, ya que existe la autorización y colaboración del Alcalde para visitar las instalaciones y el personal en proporcionar la información necesaria para el desarrollo de la investigación, con el objetivo de mejorar el desempeño en el área informática.

La presente investigación es trascendental porque mediante la aplicación de técnicas, métodos y herramientas de auditoría se determina el cumplimiento de la ley, para que a través de recomendaciones la entidad pueda mejorar la utilización de la tecnología y fomentar una cultura informática entre los empleados, para sobresalir entre las demás instituciones públicas y privadas de forma competitiva en el ámbito tecnológico.

1.5.OBJETIVOS

1.6.Objetivo General

Desarrollar una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013, para medir el grado de eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.

1.7.Objetivos Específicos

- Desarrollar un marco teórico, para el estudio de los procesos, normas y reglamentos vigentes, a utilizarse en el trabajo de investigación.

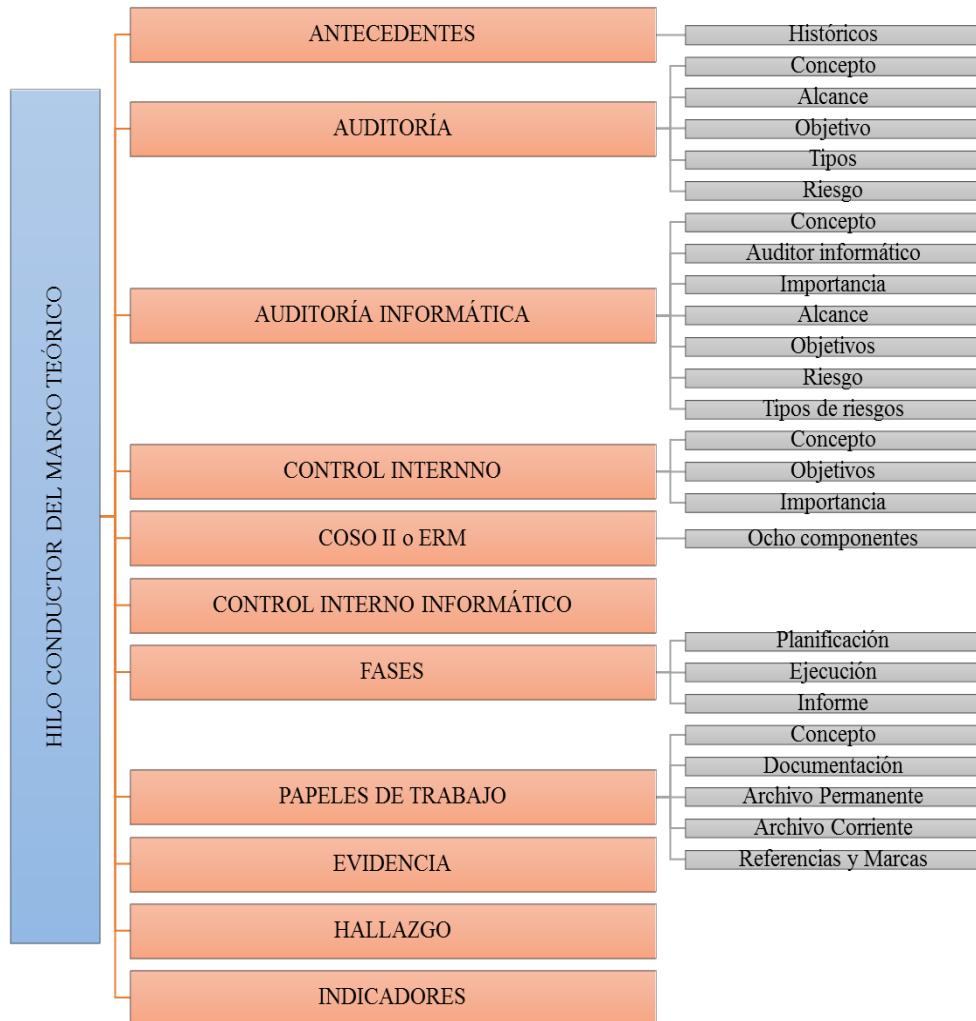
- Determinar la metodología de la auditoría informática mediante el análisis de control interno para evaluar la eficiencia, eficacia y seguridad del manejo de la información y los equipos informáticos.

- Emitir un informe con las conclusiones y recomendaciones, susceptibles de ser tomadas en cuenta para la toma de decisiones correctivas en el manejo de la información y los equipos informáticos.

CAPÍTULO II: MARCO TEÓRICO

Como guía del presente marco teórico se ha elaborado un **Hilo Conductor** para un mejor entendimiento de los temas a tratarse en el Capítulo II.

Cuadro 2. Hilo Conductor



Elaborado por: Veloz, J. (2015)

2.1. ANTECEDENTES INVESTIGATIVOS

2.2.1. Antecedentes históricos

“El concepto de auditoría informática ha estado siempre ligado al de auditoría en general y al de auditoría interna en particular, y éste ha estado unido desde tiempos históricos al de contabilidad, control, veracidad de operaciones, etc. En tiempos de los

egipcios ya se hablaba de contabilidad y de control de los registros y de las operaciones. Aun algunos historiadores fijan el nacimiento de la escritura como consecuencia de la necesidad de registrar y controlar operaciones.”

“Tanto dentro del contexto estratégico como del operativo de las organizaciones actuales, los sistemas de información y la arquitectura que los soporta desempeñan un importante papel como uno de los soportes básicos para la gestión y el control del negocio, siendo así uno de los requerimientos básicos de cualquier organización. Esto da lugar a los sistemas de información de una organización.”

“El concepto de la función de auditoría informática, en algunos casos llamada función de control informático y en ocasiones, llamada y conocida por ambos términos, arranca en su corta historia, cuando en los años cincuenta las organizaciones empezaron a desarrollar aplicaciones informáticas. Posteriormente, en función de que las organizaciones empezaron con sistemas cada vez más complejos, se hizo necesario que parte del trabajo de auditoría empezara a tratar con sistemas que utilizaban sistemas informáticos.”

“En este momento, los equipos de auditoría, tanto externos como internos, empezaron a ser mixtos, con involucración de auditores informáticos junto con auditores financieros, fue entonces cuando se comenzaron a utilizar dos tipos de enfoque diferentes que en algunos casos convergían:”

- “Trabajos en los que el equipo de auditoría informática trabajaba bajo un programa propio, aunque entroncando sus objetivos con los de la auditoría financiera; éste era el caso de trabajos en los que se revisaban controles generales de la instalación y controles específicos de las aplicaciones bajo conceptos de riesgo pero siempre unido al hecho de que el equipo de auditoría financiera utilizaría este trabajo para sus conclusiones generales sobre el componente financiero determinado.”
- “Revisiones en las que la auditoría informática consistía en la extracción de información para el equipo de auditoría financiera. En este caso el equipo o función de auditoría interna era un exponente de la necesidad de las organizaciones y departamentos de auditoría de utilizar expertos en informática para proveer al

personal de dicho departamento de información extraída del sistema informático cuando la información a auditar estaba empezando a ser voluminosa y se estaba perdiendo la pista de cómo se había creado.”

“El futuro de la auditoría informática estará en la capacidad de cubrir adecuadamente, en cuanto a experiencia y especialización, todas las áreas de los sistemas informáticos y de información de una empresa y adecuarse a los cambios que sucedan en la Tecnología de la Información. Para adecuarse a estos cambios, el auditor informático, tendrá que autogenerar su propia filosofía de gestión del cambio.”

(Piattini Velthuis y del Peso, 2008, págs. 107-109)

2.2.FUNDAMENTACIÓN TEÓRICA

2.2.1. Auditoría

2.2.1.1.Concepto

“El vocablo auditoría es sinónimo de examinar, verificar, investigar, consultar, revisar, comprobar y obtener evidencias sobre informaciones, registros, circuitos, etc. Hoy en día, la palabra auditoría se encuentra relacionada con diversos procesos de revisión o verificación que, aunque todos ellos tienen en común el estar de una u otra forma vinculados a la empresa, pueden diferenciarse en función de su finalidad económica.”

(De la Peña Gutierrez, 2011, pág. 5)

En mi opinión: Auditoría es un proceso sistemático que realiza un profesional independiente, a una entidad, un departamento o un proceso específico con la finalidad de recolectar evidencia suficiente, relevante y competente, para verificar el cumplimiento de controles, normas y leyes vigentes en la institución, ayudando a la administración a tomar decisiones correctivas en base a las recomendaciones establecidas en el informe final.

2.2.1.2. Alcance

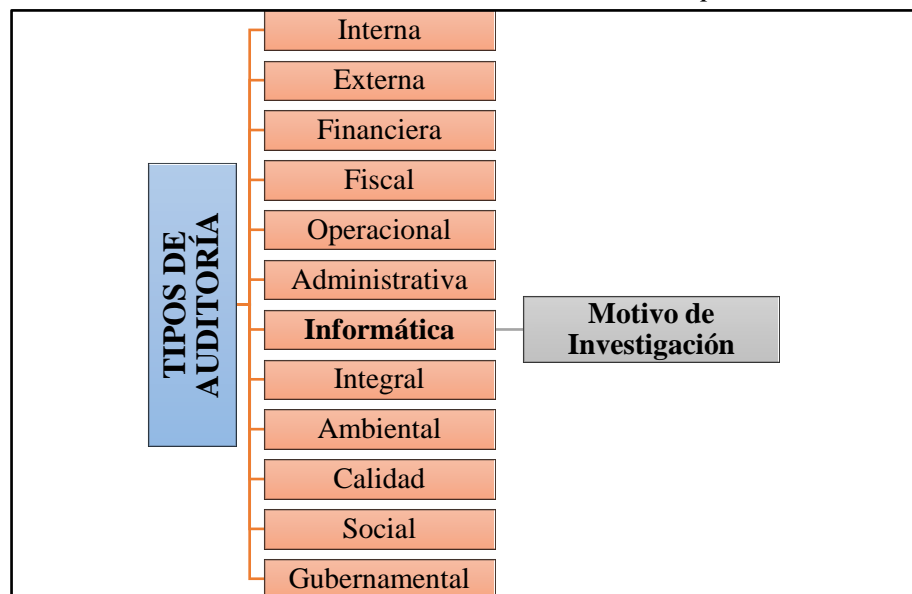
“El campo de aplicación o alcance de la auditoría responde al conjunto de necesidades del cliente y debe quedar bien definido. El alcance especificará las instalaciones y unidades que van a ser cubiertas, así como áreas de estudio que van a ser tratadas, por lo que puede centrarse en un único puesto de trabajo, en un procedimiento o conjunto de procedimientos.” (Fernández Zapico, 2010, pág. 128)

2.2.1.3. Objetivo

“Un objetivo de auditoría se refiere al propósito específico de la auditoría. Los objetivos de auditoría se suelen centrar en probar que los controles internos existen para minimizar los riesgos de la empresa. La Gerencia puede transmitir al auditor un objetivo general para que este realice la auditoría.” (Piattini, 2008, págs. 354-355)

2.2.1.4. Tipos de Auditoría

Cuadro 3. Tipos de Auditoría



Elaborado por: Veloz, J. (2015)

“Ahora que se ha consolidado la presencia de la auditoría en las organizaciones, la financiera ocupa un lugar prominente por ser la pionera en el campo evaluatorio, pero es

inegable que en el transcurso de los años se ha incrementado la realización de auditorías especializadas.” (Amador Sotomayor, 2008, pág. 15)

“**Auditoría interna:** constituye propiamente un mecanismo de control establecido en la organización, que cuenta con personal de la propia empresa designado para el desempeño de actividades de tipo interdisciplinario enfocadas al cumplimiento de los aspectos de vigilancia y sistematización.”

“**Auditoría externa:** representa un trabajo profesional independiente que va enfocado básicamente a la evaluación, pero también a la consultoría en varias especialidades; es realizado por personal ajeno a la organización, el cual presta sus servicios mediante un contrato o carta compromiso que define la actividad que habrá de desarrollarse, tiempos, honorarios, así como tipo y calidad del personal que intervendrá y la fecha de terminación.” (Amador Sotomayor, 2008, págs. 8-9)

“**Auditoría financiera:** este tipo de auditoría está plenamente identificada con las organizaciones, ya que fue la pionera en el campo evaluatorio. Sus resultados y opinión se presentan en un documento formal denominado dictamen, en donde se hace referencia a la situación financiera, estado de resultados, variaciones en el capital contable y los cambios en la situación financiera, lo cual resulta de especial importancia para los inversionistas y medio externo.”

“**Auditoría Fiscal:** en todo el mundo, el aspecto tributario merece la atención de organizaciones y gobierno, ya que ambos se benefician de él. De ahí el interés de cumplir con apego a las disposiciones de la materia y en forma solvente y oportuna.”

“**Auditoría operacional:** aparece en nuestro país como una respuesta a las inquietudes organizacionales en los ámbitos privados y públicos. Para desarrollar este tipo de auditoría resulta pertinente identificar las metas, misión, visión y filosofía de la organización”

“**Auditoría administrativa:** representa en forma general un examen de la administración y su proceso. Es ocasiones este tipo de auditoría suscita divergencias entre los profesionistas que la practican y los que se encuentran involucrados con la

auditoría operacional, situación que muchas veces surge por el celo profesional entre el contador público y el licenciado o maestro en administración, que reclaman ésta como su área natural.”

“**Auditoría informática:** la auditoría de este campo es de vital importancia en las empresas, pues informa sobre la organización, funcionalidad e idoneidad del proceso de sistematización de operaciones con que se cuenta. Asimismo, analiza sus medidas de seguridad, el tipo de hardware y software que utilizan, y la calidad del personal que participa, todo lo cual repercute en la calidad de la información.”

“**Auditoría integral:** la auditoría integral está basada en un enfoque interdisciplinario, que comprende aspectos legales, financieros, administrativos, operacionales, informáticos, entre otros, lo cual goza de aceptación en las organizaciones. Existe una asociación profesional en nuestro medio que difunde su metodología, aplicación y orientación general.”

“**Auditoría ambiental:** ha acrecentado su importancia en el mundo actual: por medio de ella se realizan exámenes técnicos en relación al impacto industrial y de desechos sobre el medio ambiente y los recursos naturales, situación que se agrava día tras día y requiere la implementación de medidas preventivas.”

“**Auditoría de calidad:** 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:** el peso de este tema evaluatorio es grande, porque considera la forma en que afecta las acciones de una empresa a la comunidad. 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: la auditoría gubernamental representa una evaluación del sector que comprende la fiscalización de ingresos, gastos, inversiones, programas, organización y sistemas, principalmente. Recibe su nombre por el sujeto pasivo que recibe la auditoría y no por el que la realiza, ya que este último puede ser un auditor del gobierno o una firma eterna contratada con este fin.”

(Amador Sotomayor, 2008, págs. 17-21)

2.2.1.5. Riesgo en Auditoría

“Es el riesgo que resulta de que los estados contables contengan errores u omisiones significativos en su conjunto, no detectados o evitados por los sistemas de control de la entidad ni por el propio proceso de auditoría. En definitiva, es el riesgo de emitir un informe de auditoría inadecuado.”

“Riesgo inherente: es el riesgo de que ocurran errores significativos en la información contable, independientemente de la existencia de los sistemas de control. Este tipo de riesgo depende de:

- Del tipo de negocio.
- De su medio ambiente.”

“Riesgo de control: es el riesgo de que el sistema de control interno del cliente no prevenga, detecte o corrija dichos errores. Este tipo de riesgo se evalúa mediante el conocimiento y comprobación, a través de pruebas de cumplimiento del sistema de control interno.”

“Riesgo de no detección: es el riesgo de que un error u omisión significativa existente no sea detectado, por último, por el propio proceso de auditoría. El nivel de riesgo de no detección está directamente relacionado con los procedimientos de auditoría de debido a:

- La ineficacia de los procedimientos de auditoría aplicados.
- La inadecuada aplicación de dichos procedimientos.
- Al deficiente alcance y oportunidad de los procedimientos seleccionados.
- A la inapropiada interpretación del resultado de los procedimientos.”

“El riesgo de auditoría se determina a partir de la siguiente fórmula:

$$\mathbf{RA = RI \times RC \times RD}$$

Siendo:

RA = Riesgo de Auditoría

RI = Riesgo Inherente

RC = Riesgo de Control

RD = Riesgo de Detección” (De la Peña Gutierrez, 2011, págs. 48-51)

En mi opinión: El riesgo de auditoría es la probabilidad de que exista un error u omisión en el área que se está auditando ya sea por la propia actividad que ejerce la organización, por la inexistencia o ineficiencia en la aplicación del sistema de control interno o por no detectar errores significativos durante el proceso de auditoría provocando que el auditor emita un informe incorrecto.

2.2.2. Auditoría informática

2.2.2.1. Concepto

“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”

(Franklin Finkowsky, 2013, pág. 20)

En mi opinión: La auditoría informática es una evaluación objetiva que realiza un profesional competente, a los controles internos, procedimientos y normativa vigente que la entidad posee para el uso y protección de los activos informáticos, además de comprobar que su utilización sea eficiente, eficaz y segura con la finalidad de recolectar evidencia relevante, suficiente y competente para emitir recomendaciones que serán expuestas en el informe final de auditoría, el mismo que servirá de apoyo en la toma de decisiones a los directivos de la organización.

2.2.2.2. Auditor Informático

“El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas por ordenador.” (Piattini, 2008, págs. 7-8)

En mi opinión: El auditor informático es un experto en la materia con ética profesional, independiente y competente, con conocimientos teóricos y experiencia suficiente para realizar una auditoría referente al tratamiento de los sistemas informáticos y el uso de sus activos, mediante la aplicación de técnicas, procedimientos y herramientas de auditoría con la finalidad de ayudar a los directivos a contrarrestar los errores encontrados durante el proceso de auditoría informática.

2.2.2.3. Importancia

“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.”

(Gallo, 2010, pág. 106)

2.2.2.4. Alcance

“El alcance ha de 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 ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas” (Gómez López, 2011, pág. 81)

2.2.2.5.Objetivos

- “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.” (Gallo, 2010, pág. 103)

2.2.2.6.Riesgo en Informática

“Se denomina riesgo a la posibilidad que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.” (Aguilera, 2010, pág. 14)

2.2.2.7.Tipos de Riesgos en Informática

“**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. (Piattini Velthuis y del Peso, 2008, págs. 571-572)

2.2.3. Control interno

2.2.3.1. Concepto

“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.” (Contraloría General del Estado, 2012)

En mi opinión: El control interno es un proceso sistemático integral que se ejecuta en forma ordenada y coherente por parte del personal de la entidad, ayudando a proteger y asegurar la integridad de los activos, evitando la aparición de riesgos que afecten a la eficiencia y eficacia de las operaciones que realiza la organización con la finalidad de cumplir con la misión y objetivos de la empresa.

2.2.3.2.Objetivos

Son objetivos del control interno de las empresas, 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.”

(Fonseca Luna, 2008, pág. 404)

2.2.3.3.Importancia del Control Interno

“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” (Mantilla, 2009, pág. 19)

2.2.4. Coso II o ERM

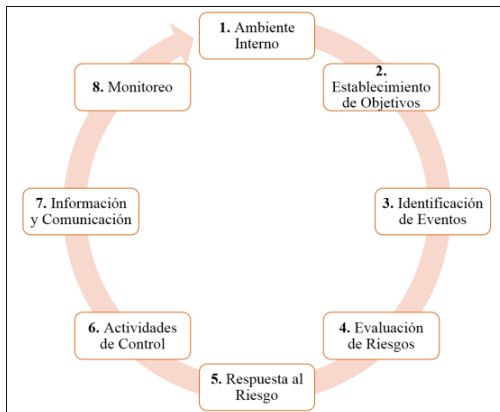
2.2.4.1.Concepto

“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.” (Fonseca Luna, 2011, pág. 285)

En mi opinión: El modelo de Gestión de Riesgos Corporativos COSO II o ERM es un proceso mediante el cual un administrador del riesgo con la colaboración de los directivos y el personal de la entidad elaboran un plan con estrategias para identificar, evaluar y dar respuesta al riesgo, los mismos que deberán ser clasificados de acuerdo al impacto negativo que cause a la organización, con el fin de asumir, eliminar, mitigar o transferir dicho riesgo para cumplir con los objetivos planteados por la empresa.

2.2.4.2. Componentes

Gráfico 1. Componentes COSO II



Elaborado por: Veloz, J. (2015)

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.”

(Fonseca Luna, 2011, págs. 286-287)

2.2.5. Control interno informático

2.2.5.1. Concepto

“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.” (Piattini, 2008, pág. 9)

En mi opinión: El control interno informático es un proceso integral que se encarga de la protección de los activos informáticos existentes en una entidad, ya que pueden ser afectados por la aparición de errores, fallas, fraudes e irregularidades causando daños significativos y pérdidas importantes.

2.2.5.2. Clases de Control Interno Informático

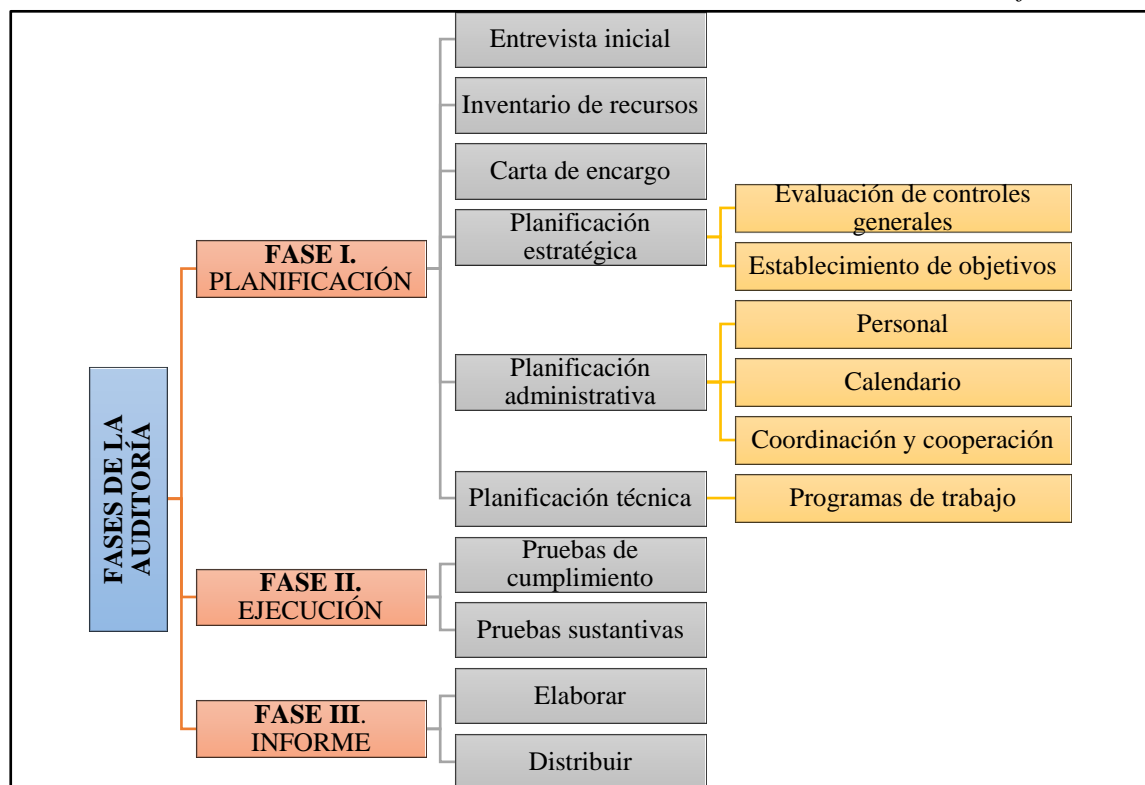
“**Controles preventivos:** para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.”

“**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.” (Piattini, 2008, pág. 9)

2.2.6. Fases de la auditoría informática

Cuadro 4. Fases de la Auditoría Informática



Elaborado por: Veloz, J. (2015)

2.2.6.1. FASE I. Planificación

“La fase de planificación se utiliza para asegurar de que el alcance y el contexto de la auditoría se ha establecido correctamente, que todos los riesgos del sistema de información se han identificado y se han cuantificado, que se asignan los recursos necesarios para que puedan realizar la auditoría, y que se ha desarrollado un plan para

tratar adecuadamente los riesgos identificados. La actividad del plan se documenta para facilitar la gestión y la trazabilidad de la auditoría.”

- **ENTREVISTA INICIAL**

“En esta reunión se le presenta al auditorio el equipo de auditores y el plan de trabajo.”

- **INVENTARIO DE RECURSOS**

“El cliente debe entregar al auditor una lista en la que se incluya una descripción muy breve de los recursos que integran el sistema de información objeto de la auditoría.”

- **CARTA DE ENCARGO**

“Antes de comenzar el trabajo de auditoría deben quedar claras las responsabilidades, la autoridad y las obligaciones del auditor y deben recogerse en un documento, contrato o carta de encargo, según el principio de formalidad expuesto.”

- **PLANIFICACIÓN ESTRATÉGICA**

“Es una revisión global que permite conocer la empresa, el sistema de información y su control interno con la intención de hacer una primera evaluación de riesgos. Según los resultados de esa evaluación establecerán los objetivos de la auditoría y se podrá determinar su alcance y pruebas que hayan de aplicarse, así como el momento de realizarlas. Para llevar a cabo esta tarea es necesario conocer entre otros aspectos los siguientes.

- Las características de los equipos informáticos.
- El sistema o los sistemas operativos.
- La organización de la empresa.
- Informes y papeles de trabajo de auditorías anteriores.
- Planes de contingencia.
- Instrucciones sobre el encendido y apagado de los equipos.
- Contrato de mantenimiento con otras empresas.
- Instrucciones sobre seguridad física y lógica.”

Evaluación de los controles internos

“Es función del auditor evaluar el nivel de control interno; también es de su responsabilidad juzgar si los procedimientos establecidos son los adecuados para salvaguardar el sistema de información.”

“Para evaluar los controles es necesario buscar evidencia sobre:

- La terminación completa de todos los procesos.
- La separación física y lógica de los programas, fuentes y objetos y de las bibliotecas de desarrollo, de pruebas y de producción.
- La existencia de normas y procedimientos para pasar los programas de una biblioteca a otra.
- Las estadísticas de funcionamiento, donde al menos se incluya:
 - Capacidad y utilización del equipo central y de los periféricos.
 - Utilización de la memoria.
 - Utilización de las telecomunicaciones.
- Las normas del nivel de servicios de los proveedores.
- La realización del mantenimiento periódico de todos los equipos.
- La evidencia de la rotación de los turnos de los operadores y de las vacaciones tomadas.”

“Una forma de encontrar evidencia es mediante entrevistas; para llevarlas a cabo se pueden elaborar cuestionarios o listas de comprobación (checklists) con el objetivo de no olvidar detalles importantes. Es conveniente que los cuestionarios y las listas de comprobación se elaboren de tal manera que de las respuestas negativas se infiera debilidad, posibilidad de riesgo; y de las positivas, fortaleza.”

Establecimiento de objetivos

“En función de la importancia de los riesgos que se hayan detectado, el auditor establecerá los objetivos de la auditoría, cuya determinación concreta permitirá definir con claridad el alcance de la misma.”

“Se considera que el riesgo es la presentación negativa de un objetivo de auditoría. Para alcanzar ese objetivo habrá que diseñar una serie de pruebas. Cada una de esas pruebas es un procedimiento. Los procedimientos pueden basarse en métodos de verificación de cumplimiento o sustantivo, así tendríamos pruebas de cumplimiento o pruebas sustantivas.”

- **PLANIFICACIÓN ADMINISTRATIVA**

“La planificación administrativa no se debe hacer hasta haber concluido la planificación estratégica. Así en esta etapa deben quedar claros los siguientes aspectos:

Evidencia.- En este punto se podrá hacer una relación con la documentación disponible en la etapa anterior, documentación que se utilizará indicando el lugar donde se encuentra para que esté a disposición del equipo de auditoría.

Personal.- De qué personal se va a disponer, qué conocimientos y experiencia es la ideal y si va a ser necesario o no contar con expertos, tanto personal de la empresa auditora como expertos externos.

Calendario.- Establecer la fecha de comienzo y de finalización de la auditoría y determinar dónde se va a realizar cada tarea: en las dependencias del cliente o en las oficinas del auditor.

Coordinación y cooperación.- Es conveniente que el auditor mantenga buenas relaciones con el auditado, que se establezca, entre ambos, un nivel de cooperación sin que deje de cumplirse el principio de independencia y que se defina con claridad el interlocutor del cliente.”

- **PLANIFICACIÓN TÉCNICA**

“En esta última fase se ha de elaborar el programa de trabajo. En la fase de planificación técnica se indican los métodos, los procedimientos, las herramientas y las técnicas que se utilizarán para alcanzar los objetivos de la auditoría.”

“El programa de auditoría deber ser flexible y abierto, de tal forma que se puedan ir introduciendo cambios a medida que se vaya conociendo mejor el sistema. El programa, y el resto de los papeles de trabajo, son propiedad del auditor. Este no tiene la obligación de mostrárselos a la empresa que se audita, debiendo custodiarlos durante el tiempo que marque la ley.”

2.2.6.2.FASE II. Ejecución

“En esta fase se llevan a cabo las decisiones adoptadas, se ejecutan los procedimientos diseñados en la fase de planificación. Consiste en llevar a cabo las **pruebas de cumplimiento y sustantivas** que se han planificado para poder alcanzar los objetivos de la auditoría.”

Objetivo General

“El objetivo general de auditoría consistiría en asegurarse de que las funciones sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada y satisfacen los requisitos empresariales.”

Objetivos específicos

“Para alcanzar el objetivo general, se puede dividir este objetivo en diversos objetivos específicos sobre los que se realizarán las pruebas oportunas para asegurarse de que el objetivo general se alcanza. El esquema de trabajo, para cada uno de los objetivos, es el siguiente:

- Comprender las tareas, las actividades del proceso que se está auditando.
Si fuera necesario se ampliará las entrevistas que se han realizado en la fase de planificación estratégica.
- Determinar si son o no apropiados los controles que están instalados.
Si fuera necesario se ampliará las pruebas que se han realizado en la fase de planificación estratégica.
- Hacer pruebas de cumplimiento para determinar si los controles que están instalados funcionan según lo establecido, de manera consistente y continua.

- Hacer pruebas sustantivas para aquellos objetivos de control con los que no se haya podido quedar satisfecho de su buen funcionamiento con las pruebas de cumplimiento.”

“Habrá que realizar el máximo número de pruebas sustantivas si:

- No existe instrumentos de medida de los controles.
- Los instrumentos de medida que existen se consideran que no son los adecuados.
- Las pruebas de cumplimiento indican que los instrumentos de medida de los controles no se han aplicado de manera consistente y continua.”

2.2.6.3.FASE III. Informe

“Una vez realizadas todas estas fases, el auditor está en condiciones de emitir un informe en el que exprese su opinión sobre el sistema auditado.”

“El informe es el instrumento que se utiliza para comunicar los objetivos de la auditoría, el alcance que se vaya a tener, las debilidades que se detecten y las conclusiones a las que se lleguen.”

Tipos de informes

“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.
2. **Desfavorable:** si el auditor considera que el sistema es un desastre.
3. **Con salvedades:** el sistema es satisfactorio, aunque contiene ciertas debilidades o incumplimientos que no lo invalidan.
4. **Denegación de opinión:** también podría ocurrir que el auditor no tenga suficientes elementos de juicio para poder opinar; en ese caso no opinaría.”

“En el caso de que las salvedades impidan al auditor formarse una opinión, ya sea por falta de información, o por no haber tenido acceso a ella por los motivos que fueren,

pero siempre ajenos a la voluntad del auditor, y no obstante, haber intentado hacer pruebas alternativas, el auditor denegará su opinión.”

Recomendaciones

“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.” (Piattini, 2008, págs. 356-379)

2.2.7. Papeles de trabajo

2.2.7.1. Concepto

“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.”

(Piattini, 2008, págs. 382-383)

2.2.7.2.Documentación

“Como ya hemos puesto de manifiesto, los papeles de trabajo constituyen la documentación que soporta el trabajo realizado por el auditor y, al tener diversas procedencias, pueden tener distintas características y tamaños en función del contenido de la información que recogen.”

“Con el fin de que puedan archivarse adecuadamente, y permitir el seguimiento de la auditoría realizada a otra persona distinta de la que ha efectuado el trabajo, es necesario que los papeles de trabajo reúnan una serie de características, que para el REA (Registro de Economistas Auditores) serían las siguientes:

Completos: el contenido y el diseño de cada hoja de trabajo estará en función de los objetivos que se pretendan alcanzar con la misma, no obstante es posible fijar una serie de datos que deberán figurar en todas las hojas o cédulas de trabajo.

Claros: la presentación y el contenido de cada papel de trabajo deben permitir que una persona no familiarizada con el trabajo pueda comprenderlos.

Concisos: sólo deben confeccionarse los papeles de trabajo que sean estrictamente necesarios, y cada uno de ellos debe contener lo esencial para su comprensión, debiéndose eliminar los detalles no necesarios.”

(De la Peña Gutierrez, 2011, pág. 73)

2.2.7.3.Referencias 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.”

(De la Peña Gutierrez, 2011, págs. 73-74)

Tabla 1. Marcas de Auditoría

MARCA	SIGNIFICADO
H	Hallazgo
D	Debilidad
Σ	Sumatoria
Ω	Sustentado con Evidencia
√	Verificado
A	Incumplimiento de normativa
¥	Confrontado con libros
μ	Corrección realizada
△	Sumas verificadas
∅	No reúne requisitos
«	Pendiente de registro
ã	Conciliado
Æ	Circularizado
¶	Sumado verticalmente

Elaborado por: Veloz, J. (2015)

2.2.7.4. Archivo Permanente

“El archivo permanente contiene todos aquellos papeles que tienen un interés continuo, una validez plurianual, tales como;

- Características de los equipos y de las aplicaciones.
- Manuales de los equipos y de las aplicaciones.
- Descripción del control interno.
- Organigramas de la empresa en general.
- Organigramas del Servicio de Información y división de funciones.
- Cuadro de planificación plurianual de auditoría.
- Escrituras y contratos.
- Consideraciones sobre el negocio.

- Consideraciones sobre el sector.
- En general toda aquella información que puede tener una importancia para auditorías posteriores.” (Piattini, 2008, págs. 383-384)

2.2.7.5. Archivo Corriente

Este archivo, a su vez, se divide en archivo general y en archivo de áreas o de procesos.

a) Archivo general

“Los documentos que se suelen archivar aquí son aquellos que no tienen cabida específica en algunas de las áreas/procesos en que hemos dividido el trabajo de auditoría, tales como:

- El Informe del Auditor.
- La Carta de recomendaciones.
- Los acontecimientos posteriores.
- El cuadro de planificación de la auditoría corriente.
- La Correspondencia que se ha mantenido con la dirección de la empresa.
- El tiempo que cada persona del equipo ha empleado en cada una de las áreas/procesos.”

b) Archivo por áreas/procesos

“Se debe preparar un archivo para cada una de las áreas o procesos en que hayamos dividido el trabajo e incluir en cada archivo todos los documentos que fueron necesarios para realizar el trabajo de esa área/proceso concreto. Al menos deberán incluirse los siguientes documentos:

- Programa de auditoría de cada una de las áreas/procesos.
- Conclusiones del área/proceso en cuestión.
- Conclusiones del procedimiento en cuestión.”

(Piattini, 2008, págs. 384-385)

2.2.8. Evidencia

“Es 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.”

(Norma Internacional de Auditoría, 2013, pág. 2)

2.2.8.1. Requisitos de la Evidencia

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

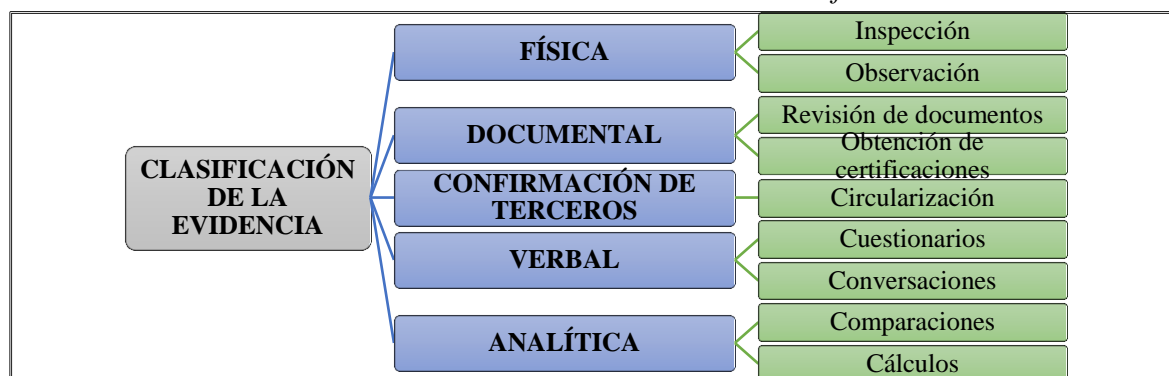
Competente: Debe ser consistente, convincente, confiable, y haber sido validada.

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.” (Franklin Finkowsky, 2013, pág. 89)

2.2.8.2. Clasificación de la Evidencia

Cuadro 5. Clasificación de la Evidencia



Elaborado por: Veloz, J. (2015)

“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.” (De la Peña Gutierrez, 2011, págs. 60-67)

2.2.9. Hallazgo

2.2.9.1. Concepto

“Resultado de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de la auditoría. Las observaciones y evidencias recopiladas durante el proceso de auditoría deberán ser evaluadas frente a los criterios de auditoría previamente definidos hasta obtener los hallazgos y posterior conclusiones de las mismas.”

(Couto, 2011, pág. 183)

2.2.9.2. Atributos

“**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.” (Maldonado, 2011, págs. 71-73)

2.2.10. Indicadores o parámetros

2.2.10.1. Concepto

“Desde el punto de vista de la organización de empresas, se define un parámetro como un elemento que caracteriza un aspecto susceptible de medida con el propósito de evaluar o establecer un control sobre tal aspecto, es una variable que en una familia de elementos sirve para identificar cada uno de ellos mediante su valor numérico.”

(Muñoz, 2010, pág. 12)

2.2.10.2. Cualidades

“**Persistencia:** es adecuado para lo que se quiere medir.

Objetividad: su cálculo no es ambiguo a partir de magnitudes observadas.

Univocidad: las modificaciones expresadas al indicador no permiten interpretaciones equivocadas.

Sensibilidad: se identifican pequeñas variaciones de la medida.

Precisión: el margen de error es aceptable.

Fidelidad: sus cualidades se mantienen a lo largo de un tiempo.

Accesibilidad: su obtención tiene un coste aceptable, fácil de interpretar y calcular.”

(Muñoz, 2010, pág. 12)

2.2.10.3. Tipos

“**Indicadores de implantación:** todo sistema de información tiene implantados, en mayor o menor grado, un conjunto de servicios de seguridad. El nivel de seguridad alcanzado, se mide en base a los mecanismos de control implantados a nivel de sistema de información, de plataforma tecnológica o de toda la empresa. La medición puede realizarse en términos absolutos, en comparación con otras empresas o comparando con algún modelo de referencia.”

“**Indicadores de eficiencia:** aportan información al proceso sobre el mejor o peor funcionamiento de los mecanismos de control ya implantados. La implantación de un antivirus no evita que se presenten incidentes debidos a esa amenaza. Miden la cantidad de incidentes relacionados con los mecanismos que forman parte del sistema de seguridad y que se ha decidido controlar.”

“**Indicadores de costes de la seguridad:** es conveniente poder disponer de esta información, si bien, obtenerla, puede suponer un trabajo excesivo para muchas empresas. Una solución inicial puede ser obtener la información a nivel de orden de magnitud en gastos e inversiones anuales asignadas a este concepto. Se puede partir de una recopilación manual de datos y alimentarlos con alguna herramienta ofimática tipo hoja de cálculo o base de datos personal.”

“**Indicadores de costes de la inseguridad:** en línea con lo planteado en el apartado anterior, los indicadores de costes de la inseguridad pretenden disponer de información a nivel de orden de la magnitud de los costes asociados a los incidentes de seguridad. La

obtención de los datos se plantea también de forma manual y en base a un formulario que se complementa en aquéllos incidentes relevantes.” (Areitio, 2008, págs. 97-98)

2.3.HIPÓTESIS

2.3.1. Hipótesis General

El desarrollo de una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, periodo 2013, mide el grado de eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.

2.3.2. Hipótesis Específicas

- El desarrollo de un marco teórico, permite estudiar los procesos, normas y reglamentos vigentes utilizados en el trabajo de investigación.
- La determinación de la metodología de la auditoría informática mediante el análisis de control interno, evalúa la eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.
- La emisión del informe con las conclusiones y recomendaciones, ayuda a la toma de decisiones correctivas en el manejo de la información y los equipos informáticos.

2.4.VARIABLES

2.4.1. Variable Independiente

- Auditoría Informática

2.4.2. Variable Dependiente

- Grado de eficiencia, eficacia y seguridad en el manejo de la información y de los equipos informáticos.

2.5.MARCO CONCEPTUAL

2.5.1. Conceptos

A

Activos Informáticos

“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.” (Aguilera, 2010, pág. 12)

Amenaza

“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.” (Aguilera, 2010, pág. 13)

Auditor

“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.” (Global, 2007, pág. 223)

Auditoría

“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” (Franklin Finkowsky, 2013, pág. 20)

Auditoría Informática

“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.” (Gallo, 2010, pág. 102)

D

Datos

“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.” (Aguilera, 2010, pág. 12)

E

Eficiencia

“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.” (Maldonado, 2011, pág. 26)

Eficacia

“La eficacia es el grado en que son alcanzados, en forma continua, los objetivos de los programas y los efectos esperados de una entidad.” (Maldonado, 2011, pág. 26)

F

Fortuito

“Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistemas, catástrofes naturales, etc.” (Aguilera, 2010, pág. 10)

Fraudulento

“Daños causados por software malicioso intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados” (Aguilera, 2010, pág. 10)

H

Hardware

“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.” (Aguilera, 2010, pág. 12)

I

Información

“Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.” (Aguilera, 2010, pág. 8)

Informática

“La informática es la ciencia que se dedica al procesamiento automático de datos o información por medio de computadoras para una aplicación específica.” (Ibanez, 2009, pág. 10)

Integridad

“Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.” (Aguilera, 2010, pág. 10)

P

Plan de Contingencia

“Es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolos tras un impacto” (Aguilera, 2010, pág. 23)

Programa de trabajo

“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.”

(Amador Sotomayor, 2008, pág. 72)

Papeles de trabajo

“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.” (García Hurtado, 2011, pág. 382)

R

Recursos

“Pueden ser físicos, como ordenadores, componentes, periféricos, y conexiones, recursos informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.” (Aguilera, 2010, pág. 8)

S

Seguridad Informática

“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.” (García Hurtado, 2011, pág. 2)

Sistema de Información

“Un sistema de información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos.” (Aguilera, 2010, pág. 8)

Sistema Informático

“Un sistema informático 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).” (Aguilera, 2010, pág. 8)

Software

“Constituido por 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.” (Aguilera, 2010, pág. 12)

CAPÍTULO III: MARCO METODOLÓGICO

3.1. MODALIDAD DE LA INVESTIGACIÓN

Los tipos de investigación que se aplicaron en el presente trabajo fueron dos, la primera cualitativa que permite describir un evento mediante la aplicación de técnicas como la observación y la segunda cuantitativa que analiza los datos recolectados de manera numérica, por ende la modalidad de la investigación es mixta.

Cualitativa.-Se realizó descripciones detalladas del manejo y seguridad de la información y de los equipos informáticos existentes en el GAD Municipal del Cantón de Penipe.

Cuantitativa.-La información se obtuvo mediante encuestas realizadas al personal del Municipio de Penipe que tiene bajo su custodia los equipos informáticos y la información almacenada en los mismos.

3.1.1. Tipos de estudios de investigación

Descriptiva.-En la investigación se describió eventos, procesos y situaciones reales sobre la información y los equipos informáticos del GAD Municipal del Cantón Penipe, con el objetivo de medir el grado de eficiencia, eficacia y seguridad con que se manejan los mismos.

Explicativa.-En el presente trabajo se explica el comportamiento de las variables con el fin de descubrir las causas que lo provocaron mediante el establecimiento de relaciones causa-efecto.

Correlacional.-Se estudia la relación que existe entre las variables independiente y dependiente establecido en la investigación, es decir, la relación entre la Auditoría informática y el grado de eficiencia, eficacia y seguridad con que se manejan la información y de los equipos informáticos.

3.1.2. Diseño de la investigación

Diseño Cuasi- Experimental.-Las variables estudiadas en la investigación no varían, puesto que se midió los resultados de las mismas mediante la evaluación del control interno para reforzar los hallazgos encontrados en los diferentes componentes del COSO II.

Estudio Longitudinal.-Se realizó este tipo de estudio puesto que el período de análisis y de recolección de datos es del año 2013, con el fin de analizar el comportamiento de las variables.

3.2. POBLACIÓN Y MUESTRA

Partiendo del concepto de población que es el conjunto de todos los elementos que va a estudiar y de muestra que es una parte significativa de la población con las mismas características se describe cuál de las dos alternativas es más factible para la presente investigación.

Para el desarrollo de la investigación se aplicaron encuestas a funcionarios y empleados del GAD Municipal del Cantón Penipe que tienen la custodia de la información y de los equipos informáticos, siendo el Universo un total de 20 personas por lo que no se tomó una muestra dado que la población es muy pequeña.

3.3. MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.3.1. Métodos

Método Deductivo.-Es un tipo de razonamiento que lleva de lo general a lo particular o de lo complejo a lo simple, este método se utilizó para el planteamiento del problema donde se detalla indicadores mundiales hasta llegar a información particular del Municipio de Penipe.

Método Inductivo.-Parte de casos particulares y se eleva a conocimientos generales, este método se utilizó para analizar el cumplimiento de las Normas de Control Interno

de la CGE por parte del Municipio de Penipe por ende se deduce que todas las entidades del sector público deben cumplir con dichas normas.

3.3.2. Técnicas

Observación directa.-Se efectuaron visitas frecuentes al Municipio de Penipe, con el objeto de recolectar información relevante y apreciar directamente el manejo de la información y de los equipos informáticos por parte de los empleados públicos.

Encuestas.-Las encuestas realizadas a los directivos y al personal del Municipio de Penipe sirvieron para recolectar información sobre el manejo y seguridad de la información y de los equipos informáticos.

Entrevistas.-Se realizó una entrevista al Alcalde del Municipio para obtener información y evidencia que sustente los hallazgos encontrados en el área de informática.

3.3.3. Instrumentos

Cuestionarios.-Se recolectó información mediante la aplicación de preguntas cerradas dirigidas al Alcalde, Contadora y Técnico de Informática con respecto al manejo de la información y los equipos informáticos.

Checklists.-Se realizó preguntas complementarias al personal del Municipio para terminar el desarrollo de la investigación.

3.4.RESULTADOS

1. ¿Se ha realizado una Auditoría Informática al GAD Municipal del Cantón Penipe antes del año 2013?

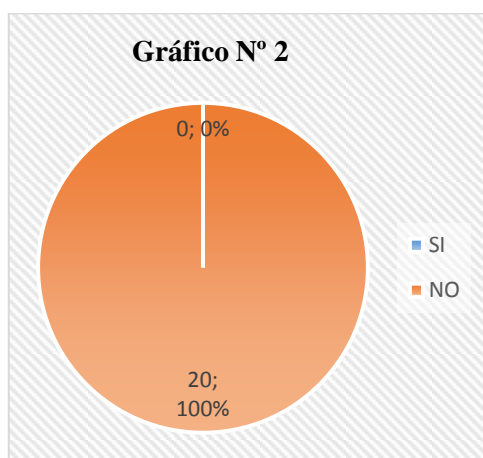
Tabla 2.Pregunta N°1. Realización de una Auditoría Informática

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	0	0%
NO	20	100%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 2.Pregunta N°1. Realización de una Auditoría Informática



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: De las encuestas realizadas a los directivos y al personal del GAD Municipal del Cantón Penipe, el 100% respondió que no se ha realizado una Auditoría Informática antes del año 2013.

2. ¿La entidad cuenta con una Unidad Informática para brindar apoyo y asesoría a los usuarios que manejan la información y los equipos informáticos?

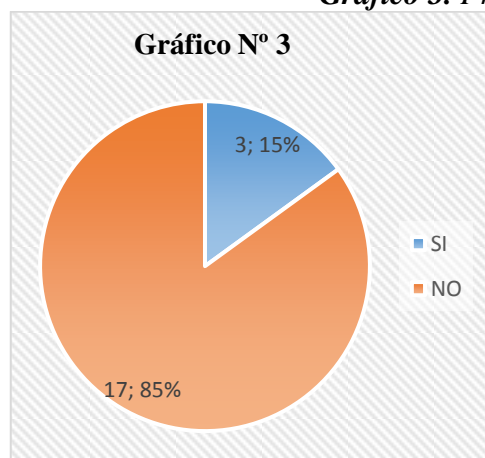
Tabla 3. Pregunta N°2. Existencia de una Unidad Informática

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	3	15%
NO	17	85%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 3. Pregunta N°2. Existencia de una Unidad Informática



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: Del total de los encuestados un 15% contestó que sí existe una Unidad Informática en el Municipio para brindar apoyo y asesoría a los usuarios que la requieran, mientras que un 85% manifestó que no existe dicha unidad.

3. ¿Considera necesario realizar una auditoría informática al GAD Municipal del Cantón Penipe para mejorar el manejo de la información y los equipos informáticos?

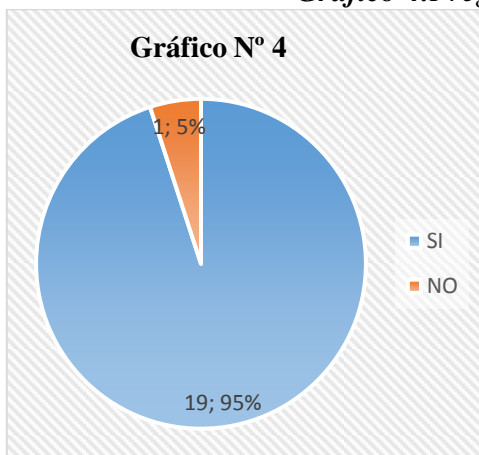
Tabla 4. Pregunta N°3. Necesidad de una Auditoría Informática

ALTERNATIVAS	Nº DE ENCUESTADOS	PORCENTAJE
SI	19	95%
NO	1	5%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 4. Pregunta N°3. Necesidad de una Auditoría Informática



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: Al aplicar las encuestas un 95% afirmó que es necesario realizar una auditoría informática al Municipio para mejorar el manejo de la información y los equipos informáticos, mientras que un 5% manifiesta que no sería necesario.

4. ¿El Municipio cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos?

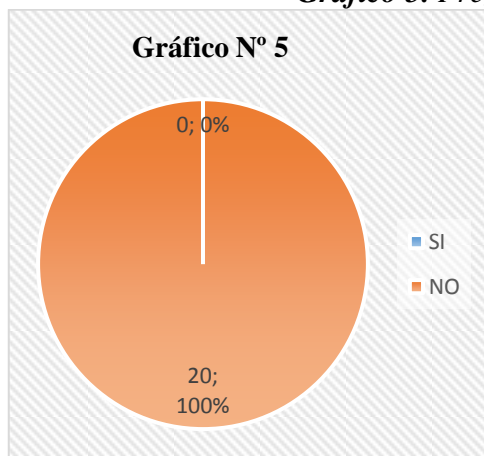
Tabla 5. *Pregunta N°4. Existencia de un Plan de Contingencias*

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	0	0%
NO	20	100%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 5. *Pregunta N°4. Existencia de un Plan de Contingencias*



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: Del total de encuestados un 100% afirmó que el Municipio de Penipe no cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos.

5. ¿Considera que el personal del Municipio maneja la información y los equipos informáticos de manera eficiente, eficaz y segura?

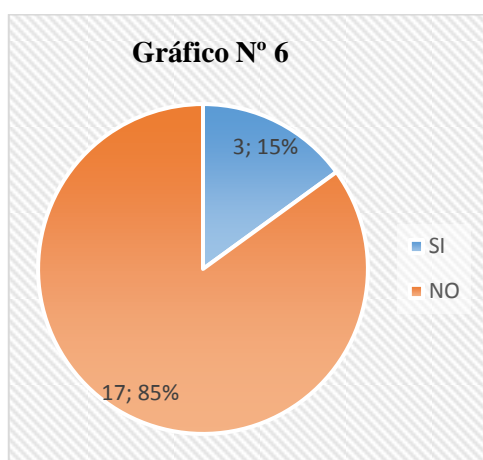
Tabla 6. Pregunta N°5. Manejo de la información y los equipos informáticos

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	3	15%
NO	17	85%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 6. Pregunta N°5. Manejo de la información y los equipos informáticos



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: El 85% de los encuestados manifiesta que no se maneja de manera eficiente, eficaz y segura la información y los equipos informáticos dentro del Municipio, mientras que el 15% considera si se cumplen con los parámetros mencionados.

6. ¿Existen medidas de seguridad para prevenir daños ambientales, tecnológicos y humanos hacia los equipos informáticos?

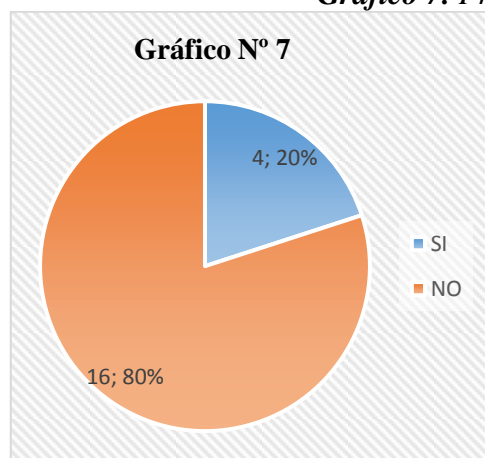
Tabla 7. Pregunta N°6. Seguridad de los equipos informáticos

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	4	20%
NO	16	80%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 7. Pregunta N°6. Seguridad de los equipos informáticos



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: El 80% de los encuestados manifiesta que no existen medidas de seguridad suficientes para proteger los equipos informáticos, mientras que un 20% considera que la seguridad es adecuada.

7. ¿El personal del municipio cuenta con un Plan de Capacitación para el correcto manejo de los activos informáticos?

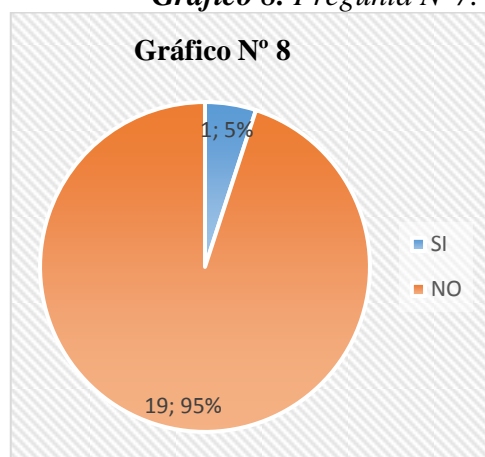
Tabla 8. Pregunta N°7. Existencia de un Plan de Capacitación Informática

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	1	5%
NO	19	95%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 8. Pregunta N°7. Existencia de un Plan de Capacitación Informática



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: Del total de encuestados el 95% manifiesta que no existe un Plan de Capacitación para manejar de manera correcta los activos informáticos, mientras que el 5% afirma que si existe una capacitación, la misma que está a cargo de la Directora Financiera.

8. ¿Utiliza firmas electrónicas para enviar o recibir información del Municipio?

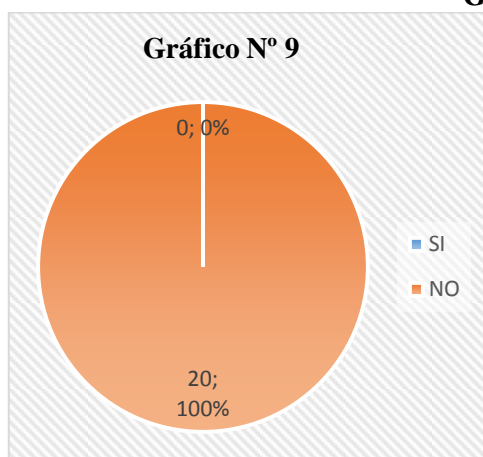
Tabla 9. Pregunta N°8. Uso de firmas electrónicas

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	0	0%
NO	20	100%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 9. Pregunta N°8. Uso de firmas electrónicas



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: Según los resultados de la encuesta realizada al personal del Municipio se concluye que ningún funcionario utiliza firmas electrónicas para enviar y/o recibir información.

9. ¿Le restringen el uso de páginas web como redes sociales, música entre otras que no tiene relación con el trabajo del Municipio?

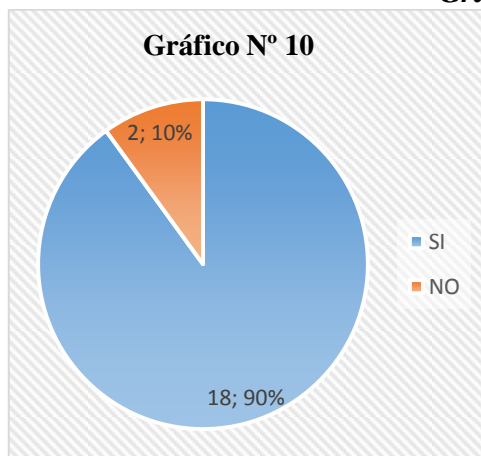
Tabla 10. Pregunta N°9. Restricción de páginas web

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	18	90%
NO	2	10%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 10. Pregunta N°9. Restricción de páginas web



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: Del total de encuestados el 90% manifiesta que se restringe el uso de ciertas páginas web que no tienen ninguna relación con el trabajo que realizan dentro del Municipio, al contrario del 10% que contestó que no les restringen dichas páginas.

10. ¿Considera que el informe de Auditoría Informática es una herramienta que permite a los directivos del Municipio tomar decisiones correctas?

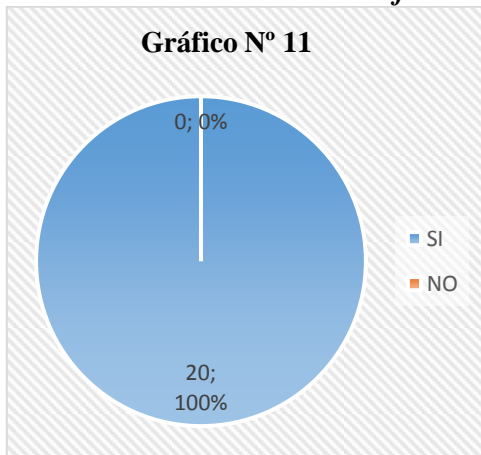
Tabla 11. Pregunta N°10. Informe de Auditoría Informática

ALTERNATIVAS	N° DE ENCUESTADOS	PORCENTAJE
SI	20	100%
NO	0	0%
TOTAL	20	100%

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Gráfico 11. Pregunta N°10. Informe de Auditoría Informática



Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Análisis: El 100% de los encuestados considera que el informe de auditoría es una herramienta que contribuirá positivamente a la toma de decisiones por parte de los directivos de la institución para mejorar el manejo de la información y los equipos informáticos del Municipio.

3.5. VERIFICACIÓN DE LA HIPÓTESIS

H₀: Hipótesis de alternativa

H₁: Hipótesis Nula

H₀: El desarrollo de una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, periodo 2013, mide el grado de eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.

H₁: El desarrollo de una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, periodo 2013, no mide el grado de eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.

Método utilizado

Con el objeto de comprobar las hipótesis establecidas en la presente investigación se emplea la prueba de **Chi-cuadrado**, el cual es un método útil para determinar si dos variables están relacionadas o no.

Determinación del grado de libertad

Tabla 12. Cálculo del Grado de libertad

DETERMINACIÓN DEL GRADO DE LIBERTAD	
FÓRMULA	CÁLCULO
$G_l = (f-1) (c-1)$, donde:	$G_l = (f-1) (c-1)$
G _l = Grado de libertad	$G_l = (2-1) (2-1)$
F = Filas	$G_l = 1$
C = Columnas	

Elaborado por: Veloz, J. (2015)

Chi- Cuadrado según la Tabla

Grado de libertad=1

Nivel de confianza =0.05

$$X^2_t = 3.84$$

$$X^2_t = 3.84$$

Tabla 13. Grados de libertad - Chi Cuadrado

Grados libertad	Probabilidad de un valor superior - Alfa (α)				
	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,6
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75

Elaborado por: Veloz, J. (2015)

Cálculo del Chi-cuadrado

- **Variable dependiente:**

Pregunta N° 3. ¿Considera necesario realizar una auditoría informática al GAD Municipal del Cantón Penipe para mejorar el manejo de la información y los equipos informáticos?

- **Variable independiente:**

Pregunta N° 5 ¿Considera que el personal del Municipio maneja la información y los equipos informáticos de manera eficiente, eficaz y segura?

Tabla 14. Cálculo del Chi-cuadrado

ALTERNATIVA	VARIABLE		TOTAL
	INDEPENDIENTE	DEPENDIENTE	
SI	19	3	22
NO	1	17	18
TOTAL	20	20	40

Fuente: Encuesta

Elaborado por: Veloz, J. (2015)

Frecuencia observada y esperada

Para obtener las frecuencias esperadas multiplicamos el total de cada fila por el total de cada columna dividido para el total de la muestra de las dos variables.

$$Fe = (T.fila * T.columna) / N$$

Tabla 15. Frecuencia observada y esperada

F. OBSERVADAS	F. ESPERADAS	$X^2 = \sum (Fo - Fe)^2 / Fe$
19	11	5,82
3	11	5,82
1	9	7,11
17	9	7,11
40	40	25,86

Resultado del Chi-cuadrado

Chi-Cuadrado calculado = **25,86**

$$X^2 c = 25,86 > X^2 t = 3,84$$

Análisis

De acuerdo a este resultado se obtuvo que $X^2 c$ es mayor que el $X^2 t$ lo cual nos lleva a aceptar la hipótesis de trabajo, es decir: “Desarrollar una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013 para medir el grado de eficiencia, eficacia y seguridad con que se maneja la información y los equipos informáticos.”, y rechazar la hipótesis nula.

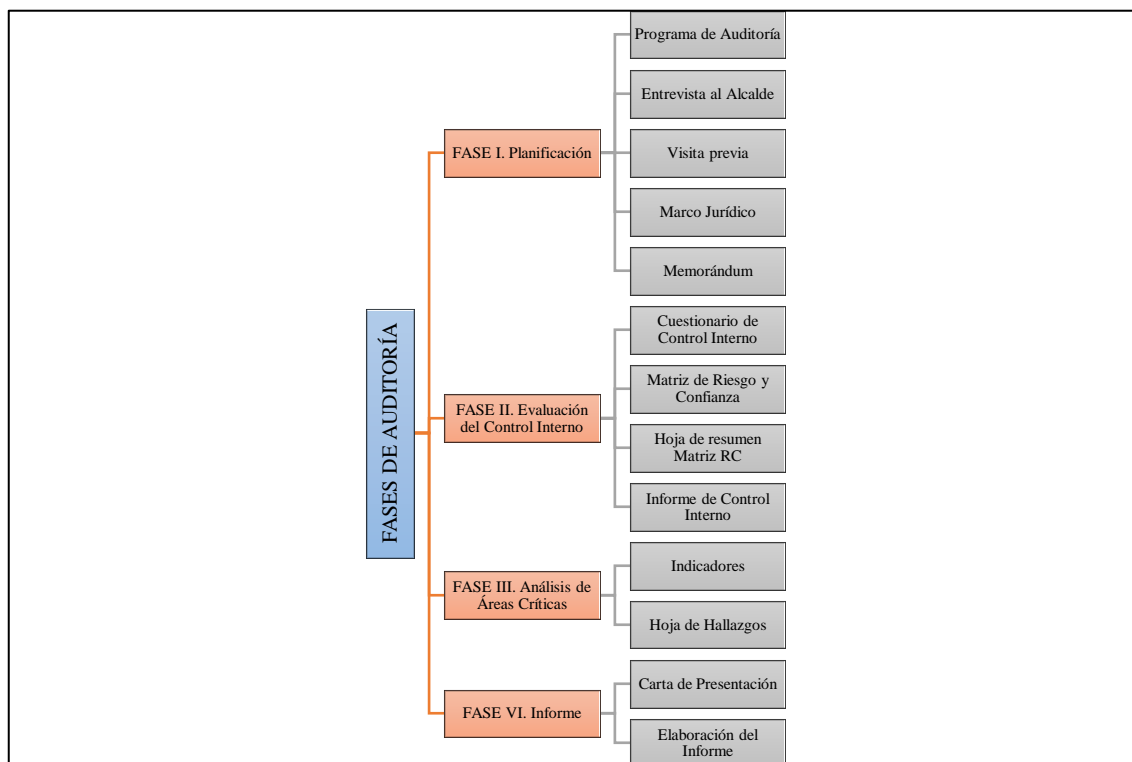
CAPÍTULO IV: MARCO PROPOSITIVO

4.1.TÍTULO

“AUDITORÍA INFORMÁTICA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE, PROVINCIA DE CHIMBORAZO, PERÍODO 2013.”

4.1.1 Metodología de la auditoría informática

Gráfico 12. Metodología de la Auditoría Informática



Elaborado por: Veloz, J. (2015)

4.2. CONTENIDO DE LA PROPUESTA

4.2.1. Archivo permanente



ARCHIVO PERMANENTE

ENTIDAD: GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE

DIRECCIÓN: SILVIO LUIS HARO 08-21 Y DAVID RAMOS (CANTÓN PENIPE)

EXAMEN: AUDITORÍA INFORMÁTICA

PERÍODO: 01 DE ENERO AL 31 DE DICIEMBRE DEL 2013

4.2.1.1. Información General

RESEÑA HISTÓRICA DEL MUNICIPIO

Debido al abandono de Guano, al sector Penipe, el pueblo se une y busca su independencia social, política y económica, organizando un comité en 1983 y tras una lucha dura y tenaz, a base de unidad y constancia, logra conseguir su cantonización el 9 de Febrero de 1984, el nuevo cantón se funda con el nombre de Penipe formada por una Parroquia Urbana y cabecera cantonal denominada Penipe y Parroquia Rurales que son: Puela, el Altar, Matus y Bayushig.

El Cantón se consolida con la elección de las autoridades cantonales, se nombra el primer Concejal al Señor Hermel Valle Mancheno y el primer concejo formado por los señores: Félix Samuel Haro, Ricardo Reinoso, Telmo Villagomez, Carlos Baldeón, Marta Veloz, Raquel Haro.

Posterior a la Cantonización se unieron las Parroquias de la Candelaria y Bilbao. El primer presupuesto asignado para el naciente cantón fue de 10 millones de sucres (400 dólares)

La Municipalidad del cantón Penipe, fue creado mediante Decreto Legislativo N° 15, publicado en el Registro Oficial N° 680 del 9 de Febrero de 1984 y el desarrollo de su vida jurídica e institucional, fue uno de los primeros cantones en integrarse al COMAGA (Consortio de Municipios Amazónicos y Galápagos), hoy en día recibe recursos por parte del gobierno a través de la ley 0.10.

MISIÓN

Administración eficiente que garantice el desarrollo integral de los habitantes asegurando mejores niveles de vida a través de un gobierno responsable y humano, sustentado en principios y valores.

VISIÓN

Ser un gobierno reconocido por la ciudadanía por brindarle servicios de calidad, oportunos y comprometidos, cumpliendo con los requisitos de gobernabilidad para alcanzar un desarrollo económico-social-productivo y equitativo.

OBJETIVOS

Objetivo General

Impulsar el desarrollo socioeconómico de PENIPE, fundamentado en el diálogo y la concertación social que permita alcanzar en el mediano y largo plazo un cantón planificado, sustentable, solidario y seguro.

Objetivos Específicos

- Organizar el territorio cantonal con soluciones para las deficiencias de ordenamiento, infraestructura, equipamiento de servicios públicos, movilidad y transporte, vivienda, ambiente y gestión de riesgos.
- Mejorar las condiciones sociales de los ciudadanos y ciudadanas, coordinando acciones que permitan satisfacer las demandas de la población con el fin de mejorar la calidad de vida.
- Alcanzar un crecimiento equilibrado y equitativo de la producción, el comercio y los servicios, de forma consensuada entre el municipio y los diferentes actores locales.
- Implementar mecanismos que permitan fortalecer y generar la participación social, con el fin de tener cercanía con la ciudadanía y trabajar con certeza en las necesidades que demanda la población.

VALORES

- Transparencia
- Responsabilidad
- Equidad

- Eficacia
- Respeto
- Trabajo en equipo
- Eficiencia

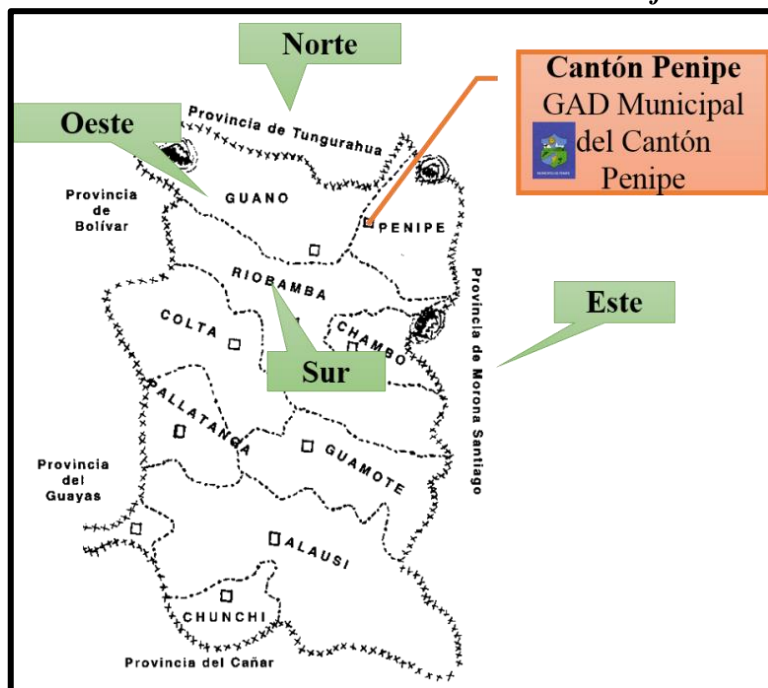
4.2.1.2.Ubicación

Ubicación del cantón Penipe

Se encuentra ubicado al nororiente de la provincia de Chimborazo a 22 Km de distancia de la ciudad de Riobamba y sus límites son:

- **Norte:** Provincia de Tungurahua
- **Sur:** Cantón Riobamba
- **Este:** Provincia de Morona Santiago
- **Oeste:** Cantón Guano

Gráfico 13. Ubicación del Cantón Penipe



Elaborado por: Veloz, J. (2015)

Ubicación del GAD Municipal del Cantón Penipe

País: Ecuador

Provincia: Chimborazo

Cantón: Penipe

Dirección: Silvio Luis Haro 08-21 y David Ramos

Gráfico 14. Ubicación del GAD Municipal del Cantón Penipe



Fuente: Google Maps

4.2.1.3.Base Legal

- Constitución Política de la República del Ecuador
- Ley Orgánica de la Contraloría General del Estado
- Ley de Presupuesto del Sector Público
- Ley Orgánica de Régimen Municipal
- Ley Orgánica de Régimen Tributario Interno
- Ley Orgánica de Servicio Civil y Carrera Administrativa y de Unificación y Homologación de las Remuneraciones del Sector Público
- Normativa de Contabilidad Gubernamental del Ministerio de Finanzas
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos
- Código Orgánico de Organización Territorial Autonomía y Descentralización
- Código de Trabajo

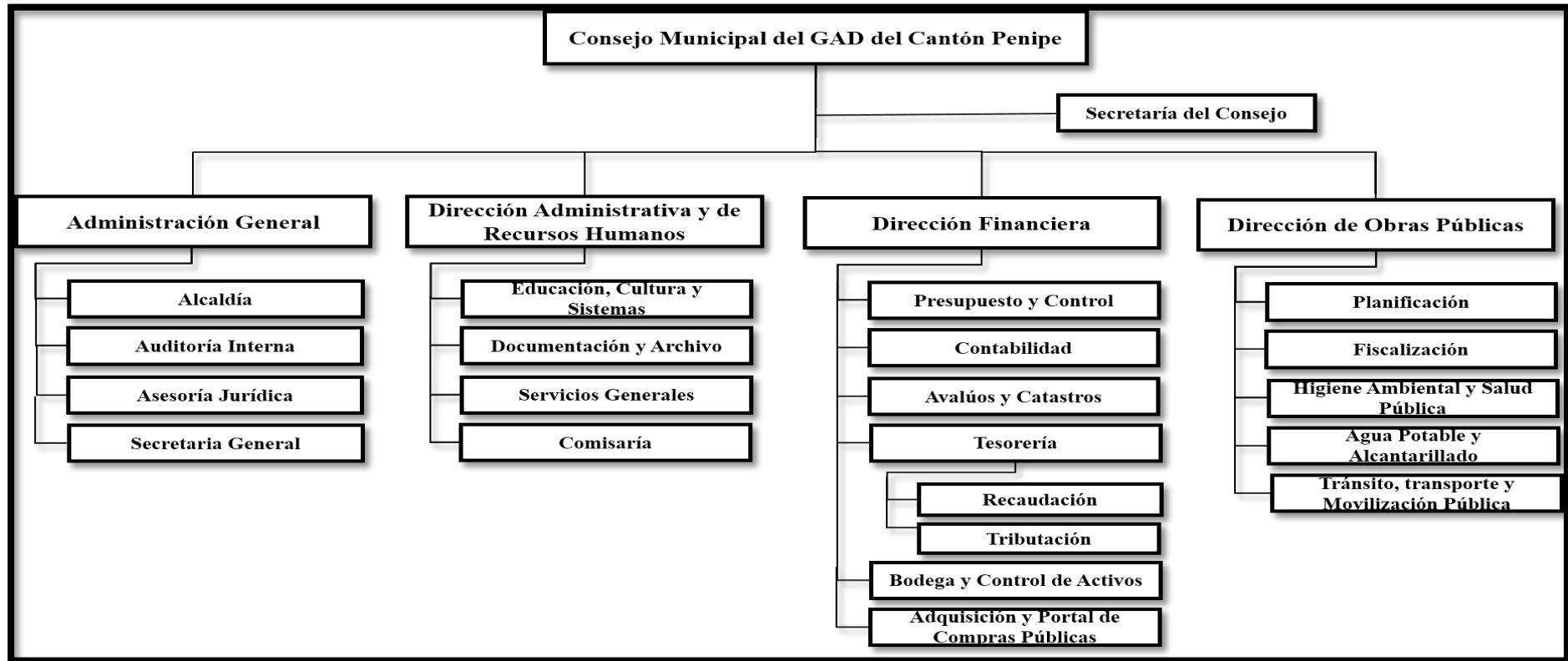
4.2.1.4. Funciones del GAD Municipal

- a) Promover el desarrollo sustentable de su circunscripción territorial cantonal, para garantizar la realización del buen vivir a través de la implementación de políticas públicas cantonales, en el marco de sus competencias constitucionales y legales;
- b) Diseñar e implementar políticas de promoción y construcción de equidad e inclusión en su territorio, en el marco de sus competencias constitucionales y legales;
- c) Establecer el régimen de uso del suelo y urbanístico, para lo cual determinará las condiciones de urbanización, parcelación, lotización, división o cualquier otra forma de fraccionamiento de conformidad con la planificación cantonal, asegurando porcentajes para zonas verdes y áreas comunales.
- d) Implementar un sistema de participación ciudadana para el ejercicio de los derechos y la gestión democrática de la acción municipal;
- e) Elaborar y ejecutar el plan cantonal de desarrollo, el de ordenamiento territorial y las políticas públicas en el ámbito de sus competencias y en su circunscripción territorial, de manera coordinada con la planificación nacional, regional, provincial y parroquial, y realizar en forma permanente, el seguimiento y rendición de cuentas sobre el cumplimiento de las metas establecidas;
- f) Ejecutar las competencias exclusivas y concurrentes reconocidas por la Constitución y la ley y en dicho marco, prestar los servicios públicos y construir la obra pública cantonal correspondiente con criterios de calidad, eficacia y eficiencia, observando los principios de universalidad, accesibilidad, regularidad, continuidad, solidaridad, interculturalidad, subsidiariedad, participación y equidad;
- g) Regular, controlar y promover el desarrollo de la actividad turística cantonal en coordinación con los demás gobiernos autónomos descentralizados, promoviendo especialmente la creación y funcionamiento de organizaciones asociativas y empresas comunitarias de turismo;
- h) Promover los procesos de desarrollo económico local en su jurisdicción, poniendo una atención especial en el sector de la economía social y solidaria, para lo cual coordinará con los otros niveles de gobierno;
- i) Implementar el derecho al hábitat y a la vivienda y desarrollar planes y programas de vivienda de interés social en el territorio cantonal;

- j) Implementar los sistemas de protección integral del cantón que aseguren el ejercicio garantía y exigibilidad de los derechos consagrados en la Constitución y en los instrumentos internacionales, lo cual incluirá la conformación de los consejos cantonales, juntas cantonales y redes de protección de derechos de los grupos de atención prioritaria. Para la atención en las zonas rurales coordinará con los gobiernos autónomos parroquiales y provinciales;
- k) Regular, prevenir y controlar la contaminación ambiental en el territorio cantonal de manera articulada con las políticas ambientales nacionales;
- l) Prestar servicios que satisfagan necesidades colectivas respecto de los que no exista una explícita reserva legal a favor de otros niveles de gobierno, así como la elaboración, manejo y expendio de víveres; servicios de faenamiento, plazas de mercado y cementerios;
- m) Regular y controlar el uso del espacio público cantonal y, de manera particular, el ejercicio de todo tipo de actividad que se desarrolle en él la colocación de publicidad, redes o señalización;
- n) Crear y coordinar los consejos de seguridad ciudadana municipal, con la participación de la Policía Nacional, la comunidad y otros organismos relacionados con la materia de seguridad, los cuales formularán y ejecutarán políticas locales, planes y evaluación de resultados sobre prevención, protección, seguridad y convivencia ciudadana;
- o) Regular y controlar las construcciones en la circunscripción cantonal, con especial atención a las normas de control y prevención de riesgos y desastres;
- p) Regular, fomentar, autorizar y controlar el ejercicio de actividades económicas, empresariales o profesionales, que se desarrollen en locales ubicados en la circunscripción territorial cantonal con el objeto de precautelar los derechos de la colectividad;
- q) Promover y patrocinar las culturas, las artes, actividades deportivas y recreativas en beneficio de la colectividad del cantón;
- r) Crear las condiciones materiales para la aplicación de políticas integrales y participativas en torno a la regulación del manejo responsable de la fauna urbana.

4.2.1.5. Estructura Organizacional

Gráfico 15. Estructura Organizacional



Fuente: GAD Municipal del Cantón Penipe

4.2.1.6.Principales Funcionarios

Tabla 16.Funcionarios del GAD de Penipe

Nro.	FUNCIONARIO	CARGO
01	Lenin Merino Rosero	Concejal
02	Demetria Velasteguí	Concejala
03	Lourdes Mancero Fray	Concejal
04	José Miguel Oñate Casco	Concejal
05	Eliana Maricela Orozco Inca	Concejal
06	Ing. Robin Velasteguí Salas	Alcalde
07	Lcda. Cecilia Padilla	Jefe de Contabilidad
08	Arq. Miguel Cano	Jefe de Planificación
09	Sr. Eduardo Gavidia	Jefe de Movilización
10	Ing. Carlos Hinojosa	Jefe de Avalúos y Catastros
11	Ing. Diego Yépez	Jefe de Compras Públicas
12	Ec. Marco Ramos	Director Financiero
13	Ing. Iván Lara	Fiscalizador
14	Ing. Verónica Granizo	Registradora de la Propiedad
15	Ing. Lucia Gavidia	Contadora
16	Ing. Paulina Alvear	Tesorera
17	Lic. Iván Acosta	Secretario del Consejo Municipal
18	Sra. Nancy Medina	Secretaria General
19	Sra. Vilma Rivera	Recaudación
20	Srta. Jessica Sánchez	Auxiliar de Tesorería

Fuente: GAD Municipal del Cantón Penipe

Elaborado por: Veloz, J. (2015)

4.2.2. Archivo de planificación



ARCHIVO DE PLANIFICACIÓN

ENTIDAD: GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE

DIRECCIÓN: SILVIO LUIS HARO 08-21 Y DAVID RAMOS (CANTÓN PENIPE)

EXAMEN: AUDITORÍA INFORMÁTICA

PERÍODO: 01 DE ENERO AL 31 DE DICIEMBRE DEL 2013

4.2.2.1.Orden de trabajo N° 001

Riobamba, 05 de enero del 2015

Ingeniero

Robin Velasteguí

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PENIPE

Presente.

De mi consideración:

Una vez presentada la propuesta del proyecto de Tesis, permítase dar la apertura necesaria para proceder a efectuar la Auditoría Informática al GAD Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013, con la finalidad de analizar los siguientes objetivos.

- Evaluar el cumplimiento de las leyes y normativas que rigen a la entidad.
- Determinar las medidas de seguridad para salvaguardar los activos informáticos.
- Determinar el grado de confiabilidad del sistema de control interno informático.
- Emitir conclusiones y recomendaciones para mejorar el manejo de la información y de los equipos informáticos.

Atentamente,

Jenny Veloz

AUDITOR

4.2.2.2. Carta de Aceptación de Auditoría

Riobamba, 12 de enero del 2015

Señorita

Jenny Veloz

AUTOR DE TESIS

Presente

De mi consideración

En respuesta a la orden de trabajo N° 001 del 05 de enero del presente año, mediante la cual solicita la apertura necesaria para la realización de su trabajo de tesis con el tema “Auditoría Informática al GAD Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013”, le comunico que el municipio se compromete a dar apertura y brindar la información necesaria para el desarrollo del trabajo de investigación.

Por la atención brindada a la presente, agradecemos

Atentamente,

Ing. Robin Velasteguí

ALCALDE MUNICIPAL DEL CANTÓN PENIPE

4.2.2.3. Contrato de Auditoría Informática

En la ciudad de Riobamba, a los 03 días del mes de marzo del dos mil quince, en forma libre y voluntaria, por una parte comparecen: el ingeniero Robin Velasteguí, en calidad de ALCALDE MUNICIPAL DEL CANTÓN PENIPE ; al cual se denominará "Contratante", y por otra a la señorita Jenny Margarita Veloz Chunata con CI. 060460218-5, egresada de la Escuela de Contabilidad y Auditoría de la FADE-ESPOCH; que también en adelante se llamarán "Contratista", quien conviene en suscribir el presente contrato, al tenor de las siguientes cláusulas:

PRIMERA. ANTECEDENTES.- De conformidad con las necesidades actuales del GAD Municipal del Cantón Penipe ha resuelto contratar los servicios de una Auditoría Informática, para que examinen el manejo de la información y de los equipos informáticos en el período 2013.

SEGUNDA. OBJETO DEL CONTRATO.- El objeto del presente contrato es la realización de la Auditoría Informática para medir la eficiencia, eficacia y seguridad del manejo de la información y de los equipos informáticos del GAD Municipal del Cantón Penipe. El Examen a realizarse y sus resultados se concluirán con la presentación del Informe Confidencial, de acuerdo a las Normas de Auditoría Generalmente Aceptadas vigentes en los períodos examinados.

TERCERA. EL PLAZO.- El Plazo estipulado para la entrega de los resultados, es de 90 días laborables, contados a partir de la fecha en que se firme dicho contrato. El plazo fijado podrá ser prorrogado por causas no imputables al contratista, por falta en la entrega oportuna de los materiales e información o por fuerza mayor debidamente comprobada.

CUARTA. VALOR DEL CONTRATO. - No se establece ningún valor del contrato debido a que el trabajo de auditoría informática a desarrollarse es con propósito de cumplir el requisito para la titulación del auditor de la Escuela de Contabilidad y Auditoría de la FADE-ESPOCH, pero se solicita la completa colaboración y facilidades

por parte del personal de la institución para acceder a la respectiva información a fin de evaluar el área indicada.

QUINTA. CONFIDENCIALIDAD.- La información proporcionada por parte de la institución auditada será considerada como confidencial y de uso exclusivo para la preparación y desarrollo de la auditoría, esta información deberá mantenerse bajo el cuidado y pertenencia del auditor no pudiendo ser divulgados salvo autorización expresa por escrito de la autoridad competente del ente auditado. El auditor deberá mantener total discreción en el manejo de la información. Sin embargo dicha condición no se aplicará a la información que por normativa legal vigente se considere de dominio público.

SEXTA. PAPELES DE TRABAJO.- Los papeles de trabajo serán considerados expresamente de propiedad de los auditores que ejecuten el presente trabajo de auditoría informática y por ningún concepto serán de propiedad de la institución auditada.

SÉPTIMA. OBLIGACIONES DEL AUDITOR.- Las obligaciones de los auditores en el presente trabajo de auditoría serán las siguientes:

- a) Aplicar la auditoría informática al GAD Municipal del Cantón Penipe por el periodo del 2013.
- b) Presentar informes semanales sobre el avance de la auditoría.
- c) Elaboración y presentación del informe final del trabajo de auditoría ante el alcalde y funcionarios del Municipio.

OCTAVA. OBLIGACIONES DEL ENTE AUDITADO.- Para la realización del presente Contrato, el GAD Municipal del Cantón Penipe, se compromete:

- a) EL Municipio, a través de sus representantes y demás funcionarios facultados mantendrá un seguimiento de los trabajos realizados por los auditores.

b) EL Municipio, conviene en brindar a los auditores las siguientes facilidades, exclusivamente para el normal desempeño de sus labores:

- Espacio físico;
- Información verbal;
- Información documentada.

NOVENA. DOMICILIO Y JURISDICCIÓN.- Para todos los efectos de este contrato, las partes convienen en fijar su domicilio en la ciudad de Riobamba, renunciando expresamente su domicilio anterior cualquiera que este fuera. Las derivaciones que surgieren entre las partes y que no hubieren podido solucionarse directamente por las mismas, serán sometidas al trámite verbal sumario y a la jurisdicción de los jueces de lo civil de la ciudad de Riobamba.

DECIMA. ACEPTACIÓN.- Las partes en señal de aceptación y conformidad con los términos establecidos en todas y cada una de las cláusulas del presente contrato los suscriben con su firma y rúbrica en el mismo lugar y fecha ya indicados.

En la ciudad de Riobamba, a los tres días del mes de marzo del 2015.

Ing. Robin Velasteguí
**ALCALDE MUNICIPAL
DEL CANTÓN PENIPE**

Srta. Jenny Veloz
AUTOR DE TESIS

4.2.2.4. Notificación de inicio de examen

Riobamba, 09 de marzo del 2015

Ingeniero

Robin Velasteguí

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PENIPE

Presente.

De mi consideración:

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, notifico a usted, que se iniciará la Auditoría Informática al GAD Municipal de Cantón Penipe, por el período comprendido entre el 01 de enero al 31 de diciembre del 2013, por lo que se solicita entregar la documentación e información necesaria para el desarrollo del presente examen.

Para el desarrollo de la auditoría el equipo de auditores estará conformado por: La Srta. Jenny Veloz, Auditor Junior; Ing. Cristóbal Erazo, Supervisor y el Ing. Carlos Ebla, Auditor Senior.

Atentamente,


Jenny Veloz

AUDITOR

4.2.2.5. Equipo de Trabajo*Tabla 17. Equipo de Trabajo*


Nro.	NOMBRES Y APELLIDOS	CARGO	SIGLAS
01	Ing. Cristóbal Edison Erazo Robalino	Supervisor	C.E.E.R
02	Ing. Carlos Alfredo Ebla Olmedo	Senior	C.A.E.O
03	Srta. Jenny Margarita Veloz Chunata	Junior	J.M.V.CH

4.2.2.6. Índice de Auditoría

	ÍNDICE DE AUDITORÍA Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	APL 6_IA 1/2																																														
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática																																																
<table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 15%;">AP</td><td>Archivo Permanente</td></tr> <tr><td>AP 1_IG</td><td>Información General</td></tr> <tr><td>AP 2_UB</td><td>Ubicación</td></tr> <tr><td>AP 3_BL</td><td>Base Legal</td></tr> <tr><td>AP 4_FG</td><td>Funciones del GAD Municipal</td></tr> <tr><td>AP 5_OE</td><td>Organigrama Estructural</td></tr> <tr><td>AP 6_PF</td><td>Principales Funcionarios</td></tr> <tr><td>APL</td><td>Archivo de Planificación</td></tr> <tr><td>APL 1_OT</td><td>Orden de Trabajo</td></tr> <tr><td>APL 2_CAA</td><td>Carta de Aceptación de Auditoría</td></tr> <tr><td>APL 3_CAI</td><td>Contrato de Auditoría Informática</td></tr> <tr><td>APL 4_NIE</td><td>Notificación de Inicio de Examen</td></tr> <tr><td>APL5_EA</td><td>Equipo de Auditoría</td></tr> <tr><td>APL 6_IA</td><td>Índices de Auditoría</td></tr> <tr><td>APL 7_MA</td><td>Marcas de Auditoría</td></tr> <tr><td>AC</td><td>Archivo Corriente</td></tr> <tr><td>AC 1_PA</td><td>Programa de Auditoría</td></tr> <tr><td>AC 1_EAL</td><td>Entrevista al Alcalde</td></tr> <tr><td>AC 1_VPI</td><td>Visita Previa a las Instalaciones</td></tr> <tr><td>AC 1_MJ</td><td>Marco Jurídico</td></tr> <tr><td>AC 1_MP</td><td>Memorándum de Planificación</td></tr> <tr><td>AC 2_CCI</td><td>Cuestionario de Control Interno</td></tr> <tr><td>AC 2_MRC</td><td>Matriz de Riesgo y Confianza</td></tr> </table>			AP	Archivo Permanente	AP 1_IG	Información General	AP 2_UB	Ubicación	AP 3_BL	Base Legal	AP 4_FG	Funciones del GAD Municipal	AP 5_OE	Organigrama Estructural	AP 6_PF	Principales Funcionarios	APL	Archivo de Planificación	APL 1_OT	Orden de Trabajo	APL 2_CAA	Carta de Aceptación de Auditoría	APL 3_CAI	Contrato de Auditoría Informática	APL 4_NIE	Notificación de Inicio de Examen	APL5_EA	Equipo de Auditoría	APL 6_IA	Índices de Auditoría	APL 7_MA	Marcas de Auditoría	AC	Archivo Corriente	AC 1_PA	Programa de Auditoría	AC 1_EAL	Entrevista al Alcalde	AC 1_VPI	Visita Previa a las Instalaciones	AC 1_MJ	Marco Jurídico	AC 1_MP	Memorándum de Planificación	AC 2_CCI	Cuestionario de Control Interno	AC 2_MRC	Matriz de Riesgo y Confianza
AP	Archivo Permanente																																															
AP 1_IG	Información General																																															
AP 2_UB	Ubicación																																															
AP 3_BL	Base Legal																																															
AP 4_FG	Funciones del GAD Municipal																																															
AP 5_OE	Organigrama Estructural																																															
AP 6_PF	Principales Funcionarios																																															
APL	Archivo de Planificación																																															
APL 1_OT	Orden de Trabajo																																															
APL 2_CAA	Carta de Aceptación de Auditoría																																															
APL 3_CAI	Contrato de Auditoría Informática																																															
APL 4_NIE	Notificación de Inicio de Examen																																															
APL5_EA	Equipo de Auditoría																																															
APL 6_IA	Índices de Auditoría																																															
APL 7_MA	Marcas de Auditoría																																															
AC	Archivo Corriente																																															
AC 1_PA	Programa de Auditoría																																															
AC 1_EAL	Entrevista al Alcalde																																															
AC 1_VPI	Visita Previa a las Instalaciones																																															
AC 1_MJ	Marco Jurídico																																															
AC 1_MP	Memorándum de Planificación																																															
AC 2_CCI	Cuestionario de Control Interno																																															
AC 2_MRC	Matriz de Riesgo y Confianza																																															
ELABORADO POR: J.M.V.CH		FECHA: 09-03-2015																																														
REVISADO POR: C.E.E.R		FECHA: 10-03-2015																																														

	ÍNDICE DE AUDITORÍA Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	APL 6_IA 2/2
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática		
AC 2_HR_CCI Hoja de resumen de Confianza y Riesgo AC 3_IND Indicadores AP 3_HA Hoja de Hallazgos		
ELABORADO POR: J.M.V.CH		FECHA: 09-03-2015
REVISADO POR: C.E.E.R		FECHA: 10-03-2015

4.2.2.7. Marcas de Auditoría

	<p>MARCAS DE AUDITORÍA Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA</p>	<p>APL 7_MA 1/1</p>														
<p>Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática</p>																
<table border="1"> <thead> <tr> <th data-bbox="323 689 549 734">MARCA</th> <th data-bbox="549 689 1345 734">SIGNIFICADO</th> </tr> </thead> <tbody> <tr> <td data-bbox="323 734 549 786">H</td> <td data-bbox="549 734 1345 786">Hallazgo</td> </tr> <tr> <td data-bbox="323 786 549 837">D</td> <td data-bbox="549 786 1345 837">Debilidad</td> </tr> <tr> <td data-bbox="323 837 549 889">Σ</td> <td data-bbox="549 837 1345 889">Sumatoria</td> </tr> <tr> <td data-bbox="323 889 549 940">Ω</td> <td data-bbox="549 889 1345 940">Sustentado con Evidencia</td> </tr> <tr> <td data-bbox="323 940 549 992">√</td> <td data-bbox="549 940 1345 992">Verificado</td> </tr> <tr> <td data-bbox="323 992 549 1043">A</td> <td data-bbox="549 992 1345 1043">Incumplimiento de normativa</td> </tr> </tbody> </table>			MARCA	SIGNIFICADO	H	Hallazgo	D	Debilidad	Σ	Sumatoria	Ω	Sustentado con Evidencia	√	Verificado	A	Incumplimiento de normativa
MARCA	SIGNIFICADO															
H	Hallazgo															
D	Debilidad															
Σ	Sumatoria															
Ω	Sustentado con Evidencia															
√	Verificado															
A	Incumplimiento de normativa															
<p>ELABORADO POR: J.M.V.CH</p>		<p>FECHA: 09-03-2015</p>														
<p>REVISADO POR: C.E.E.R</p>		<p>FECHA: 10-03-2015</p>														

4.2.3. Archivo corriente



ARCHIVO CORRIENTE


ENTIDAD: GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE


DIRECCIÓN: SILVIO LUIS HARO 08-21 Y DAVID RAMOS (CANTÓN PENIPE)


EXAMEN: AUDITORÍA INFORMÁTICA


PERÍODO: 01 DE ENERO AL 31 DE DICIEMBRE DEL 2013


4.2.3.1.Fase I: Planificación



		PROGRAMA DE AUDITORÍA PLANIFICACIÓN Período del 01 de enero al 31 de diciembre 2013		AC 1_PA 2/1
Entidad:		GAD Municipal del Cantón Penipe		
Tipo de Examen:		Auditoría		
Componente:		Informática		
Objetivo General:				
<p>Determinar la influencia de la eficacia, eficiencia y seguridad en el manejo de la información y los equipos informáticos.</p>				
Objetivos Específicos:				
<ul style="list-style-type: none"> • Recopilar información relevante, pertinente y competente para el desarrollo de las fases de auditoría. • Evaluar el control interno informático con el fin de determinar hallazgos y evidencias mediante la aplicación de los componentes del COSO II. • Emitir un informe en donde las conclusiones y recomendaciones ayuden a mejorar el manejo de la información y los equipos informáticos del GAD Municipal del Cantón Penipe. 				
Nº	PROCEDIMIENTO	REF. P/T	REALIZADO POR:	FECHA
PLANIFICACIÓN				
01	Elabore el programa de auditoría	AC 1_PA	J.M.V.CH	11/03/2015
02	Efectúe una entrevista al Alcalde del Municipio.	AC 1_EAL	J.M.V.CH	18/03/2015
03	Realice una visita preliminar a las instalaciones del Municipio.	AC 1_VPI	J.M.V.CH	18/03/2015
04	Recopile información y documentación sobre la base legal vigente en la entidad.	AC 1_MJ	J.M.V.CH	19/03/2015
05	Elabore el memorándum de planificación.	AC 1_MP	J.M.V.CH	23/03/2015
EVALUACIÓN DEL CONTROL INTERNO				
06	Elabore y aplique los cuestionarios de Control Interno basados en los componentes de COSO II.	AC 2_CCI	J.M.V.CH	26/03/2015
ELABORADO POR: J.M.V.CH			FECHA: 11-03-2015	
REVISADO POR: C.E.E.R			FECHA: 13-03-2015	


		PROGRAMA DE AUDITORÍA PLANIFICACIÓN Período del 01 de enero al 31 de diciembre 2013		AC 1_PA 2/2
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática				
Objetivo General: Determinar la influencia de la eficacia, eficiencia y seguridad en el manejo de la información y los equipos informáticos.				
Objetivos Específicos: <ul style="list-style-type: none"> • Recopilar información relevante, pertinente y competente para el desarrollo de las fases de auditoría. • Evaluar el control interno informático con el fin de determinar hallazgos y evidencias mediante la aplicación de los componentes del COSO II. • Emitir un informe en donde las conclusiones y recomendaciones ayuden a mejorar el manejo de la información y los equipos informáticos del GAD Municipal del Cantón Penipe. 				
Nº	PROCEDIMIENTO	REF. P/T	REALIZADO POR:	FECHA
07	Elabore la matriz de riesgo y confianza.	AC 2_MRC	J.M.V.CH	26/03/2015
08	Elabore una Hoja de Resumen de Confianza y Riesgo del Sistema de Control Interno por componente _COSO II.	AC 2_HR_CCI	J.M.V.CH	26/03/2015
09	Elabore un Informe de Control Interno.		J.M.V.CH	01/04/2015
ANÁLISIS DE ÁREAS CRÍTICAS				
10	Elabore indicadores de eficiencia, eficacia y seguridad informática.	AC 3_IND	J.M.V.CH	04/04/2015
11	Elabore la Hoja de Hallazgos.	AC 3_HA	J.M.V.CH	11/04/2015
INFORME				
12	Elabore una carta de presentación		J.M.V.CH	18/05/2015
13	Elabore el informe final de auditoría informática.		J.M.V.CH	18/05/2015
ELABORADO POR: J.M.V.CH			FECHA: 11-03-2015	
REVISADO POR: C.E.E.R			FECHA: 13-03-2015	


	PLANIFICACIÓN ENTREVISTA AL ALCALDE Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	AC 1_EAL 1/3
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática		
Nombre del entrevistado: Ing. Robin Velasteguí Cargo: Alcalde del Municipio Entrevistador: Jenny Veloz Día Previsto: 16-03-2015 Hora: 10:00 am		
<p>1. ¿Se ha realizado una Auditoría informática al Municipio de Penipe hasta la actualidad?</p> <p>El Alcalde manifiesta que no se ha realizado una auditoría informática, puesto que los Organismos de Control se enfocan más en evaluar la parte financiera y de gestión, dado que los recursos que manejan son públicos y se emplean en proyectos que benefician a la comunidad de Penipe.</p> <p>2. ¿Existe un departamento destinado al manejo y control de la informática?</p> <p>El Alcalde se basa en el organigrama de la institución para manifestar que no existe un área o departamento destinado para el control del manejo de la información y de los equipos informáticos.</p> <p>3. ¿Se aplican las Normas de Control Interno de la CGE, específicamente el numeral 410 que trata sobre la Tecnología de la Información?</p> <p>El ingeniero supo manifestar que se conoce sobre el contenido de las Normas de Control Interno de la CGE, pero no se aplican todos los numerales expuestos en el mismo por falta de presupuesto, tiempo y personal.</p> <p>4. ¿Se realizan capacitaciones al personal de la entidad sobre el manejo correcto de la información y los equipos informáticos bajo su custodia?</p> <p>Las capacitaciones se dan solo al personal de contabilidad, cuyo tema son los paquetes contables que utilizan, en este caso el SINFO, para los demás empleados no se ha contemplado ningún tipo de capacitación en el ámbito de la informática.</p>		
ELABORADO POR: J.M.V.CH		FECHA: 18-03-2015
REVISADO POR: C.E.E.R		FECHA: 19-03-2015


	PLANIFICACIÓN ENTREVISTA AL ALCALDE Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	AC 1_EAL 2/3
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
Nombre del entrevistado: Ing. Robin Velasteguí Cargo: Alcalde del Municipio Entrevistador: Jenny Veloz Día Previsto: 16-03-2015 Hora: 10:00 am		
<p>5. ¿Usted usa firmas electrónicas para validar los documentos que redacta y envía en representación del municipio?</p> <p>El Alcalde manifestó que no utiliza firmas electrónicas para ningún tipo de trámite, pero se realizó la petición de un Token (Certificado de firma electrónica) al Banco Central del Ecuador.</p> <p>6. ¿Considera usted que existe suficiente seguridad para proteger los equipos informáticos y la información almacenada en los mismos?</p> <p>La seguridad en el Municipio es muy baja para proteger dichos activos, ya que el presupuesto no cubre la instalación de dispositivos de seguridad como pararrayos, cámaras de seguridad, o respaldos fuera de la entidad, el alcalde manifiesta que cada empleado cuida la información y los equipos a su cargo mientras dura la jornada de trabajo.</p> <p>7. ¿Según su criterio considera necesario realizar una auditoría informática al Municipio?</p> <p>El ingeniero afirma que es necesario realizar este tipo de auditoría para mejorar el manejo de la información y los equipos informáticos así como su eficiencia, eficacia y seguridad para evitar pérdida de recursos, tiempo y reducir los riesgos que amenazan la integridad de dichos activos.</p>		
ELABORADO POR: J.M.V.CH		FECHA: 18-03-2015
REVISADO POR: C.E.E.R		FECHA: 19-03-2015


	PLANIFICACIÓN ENTREVISTA AL ALCALDE Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	AC 1_EAL 3/3
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática		
Nombre del entrevistado: Ing. Robin Velasteguí Cargo: Alcalde del Municipio Entrevistador: Jenny Veloz Día Previsto: 16-03-2015 Hora: 10:00 am		
<p>8. ¿Cuenta el Municipio con un sistema de control interno informático?</p> <p>La entidad no cuenta con un sistema de control interno para el área informática.</p> <p>9. ¿Existe un plan de contingencias para contrarrestar los riesgos informáticos?</p> <p>El alcalde manifiesta que no se ha implementado un plan de contingencias por lo cual existe mayor probabilidad de que aparezcan amenazas afectando a los activos informáticos.</p> <p>10. ¿Existe partida presupuestaria suficiente para adquirir equipos informáticos?</p> <p>El Municipio cuenta con partida presupuestaria para adquirir equipos informáticos, según certificado del Director Financiero.</p>		
ELABORADO POR: J.M.V.CH		FECHA: 18-03-2015
REVISADO POR: C.E.E.R		FECHA: 19-03-2015


	PLANIFICACIÓN VISITA PREVIA A LAS INSTALACIONES Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	AC 1_VPI 1/1
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
<p>Visita al Municipio</p> <p>El GAD Municipal del Cantón Penipe se encuentra ubicado en las calles Silvio Luis Haro 08-21 y David Ramos a 27,79 Km de la ciudad de Riobamba.</p> <div style="text-align: center;">  </div> <p>Durante la visita a las instalaciones del municipio se pudo constatar que la división de los departamentos y la distribución de los empleados están acorde al organigrama institucional de la entidad.</p> <p>Cada uno de los departamentos cuenta por lo menos con un computador para facilitar el trabajo que realizan los empleados públicos, los cuales son responsables de los equipos informáticos y de la información almacenada en los mismos.</p> <p>El sistema operativo que utilizan en las computadoras de la entidad es el Windows 7, y el antivirus denominado AVAST, existe una impresora multifunción para cada piso, en total son tres.</p> <p>El Alcalde y los empleados de la institución están dispuestos a brindar la información y documentación necesaria para realizar la auditoría informática.</p> <p>El Municipio de Penipe mantiene un horario de atención a sus clientes externos e internos de lunes a viernes, en la mañana de 8:00am a 12:00pm y en la tarde de 14:00pm a 18:00pm.</p>		
ELABORADO POR: J.M.V.CH		FECHA: 18-03-2015
REVISADO POR: C.E.E.R		FECHA: 19-03-2015

	<p style="text-align: center;">PLANIFICACIÓN MARCO JURÍDICO Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA</p>	<p style="text-align: center;">AC 1_MJ 1/3</p>
<p>Entidad: Tipo de Examen: Componente:</p>	<p>GAD Municipal del Cantón Penipe Auditoría Informática</p>	
<p style="text-align: center;">MARCO JURÍDICO</p> <ul style="list-style-type: none"> • Constitución Política de la República del Ecuador • Ley Orgánica de la Contraloría General del Estado • Ley de Presupuesto del Sector Público • Ley Orgánica de Régimen Municipal • Ley Orgánica de Régimen Tributario Interno • Ley Orgánica de Servicio Civil y Carrera Administrativa y de Unificación y Homologación de las Remuneraciones del Sector Público • Normativa de Contabilidad Gubernamental del Ministerio de Finanzas • Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos • Código Orgánico de Organización Territorial Autonomía y Descentralización • Código de Trabajo <p style="text-align: center;">NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS</p> <p>100 NORMAS GENERALES</p> <p>100-01 Control Interno El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.</p> <p>200 AMBIENTE DE CONTROL</p> <p>200-01 Integridad y valores éticos</p>		
<p>ELABORADO POR: J.M.V.CH</p>	<p>FECHA: 19-03-2015</p>	
<p>REVISADO POR: C.E.E.R</p>	<p>FECHA: 20-03-2015</p>	

	PLANIFICACIÓN MARCO JURÍDICO Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	AC 1_MJ 2/3
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
<p>La máxima autoridad de cada entidad emitirá formalmente las normas propias del código de ética, para contribuir al buen uso de los recursos públicos y al combate a la corrupción.</p>		
<p>410 TECNOLOGÍA DE LA INFORMACIÓN</p>		
<p>410-01 Organización informática</p>		
<p>La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.</p>		
<p>410-04 Políticas y procedimientos</p>		
<p>Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos. Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño.</p>		
<p>Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.</p>		
<p>410-09 Mantenimiento y control de la infraestructura tecnológica</p>		
<p>6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.</p>		
<p>410-10 Seguridad de tecnología de información</p>		
<p>4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;</p>		
ELABORADO POR: J.M.V.CH	FECHA: 19-03-2015	
REVISADO POR: C.E.E.R	FECHA: 20-03-2015	


	PLANIFICACIÓN MARCO JURÍDICO Período del 01 de enero al 31 de diciembre 2013 CÉDULA NARRATIVA	AC 1_MJ 3/3
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
<p>6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;</p>		
<p>8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.</p>		
<p>410-11 Plan de contingencias</p>		
<p>6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.</p>		
<p>410-12 Administración de soporte de tecnología de información</p>		
<p>2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.</p>		
<p>410-15 Capacitación informática</p>		
<p>Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.</p>		
<p>410-17 Firmas electrónicas</p>		
<p>Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.</p>		
ELABORADO POR: J.M.V.CH		FECHA: 19-03-2015
REVISADO POR: C.E.E.R		FECHA: 20-03-2015

	PLANIFICACIÓN MEMORANDUM DE PLANIFICACIÓN Período del 01 de enero al 31 de diciembre 2013	AC 1_MP 1/3
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
<p style="text-align: center;">1. INFORMACIÓN GENERAL</p> <p>La Municipalidad del cantón Penipe, fue creado mediante Decreto Legislativo N° 15, publicado en el Registro Oficial N° 680 del 9 de Febrero de 1984 y el desarrollo de su vida jurídica e institucional, fue uno de los primeros cantones en integrarse al COMAGA (Consortio de Municipios Amazónicos y Galápagos), hoy en día recibe recursos por parte del gobierno a través de la ley 0.10.</p>		
<p style="text-align: center;">2. MOTIVO DEL EXAMEN</p> <p>La Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, se realizará mediante Orden de Trabajo N° 001.</p>		
<p style="text-align: center;">3. OBJETIVO DEL EXAMEN</p> <p>Desarrollar una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013, para medir el grado de eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.</p>		
<p style="text-align: center;">4. ALCANCE</p> <p>Esta investigación abarca la auditoría informática que se realizará al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, en el período comprendido entre el 01 de Enero al 31 de Diciembre del 2013.</p>		
<p style="text-align: center;">5. REQUERIMIENTOS DE AUDITORÍA</p> <ul style="list-style-type: none"> ✓ Informe de Auditoría ✓ Conclusiones ✓ Recomendaciones 		
ELABORADO POR: J.M.V.CH		FECHA: 23-03-2015
REVISADO POR: C.E.E.R		FECHA: 25-03-2015

	PLANIFICACIÓN MEMORANDUM DE PLANIFICACIÓN Período del 01 de enero al 31 de diciembre 2013	AC 1_MP 2/3
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
6. FECHAS DE INTERVENCIÓN ESTIMADA		
Orden de trabajo Inicio del trabajo de campo Finalización de trabajo de campo Elaboración del borrador del informe Emisión del informe final de auditoría	05 de enero del 2015 09 de marzo del 2015 26 de marzo del 2015 4 de mayo del 2015 18 de mayo del 2015	
7. EQUIPO MULTIDISCIPLINARIO		
Ing. Cristóbal Edison Erazo Robalino Ing. Carlos Alfredo Ebla Olmedo Srta. Jenny Margarita Veloz Chunata	Supervisor Senior Junior	
8. RECURSOS FINANCIEROS Y MATERIALES		
Materiales (copias, impresiones) Transporte Alimentación	USD. 60 USD. 80 USD. 40	
9. COLABORACIÓN ✓ Alcalde Ing. Robin Velasteguí ✓ Personal del Municipio que tiene bajo su custodia equipos informáticos e información almacenada en los mismos.		
10. OTROS ASPECTOS ✓ Se anexara la documentación relacionada al archivo permanente de la auditoría informática. ✓ Los hallazgos se basan en la evaluación del control interno según COSO II. ✓ El informe de auditoría irá dirigido al Alcalde y al Concejo Municipal.		
ELABORADO POR: J.M.V.CH	FECHA: 23-03-2015	
REVISADO POR: C.E.E.R	FECHA: 25-03-2015	

	PLANIFICACIÓN MEMORANDUM DE PLANIFICACIÓN Período del 01 de enero al 31 de diciembre 2013	AC 1_MP 3/3		
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática			
11. FIRMAS DE RESPONSABILIDAD <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; text-align: center;"> ----- Srta. Jenny Veloz AUDITOR JUNIOR </td> <td style="width: 50%; text-align: center;"> ----- Ing. Cristóbal Erazo SUPERVISOR </td> </tr> </table>			----- Srta. Jenny Veloz AUDITOR JUNIOR	----- Ing. Cristóbal Erazo SUPERVISOR
----- Srta. Jenny Veloz AUDITOR JUNIOR	----- Ing. Cristóbal Erazo SUPERVISOR			
ELABORADO POR: J.M.V.CH		FECHA: 23-03-2015		
REVISADO POR: C.E.E.R		FECHA: 25-03-2015		

4.2.3.2.Fase II: Evaluación del Control Interno

		CUESTIONARIO DE CONTROL INTERNO Período del 01 de enero al 31 de diciembre 2013 AMBIENTE INTERNO						AC 2_CCI 1/13
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática								
N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿La institución cuenta con un código de ética que rija la conducta del personal?		X		X		X	H₁ No se ha elaborado un código de ética en el año 2013.
02	¿Se ha definido valores éticos para incentivar la cultura organizacional del Municipio?	X		X		X		
03	¿Existe un buen ambiente laboral entre los empleados de la entidad y sus directivos?	X			X	X		
04	¿Se capacita a todo el personal del Municipio sobre el manejo y seguridad de los activos informáticos?		X		X		X	H₂ No se capacita al personal sobre manejo y seguridad de los activos informáticos.
05	¿Se toma en cuenta las habilidades, conocimientos y experiencia para contratar al Talento Humano del Municipio?	X		X			X	
ELABORADO POR: J.M.V.CH						FECHA: 26-03-2015		
REVISADO POR: C.E.E.R						FECHA: 27-03-2015		



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
AMBIENTE INTERNO

AC 2_CCI

2/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
06	¿El personal del Municipio posee conocimientos básicos sobre la informática?	X		X		X		
07	¿Se encuentran definidas las líneas de autoridad y responsabilidad en cada departamento de la entidad?	X			X	X		
08	¿Está definido el Organigrama Estructural del Municipio?	X		X		X		
09	¿Se contempla en el organigrama una Unidad designada para el área Informática?		X		X		X	H₃ No existe una Unidad de Informática dentro del Municipio.
10	¿La Misión, Visión y Objetivos institucionales cubren las necesidades tecnológicas del Municipio?		X		X		X	D₁ La Misión, Visión y Objetivos institucionales no cumplen con las necesidades tecnológicas del Municipio.
11	¿El personal conoce sobre la existencia de las Normas de Control Interno de la CGE?	X		X			X	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015



CUESTIONARIO DE CONTROL INTERNO
 Período del 01 de enero al 31 de diciembre 2013
AMBIENTE INTERNO

AC 2_CCI

3/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
12	¿Se aplican las Normas de Control Interno de la CGE, el numeral 410-Tecnología de la Información en la entidad?		X		X		X	D₂ No se aplican las Normas de Control Interno de la CGE - numeral 410, referente a las Tecnologías de la Información.
TOTAL Σ		7	5	5	7	5	7	

ELABORADO POR: J.M.V.CH **FECHA: 26-03-2015**

REVISADO POR: C.E.E.R **FECHA: 27-03-2015**

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{17}{36} * 100$ $NC = 47,22\%$	$NR = 100 - NC$ $NR = 100 - 47,22$ $NR = 52,78\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
		5%-24%	25%-49%	50%-85%



CUESTIONARIO DE CONTROL INTERNO
 Período del 01 de enero al 31 de diciembre 2013
ESTABLECIMIENTO DE OBJETIVOS

AC 2_CCI

4/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿Se encuentran definidos los objetivos institucionales del Municipio?	X		X		X		
02	¿Los objetivos institucionales contribuyen al cumplimiento de la misión y visión del Municipio?	X			X	X		
03	¿Existen mecanismos para evaluar el riesgo si no se cumplen con los objetivos institucionales?	X		X			X	
04	¿El personal conoce sobre la existencia de los objetivos institucionales?	X		X			X	
05	¿Se actualizan con frecuencia los objetivos institucionales?		X		X		X	D₃ No se actualizan los objetivos institucionales.
	TOTALΣ	4	1	3	2	2	3	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{9}{15} * 100$ $NC = 60\%$	$NR = 100 - NC$ $NR = 100 - 60$ $NR = 40\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
		5%-24%	25%-49%	50%-85%



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
IDENTIFICACIÓN DE EVENTOS

AC 2_CCI

5/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿La Administración conoce sobre los cambios que se dan en el aspecto tecnológico?	X		X			X	
02	¿Existen mecanismos para identificar los riesgos informáticos?		X		X		X	H₄ No existen mecanismos para identificar los riesgos informáticos.
03	¿El personal del Municipio contribuye para identificar los posibles riesgos que pueden afectar a los activos informáticos?		X		X		X	D₄ El personal no identifica los posibles riesgos que afectan a los activos informáticos.
04	¿La administración identifica los riesgos externos que pueden afectar a la integridad de la información y de los equipos informáticos del Municipio?		X		X		X	D₅ La administración no analiza los riesgos externos que pueden afectar a la información y equipos informáticos.
05	¿Se socializan los riesgos identificados con todo el personal de la entidad?	X			X	X		
TOTALΣ		2	3	1	4	1	4	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{4}{15} * 100$ $NC = 26,67\%$	$NR = 100 - NC$ $NR = 100 - 26,67$ $NR = 73,33\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
		5%-24%	25%-49%	50%-85%



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DE RIESGOS

AC 2_CCI

6/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿Existe un Sistema de Control Interno Informático?		X		X		X	H ₅ No existe un Sistema de Control Interno Informático.
02	¿Luego de identificar los riesgos, los mismos son clasificados según el impacto que provocan?	X		X			X	
03	¿Se valora el grado de ocurrencia y el impacto que puede provocar el riesgo a los activos informáticos?	X			X	X		
04	¿Se identifican los factores que pueden provocar la ocurrencia del riesgo informático?	X		X			X	
TOTALΣ		3	1	2	2	1	3	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{6}{12} * 100$ $NC = 50\%$	$NR = 100 - NC$ $NR = 100 - 50$ $NR = 50\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
		5%-24%	25%-49%	50%-85%



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
RESPUESTA AL RIESGO

AC 2_CCI

7/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿La entidad cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos?		X		X		X	H₆ La entidad no cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos.
02	¿Se aplican procedimientos, herramientas o técnicas para disminuir la ocurrencia e impacto del riesgo?		X		X		X	D₆ No se aplican procedimiento, herramienta o técnica para disminuir la ocurrencia e impacto del riesgo informático.
03	¿Después de identificar el riesgo, se aplican acciones correctivas inmediatamente?	X			X	X		
	TOTALΣ	1	2	0	3	1	2	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{2}{9} * 100$ $NC = 22,22\%$	$NR = 100 - NC$ $NR = 100 - 22,22$ $NR = 77,78\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
	5%-24%	25%-49%	50%-85%	



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
ACTIVIDADES DE CONTROL

AC 2_CCI

8/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
	MANEJO Y SEGURIDAD DE LA INFORMACIÓN ALMACENADA EN LOS EQUIPOS DE INFORMÁTICOS							
01	¿Se guardan respaldos de la información relevante que posee la entidad?	X		X			X	
02	¿Los respaldos de la información se guardan en lugares externos al Municipio?		X		X		X	H₇ No se guardan los respaldos de la información en lugares externos al Municipio.
03	¿El personal ingresa al computador utilizando una contraseña?	X		X			X	
04	¿Se restringe el uso de páginas web que no tienen relación con las actividades propias del Municipio?		X	X		X		
05	¿El Municipio posee un seguro que cubra la pérdida o robo de la información?		X		X		X	D₇ No existe un seguro que cubra la pérdida o robo de la información del Municipio.

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
ACTIVIDADES DE CONTROL

AC 2_CCI

9/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Técnico		Secretario		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
06	¿Se actualizan con frecuencia los antivirus de los equipos informáticos para evitar la pérdida de información?	X			X	X		
07	¿El personal que tiene acceso autorizado a la información está controlado mediante una tarjeta de identificación?		X		X		X	H₈ El personal no maneja tarjetas de identificación para acceder a la información.
08	¿Se restringe el acceso a la información a personas ajenas a la entidad?	X		X		X		
09	¿Se utilizan firmas electrónicas para enviar y recibir información?		X		X		X	H₉ No se utiliza firmas electrónicas en el Municipio.
	MANEJO Y SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS							
10	¿Se realiza mantenimiento preventivo a los equipos informáticos?		X		X		X	H₁₀ No se realiza mantenimiento preventivo a los equipos informáticos.

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
ACTIVIDADES DE CONTROL

AC 2_CCI

10/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
11	¿Existe partida presupuestaria para la adquisición de equipos informáticos?	X		X			X	
12	¿Se toma en cuenta la marca, modelo, capacidad y costo-beneficio para la adquisición de los equipos informáticos?	X			X	X		
13	¿Durante el año 2013 se ha realizado adquisición de infraestructura tecnológica mediante el portal de compras públicas?		X		X		X	La adquisición de infraestructura electrónica no se realizó en el portal de compras públicas.
14	¿Las instalaciones físicas del Municipio cuentan con dispositivos de seguridad para controlar el fuego, la humedad y temperatura que pueden afectar a la integridad de los activos informáticos?		X		X		X	H₁₁ Las instalaciones del Municipio no cuentan con dispositivos de seguridad para proteger los activos informáticos.

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
ACTIVIDADES DE CONTROL

AC 2_CCI

11/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
15	¿La ubicación de los equipos informáticos es adecuada para su correcto manejo?	X		X			X	
16	¿Existe un especialista para dar mantenimiento a los equipos informáticos?	X		X		X		
17	¿Existen cámaras de vigilancia dentro del Municipio?		X		X		X	D₉ No existen cámaras de vigilancia en el Municipio.
18	¿Las oficinas del Municipio se cierran con llave después de la jornada laboral?	X		X		X		
19	¿Se contratan vigilantes de seguridad para cuidar las instalaciones por las noches y los fines de semana?		X		X		X	H₁₂ El Municipio no contrata vigilantes de seguridad para las noches y los fines de semana.
20	¿Se realizan Actas de Entrega de Recepción de los equipos informáticos?	X		X			X	
	TOTAL Σ	10	10	9	11	6	14	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{25}{60} * 100$ $NC = 41,67\%$	$NR = 100 - NC$ $NR = 100 - 41,67$ $NR = 58,33\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
	5%-24%	25%-49%	50%-85%	



CUESTIONARIO DE CONTROL INTERNO
 Período del 01 de enero al 31 de diciembre 2013
INFORMACIÓN Y COMUNICACIÓN

AC 2_CCI

12/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿Existe una comunicación abierta entre la Administración y el personal del Municipio?	X		X			X	
02	¿Se utiliza herramientas como el internet para comunicar información importante entre los departamentos de la entidad?	X		X		X		
03	¿Las comunicaciones verbales y escritas se socializan de manera oportuna a todo el personal de la entidad?	X			X	X		
04	¿Se comunica oportunamente al personal cuando se realizan cambios imprevistos en la entidad?	X			X	X		
		4		2	2	3	1	
	TOTAL Σ							

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{9}{12} * 100$ $NC = 75\%$	$NR = 100 - NC$ $NR = 100 - 75$ $NR = 25\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
		5%-24%	25%-49%	50%-85%



CUESTIONARIO DE CONTROL INTERNO
Período del 01 de enero al 31 de diciembre 2013
MONITOREO

AC 2_CCI

13/13

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

N°	PREGUNTA	Alcalde		Contadora		Técnico		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	
01	¿Se supervisa el manejo de los equipos informáticos?		X		X		X	H₁₃ No se supervisa el manejo de los equipos informáticos.
02	¿Se controla que los equipos informáticos estén en buenas condiciones?	X			X	X		
03	¿Se realiza un monitoreo de las entadas y salidas del personal a la entidad?	X		X		X		
	TOTALΣ	2	1	1	2	2	1	

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 27-03-2015

CÁLCULO		MATRIZ DE RIESGO Y CONFIANZA		
Nivel de Confianza	Nivel de Riesgo	CONFIANZA		
$NC = \frac{CT}{CP} * 100$ $NC = \frac{5}{9} * 100$ $NC = 55,56\%$	$NR = 100 - NC$ $NR = 100 - 55,56$ $NR = 44,44\%$	Bajo	Moderado	Alto
		15%-50%	51%-75%	76%-95%
		RIESGO		
		Bajo	Moderado	Alto
		5%-24%	25%-49%	50%-85%



MATRIZ DE RIESGO Y CONFIANZA
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC
2_MRC
1/2

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

CÁLCULO DE RIESGO Y CONFIANZA

- A continuación se describe la fórmula bajo la cual se determinó el nivel de riesgo y confianza del Sistema de Control Interno Informático, a través de los cuestionarios realizados al personal del Municipio.

Nivel de Confianza

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

Nivel de Riesgo

$$NR = 100 - NC$$

Dónde:

NC= Nivel de confianza
 CT= Confianza total
 CP= Confianza prevista
 NR= Nivel de riesgo

MATRIZ DE PONDERACIÓN DE RIESGO Y CONFIANZA

- Según la siguiente matriz se ponderó el nivel de riesgo y confianza de los cuestionarios de control interno aplicados al personal del Municipio.

Nivel de confianza		
Bajo	Moderado	Alto
15% - 50%	51% - 75%	76% - 95%
Nivel de riesgo		
Alto	Moderado	Bajo
85% - 50%	49% - 25%	24% - 5%

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 26-03-2015



MATRIZ DE RIESGO Y CONFIANZA
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_MRC
2/2

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

RESUMEN DE EVALUACIÓN DE RIESGO Y CONFIANZA POR COMPONENTE

N°	COMPONENTES COSO II	N° PREGUNTAS	ALCALDE		CONTADORA		TÉCNICO		CONFIANZA PREVISTA	CONFIANZA TOTAL (SI)	NIVEL DE CONFIANZA		NIVEL DE RIESGO	
			SI	NO	SI	NO	SI	NO			Ponderación		Ponderación	
1	AMBIENTE INTERNO	12	7	5	5	7	5	7	36	17	47,22%	Bajo	52,78%	Alto
2	ESTABLECIMIENTO DE OBJETIVOS	5	4	1	3	2	2	3	15	9	60,00%	Moderado	40,00%	Moderado
3	IDENTIFICACIÓN DE EVENTOS	5	2	3	1	4	1	4	15	4	26,67%	Bajo	73,33%	Alto
4	EVALUACIÓN DE RIESGOS	4	3	1	2	2	1	3	12	6	50,00%	Bajo	50,00%	Alto
5	RESPUESTA AL RIESGO	3	1	2	0	3	1	2	9	2	22,22%	Bajo	77,78%	Alto
6	ACTIVIDADES DE CONTROL	20	10	10	9	11	6	14	60	25	41,67%	Bajo	58,33%	Alto
7	INFORMACIÓN Y COMUNICACIÓN	4	4	0	2	2	3	1	12	9	75,00%	Moderado	25,00%	Moderado
8	MONITOREO	3	2	1	1	2	2	1	9	5	55,56%	Moderado	44,44%	Moderado
TOTAL Σ											47,29%	BAJO	52,71%	ALTO

ELABORADO POR: J.M.V.CH

FECHA: 26-03-2015

REVISADO POR: C.E.E.R

FECHA: 26-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE

AC 2_HR_CCI 1/9

_COSO II

Período del 01 de enero al 31 de diciembre 2013

EVALUACIÓN DEL CONTROL INTERNO

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
AMBIENTE DE CONTROL	Al analizar el primer componente del COSO II se ha obtenido un nivel de confianza Bajo del 47,22% y un riesgo Alto del 52,78%.	a.- El Municipio no ha elaborado un código de ética que rija la conducta del personal durante el año 2013. H₁	Dirección de Recursos Humanos a.- Elaborar y difundir un Código de Ética que permita crear un buen ambiente de trabajo y compromiso hacia la organización.
		b.- La entidad no capacita al personal sobre el manejo y seguridad de los activos informáticos. H₂	Dirección de Recursos Humanos b.- Elaborar un Plan de Capacitación Informática de acuerdo a las necesidades de cada puesto de trabajo para contribuir al desempeño laboral.
		c.- No existe una Unidad de Informática dentro del Organigrama del Municipio para efectuar actividades de apoyo y asesoría a las unidades usuarias. H₃	Dirección de Recursos Humanos c.- Reestructurar el Organigrama Institucional con el fin de incluir una Unidad de Informática según las necesidades tecnológicas de la entidad.
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE
_COSO II
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_HR_CCI 2/9

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
		d.- La Misión, Visión y Objetivos institucionales no cumplen con las necesidades tecnológicas del Municipio. D₁	Administración General d.- Incluir aspectos tecnológicos en la Misión, Visión y Objetivos institucionales con el fin de cubrir las necesidades tecnológicas del Municipio.
		e.- No se cumplen con todos los numerales expuestos en las Normas de Control Interno para Entidades del Sector Público. D₂	Concejo Municipal e.- Supervisar que se dé cumplimiento a las Normas de Control Interno, en todos sus numerales por parte de los directivos y del personal que labora en la entidad.
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE
_COSO II
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_HR_CCI 3/9

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
ESTABLECIMIENTO DE OBJETIVOS	Al analizar el segundo componente del COSO II se ha obtenido un nivel de confianza Moderado del 60% y un riesgo Moderado del 40%.	a.- No se actualizan los objetivos institucionales. D₃	Administración General a.- Reunir a representantes de cada departamento para actualizar los objetivos institucionales de acuerdo a las necesidades de cada uno de ellos y de la entidad en general.
IDENTIFICACIÓN DE EVENTOS	Al analizar el tercer componente del COSO II se ha obtenido un nivel de confianza Bajo del 26,67% y un riesgo Alto del 73,33%.	a.- No existen mecanismos como controles, sistemas de aseguramiento o gestión de riesgos para identificar los riesgos informáticos. H₄	Administración General a.- Redactar políticas y procedimientos para identificar los riesgos informáticos, los mismos que deberán ser documentados y socializados con el personal del Municipio.
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE

AC 2_HR_CCI 4/9

_COSO II

Período del 01 de enero al 31 de diciembre 2013

EVALUACIÓN DEL CONTROL INTERNO

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
		b.- El personal del Municipio no identifica los posibles riesgos que afectan a los activos informáticos. D₄	Personal b.- Observar, identificar y comunicar a la dirección los posibles riesgos que pueden afectar la integridad de los activos informáticos.
		c.- La administración no analiza los riesgos externos que pueden afectar a la información y equipos informáticos. D₅	Administración General c.- Redactar políticas y procedimientos para identificar los riesgos externos que pueden afectar a la integridad de la información y equipos informáticos.
EVALUACIÓN DE RIESGOS	Al analizar el cuarto componente del COSO II se ha obtenido un nivel de confianza Bajo del 50% y un riesgo Alto del 50%.	a.- La entidad no cuenta con un Sistema de Control Interno para proteger la integridad de la información y de los equipos informáticos. H₅	Administración General a.- Diseñar e implementar un Sistema de Control Interno para proteger los activos informáticos que forman parte de los recursos públicos de la entidad, con la participación de los directivos y el personal que labora en el Municipio.
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE

AC 2_HR_CCI 5/9

_COSO II

Período del 01 de enero al 31 de diciembre 2013

EVALUACIÓN DEL CONTROL INTERNO

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
RESPUESTA AL RIESGO	Al analizar el quinto componente del COSO II se ha obtenido un nivel de confianza Bajo del 22,22% y un riesgo Alto del 77,78%.	a.- La entidad no cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos. H₆	Administración General a.- Diseñar e Implementar un Plan de Contingencias con la finalidad de salvaguardar los activos informáticos cuando existan emergencias o fallos en los sistemas computacionales.
		b.- No se aplican procedimientos, herramientas o técnicas para disminuir la ocurrencia e impacto de los riesgos informáticos. D₆	Administración General b.- Elaborar un documento escrito donde se detalle procedimientos, herramientas y técnicas para contrarrestar la ocurrencia e impacto de los riesgos informáticos.
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE
_COSO II
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_HR_CCI 6/9

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
ACTIVIDADES DE CONTROL	Al analizar el sexto componente del COSO II se ha obtenido un nivel de confianza Baja del 41,67% y un riesgo Alto del 58,33%.	a.- Los respaldos de la información almacenada en los equipos informáticos no se guardan en lugares externos al Municipio. H₇	Concejo Municipal a.- Conseguir un lugar adecuado y seguro fuera de la entidad para tener respaldos de la información crítica y sensible.
		b.- El Municipio no cuenta con un seguro para cubrir la pérdida o robo de la información almacenada en los equipos informáticos. D₇	Administración General b.- Contratar un seguro para proteger la información almacenada en los equipos informáticos de posibles robos o pérdida por fallas del sistema informático.
		c.- El personal no maneja tarjetas de identificación para acceder a la información almacenada en los equipos informáticos. H₈	Dirección de Recursos Humanos c.- Entregar tarjetas de identificación al personal interno, externo y temporal de la entidad para que puedan acceder a la información almacenada en los equipos informáticos.
ELABORADO POR: J.M.V.CH		FECHA: 26-03-2015	
REVISADO POR: C.E.E.R		FECHA: 30-03-2015	



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE
_COSO II
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_HR_CCI 7/9

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
		d.- El personal de la entidad no utiliza firmas electrónicas para enviar y recibir información del Municipio. H₉	Concejo Municipal d.- Gestionar la autorización correspondiente para que los directivos y el personal utilicen las firmas electrónicas en las operaciones que realizan según los puestos de trabajo y normativa legal.
		e.- No se realizan mantenimientos preventivos a los equipos informáticos. H₁₀	Dirección de Recursos Humanos e.- Contratar un Técnico en Informática que se encargue de realizar revisiones periódicas y monitoreo a los equipos informáticos con el fin de evitar daños irreparables.
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE
_COSO II
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_HR_CCI 8/9

Entidad: GAD Municipal del Cantón Penipe
Tipo de Examen: Auditoría
Componente: Informática

COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
		f.- Las instalaciones del Municipio no cuentan con dispositivos de seguridad para proteger los activos informáticos. H₁₁	Concejo Municipal f.- Establecer mecanismos de seguridad que protejan y salvaguarden los medios físicos y la información que se procesa mediante sistemas informáticos.
		g.- No se han instalado cámaras de vigilancia en el Municipio como medida de seguridad. D₈	Dirección Administrativa g.- Instalar cámaras de vigilancia al interior y exterior del Municipio para controlar los movimientos de los usuarios internos y externos que entran y salen de la entidad.
		h.- No se contratan vigilantes de seguridad para cuidar las instalaciones del Municipio por las noches y fines de semana. H₁₂	Dirección de Recursos Humanos h.- Contratar vigilantes de seguridad de lunes a domingo, las 24 horas para proteger las instalaciones del Municipio y los recursos públicos que posee.

ELABORADO POR: J.M.V.CH **FECHA: 26-03-2015**

REVISADO POR: C.E.E.R **FECHA: 30-03-2015**



HOJA DE RESUMEN DE CONCLUSIONES Y RECOMENDACIONES DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO POR COMPONENTE
_COSO II
Período del 01 de enero al 31 de diciembre 2013
EVALUACIÓN DEL CONTROL INTERNO

AC 2_HR_CCI 9/9

Entidad:	GAD Municipal del Cantón Penipe		
Tipo de Examen:	Auditoría		
Componente:	Informática		
COMPONENTE	ANÁLISIS DE NIVEL DE RIESGO Y CONFIANZA	CONCLUSIONES	RECOMENDACIONES
INFORMACIÓN COMUNICACIÓN	Y Al analizar el séptimo componente del COSO II se ha obtenido un nivel de confianza Moderada del 75% y un riesgo Moderado del 25%.		
MONITOREO	Al analizar el octavo componente del COSO II se ha obtenido un nivel de confianza Moderada del 55,56% y un riesgo Moderado del 44,44%.	a.-No se supervisa el manejo de los equipos informáticos. H₁₃	Dirección de Recursos Humanos a.- Contratar personal para supervisar el manejo de los equipos informáticos y las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño.
Luego de aplicar los Cuestionarios de Control Interno al personal del Municipio y realizar la matriz de riesgo y confianza de cada componente del COSO II, el Sistema de Control Interno obtuvo un nivel de confianza BAJO del 47,29% y un riesgo ALTO del 52,71%., poniendo en consideración las respectivas recomendaciones para cada uno de los componentes.			
ELABORADO POR: J.M.V.CH			FECHA: 26-03-2015
REVISADO POR: C.E.E.R			FECHA: 30-03-2015

INFORME DE CONTROL INTERNO

Riobamba, 1 de abril del 2015

Ingeniero

Robin Velasteguí

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PENIPE

Presente.-

De mi consideración:

Realizada la evaluación del control interno al GAD Municipal del Cantón Penipe con la finalidad de determinar el grado de eficacia, eficiencia y seguridad en el manejo de la información y los equipos informáticos, se obtuvo los siguientes resultados preliminares:

➤ **Inexistencia de un Código de Ética.**

El Municipio no ha elaborado un código de ética que rija la conducta del personal durante el año 2013. **H₁** Según las Normas de Control Interno de la CGE **200-01 Integridad y Valores Éticos** señala: La máxima autoridad de cada entidad emitirá formalmente las normas propias del código de ética, para contribuir al buen uso de los recursos públicos y al combate a la corrupción.

➤ **Falta de Capacitación Informática.**

La entidad no capacita al personal sobre el manejo y seguridad de los activos informáticos. **H₂** Según las Normas de Control Interno de la CGE **410-15 Capacitación informática** señala: Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

➤ **Inexistencia de una Unidad de Informática.**

No existe una Unidad de Informática dentro del Organigrama del Municipio para efectuar actividades de apoyo y asesoría a las unidades usuarias.**H₃**Según las Normas de Control Interno de la CGE **410-01 Organización informática** señala: La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

➤ **Inexistencia de mecanismos para identificar riesgos informáticos.**

No existen mecanismos como controles, sistemas de aseguramiento o gestión de riesgos para identificar los riesgos informáticos.**H₄**Según las Normas de Control Interno de la CGE **410-04 Políticas y procedimientos** señala: Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

➤ **Inexistencia de un Sistema de Control Interno.**

La entidad no cuenta con un Sistema de Control Interno para proteger la integridad de la información y de los equipos informáticos.**H₅** Según las Normas de Control Interno de la CGE **100-01 Control Interno** señala: El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.

➤ **Inexistencia de un Plan de Contingencias.**

La entidad no cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos.**H₆**Según las Normas de Control Interno de la CGE **410-11 Plan de contingencias** señala: **6.** El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

➤ **Inexistencia de lugares externos para guardar los respaldos de la información.**

Los respaldos de la información almacenada en los equipos informáticos no se guardan en lugares externos al Municipio. **H₇** Según las Normas de Control Interno de la CGE **410-10 Seguridad de tecnología de información** señala: **4.** Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.

➤ **Inexistencia de tarjetas de identificación para el personal.**

El personal no maneja tarjetas de identificación para acceder a la información almacenada en los equipos informáticos. **H₈** Según las Normas de Control Interno de la CGE **410-12 Administración de soporte de tecnología de información** señala: **2.** Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.

➤ **No se utiliza firmas electrónicas.**

El personal de la entidad no utiliza firmas electrónicas para enviar y recibir información del Municipio. **H₉** Según las Normas de Control Interno de la CGE **410-17 Firmas electrónicas** señala: Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.

➤ **Falta de mantenimiento preventivo a los equipos informáticos.**

No se realizan mantenimientos preventivos a los equipos informáticos. **H₁₀** Según las Normas de Control Interno de la CGE **410-09 Mantenimiento y control de la infraestructura tecnológica** señala: **6.** Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

➤ **Inexistencia de dispositivos de seguridad.**

Las instalaciones del Municipio no cuentan con dispositivos de seguridad para proteger los activos informáticos.**H₁₁** Según las Normas de Control Interno de la CGE **410-10 Seguridad de tecnología de información** señala: **6.** Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros.

➤ **Falta de personal de seguridad.**

No se contratan vigilantes de seguridad para cuidar las instalaciones del Municipio por las noches y fines de semana.**H₁₂** Según las Normas de Control Interno de la CGE **410-10 Seguridad de tecnología de información** señala: **8.** Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

➤ **Falta de supervisión en el manejo de los equipos informáticos.**

No se supervisa el manejo de los equipos informáticos.**H₁₃** Según las Normas de Control Interno de la CGE **410-04 Políticas y procedimientos** señala: Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.

Luego de aplicar los Cuestionarios de Control Interno al personal del Municipio y realizar la matriz de riesgo y confianza de cada componente del COSO II, el Sistema de Control Interno obtuvo un nivel de confianza **BAJO** del 47,29% y un riesgo **ALTO** del 52,71%., poniendo en consideración las respectivas recomendaciones para cada uno de los componentes.


Particular que le comunicamos para los fines consiguientes.


Atentamente,


Srta. Jenny Veloz


AUTORA DE TESIS


4.2.3.3.Fase III: Análisis de Áreas Críticas


	INDICADORES Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 2_IND 1/5
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática		
INVENTARIO DE COMPUTADORAS DEL GAD MUNICIPAL		
ÁREA	Nº DE COMPUTADORAS	
Administración General	8	
Alcaldía	1	
Auditoría Interna	1	
Asesoría Jurídica	3	
Secretaría General	3	
Dirección Administrativa y de Recursos Humanos	7	
Educación, Cultura y Sistemas	2	
Documentación y Archivo	2	
Servicios Generales	1	
Comisaría	2	
Dirección Financiera	16	
Presupuesto y Control	3	
Contabilidad	4	
Avalúos y Catastros	3	
Tesorería	2	
ELABORADO POR: J.M.V.CH	FECHA: 04-04-2015	
REVISADO POR: C.E.E.R	FECHA: 06-04-2015	


	INDICADORES Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 2_IND 2/5
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
INVENTARIO DE COMPUTADORAS DEL GAD MUNICIPAL		
ÁREA	Nº DE COMPUTADORAS	
Tributación	1	
Recaudación	1	
Bodega y Control de Activos	1	
Compras Públicas	1	
Dirección de Obras Públicas	10	
Planificación	2	
Fiscalización	1	
Higiene Ambiental y Salud Pública	4	
Agua Potable y Alcantarillado	2	
Tránsito, Transporte y Movilización Pública	1	
TOTAL Σ	41	
ELABORADO POR: J.M.V.CH	FECHA: 04-04-2015	
REVISADO POR: C.E.E.R	FECHA: 06-04-2015	


	INDICADORES Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 2_IND 3/5
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
<p>Para elaborar los indicadores se ha tomado en cuenta un total de 41 computadoras para verificar la eficiencia, eficacia y seguridad en el manejo de la información y equipos informáticos.</p> <p>Las técnicas aplicadas son la observación y entrevistas a los responsables de los equipos informáticos.</p> <p>EFICIENCIA</p> <p>Presupuesto informático = $\frac{\text{Presupuesto equipos informáticos}}{\text{Presupuesto total}} * 100 = \frac{8.426,09 \text{ USD}}{1\ 679.755,18 \text{ USD}} = 0,5\%$</p> <p>ANÁLISIS:</p> <p>Del presupuesto asignado para el Municipio en el año 2013, el 0,5% corresponde a los equipos, sistemas y paquetes informáticos, un valor muy bajo con respecto a las necesidades reales que tiene la entidad tanto en activos informáticos como en dispositivos para la seguridad. Ω</p> <p>EFICACIA</p> <p>Sistema Operativo Actualizado = $\frac{\# \text{ Computadoras con Windows 8}}{\# \text{ Total Computadoras}} * 100 = \frac{0}{41} = 0\%$</p> <p>ANÁLISIS:</p> <p>Ninguna computadora del Municipio cuenta con un sistema operativo actualizado, el personal sigue utilizando Windows 7, el mismo que funciona correctamente para la realización de las actividades cotidianas de la entidad. √</p>		
ELABORADO POR: J.M.V.CH		FECHA: 04-04-2015
REVISADO POR: C.E.E.R		FECHA: 06-04-2015


	INDICADORES Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_IND 4/5
Entidad: GAD Municipal del Cantón Penipe Tipo de Examen: Auditoría Componente: Informática		
<p>Acceso a Internet = $\frac{\# \text{ Computadoras con Internet}}{\# \text{ Total Computadoras}} * 100 = \frac{41}{41} = 100\%$</p> <p>ANÁLISIS:</p> <p>Según el indicador de eficacia se concluye que el 100% de las computadoras cuentan con acceso a internet, cumpliendo con las necesidades de los usuarios de los equipos informáticos. ✓</p> <p>Mantenimiento preventivo = $\frac{\# \text{ Computadoras que se realiza mantenimiento preventivo}}{\# \text{ Total Computadoras}} * 100 = \frac{0}{41} = 0\%$</p> <p>ANÁLISIS:</p> <p>A ningún equipo de cómputo se realiza un mantenimiento preventivo, ya que el técnico que trabaja en el Municipio no tiene el suficiente tiempo para realizar esta actividad, es por esto que se realiza solo acciones correctivas cuando ya ha ocurrido el daño.</p> <p>Actas de Entrega/Recepción = $\frac{\# \text{ Computadoras entregadas con actas de entrega/recepción}}{\# \text{ Total Computadoras}} * 100 = \frac{41}{41} = 100\%$</p> <p>ANÁLISIS:</p> <p>El 100% de las computadoras son entregadas con sus respectivas actas de entrega/recepción para constatar de forma documentada que el personal recibió el equipo. Ω</p>		
ELABORADO POR: J.M.V.CH		FECHA: 04-04-2015
REVISADO POR: C.E.E.R		FECHA: 06-04-2015


	INDICADORES Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_IND 5/5
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
<p>INDICADORES DE SEGURIDAD</p> <p>Seguridad para ingresar al computador = $\frac{\# \text{ Computadoras con contraseña}}{\# \text{ Total Computadoras}} * 100 = \frac{40}{41}$ 97,56%</p> <p>ANÁLISIS:</p> <p>Se ha determinado que de las 41 computadoras examinadas, 40 cuentan con una contraseña para ingresar al sistema operativo, las mismas representan un 97,56% de cumplimiento en seguridad. ✓</p> <p>Restricción de ingreso a Redes Sociales = $\frac{\# \text{ Computadoras con restricción}}{\# \text{ Total Computadoras}} * 100 = \frac{39}{41}$ 95,12%</p> <p>ANÁLISIS:</p> <p>De las 41 computadoras examinadas 39 tienen restricción para acceder a redes sociales como Facebook, Twitter e incluso música, las mismas corresponden al 95,12% de seguridad. ✓</p> <p>Antivirus Actualizado = $\frac{\# \text{ Computadoras con antivirus actualizado}}{\# \text{ Total Computadoras}} * 100 = \frac{36}{41} = \mathbf{87,80\%}$</p> <p>ANÁLISIS:</p> <p>Las computadoras que tienen instalado un antivirus, el mismo que está actualizado cada año con su respectiva licencia corresponde al 87,80% de un total de 41 computadoras examinadas, un nivel aceptable de seguridad. ✓</p>		
ELABORADO POR: J.M.V.CH		FECHA: 04-04-2015
REVISADO POR: C.E.E.R		FECHA: 06-04-2015


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 1/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₁ INEXISTENCIA DE UN CÓDIGO DE ÉTICA	AC 2_HR_CCI 1/9	
Condición El Municipio no ha elaborado un código de ética que rija la conducta del personal durante el año 2013.		
Criterio Según las Normas de Control Interno de la CGE 200-01 Integridad y Valores Éticos señala: La máxima autoridad de cada entidad emitirá formalmente las normas propias del código de ética, para contribuir al buen uso de los recursos públicos y al combate a la corrupción.		
Causa Existen temas de mayor relevancia que se tratan en las juntas directivas del Municipio, dejando un lado el análisis de la conducta del personal y el ambiente laboral de la entidad.		
Efecto Al no tener un código de ética, el clima organizacional del Municipio no es adecuado para el personal que labora en los diferentes departamentos de la entidad.		
CONCLUSIÓN: El Municipio no cuenta con un código de ética documentado que rija la conducta del personal, sin embargo cada empleado aplica los valores y principios que posee para mantener un ambiente laboral adecuado.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Elaborar y difundir un Código de Ética que permita crear un ambiente de trabajo adecuado entre los directivos y el personal que laboran en el Municipio, además de incentivar el compromiso hacia la organización.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 2/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₂ FALTA DE CAPACITACIÓN INFORMÁTICA.	AC 2_HR_CCI 1/9	
Condición La entidad no capacita al personal sobre el manejo y seguridad de los activos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-15 Capacitación informática señala: Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.		
Causa No se capacita al personal del Municipio puesto que no existe partida presupuestaria para dicho fin.		
Efecto El personal del Municipio no cuenta con habilidades y conocimientos suficientes para manejar la información y los equipos informáticos, siendo ineficientes e ineficaces en el uso de los activos informáticos.		
CONCLUSIÓN: El Municipio no cuenta con un plan de capacitación para el personal que utiliza los activos informáticos, los mismos se capacitan por cuenta propia para desempeñar de manera eficiente sus actividades.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Elaborar un Plan de Capacitación Informática de acuerdo a las necesidades de cada puesto de trabajo para contribuir al desempeño laboral y cumplimiento de los objetivos institucionales.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 3/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₃ INEXISTENCIA DE UNA UNIDAD INFORMÁTICA	AC 2_HR_CCI 1/9	
Condición No existe una Unidad de Informática dentro del Organigrama del Municipio para efectuar actividades de apoyo y asesoría a las unidades usuarias.		
Criterio Según las Normas de Control Interno de la CGE 410-01 Organización informática señala: La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.		
Causa Falta de interés por parte de los directivos del Municipio para crear una Unidad de Informática, además que no existe partida presupuestaria para implementar y contratar personal para la unidad antes mencionada.		
Efecto No existe asesoría y apoyo en el ámbito tecnológico para los usuarios internos y externos de la entidad impidiendo un avance tecnológico para el Municipio.		
CONCLUSIÓN: No existe dentro del organigrama institucional una Unidad de Informática que permita dar apoyo y asesoría tecnológica a los usuarios internos y externos de la entidad teniendo que llamar a un técnico cuando ocurra algún daño en los activos informáticos.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Restructurar el Organigrama con el fin de incluir una Unidad de Informática según las necesidades tecnológicas de la entidad.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 4/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO		REFERENCIA
H₄ INEXISTENCIA DE MECANISMOS PARA IDENTIFICAR RIESGOS INFORMÁTICOS		AC 2_HR_CCI 3/9
Condición No existen mecanismos como controles, sistemas de aseguramiento o gestión de riesgos para identificar los riesgos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-04 Políticas y procedimientos señala: Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.		
Causa Por falta de interés de la Administración del Municipio no se ha redactado políticas y procedimientos donde consten mecanismos para identificar los riesgos informáticos.		
Efecto No se pueden identificar riesgos significativos que dañen la integridad de la información y los equipos informáticos, pudiendo perder información importante por fallas en los sistemas computacionales.		
CONCLUSIÓN: No existen políticas, procedimientos, controles o mecanismos que ayuden a identificar los riesgos informáticos impidiendo contrarrestar posibles daños a los equipos informáticos y pérdidas de información relevante para el Municipio.		
RECOMENDACIÓN: A la Administración General: Redactar políticas y procedimientos para identificar los riesgos informáticos, los mismos que deberán ser documentados y socializados con el personal del Municipio.		
ELABORADO POR: J.M.V.CH		FECHA: 11-04-2015
REVISADO POR: C.E.E.R		FECHA: 12-04-2015


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 5/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₅ INEXISTENCIA DE UN SISTEMA DE CONTROL INTERNO	AC 2_HR_CCI 4/9	
Condición La entidad no cuenta con un Sistema de Control Interno para proteger la integridad de la información y de los equipos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 100-01 Control Interno señala: El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.		
Causa El Consejo Municipal no ha implementado un Sistema de Control Interno para proteger los activos informáticos, puesto que no hay suficiente presupuesto ni tampoco personal para diseñar dicho sistema.		
Efecto Al no existir un Sistema de Control Interno, los riesgos no son identificados a tiempo y dañan la integridad y seguridad de los activos informáticos, perdiendo tiempo y recursos públicos que pertenecen a la comunidad de Penipe.		
CONCLUSIÓN: El Municipio no cuenta con un Sistema de Control Interno adecuado que proteja la integridad de los activos informáticos, la única garantía es confiar en el personal que utiliza dichos activos.		
RECOMENDACIÓN: A la Administración General: Diseñar e implementar un Sistema de Control Interno para proteger los activos informáticos que forman parte de los recursos públicos de la entidad, con la participación de los directivos y el personal que labora en el Municipio.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 6/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO		REFERENCIA
H₆ INEXISTENCIA DE UN PLAN DE CONTINGENCIAS		AC 2_HR_CCI 5/9
Condición La entidad no cuenta con un Plan de Contingencias para contrarrestar los riesgos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-11 Plan de contingencias señala: 6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.		
Causa La Administración del Municipio no ha diseñado un plan de contingencias que proteja los activos informáticos por falta de interés, tiempo, presupuesto y personal.		
Efecto El personal del Municipio que utiliza los activos informáticos no sabe qué medidas preventivas, detectivas o correctivas aplicar ante una emergencia o fallo en los sistemas computacionales, perdiendo tiempo, información y recursos que afectan a la economía de la entidad.		
CONCLUSIÓN: El Municipio no cuenta con un Plan de contingencias para que los directivos y el personal contrarresten los posibles riesgos informáticos mediante medidas preventivas, detectivas y correctivas.		
RECOMENDACIÓN: A la Administración General: Diseñar e Implementar un Plan de Contingencias con la finalidad de salvaguardar los activos informáticos cuando existan emergencias o fallos en los sistemas computacionales.		
ELABORADO POR: J.M.V.CH		FECHA: 11-04-2015
REVISADO POR: C.E.E.R		FECHA: 12-04-2015


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 7/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₇ INEXISTENCIA DE LUGARES EXTERNOS PARA GUARDAR LOS RESPALDOS DE LA INFORMACIÓN	AC 2_HR_CCI 6/9	
Condición Los respaldos de la información almacenada en los equipos informáticos no se guardan en lugares externos al Municipio.		
Criterio Según las Normas de Control Interno de la CGE 410-10 Seguridad de tecnología de información señala: 4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.		
Causa El Municipio no cuenta con un lugar externo adecuado para guardar los respaldos de la información por falta de presupuesto.		
Efecto Si ocurre algún desastre dentro del Municipio como incendio, inundación, corto circuito o robo se perderá totalmente la información almacenada en los equipos informáticos afectando a las actividades normales que se realizan en la entidad.		
CONCLUSIÓN: La información crítica y sensible que se almacena en los equipos informáticos no tiene respaldos en lugares externos al Municipio, poniendo en riesgo su integridad y seguridad.		
RECOMENDACIÓN: Al Concejo Municipal: Conseguir un lugar adecuado y seguro fuera de la entidad para tener respaldos de la información crítica y sensible.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	


	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 2_HA 8/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO		REFERENCIA
H₈ INEXISTENCIA DE TARJETAS DE IDENTIFICACIÓN PARA EL PERSONAL		AC 2_HR_CCI 6/9
Condición El personal no maneja tarjetas de identificación para acceder a la información almacenada en los equipos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-12 Administración de soporte de tecnología de información señala: 2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.		
Causa Por falta de interés de los directivos del Municipio no se ha elaborado tarjetas de identificación para los usuarios internos, externos y temporales de la información.		
Efecto Personas no autorizadas y ajenas a la entidad pueden acceder a la información almacenada en los equipos informáticos y dar mal uso de ella perjudicando a la integridad del Municipio.		
CONCLUSIÓN: Los usuarios internos, externos y temporales de la información no tienen una tarjeta de identificación para acceder a la misma provocando que cualquier persona pueda manipular los equipos de cómputo haciendo mal uso de su contenido.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Entregar tarjetas de identificación al personal interno, externo y temporal de la entidad para que puedan acceder a la información almacenada en los equipos informáticos sin excepciones.		
ELABORADO POR: J.M.V.CH		FECHA: 11-04-2015
REVISADO POR: C.E.E.R		FECHA: 12-04-2015

	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 9/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₉ NO SE UTILIZA FIRMAS ELECTRÓNICAS	AC 2_HR_CCI 7/9	
Condición El personal de la entidad no utiliza firmas electrónicas para enviar y recibir información del Municipio.		
Criterio Según las Normas de Control Interno de la CGE 410-17 Firmas electrónicas señala: Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.		
Causa Los directivos y el personal de la entidad no utilizan firmas electrónicas porque no se ha gestionado la autorización correspondiente por parte del Banco Central del Ecuador.		
Efecto El Municipio pierde tiempo y recursos al no poder enviar y recibir información por medios electrónicos y tiene que hacerlo por medio de documentación impresa.		
CONCLUSIÓN: Los directivos y el personal del Municipio no utilizan firmas electrónicas para enviar y recibir información puesto que no tienen un Token otorgado por el Banco Central del Ecuador.		
RECOMENDACIÓN: Al Concejo Municipal: Gestionar la autorización correspondiente para que los directivos y el personal utilicen las firmas electrónicas en las operaciones que realizan según los puestos de trabajo y normativa legal.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	

	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 10/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₁₀ FALTA DE MANTENIMIENTO PREVENTIVO A LOS EQUIPOS INFORMÁTICOS	AC 2_HR_CCI 7/9	
Condición No se realizan mantenimientos preventivos a los equipos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-09 Mantenimiento y control de la infraestructura tecnológica señala: 6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.		
Causa Por falta de personal en el área de mantenimiento no se realizan revisiones o monitoreo previos a la ocurrencia de eventos que dañan los equipos informáticos.		
Efecto Los equipos informáticos se dañan con más frecuencia de lo normal, interrumpiendo las actividades de los usuarios que custodian dichos equipos perdiendo tiempo y recursos del Municipio.		
CONCLUSIÓN: No se da un mantenimiento preventivo a los equipos informáticos, puesto que existe un solo técnico para arreglar problemas que aparecen en las computadoras, impresoras, infocus, hardware y software, provocando que el personal se retrase en las actividades que realizan en el Municipio.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Contratar un Técnico en Informática que se encargue de realizar revisiones periódicas y monitoreo a los equipos informáticos con el fin de evitar daños irreparables.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	

	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 11/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO		REFERENCIA
H₁₁ INEXISTENCIA DE DISPOSITIVOS DE SEGURIDAD		AC 2_HR_CCI 8/9
Condición Las instalaciones del Municipio no cuentan con dispositivos de seguridad para proteger los activos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-10 Seguridad de tecnología de información señala: 6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros.		
Causa Por falta de presupuesto los directivos del Municipio no dan la orden para instalar dispositivos de seguridad.		
Efecto Al no existir dispositivos de seguridad aumenta el riesgo de que ocurran eventos inesperados que dañen los activos informáticos.		
CONCLUSIÓN: No se ha instalado dispositivos de seguridad como cámaras de vigilancia, sensores de temperatura, sensores de humo, extractores de calor, etc. en las instalaciones del Municipio provocando que los activos informáticos queden vulnerables al riesgo informático.		
RECOMENDACIÓN: Al Concejo Municipal: Establecer mecanismos de seguridad que protejan y salvaguarden los medios físicos y la información que se procesa mediante sistemas informáticos.		
ELABORADO POR: J.M.V.CH		FECHA: 11-04-2015
REVISADO POR: C.E.E.R		FECHA: 12-04-2015

	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 12/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO		REFERENCIA
H₁₂ FALTA DE PERSONAL DE SEGURIDAD		AC 2_HR_CCI 8/9
Condición No se contratan vigilantes de seguridad para cuidar las instalaciones del Municipio por las noches y fines de semana.		
Criterio Según las Normas de Control Interno de la CGE 410-10 Seguridad de tecnología de información señala: 8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.		
Causa No está dentro del presupuesto contratar personal de seguridad para las noches y fines de semana.		
Efecto Posible riesgo de robo de los activos informáticos durante el horario que no se encuentran protegidas las instalaciones del Municipio provocando pérdidas grandes de información y recursos económicos.		
CONCLUSIÓN: El Municipio contrata personal de seguridad de lunes a viernes, de 8:00am-12:00am y de 12:00am-18_00pm, mas no para las noches y fines de semana lo cual provoca riesgo de robo de los activos informáticos dentro de dicho horario.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Contratar vigilantes de seguridad de lunes a domingo, las 24 horas para proteger las instalaciones del Municipio y los recursos públicos que posee.		
ELABORADO POR: J.M.V.CH		FECHA: 11-04-2015
REVISADO POR: C.E.E.R		FECHA: 12-04-2015

	HOJA DE HALLAZGOS Período del 01 de enero al 31 de diciembre 2013 ANÁLISIS DE ÁREAS CRÍTICAS	AC 3_HA 13/13
Entidad: Tipo de Examen: Componente:	GAD Municipal del Cantón Penipe Auditoría Informática	
HALLAZGO	REFERENCIA	
H₁₃FALTA DE SUPERVISIÓN EN EL MANEJO DE LOS EQUIPOS INFORMÁTICOS	AC 2_HR_CCI 9/9	
Condición No se supervisa al personal el manejo de los equipos informáticos.		
Criterio Según las Normas de Control Interno de la CGE 410-04 Políticas y procedimientos señala: Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.		
Causa No se contrata personal para supervisar el manejo de los equipos informáticos por falta de partida presupuestaria y recursos económicos, los mismos que son utilizados para otros fines.		
Efecto El personal puede hacer mal uso de los equipos informáticos e incluso dañar dichos equipos por manipular de manera inadecuada los sistemas operativos, provocando la pérdida de tiempo, información y recursos que le cuestan al Municipio de Penipe.		
CONCLUSIÓN: El Municipio no cuenta con una persona que se encargue de supervisar y monitorear el manejo adecuado de los equipos informáticos, el personal utiliza dichos equipos de acuerdo a los conocimientos y experiencia que posee.		
RECOMENDACIÓN: A la Dirección de Recursos Humanos: Contratar personal para supervisar el manejo de los equipos informáticos y las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño.		
ELABORADO POR: J.M.V.CH	FECHA: 11-04-2015	
REVISADO POR: C.E.E.R	FECHA: 12-04-2015	

4.2.3.4.Fase IV: Informe

J.V AUDITOR CIA. LTDA



ENTIDAD EXAMINADA

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN
PENIPE

INFORME DE AUDITORÍA

Informe de Auditoría Informática al Gobierno Autónomo Descentralizado
Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013.

RIOBAMBA - ECUADOR
2015

CARTA DE PRESENTACIÓN

Riobamba, 18 de mayo del 2015.

Ing.

Robin Velasteguí

ALCALDE DEL GAD MUNICIPAL DEL CANTÓN PENIPE

Presente.-

De mi consideración:

Se ha realizado la “Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, periodo 2013”, el mismo que se realizó de acuerdo a las Normas de Auditoría Generalmente Aceptadas, Principios de Control Interno, Manual de Contraloría General del Estado y demás procedimientos técnicos considerados necesarios para la auditoría.

Para la evaluación de Control Interno, se aplicó los componentes del COSO II, los mismos que facilitaron la evaluación y ayudaron a determinar áreas críticas que podrían afectar a la consecución de los objetivos institucionales.

En la auditoría constan los resultados obtenidos en base al análisis realizado, incluyendo los respectivos comentarios, conclusiones y recomendaciones que de seguro serán de beneficio para el Alcalde y Concejo Municipal.

Atentamente,

Srta. Jenny Veloz

AUTORA DE TESIS

**GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN
PENIPE**

INFORME DE AUDITORÍA

DEL 01 DE ENERO 2013 AL 31 DE DICIEMBRE DEL 2013.

CAPÍTULO I

MOTIVO

La realización de la Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, se llevó a cabo de conformidad a la Orden de Trabajo No. 001 del 05 de enero del 2015, emitida por la Srta. Jenny Veloz Autora de Tesis; y, conforme al Plan de Investigación aprobado por el H. Consejo Directivo de la Facultad de Administración de Empresas de la Escuela Superior Politécnica de Chimborazo con la finalidad de evaluar los procedimientos efectuados en la institución.

OBJETIVOS DEL EXAMEN

Objetivo General:

Desarrollar una Auditoría Informática al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, Provincia de Chimborazo, período 2013, para medir el grado de eficiencia, eficacia y seguridad en el manejo de la información y los equipos informáticos.

Objetivos Específicos

- Desarrollar un marco teórico, para el estudio de los procesos, normas y reglamentos vigentes, a utilizarse en el trabajo de investigación.
- Determinar la metodología de la auditoría informática mediante el análisis de control interno para evaluar la eficiencia, eficacia y seguridad del manejo de la información y los equipos informáticos.

- Emitir un informe con las conclusiones y recomendaciones, susceptibles de ser tomadas en cuenta para la toma de decisiones correctivas en el manejo de la información y los equipos informáticos.

ALCANCE DE LA AUDITORÍA

La Auditoría Informática se realizó al Gobierno Autónomo Descentralizado Municipal del Cantón Penipe, en el período comprendido entre el 01 de Enero al 31 de Diciembre del 2013, este examen tendrá una duración de 90 días laborables.

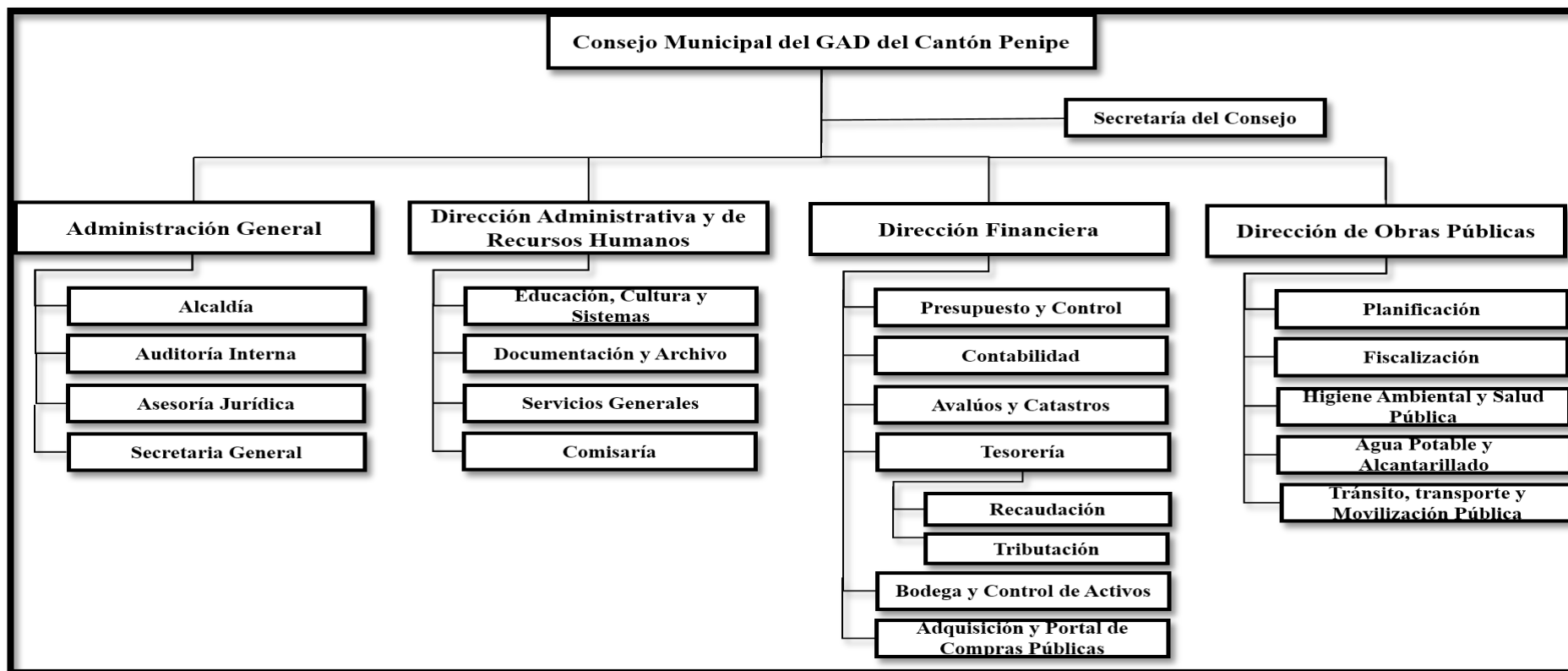
BASE LEGAL

La Municipalidad del cantón Penipe, fue creado mediante Decreto Legislativo N° 15, publicado en el Registro Oficial N° 680 del 9 de Febrero de 1984 y el desarrollo de su vida jurídica e institucional, fue uno de los primeros cantones en integrarse al COMAGA (Consortio de Municipios Amazónicos y Galápagos), hoy en día recibe recursos por parte del gobierno a través de la ley 0.10.

La administración y personal del GAD Municipal del Cantón Penipe ejerce sus actividades en función a la siguiente base legal:

- Constitución Política de la República del Ecuador
- Ley Orgánica de la Contraloría General del Estado
- Ley de Presupuesto del Sector Público
- Ley Orgánica de Régimen Municipal
- Ley Orgánica de Régimen Tributario Interno
- Ley Orgánica de Servicio Civil y Carrera Administrativa y de Unificación y Homologación de las Remuneraciones del Sector Público
- Normativa de Contabilidad Gubernamental del Ministerio de Finanzas
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos
- Código Orgánico de Organización Territorial Autonomía y Descentralización
- Código de Trabajo

ESTRUCTURA ORGÁNICA



CAPÍTULO II

RESULTADOS DE LA AUDITORÍA

Durante el desarrollo del examen se estableció las siguientes conclusiones y recomendaciones:

1. Inexistencia de un Código de Ética.

Según las Normas de Control Interno de la CGE **200-01 Integridad y Valores Éticos** señala: La máxima autoridad de cada entidad emitirá formalmente las normas propias del código de ética, para contribuir al buen uso de los recursos públicos y al combate a la corrupción.

Conclusión:

El Municipio no cuenta con un código de ética documentado que rija la conducta del personal, sin embargo cada empleado aplica los valores y principios que posee para mantener un ambiente laboral adecuado.

Recomendación:

A la Dirección de Recursos Humanos

Elaborar y difundir un Código de Ética que permita crear un ambiente de trabajo adecuado entre los directivos y el personal que laboran en el Municipio, además de incentivar el compromiso hacia la organización.

2. Falta de Capacitación Informática.

Según las Normas de Control Interno de la CGE **410-15 Capacitación informática** señala: Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos

de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

Conclusión:

El Municipio no cuenta con un plan de capacitación para el personal que utiliza los activos informáticos, los mismos se capacitan por cuenta propia para desempeñar de manera eficiente sus actividades.

Recomendación:

A la Dirección de Recursos Humanos

Elaborar un Plan de Capacitación Informática de acuerdo a las necesidades de cada puesto de trabajo para contribuir al desempeño laboral y cumplimiento de los objetivos institucionales.

3. Inexistencia de una Unidad Informática.

Según las Normas de Control Interno de la CGE **410-01 Organización informática** señala: La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

Conclusión:

No existe dentro del organigrama institucional una Unidad de Informática que permita dar apoyo y asesoría tecnológica a los usuarios internos y externos de la entidad teniendo que llamar a un técnico cuando ocurra algún daño en los activos informáticos.

Recomendación:

A la Dirección de Recursos Humanos

Reestructurar el Organigrama Institucional con el fin de incluir una Unidad de Informática según las necesidades tecnológicas de la entidad.

4. Inexistencia de mecanismos para identificar riesgos informáticos.

Según las Normas de Control Interno de la CGE **410-04 Políticas y procedimientos** señala: Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Conclusión:

No existen políticas, procedimientos, controles o mecanismos que ayuden a identificar los riesgos informáticos impidiendo contrarrestar posibles daños a los equipos informáticos y pérdidas de información relevante para el Municipio.

Recomendación:

A la Administración General

Redactar políticas y procedimientos para identificar los riesgos informáticos, los mismos que deberán ser documentados y socializados con el personal del Municipio.

5. Inexistencia de un Sistema de Control Interno.

Según las Normas de Control Interno de la CGE **100-01 Control Interno** señala: El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.

Conclusión:

El Municipio no cuenta con un Sistema de Control Interno adecuado que proteja la integridad de los activos informáticos, la única garantía es confiar en el personal que utiliza dichos activos.

Recomendación:

A la Administración General

Diseñar e implementar un Sistema de Control Interno para proteger los activos informáticos que forman parte de los recursos públicos de la entidad, con la participación de los directivos y el personal que labora en el Municipio.

6. Inexistencia de un Plan de Contingencias.

Según las Normas de Control Interno de la CGE **410-11 Plan de contingencias** señala: El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

Conclusión:

El Municipio no cuenta con un Plan de contingencias para que los directivos y el personal contrarresten los posibles riesgos informáticos que pueden aparecer mediante medidas preventivas, detectivas y correctivas.

Recomendación:

A la Administración General

Diseñar e Implementar un Plan de Contingencias con la finalidad de salvaguardar los activos informáticos cuando existan emergencias o fallos en los sistemas computacionales.

7. Inexistencia de lugares externos para guardar los respaldos de la información.

Según las Normas de Control Interno de la CGE **410-10 Seguridad de tecnología de información** señala: **4.** Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.

Conclusión:

La información crítica y sensible que se almacena en los equipos informáticos no tiene respaldos en lugares externos al Municipio, poniendo en riesgo su integridad y seguridad.

Recomendación:

Al Concejo Municipal

Conseguir un lugar adecuado y seguro fuera de la entidad para tener respaldos de la información crítica y sensible.

8. Inexistencia de Tarjetas de Identificación para el personal.

Según las Normas de Control Interno de la CGE **410-12 Administración de soporte de tecnología de información** señala: **2.** Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.

Conclusión:

Los usuarios internos, externos y temporales de la información no tienen una tarjeta de identificación para acceder a la misma, provocando que cualquier persona pueda manipular los equipos de cómputo haciendo mal uso de su contenido.

Recomendación:

A la Dirección de Recursos Humanos

Entregar tarjetas de identificación al personal interno, externo y temporal de la entidad para que puedan acceder a la información almacenada en los equipos informáticos sin excepciones.

9. No se utiliza firmas electrónicas.

Según las Normas de Control Interno de la CGE **410-17 Firmas electrónicas** señala: Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.

Conclusión:

Los directivos y el personal del Municipio no utilizan firmas electrónicas para enviar y recibir información puesto que no tienen un Token otorgado por el Banco Central del Ecuador.

Recomendación:**Al Concejo Municipal**

Gestionar la autorización correspondiente para que los directivos y el personal del Municipio utilicen las firmas electrónicas en las operaciones que realizan según los puestos de trabajo y normativa legal.

10. Falta de mantenimiento preventivo a los equipos informáticos.

Según las Normas de Control Interno de la CGE **410-09 Mantenimiento y control de la infraestructura tecnológica** señala: **6.** Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

Conclusión:

No se da un mantenimiento preventivo a los equipos informáticos, puesto que existe un solo técnico para arreglar problemas que aparecen en las computadoras, impresoras, proyectores, hardware y software.

Recomendación:**A la Dirección de Recursos Humanos**

Contratar un Técnico en Informática que se encargue de realizar revisiones periódicas y monitoreo a los equipos informáticos con el fin de evitar daños irreparables.

11. Inexistencia de dispositivos de seguridad.

Según las Normas de Control Interno de la CGE **410-10 Seguridad de tecnología de información** señala: **6.** Instalaciones físicas adecuadas que incluyan mecanismos,

dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros.

Conclusión:

No se ha instalado dispositivos de seguridad como cámaras de vigilancia, sensores de temperatura, sensores de humo, extractores de calor, etc. en las instalaciones del Municipio provocando que los activos informáticos queden vulnerables al riesgo informático.

Recomendación:

Al Concejo Municipal

Establecer mecanismos de seguridad que protejan y salvaguarden los medios físicos y la información que se procesa mediante sistemas informáticos.

12. Falta de Personal de seguridad.

Según las Normas de Control Interno de la CGE **410-10 Seguridad de tecnología de información** señala: **8.** Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

Conclusión:

El Municipio contrata personal de seguridad de lunes a viernes, de 8:00am-12:00am y de 12:00am-18_00pm, mas no para las noches y fines de semana lo cual provoca riesgo de robo de los activos informáticos dentro de dicho horario.

Recomendación:

A la Dirección de Recursos Humanos

Contratar vigilantes de seguridad de lunes a domingo, las 24 horas para proteger las instalaciones del Municipio y los recursos públicos que posee.

13. Falta de supervisión en el manejo de los equipos informáticos.

Según las Normas de Control Interno de la CGE **410-04 Políticas y procedimientos** señala: Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.

Conclusión:

El Municipio no cuenta con una persona que se encargue de supervisar y monitorear el manejo adecuado de los equipos informáticos, el personal utiliza dichos equipos de acuerdo a los conocimientos y experiencia que posee.

Recomendación:

A la Dirección de Recursos Humanos

Contratar personal para supervisar el manejo de los equipos informáticos y las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño.

INDICADORES

NOMBRE DEL INDICADOR	FÓRMULA DE CÁLCULO	ANÁLISIS
EFICIENCIA		
Presupuesto informático	$\frac{\text{Presupuesto equipos informáticos}}{\text{Presupuesto total}} * 100 =$ $\frac{8.426,09 \text{ USD}}{1\ 679.755,18 \text{ USD}} = \mathbf{0,5\%}$	Del presupuesto asignado para el Municipio en el año 2013, el 0,5% corresponde a los equipos, sistemas y paquetes informáticos, un valor muy bajo con respecto a las necesidades reales que tiene la entidad tanto en activos informáticos como en dispositivos para

		la seguridad.
EFICACIA		
Sistema Operativo Actualizado	$\frac{\# \text{ Computadoras con Windows 8}}{\# \text{ Total Computadoras}} * 100 = \frac{0}{41} =$ <p>0%</p>	Ninguna computadora del Municipio cuenta con un sistema operativo actualizado, el personal sigue utilizando Windows 7, el mismo que funciona correctamente para la realización de las actividades cotidianas de la entidad.
Acceso a Internet	$\frac{\# \text{ Computadoras con Internet}}{\# \text{ Total Computadoras}} * 100 = \frac{41}{41} =$ <p>100%</p>	Según el indicador de eficacia se concluye que el 100% de las computadoras cuentan con acceso a internet, cumpliendo con las necesidades de los usuarios de los equipos informáticos.
Mantenimiento preventivo	$\frac{\# \text{ Computadoras con mantenimiento preventivo}}{\# \text{ Total Computadoras}} * 100 = \frac{0}{41} =$ <p>0%</p>	A ningún equipo de cómputo se realiza un mantenimiento preventivo, ya que el técnico que trabaja en el Municipio no tiene el suficiente tiempo para realizar esta actividad, es por esto que se realiza solo acciones correctivas cuando ya ha ocurrido el

		daño.
Actas de Entrega/Recepción	$\frac{\# \text{ Computadoras con actas de entrega/recepción}}{\# \text{ Total Computadoras}} * 100 = \frac{41}{41} = 100\%$	El 100% de las computadoras son entregadas con sus respectivas actas de entrega/recepción para constatar de forma documentada que el personal recibió el equipo.
SEGURIDAD		
Seguridad para ingresar al computador	$\frac{\# \text{ Computadoras con contraseña}}{\# \text{ Total Computadoras}} * 100 = \frac{40}{41} = 97,56\%$	Se ha determinado que de las 41 computadoras examinadas, 40 cuentan con una contraseña para ingresar al sistema operativo, las mismas representan un 97,56% de cumplimiento en seguridad.
Restricción de ingreso a Redes Sociales	$\frac{\# \text{ Computadoras con restricción}}{\# \text{ Total Computadoras}} * 100 = \frac{39}{41} = 95,12\%$	De las 41 computadoras examinadas 39 tienen restricción para acceder a redes sociales como Facebook, Twitter e incluso música, las mismas corresponden al 95,12% de seguridad.
Antivirus Actualizado	$\frac{\# \text{ Computadoras con antivirus actualizado}}{\# \text{ Total Computadoras}} * 100 = \frac{36}{41} = 87,80\%$	Las computadoras que tienen instalado un antivirus, el mismo que esta

		actualizado cada año con su respectiva licencia corresponde al 87,80% de un total de 41 computadoras examinadas, un nivel aceptable de seguridad.
--	--	---

Srta. Jenny Veloz
AUTORA DE TESIS

Ing. Cristóbal Erazo
DIRECTOR DE TESIS

CONCLUSIONES

- El Gobierno Autónomo Descentralizado Municipal del Cantón Penipe no ha sido objeto de una Auditoría Informática, evitando contar con una herramienta de control para determinar el grado de eficiencia, eficacia y seguridad en el manejo de la información y equipos informáticos.
- No se cumplen con las Normas de Control Interno de la CGE, puesto que los directivos no tienen interés ni presupuesto para implementar todos los numerales referentes a las Tecnologías de la Información.
- El Municipio no cuenta con una Unidad Informática que se encargue de regular, estandarizar, asegurar y generar la cobertura de servicios tecnológicos a todas las unidades de la entidad.
- El Municipio no cuenta con un Plan de Contingencias que ayude a proteger la integridad de los activos informáticos, mediante procedimientos que contrarresten el impacto de los riesgos.
- Las instalaciones del Municipio no cuenta con dispositivos de seguridad (extractores de calor, sensores de humo, sensores de temperatura, extintores, pararrayos, entre otros) para proteger los activos informáticos por falta de presupuesto.
- La Dirección de Talento Humano no ha establecido un Plan de Capacitación para el personal de la entidad con temas relacionados al manejo y seguridad de los activos informáticos.
- Al culminar el examen de auditoría se emitió un informe final que contiene las conclusiones y recomendaciones dirigidas a las autoridades correspondientes, que permitirá contribuirá la toma correcta de decisiones, y así mejorar el manejo de la información y equipos informáticos.

RECOMENDACIONES

- Al Auditor Interno realizar una Auditoría Informática por lo menos una vez al año con la finalidad de contar con una herramienta de control que permita mejorar el grado de eficiencia, eficacia y seguridad en el manejo de la información y equipos informáticos.
- A los Directivos y Personal cumplir y hacer cumplir con las Normas de Control Interno de la CGE con la finalidad de proteger los activos informáticos mediante el numeral 410-Tecnologías de la Información.
- A los Directivos del Municipio crear una Unidad Informática que conste en el organigrama institucional para que controle, supervise y asegure la integridad, confiabilidad y disponibilidad de los activos informáticos.
- Se recomienda a la Dirección de Recursos Humanos diseñar, implementar y socializar un Plan de Contingencias para dar respuesta a emergencias o fallas en los equipos computacionales, con la participación de los directivos y el personal de la entidad.
- A los Directivos buscar financiamiento para instalar dispositivos de seguridad dentro de las instalaciones con el propósito de proteger la integridad de la información y los equipos informáticos evitando daños o pérdidas innecesarias.
- A la Dirección de Recursos Humanos coordinar con el Alcalde para crear un Plan de Capacitación para el personal de la entidad con la finalidad de que aprendan a usar de manera eficaz, eficiente y segura los activos informáticos bajo su responsabilidad.
- A los Directivos del Municipio analizar las conclusiones y recomendaciones expuestas en el informe final de auditoría, con la finalidad de tomar las acciones correctivas para mejorar el manejo de la información y equipos informáticos, y así contribuir al cumplimiento de las metas y objetivos institucionales.

BIBLIOGRAFÍA

- Aguilera, P. (2010). Seguridad Informática. Madrid: Editex.
- Amador Sotomayor, A. (2008). Auditoría Administrativa: Proceso y Aplicación. México: Mc Graw-Hill Interamericana
- Areitio, J. (2008). Seguridad de la información: Redes, Informática y sistemas de información. Madrid: Paraninfo.
- Contraloría General del Estado. (2012). Ley Orgánica. Quito: C.G.E.
- Couto, L. (2011). Auditoría del sistema Appcc. Madrid: Días de Santos.
- De la Peña Gutierrez, A. (2011). Auditoría: Un enfoque práctico. Madrid: Paraninfo.
- Fernández Zapico, F. (2010). Manual para la formación del auditor en prevención de riesgos laborales: Aplicaciones y casos prácticos (3a ed.). Madrid: Lex Nova.
- Fonseca Luna, O. (2008). Vademecúm Contralor. Lima: Publicidad y Matiz.
- Fonseca Luna, O. (2011). Sistemad de Control Interno para Organizaciones: Guía práctica y orientaciones para evaluar el control interno. Lima: Publicidad & Matiz.
- Franklin Finkowsky, E. B. (2013). Auditoría Administrativa: Evaluación y Diagnóstico Empresarial (3a ed.). México: Pearson Educación.
- Gallo, F. (2010). Inseguridad Informática. Madrid: Igor Unnamed.
- García Hurtado, A. (2011). Seguridad Informática. Madrid: Ediciones Paraninfo.
- Global, F. E. (2007). El Auditor de Calidad. Madrid: Fundación Confemetal.
- Gómez López, R. (2011). Generalidades en la Auditoría. México: Eumed.
- Ibanez, P. (2009). Informática I. México: Cengage Learning.
- Maldonado, M. (2011). Auditoría de Gestión (4a ed.). Quito: Abya-Yala.
- Mantilla, A. (2009). Auditoría de Control Interno (2a ed.). Bogotá: Ecoe Ediciones.
- Muñoz, M. (2010). Gestión de la Rsc. Madrid: Netbiblo.

- Norma Internacional de Auditoría. (2013). Evidencia de auditoría. Madrid.
- Piattini Velthuis y del Peso, E. (2008). Auditoría Informática: Un enfoque práctico (2a ed.). México: Alfaomega.
- Piattini, M. (2008). Auditoría de Tecnologías y Sistemas de Información. México: Alfaomega.

ANEXOS

Anexo 1. Solicitud dirigida al Alcalde para recabar información

Riobamba, 10 de febrero del 2015

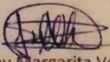
Ingeniero
Robin Velastegui Salas
ALCALDE MUNICIPAL DEL CANTÓN PENIPE
Presente

#3
VUS

Expreso a usted un cordial y atento saludo como estudiante de la Escuela de Contabilidad y Auditoría de la ESPOCH, al mismo tiempo, me permito solicitarle el ingreso a la institución, con la finalidad de recabar información mediante entrevistas y encuestas a los empleados para culminar el trabajo de tesis cuyo tema es "AUDITORÍA INFORMÁTICA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE, PROVINCIA DE CHIMBORAZO".

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

ATENTAMENTE


Jenny Margarita Veloz
ESTUDIANTE EICA
C.I. 060460218-5

GAD. MUNICIPAL DE PENIPE
SECRETARIA GENERAL
Fecha 2015-02-10
Hora 11:11
N° de Trámite
Recibido por [Handwritten Signature]

Anexo 2. Certificado de Partida Presupuestaria para Equipos Informáticos



GAD. MUNICIPAL DEL CANTÓN PENIPE
DIRECCIÓN FINANCIERA
CHIMBORAZO- ECUADOR
FONO: 032-907 186 ExL106 FAX: 032-907 187

C. No. 293-DFMP.

Penipe, 30 de octubre de 2013.

El suscrito Ing. Carlos Sandoval, en calidad de DIRECTOR FINANCIERO DEL GAD. MUNICIPAL DEL CANTÓN PENIPE, y para los fines consiguientes:

CERTIFICO

De acuerdo al memorando al MEMO-PROMUC.0262-2013 de fecha 30 de octubre del presente año, suscrito por la Ing. Noemi Garcia, en calidad de **PROVEEDORA MUNICIPAL**, solicita partida presupuestaria para la adquisición de Equipo de Cómputo, impresoras e infocus para las oficinas de Recaudación, Movilización Jurídico, infocentro, Alcaldía, sobre la base del Art. 341 literal (a) de la COOTAD y Art. 24 de la LOSCP.- Certifico que existe la siguiente Partida Presupuestaria en el presupuesto del presente año incluye IVA

PARTIDA No.	DENOMINACION	VALOR DÓLARES
12.8.4.01.07	EQUIPO,SISTEMAS Y PAQUETES INFORMATICO	3248.25
25.8.4.01.07	EQUIPO,SISTEMAS Y PAQUETES INFORMATICO	1244.79
11.8.4.01.07	EQUIPO,SISTEMAS Y PAQUETES INFORMATICO	2601.45
21.8.4.01.07	EQUIPO,SISTEMAS Y PAQUETES INFORMATICO	1433.60
TOTAL		8425.09

Nota. Válida hasta el 31 de diciembre de 2013

Es todo cuanto puedo certificar en honor a la verdad.

Atentamente,

Ing. Carlos Sandoval.
DIRECTOR FINANCIERO MUNICIPAL
C.c. Archivo.

G.A.D. MUNICIPAL DEL CANTÓN PENIPE	
PROVEEDURIA	
Recibido Fecha: 01/11/2013	
Nº Pág: 1	Hoja: 11/25
Firma:	



Anexo 3. Informe Técnico de Petición de Token (Firma Electrónica) al BCE



GAD MUNICIPAL DEL CANTON PENIPE

JEFATURA DE INFORMATICA

Informe Técnico

De acuerdo al Oficio Circular de la DINARDAP-DN-2013-000428-OFC en el que indican que: "toda comunicación enviada y recibida por esta Dirección Nacional o por las Direcciones Regionales, se efectuará solamente a través de correo electrónico, para lo cual es indispensable que se sirva obtener un certificado de firma electrónica (Token) en una de las entidades de certificación de información autorizadas para este efecto que son Banco Central, Security Data y ANF Ecuador".

Siendo el BANCO CENTRAL DEL ECUADOR una entidad certificadora y en su calidad de Institución Pública que brinda estos servicios de Certificación de Firma Electrónica y la oficina de Registro de la Propiedad necesitando este instrumento para el desarrollo de sus actividades cargó los formularios requisito para la obtención de la firma digital tipo token; en la página del Banco Central habilitada para esta finalidad.

En cuanto al Certificado de Firma Electrónica de Persona Jurídica que entregó el Banco Central sirve para varios propósitos, permite identificar a una persona jurídica de derecho privado, a través de su representante legal o de las personas que están perteneciendo a la empresa, quienes serán responsables en tal calidad de todo lo que firmen dentro del ámbito de su actividad y límites de uso que correspondan.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en la DPC, en la PC del Certificado de firma electrónica de persona Jurídica y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

El soporte para el almacenamiento de las claves y el certificado será un dispositivo criptográfico TOKEN. El acceso al dispositivo criptográfico, donde se encuentra la clave privada, se realizará a través de contraseña (PIN). Para realizar una firma electrónica es necesario introducir el PIN que únicamente conoce el suscriptor. En la generación de las claves no se permite realizar una copia de seguridad de las mismas.

Es todo cuanto puedo indicar acerca del token que se requirió al Banco Central del Ecuador.

Atentamente


Ing. Gabriela Vinuesa
JEFE DE INFORMATICA

Anexo 4. Acta de Entrega de Recepción de Bienes para Activos Informáticos.

**GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN PENIPE**

**DIRECCION ADMINISTRATIVA
BODEGA Y CONTROL ACTIVOS**

ACTA DE ENTREGA RECEPCION DE BIENES N° 2015-0001

MOTIVO	ENTREGA INTERNA	CAMBIO ADMINISTRATIVO	DEVOLUCION	COMODATO / PRESTAMO USO	TRANSFERENCIA GRATUITA
	X				

En la ciudad de Penipe, a los diez días del mes de octubre del dos mil catorce, comparecen a la suscripción del presente documento, entre la señora Ing. Gabriela Soledad Vinuesa Oñate, en su calidad de Guardalmacén; y, por otra el señor Abg. Alex Fabricio Lluquin Valdiviezo, Jefe de la Unidad de Tránsito, Transporte Terrestre y Seguridad Vial; con la finalidad de dejar constancia de la entrega recepción de equipos de cómputo y mobiliario, al tenor de las siguientes cláusulas.

PRIMERA.- ANTECEDENTES.- Mediante Memorando 2014-0562-DAJ, el señor Abg. Alex Fabricio Lluquin Valdiviezo Jefe de la Jefe de la Unidad de Tránsito, Transporte Terrestre y Seguridad Vial, solicita que le provean de equipos informáticos y mobiliario, en vista que las competencias de Tránsito, Transporte Terrestre y Seguridad Vial fueron asumidas desde el primero de enero del año en curso.

SEGUNDA: En base a este antecedente y atendiendo a la sumilla inserta en Memorando 2014-0562-DAJ, se procede a entregar los siguientes bienes:

CANTIDAD	DESCRIPCION DEL BIEN	N° DE SERIE
3	Computador de escritorio core i5 2400 3,10 GHz / RAM 2GB / Disco Duro 500GB; Marca HP; Modelo 6200 PRO incluye teclado y mouse	MXL215191F
	Teclado HP	BAUDU00VBZ09LQ
	Mouse HP	FCGLH0D9W2DW9P
1	Monitor 18,5", Marca HP; Modelo LV1911	6CM2070MVL
1	Escritorios para computador, bandeja de teclado fijo, estructura metálica	S/N
1	Silla fija de tubo color negro	S/N

TERCERA: ENTREGA RECEPCION: Por su parte el señor Abg. Alex Fabricio Lluquin Valdiviezo, Jefe de la Jefe de la Unidad de Tránsito, Transporte Terrestre y Seguridad Vial, recibe a completa y entera satisfacción lo antes descrito, en buen estado de funcionamiento, además se compromete a dar cumplimiento al Artículo 3 del Reglamento General de Bienes de Sector Público en cuya parte pertinente dice: "El daño, pérdida o destrucción del bien, por negligencia comprobada o su mal uso, no imputable al deterioro normal de las cosas, será responsabilidad del servidor que lo tiene a su cargo, ...", asumirá la total reposición o reparación hasta que se compruebe lo contrario, de existir algún tipo de novedad será de su obligación informar inmediatamente al señor Director Administrativo.



**GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN PENIPE**

**DIRECCION ADMINISTRATIVA
BODEGA Y CONTROL ACTIVOS**

Para constancia y fe de lo anotado los actuantes firman en original y tres copias de igual tenor y efecto.

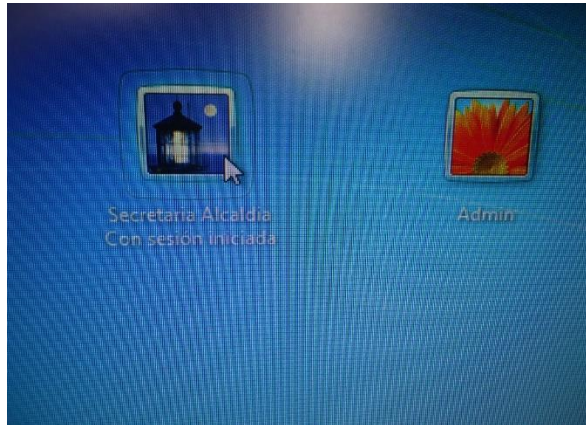
RECIBI CONFORME

ENTREGUE CONFORME

Abg. Alex Fabricio Lluquin Valdiviezo
JEFE DE LA UNIDAD DE TRÁNSITO, TRANSPORTE Y
SEGURIDAD VIAL

Ing. Gabriela Soledad Vinuesa Oñate
GUARDAALMACEN

Anexo 5. Ingreso al Sistema Operativo sin contraseña



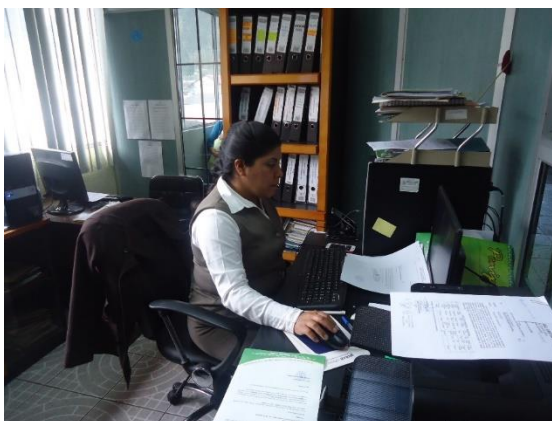
Anexo 6. Ingreso al Sistema Operativo con contraseña



Anexo 7. Registro de Entrada de usuarios externos al Municipio

INGRESO DE PERSONAS AL GAD MUNICIPAL					Nº	DIRECCION ADMINISTRATIVA	
FECHA	HORA	#CEDULA	NOMBRE DE QUIEN INGRESA	DEPARTAMENTO AL QUE INGRESA	FIRMA	OBSERVACIONES	
10/08/2011	08:11	06012886-3	Maria Asunción Torres	Secretaria	[Firma]	08:11	
10/08/2011	08:11	06012886-3	Carlos Guzmán	Secretaria	[Firma]	08:11	
10/08/2011	08:38	06012886-3	Laura Guzmán	Secretaria	[Firma]	08:20	
10/08/2011	08:38	06012886-3	Luisa Edson	R.S. M.H.	[Firma]	08:30	
10/08/2011	08:38	06012886-3	Guatemala	Transparencia	[Firma]	08:57	
10/08/2011	08:55	06012886-3	Guatemala	Catálogos	[Firma]	10:00	
10/10/2011	08:46	06012886-3	Tanya	Transparencia	[Firma]	10:34	
10/21/2011	08:21	06012886-3	Santiago Magdalena	Transparencia	[Firma]	10:44	
10/21/2011	08:21	06012886-3	Guatemala	O.P.P.	[Firma]	10:44	
10/21/2011	08:21	06012886-3	Guatemala	Transparencia	[Firma]		
GUARDIA ENCARGADO PUERTA			COMISARIO MUNICIPAL	JEFE DE POLICIA	JEFE DE SEGURIDAD MUN		

Anexo 8. Secretaria General del Municipio



Anexo 9. Oficina del Técnico de Informática



Anexo 10. Departamento de Higiene Ambiental y Salud Pública



Anexo 11. Concejala del Municipio

