



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORIA

INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

TRABAJO DE TITULACIÓN

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA.

TEMA:

**AUDITORÍA INFORMÁTICA A LA UNIDAD DE TECNOLOGÍA
INFORMACIÓN Y COMUNICACIÓN DEL GOBIERNO AUTÓNOMO
DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE,
PERÍODO 2014.**

AUTOR:

LUIS ERNESTO CHIMBO CAIZAGUANO

RIOBAMBA – ECUADOR
2016

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de titulación ha sido desarrollado por el Sr. LUIS ERNESTO CHIMBO CAIZAGUANO, ha cumplido con las normas de investigación científica y una vez revisado en su totalidad, se autoriza su presentación.

Para constancia firman.

Ing. Oscar Omar Espíndola Lara
DIRECTOR

Ing. Wilson Antonio Velasteguí Ojeda
MIEMBRO DE TRIBUNAL

DECLARACIÓN DE AUTENTICIDAD

Yo, **LUIS ERNESTO CHIMBO CAIZAGUANO**, declaro que el presente trabajo de titulación es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente, están debidamente citados y referenciados.

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

Riobamba, 24 de febrero del 2016

Luis Ernesto Chimbo Caizaguano
0604125310
AUTOR

DEDICATORIA

A la Escuela Superior Politécnica de Chimborazo, a mí querida Escuela de Ingeniería en Contabilidad y Auditoría por haber honrado con ser su alumno, deportista y dirigente.

A mis catedráticos que me preparó, para ver culminado mi sueño, de ser profesional.

A mi hermosa familia Chimbo Caizaguano por su invaluable apoyo durante mi formación.

A mi hijito Ariel, por ser mi felicidad y razón de mi existencia.

Luis Ernesto Chimbo Caizaguano

AGRADECIMIENTO

Al Padre celestial que ha estado conmigo en cada paso que doy, cuidándome y dándome fortaleza para continuar.

A mis padres Doroteo y Rosa, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento.

A mis hermanos, Ángel, Carlos, Alicia y Mario por ser el pilar fundamental, Sin ellos jamás hubiese podido conseguir nada. Su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir.

A mis amores, Marisol, Ariel y Ernesto, su amor y confianza ha sido primordial en mi vida.

A ellos quienes depositaron su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en Mí. Es por ello que soy lo que soy ahora. Los amo con mi vida.

Luis Ernesto Chimbo Caizaguano

ÍNDICE GENERAL

Portada	i
Certificación del Tribuna	ii
Declaración de Autenticidad.....	iii
Dedicatoria.....	iv
Agradecimiento.....	v
Índice General.....	vi
Índice de Cuadros	ix
Índice de Gráficos.....	ix
Índice de Figuras.....	ix
Índice de Anexos	ix
Resumen.....	x
Abstract.....	xi
Introducción	1
CAPÍTULO I: PROBLEMA	2
1.1 PLANTEAMIENTO DEL PROBLEMA	2
1.1.1. Formulación del Problema	3
1.1.2. Delimitación del Problema.....	3
1.1.3. Justificación	3
1.3. OBJETIVOS	4
1.3.1 Objetivo General	4
1.3.2 Objetivos Específicos.....	4
CAPÍTULO II: MARCO TEÓRICO.....	5
2.1. GENERALIDADES DE AUDITORÍA INFORMÁTICA	5
2.1.1. Antecedentes	5
2.1.2. Definición.....	6
2.1.3. Alcance.....	7
2.1.4. Importancia de la Auditoría Informática.....	7
2.1.5. Objetivos de la Auditoría Informática	7
2.2. PROCESO DE UNA AUDITORÍA INFORMÁTICA.....	8
2.2.1. Planificación de la Auditoría Informática	9
2.2.2. Ejecución de la Auditoría Informáticap.....	9

2.2.3.	Dictamen de la Auditoría Informática	10
2.2.4	Papeles de Trabajo	10
2.2.5	Marcas de Auditoría.....	11
2.3.	CONTROL INTERNO	11
2.3.1	Componentes del Control Interno:.....	12
2.	CONTROLES DE APLICACIÓN	15
2.5.	TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)	16
2.6.	ANÁLISIS FODA.....	17
2.7.	HALLAZGOS DE AUDITORÍA	18
2.8.	NORMAS DE CONTROL INTERNO PARA LA AUDITORÍA INFORMÁTICA	19
2.9.	IDEA A DEFENDER	30
2.9.1	Idea General	30
	CAPÍTULO III: MARCO METODOLÓGICO	31
3.1.	MODALIDAD DE INVESTIGACIÓN.....	31
3.2.	TIPOS DE INVESTIGACIÓN	31
3.3.	POBLACIÓN Y MUESTRA.....	31
3.4.	MÉTODOS, TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN	31
3.5.	RESULTADOS.....	32
	CAPÍTULO IV: MARCO PROPOSITIVO.....	33
4.1	AUDITORÍA INFORMÁTICA A LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN GAD MUNICIPAL GUAMOTE PERÍODO 2014.	33
4.1.1	Orden de trabajo.....	34
4.1.2.	Índice del Archivo Permanente.....	36
4.1.3.	Información General	37
4.2	ARCHIVO CORRIENTE	49
4.2.1.	ÍNDICE DEL ARCHIVO CORRIENTE.....	49
	Fase I	50
	Fase II	55
	Fase III.....	99
4.3.1	Informe Final de Auditores Independientes.....	100
	CONCLUSIONES	112

RECOMENDACIONES.....	113
BIBLIOGRAFÍA	114
ANEXOS	115

ÍNDICE DE CUADROS

1	Etapas de Auditoría.....	9
2	Propuesta de símbolos convencionales utilizados en una auditoría Informática.....	12
3	Índice de archivo permanente	36
4	Nómina del personal.....	43
5	Estándares mínimos para la configuración del sistema operativo.....	38
6	Diagnóstico Situacional de la UTIC.....	44
7	Hoja de referencias	40
8	Marcas de Auditoría.....	47
9	Índice del archivo corriente	42
10	Evaluación de la confianza y riesgo.....	84
11	Matriz de Debilidades Identificadas en los Cuestionarios de Control Interno.....	86
12	Conoce usted un plan de contingencia con el que cuente la institución.....	45

ÍNDICE DE GRÁFICOS

1	Tabulación de la matriz de confianza y riesgo.....	85
---	--	----

ÍNDICE DE FIGURAS

1	GAD Municipal del Cantón Guamote.....	39
2	Ubicación GAD Municipal de Cantón Guamote.....	40
3	Estructura Administrativa Organización.....	56

ÍNDICE DE ANEXOS

1	Encuesta al Alcalde de GAD Municipal del Cantón Guamote.....	117
2	Encuesta al Jefe de Unidad de TIC del GAD Municipal del Cantón Guamote.....	118
3	Entrevista a los usuarios de las Tecnologías de Información y Comunicación.....	119
4	Organigrama estructural del GAD Municipal del Cantón Guamote.....	120
5	Reseña fotográfica.....	121

RESUMEN

El presente proyecto tiene por objetivo la realización de una Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote. Para mejorar la calidad y seguridad de la información, verificando el cumplimiento de las disposiciones legales, reglamentarias y normativas aplicables para la ejecución de las actividades desarrolladas inherentes al Sistema de Información y Comunicación.

Para el desarrollo de la investigación se utilizó técnicas de recolección como: las entrevistas, observación directa y encuestas realizada a todo el personal que posee un equipo informático, se pudo obtener un panorama real de la situación del UTIC, así como los problemas que existe en la misma.

Este trabajo se desarrolló aplicando fases de auditoría informática y el método COSO con el objetivo de establecer el nivel de cumplimiento de las Normas de Control Interno emitidas por la Contraloría General del Estado

La realización de la Auditoría Informática servirá de gran ayuda al GAD Municipal del Cantón Guamote, ya que por medio de las recomendaciones implantadas en el informe final podrá dar solución a las falencias encontradas, con la finalidad de mejorar la utilización de recursos tecnológicos de manera eficiente y eficaz.

Palabras claves: Auditoría Informática, Seguridad Física, Seguridad Lógica y TIC'S

Ing. Oscar Omar Espíndola Lara
DIRECTOR DE TRABAJO DE TITULACIÓN

ABSTRACT

The objective of this project was to carry out a Computer Auditing at the information and Communication Technologies Unit (ICTU) of the Decentralized Autonomous Government (DAG) from Guamote Canton. To improve both quality and security of the information, verifying the compliance of legal regulation, regulatory requirements, and applicable regulations in order to implement the activities inherent to the Information and Communication System.

For this research techniques for collecting data were used such as: interviews, direct observation and surveys applied to all the personnel who have a computer equipment, obtaining both a clear situation in the (ICTU) and the problems which have existed in the Unit.

This research has been developed applying Computer Auditing phases and the COSO method in order to establish the compliance level of the Internal Control Standards by The Comptroller General of the State.

The Computer Auditing realization will be useful for the (DAG) Municipality of the Guamote Canto. With recommendations proposed in the final report could offer solutions to the deficiencies encountered, in order to improve the use of the technological resources efficiently and effectively.

Keywords: Computer Auditing, Physical Security, Logical Security and ICT

INTRODUCCIÓN

Se pone en consideración el presente trabajo de investigación que tiene el propósito de realizar una Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, con la finalidad de mejorar la calidad y seguridad de la información para de esa manera conseguir los objetivos que la Institución se ha planteado, partiendo del análisis situacional que permitan proveer información oportuna y verás para la correcta toma de decisiones.

Esta propuesta consta de cinco capítulos a mencionar: El problema de investigación, marco teórico, marco metodológico, marco propositivo y conclusiones recomendaciones.

El Capítulo I, contiene el tema del proyecto investigativo, la formulación del problema, delimitación de la misma, la justificación y objetivos de la investigación.

Capítulo II, Consta de Marco Contextual en los que se presentan definiciones y conceptos de: Control Interno, Auditoría, Auditoría Informática, con sus respectivos objetivos, importancias y clasificaciones, lo cual es la base de nuestro trabajo de investigación.

Capítulo III, Consta del diseño metodológico y el tipo de investigación a realizarse, el cómo y con qué instrumentos se llevará a cabo la investigación.

Capítulo IV, Se explica cada una de las fases de Auditoría Informática, el cual contiene estudio: archivo permanente, archivo corriente, programas, cuestionarios, evaluación del control interno y análisis de áreas críticas.

Capítulo V, Una vez realizado el proyecto investigativo y analizado cada uno de los capítulos y fases de auditoría se procederá a determinar conclusiones y recomendaciones respectivas para la unidad auditada.

CAPÍTULO I: PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

El Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, en concordancia con lo decretado en la Constitución Política de la República del Ecuador de 2008, gozará de autonomía política, administrativa y financiera, y se regirán por los principios de solidaridad, subsidiariedad, equidad interterritorial, integración y participación ciudadana. Son las competencias de los Gobiernos Municipales, siendo estas la de planificar el desarrollo urbano cantonal, regulando la ocupación del suelo urbano y rural, ejercer el control de los mismos, formar y administrar los catastros inmobiliarios tanto urbano como rurales.

Para la realización de una gestión eficaz y eficiente es de suma importancia contar con una Unidad de Tecnología de la Información y Comunicación, ajustada a la necesidad, de tal forma que asegure el buen uso de los equipos informáticos, apoyando la continua aplicación de nuevas tecnologías de hardware y software. Disminuye gastos, agilite y reduzca trámites, etc. Y así alcanzar a ser un cantón de derechos, confiable, ordenado, seguro, participativo y corresponsable, un polo de desarrollo económico productivo. Actualmente en GAD Municipal del Cantón Guamote, existen varios departamentos o unidades, que utilizan sistemas informáticos, para llevar a cabo las funciones asignadas a ellos; ya sea por el Concejo Municipal o por una ley específica, que rige su funcionamiento; entre estos tenemos: Quipux, SIGAD, e-SIGEF y Ushay.

La Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, no ha efectuado una auditoría informática por lo cual ha originada los siguientes inconvenientes:

- No cuenta con un plan estratégico de tecnologías de información y comunicaciones.
- No cuenta con plan de contingencia en caso de emergencia.
- No tiene un mecanismo adecuado que proteja y salvaguarde contra las pérdidas y medios físicos.
- No dispone de un plan de capacitación para el personal y usuarios de la Unidad de Tecnología Información y Comunicación (UTIC)

- No dispone de un plan adecuado de mantenimiento de la Infraestructura o plataforma Tecnológico.

1.1.1. Formulación del Problema

¿Cómo la Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, período 2014, ayuda mejorar la calidad y seguridad de la información y dar solución a los inconvenientes encontrados?

1.1.1.1. Delimitación del Problema

Campo: Auditoría Informática

Área: Unidad de Tecnología Información y Comunicación

Tiempo: Periodo 2014

Espacio: Gobierno Autónomo Descentralizado Municipal del Cantón Guamote

1.1.2. JUSTIFICACIÓN

La evolución de los sistemas de información y comunicación en nuestro país, ha generado la necesidad de implementar la Unidad de TIC en las diferentes instituciones; para obtener seguridad, confiabilidad en todos los ámbitos que a estos corresponden.

Por medio de las fases de Auditoría de Informática lograremos familiarizarnos con la organización y revisión de la normativa de la Contraloría General del Estado, evaluar el control interno aplicando cuestionarios basado en la norma 410 de control interno referente a la Tecnología de Información, determinar áreas críticas para establecer la situación actual de la unidad de TIC y por último preparar un informe de auditoría brindando soluciones para mejorar la eficiencia y la eficacia de los recursos informáticos.

La Auditoría Informática no solo ayuda a los funcionarios y empleados de la UTIC sino a todo el personal del GADMCG que utiliza la infraestructura tecnológica como principal herramienta de trabajo, por lo cual es de vital importancia su correcta utilización para que impacte positivamente en los recursos de la organización.

El presente trabajo de investigación es factible su elaboración ya que existe disponibilidad de información necesaria debidamente documentada otorgada por los funcionarios de la UTIC del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote.

Finalmente es importante señalar que esta investigación permitirá poner en evidencia los conocimientos adquiridos durante la etapa de aprendizaje, cumpliendo así con un requisito indispensable y necesario previo a la obtención del título de Ingeniero en Contabilidad y Auditoría CPA.

1.3. OBJETIVOS

1.3.1 Objetivo General

Desarrollar una Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, período 2014. Para mejorar la calidad y seguridad de la información y dar solución a los inconvenientes encontrados.

1.3.2 Objetivos Específicos

- Verificar el cumplimiento de las disposiciones legales, reglamentarias y normativas aplicables para la ejecución de las actividades desarrolladas inherentes al Sistema de Información y Comunicación.
- Aplicar fases de auditoría informática para diagnosticar las áreas críticas y determinar la situacional real de la Unidad de TIC.
- Emitir un informe con sus respectivas conclusiones y recomendaciones proporcionando las debidas soluciones para mejorar la eficiencia y eficacia de los recursos informáticos.

CAPÍTULO II: MARCO TEÓRICO

2.1. GENERALIDADES DE AUDITORÍA INFORMÁTICA

2.1.1. Antecedentes

Al igual que en resto de auditorías, en la auditoría de sistemas computacionales también existen antecedentes, citaremos a los principales autores sobre este tema:

En 1988, Echenique publicó su libro Auditoría de sistemas, en el cual establece las principales bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico-práctico sobre el tema.

En 1992, Lee presentó un libro en el cual enuncia los principales aspectos a evaluar en una auditoría de sistemas, mediante una especie de guía que le indica al auditor los aspectos que debe evaluar en este campo.

En 1993, Rosalva Escobedo Valenzuela presenta una tesis de auditoría a los centros de cómputo, como apoyo a la gerencia.

En 1994, G. Haffes, F. Holguín y A. Galán, en su libro sobre auditoría de los estados financieros, presentan una parte relacionada con la auditoría de sistemas, que profundiza en los aspectos básicos de control de sistemas y se complementa con una serie de preguntas que permiten evaluar aspectos relacionados con este campo.

En 1995, Ma. Guadalupe Buendía Aguilar y Edith Antonieta Campos de la O. presentan un tratado de auditoría informática (apoyándose en lo señalado por el maestro Echenique), en el cual presentan metodologías y cuestionarios útiles para realizar esta especialidad.

En 1995, Yann Darrien presenta un enfoque particular sobre la auditoría de sistemas.

En 1996, Alvin A. Arens y James K. Loebbecke, en su libro Auditoría. Un enfoque integral, de Prentice Hall Hispanoamericana, S. A., nos presentan una parte de esta obra como Auditoría de Sistemas.

En 1996, Hernández propone la auditoría en informática, en la cual da ciertos aspectos relacionados con esta disciplina.

En 1997, Francisco Ávila obtiene mención honorífica en su examen profesional, en la UVM, Campus San Rafael, con una tesis en la cual propone un caso práctico de auditoría de sistemas realizado en una empresa paraestatal.

En 1998, Yann Darrien presenta técnicas de auditoría, donde hace una propuesta de diversas herramientas de esta disciplina.

En 1998, Mario G. Piattini y Emilio del Peso presentan Auditoría informática, un enfoque práctico, donde mencionan diversos enfoques y aplicaciones de esta disciplina. Según (Muñoz Raso, 2002, págs. 9-10)

2.1.2. Definición

Según Mario Piattini Velthuis, la auditoría informática es “el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos

Según José A. Echenique, la auditoría en informática “es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Según Echenique, la auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización específica que hará posible el uso de los equipos de cómputo” Desde el punto de vista administrativo, cuando se habla de auditoría sistemas se refiere a los Sistemas de Información utilizados en las empresas públicas o privadas, mas no al computador como tal, que en sí es una herramienta de los sistemas de información. Se debe tener presente que la administración es un sistema abierto y por tanto cambiante en sus conceptos, técnicas y que está influenciada por lo que acontece en su alrededor. La auditoría de los sistemas de información se define como cualquier auditoría que abarca

la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes; también se puede decir que es el examen y evaluación de los procesos del área de Procesamiento Electrónico de Datos (PED) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas. (Echenique)

2.1.3. Alcance

El alcance ha de definir con exactitud el entorno y los límites en que va a desarrollarse la auditoría informática, se completa con los objetivos de ésta. El alcance ha de plasmar explícitamente en el Informe Final, de manera que esté perfectamente determinado no únicamente hasta que puntos se ha alcanzado, sino cuales elementos fronterizas han sido incorrectos.

2.1.4. Importancia de la Auditoría Informática

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos.

2.1.5. Objetivos de la Auditoría Informática

Según Carlos Muñoz, La evaluación a los sistemas computacionales, a la administración del centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos:

Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.

- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo.
- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.
- Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio de la computadora. (Muñoz, 2002)

2.2. Proceso de una Auditoría Informática

A continuación se mencionan las fases o pasos que pueden ser aplicables para auditoría Informática.

Cuadro No 1: Etapas de Auditoría

FASE	ACTUACIONES RELEVANTES DEL AUDITOR
1. Planeación de la auditoría	<ul style="list-style-type: none"> ➤ Recopilación de información general de la entidad tales como: <ul style="list-style-type: none"> - Como se encuentran distribuidos los sistemas en el área. - Como y de qué tipo son los equipos que están instalados en el centro de sistemas. ➤ Establecer los objetivos de la auditoría. ➤ Determinar los puntos que serán evaluados en la auditoría. ➤ Elaborar planes, programas y presupuestos para realizar la auditoría.

	<ul style="list-style-type: none"> ➤ Identificar y seleccionar los métodos, procedimientos y herramientas necesarias para la auditoría. ➤ Realizar una evaluación preliminar del sistema de control interno, área informática.
2. Ejecución de la auditoría informática	<ul style="list-style-type: none"> ➤ Aplicar los instrumentos y herramientas para la auditoría. ➤ Asignar los recursos y actividades conforme a los planes y programas. ➤ Recopilar la documentación y evidencia de la auditoría. ➤ Identificar y elaborar documentos de desviaciones. ➤ Integrar los documentos y papeles de trabajo. ➤ Elaborar el borrador de desviaciones.
3. Informe de auditoría	<ul style="list-style-type: none"> ➤ Comentar las situaciones encontradas con los auditados encontrar, conjuntamente con los auditados, las causas de las desviaciones y posibles soluciones. ➤ Analizar, depurar y corregir las desviaciones encontradas jerarquizar las desviaciones encontradas y concentrar las más importantes. ➤ Comentar las situaciones relevantes con los directivos del área de sistemas y confirmar las causas y soluciones. ➤ Concentrar, depurar y elaborar el informe final de auditoría. ➤ Presentar el informe.

Fuente: (Muñoz, C. (2002) p. 185)

Elaborado: Luis Ernesto Chimbo Caizaguano

2.2.1. Planificación de la Auditoría Informática

Consta de la definición y formalización de proyectos. Abarca las actividades desarrolladas por el auditor en informática que tiene como objetivo principal elaborar y presentar un conjunto de proyectos inherentes a la función de auditoría informática a la alta dirección, los estarán orientados primordialmente al acercamiento de la calidad y control de diferentes elementos que se encuentran relacionados con los recursos de informática.

Es importante aclarar que este proceso de planeación depende en gran medida del diagnóstico previo que lleve a cabo el auditor en informática sobre la situación que prevalece en cada una de las áreas o servicios de la función de informática. También se deben considerar las necesidades o prioridades que tenga la alta dirección de auditar o evaluar un área específica de informática. (Hernandez, 2012)

2.2.2. Ejecución de la Auditoría Informática

- Realizar las acciones programadas para la auditoría.
- Aplicar los instrumentos y herramientas para la auditoría.

- Identificar y elaborar los hallazgos de auditoría.
- Elaborar el dictamen de auditoría y presentarlo a discusión

2.2.3. Dictamen de la Auditoría Informática

- Recolección de la información y elaboración de un informe de situaciones detectadas
- Elaboración de dictamen final
- Presentación del informe

2.2.4 Papeles de Trabajo

Los papeles de trabajo son el conjunto de cedulas y documentos elaborados y obtenidos por el auditor en el transcurso del examen hasta el momento de emitir su informe y sirve para:

- Evidenciar en forma suficiente y competente el trabajo realizado; y
- Respalda el dictamen, y las conclusiones y recomendaciones del informe.
- La cantidad y el tipo de papeles de trabajo a ser elaborados dependerán, entre otros de diversos factores:
- La condición y características de la empresa a ser auditada;
- El nivel de confianza en los controles internos;
- La naturaleza del informe de auditoría.

Los papeles de trabajo se mantendrán en el archivo: permanente y corriente.

Archivo Permanente: Es la base para la aplicación y programación de la auditoría, permite optimizar el tiempo de los auditores, es necesario que el auditor cuente con un archivo permanente estructurado, de tal manera que facilite la utilización de la amplia información acumulada.

Archivo Corriente: Es el que mantiene todos los papeles de trabajo que corresponden a la ejecución del trabajo, es decir los papeles de trabajo que sustentarán el dictamen y los comentarios conclusiones y recomendaciones emitidas en el informe.

Se mantendrá un archivo corriente por cada auditoría realizada y al igual que los anteriores archivos debe mantener sus papeles de trabajo debidamente identificados con índices, referencias y marcas. (Hermoso, 2013)

2.2.5 Marcas de Auditoria

Son las marcas de carácter informal que utiliza exclusivamente el auditor o el grupo de auditores que realizan la auditoría, con el fin de facilitar la uniformidad de los papeles de trabajo y para identificarlos mejor.

Cuadro No 2: Propuesta de símbolos convencionales utilizados en una auditoría Informática

MARCA	SIGNIFICADO/INTERPRETACIÓN
✓	Verificado una vez
✗	Verificado dos veces
✓✓	Dato Correcto
X	Dato con error
N/A	No aplica
≠	Diferencias Detectadas
A	Archivo verificado
OBS	Observación
ENT	Entrevista
EF	Entrevista Funcionario
EP	Entrevista al Personal
CUES	Cuestionario

Fuente: (Muñoz, C. (2002) p. 264)

Elaborado por: Luis Ernesto Chimbo Caizaguano

2.3. Control Interno

Según (Mantilla, 2009) Para COSO el control interno es un sistema / proceso, ubicado en el más alto nivel organizacional, con direccionamiento estratégico y una clara presión desde arriba hacia abajo, que combina objetivos, componentes y niveles. Es una herramienta extremadamente útil para el diseño, la implementación, el mejoramiento, la evaluación del control interno, así como para la presentación de reportes sobre control interno. No hace referencia ni a la auditoria ni a la supervisión del control interno. (pág.97)

Para (Mantilla, 2009) Es un lineamiento que establece la administración con ayuda del personal de la entidad, para tener una razonabilidad, en relación con el logro de los objetivos en tres categorías: efectividad y eficiencia de las operaciones; confiabilidad del proceso de presentación de reportes financieros y; cumplimiento con leyes y regulaciones

aplicables. COSO señalo adicionalmente que el control interno consta de; el ambiente de control, valoración de riesgos, actividades de control información y comunicación, y monitoreo. (pág. 98) (Mantilla, 2009)

2.3.1 Componentes del Control Interno:

Ambiente de Control

Cosiste en el establecimiento de un entorno que se estimule e inflencie la actividad del personal con respecto al control de sus actividades.

Es la base de los demás componentes de control a proveer disciplina y estructura para el control e incidir en la manera como:

- Se estructuran las actividades del negocio.
- Se asigna autoridad y responsabilidad.
- Se organiza y desarrolla la gente.
- Se comparten y comunican los valores.
- El personal toma conciencia de la importancia del control.

Factores del Ambiente de Control:

- La integridad y los valores éticos.
- El compromiso a ser competente.
- Las actividades de la junta directiva y el comité de auditoría.
- La mentalidad y estilo de operación de la gerencia.
- La estructura de la organización.
- La asignación de autoridad y responsabilidades.
- Las políticas y prácticas de recursos humanos.

El ambiente de control tiene gran influencia en la forma como se desarrollan las operaciones, se establecen los objetivos y se minimizan los riesgos. Tiene que ver igualmente en el comportamiento de los sistemas de información y con la supervisión en general. A su vez es influenciado.

b) Evaluación de Riesgos

Es la identificación y análisis de riesgos relevantes para el logro de los objetivos y la base para determinar la forma en que tales riesgos deben ser mejorados. Así mismo, se refiere a los mecanismos necesarios para identificar y manejar riesgos específicos asociados con los cambios, tanto los que influyen en el entorno de la organización como en su interior.

En toda entidad, es indispensable el establecimiento de objetivos tanto globales de la organización como de actividades relevantes, obteniendo con ello una base sobre la cual sean identificados y analizados los factores de riesgo que amenazan su oportuno cumplimiento.

La evolución de riesgos debe ser una responsabilidad ineludible para todos los niveles que están involucrados en el logro de los objetivos. Esta actividad de autoevaluación debe ser revisada por los auditores interno para asegurar que tanto el objetivo, enfoque, alcance y procedimiento han sido apropiadamente llevados a cabo.

Toda entidad enfrenta una variedad de riesgos provenientes de fuentes externas e internas que deben ser evaluados por la gerencia, quien a su vez, establece objetivos generales y específicos e identifica y analiza los riesgos de que dichos objetivos no se logren o afecten su capacidad para salvaguardar sus bienes y recursos, mantener ventaja ante la competencia. Construir y conservar su imagen, incrementar y mantener su solidez financiera, crecer, etc.

Las categorías de los objetivos son las siguientes:

- Objetivos de Cumplimiento. Están dirigidos a la adherencia a leyes y reglamentos, así como también a las políticas emitidas por la administración.
- Objetivos de Operación. Son aquellos relacionados con la efectividad y eficacia de las operaciones de la organización.
- Objetivos de la Información Financiera. Se refieren a la obtención de información financiera confiable.

El logro de los objetivos antes mencionados está sujeto a los siguientes eventos:

1. Los controles internos efectivos proporcionan una garantía razonable de que los objetivos de información financiera y de cumplimiento serán logrados, debido a que están dentro del alcance de la administración.

2. En relación a los objetivos de operación, la situación difiere de la anterior debido a que existen eventos fuera de control del ente o controles externos. Sin embargo, el propósito de los controles en esta categoría está dirigido a evaluar la consistencia e interrelación entre los objetivos y metas en los distintos niveles, la identificación de factores críticos de éxito y la manera en que se reporta el avance de los resultados y se implementan las acciones indispensables para corregir desviaciones.

Los riesgos de actividades también deben ser identificados, ayudando con ello a administrar los riesgos en las áreas o funciones más importantes; las causas en este nivel pertenecen a un rango amplio que va desde lo obvio hasta lo complejo y con distintos grados de significación, deben incluir entre otros aspectos los siguientes:

- La estimación de la importancia del riesgo y sus efectos.
- La evaluación de la probabilidad de ocurrencia.
- El establecimiento de acciones y controles necesarios.
- La evaluación periódica del proceso anterior.

c) Actividades de Control

Son aquellas que realizan la gerencia y demás personal de la organización para cumplir diariamente con las actividades asignadas. Estas actividades están expresadas en las políticas, sistemas y procedimientos.

Las actividades de control tienen distintas características. Pueden ser manuales o computarizadas, administrativas u operacionales, generales o específicas, preventivas o defectivas. Sin embargo, lo trascendente es que sin importar su categoría o tipo, todas ellas están apuntando hacia los riesgos (reales o potenciales) en beneficio de la organización, su misión y objetivos, así como la protección de los recursos propios o de terceros en su poder.

d) Información y Comunicación

Están diseminados en todo el ente y todos ellos atienden a uno o más objetivos e control. De manera amplia, se considera que existen controles generales y controles de aplicación sobre los sistemas de información.

1. Controles Generales: Tienen como propósito asegurar una operación y continuidad adecuada, e incluyen al control sobre el centro de procesamiento de datos y su seguridad física, contratación y mantenimiento del hardware y software, así como la operación propiamente dicha. También se relacionan con las funciones de desarrollo y mantenimiento de sistemas, soporte técnico y administración de base de datos.

2. Controles de Aplicación: Están dirigidos hacia el interior de cada sistema y funcionan para lograr el procesamiento, integridad y confiabilidad, mediante la autorización y validación correspondiente. Desde luego estos controles cubren las aplicaciones destinadas a las interfaces con otros sistemas de los que se reciben o entregan información.

Los sistemas de información y tecnología son y serán sin duda un medio para incrementar la productividad y competitividad. Ciertos hallazgos sugieren que la integración de la estrategia, la estructura organizacional y la tecnología de información es un concepto clave para el nuevo siglo.

e) Supervisión y Seguimiento

En general, los sistemas de control están diseñados para operar en determinadas circunstancias. Claro está que para ello se tomaron en consideración los objetivos, riesgos y las limitaciones inherentes al control; sin embargo, las condiciones evolucionan debido tanto a factores externos como internos, provocando con ello que los controles pierdan su eficiencia.

Como resultado de todo ello, la gerencia debe llevar a cabo la revisión y evaluación sistemática de los componentes y elementos que forman parte de los sistemas de control. Lo anterior no significa que tenga que revisarse todos los componentes y elementos, como tampoco que deba hacerse al mismo tiempo.

La evaluación debe conducir a la identificación de los controles débiles, insuficientes o innecesarios, para promover con el apoyo decidido de la gerencia, su robustecimiento e implantación. Esta evaluación puede llevarse a cabo de tres formas: durante la realización de las actividades diarias en los distintos niveles de la organización; de manera separada por personal que no es el responsable directo de la ejecución de las actividades (incluidas las de control) y mediante la combinación de las dos formas anteriores. Para un adecuado seguimiento (monitoreo) se deben tener en cuenta las siguientes reglas:

- El personal debe obtener evidencia de que el control interno está funcionando.
- Sí las comunicaciones externas corroboran la información generada internamente.
- Se deben efectuar comparaciones periódicas de las cantidades registradas en el sistema de información contable con el físico de los activos.
- Revisar si se han implementado controles recomendados por los auditores internos y externos; o por el contrario no se ha hecho nada o poco.
- Sí son adecuadas, efectivas y confiables las actividades del departamento de la auditoría interna. (Javier., 2012)

2.5. Tecnologías de la Información y Comunicación (TIC)

Las Tecnologías de la Información y la Comunicación TIC, así como otras estrategias de innovación tecnológica y científica, presentan una relación directa con cambios de tipo procedimental, cultural, estratégico, productivo, etc. Estos cambios, implican que organizaciones y personas desarrollen una serie de pasos, que les permitan asimilar y adaptarse a dichos cambios, para posteriormente aceptar e implementar las nuevas prácticas y estrategias que esto conlleva.

De esta manera, la innovación tecnológica y más específicamente, las TIC, cuya evolución avanza a pasos agigantados día tras día, exigen de las personas y organizaciones que evolucionen al mismo ritmo, so pena de quedar relegados en el pasado tecnológico. En su afán por caminar junto o tratar de alcanzar estas tecnologías, las personas y organizaciones deben cambiar constantemente sus costumbres, políticas, prioridades, etc., lo cual les será beneficioso hasta cierto punto, siempre y cuando ello no atente contra sus principios ni viole aquellas conductas relacionadas con la integridad de cada estructura y sus correctas prácticas. (Piattini, Auditoría de Control Interno, 2006)

Ventajas

Desde la perspectiva del aprendizaje, las TIC favorecen la continua actividad intelectual y desarrollan la creatividad y el aprendizaje cooperativo. Así mismo, mejoran las competencias de expresión y creatividad y desarrolla habilidades de búsqueda y selección de información. También son un canal de fácil acceso a mucha información de todo tipo.

Organizacionalmente, las TIC favorecen el incremento de la productividad y el acceso a nuevas tecnologías, que las empresas pueden apropiarse mediante procesos exógenos, lo cual moviliza las capacidades de la organización.

Desventajas

Desde la perspectiva del aprendizaje, las TIC pueden generar distracciones, dispersión, pérdida de tiempo, información poco fiable, aprendizaje superficial y dependencia de los demás.

Organizacionalmente, las TIC pueden llegar a ser promotoras de la disminución de puestos de trabajo, ya que estos son reemplazados por tecnologías mayormente eficientes y económicas. (Piattini, Auditoría Informática un enfoque práctico, 2001)

2.6. Análisis FODA

El análisis FODA es una de las herramientas esenciales que provee de los insumos necesarios al proceso de planeación estratégica, proporcionando la información necesaria para la implantación de acciones y medidas correctivas y la generación de nuevos proyectos o proyectos de mejora.

Es un método para analizar:

- Fortalezas.
- Oportunidades.
- Debilidades.
- Amenazas.

En el proceso de análisis FODA, se consideran los factores económicos, políticos, sociales y culturales que representan las influencias del ámbito externo a la organización, que inciden sobre su quehacer interno.

El objetivo primario del análisis FODA consiste en obtener conclusiones sobre la forma en que el objeto estudiado será capaz de afrontar los cambios y las turbulencias en el

contexto, (oportunidades y amenazas) a partir de sus fortalezas y debilidades internas. (Maldonado, 2011)

2.7. Hallazgos de Auditoría

Se denomina hallazgo de auditoría resultado de la comparación que se realiza entre un CRITERIO y la SITUACIÓN actual encontrada durante el examen a un departamento, un área, actividad u operación.

Es toda información que a juicio del auditor le permite identificar hechos o circunstancias importantes que inciden en la gestión de recursos en la organización, programa o proyectos bajo examen que merecen ser comunicados en el informe.

Sus elementos son: condición, criterio, causa y efecto

La palabra hallazgo en la Auditoría Informática se lo emplea para referirse a cualquier situación deficiente y relevante que se determina por medio de la aplicación de los diferentes componentes de la auditoría, debiendo ser estructurado de acuerdo a sus atributos y obviamente que sean de interés para la organización auditada.

CONDICIÓN: Situaciones actuales encontradas. Lo que es. Este término se refiere al hecho irregular o deficiencia determinada por el auditor interno, cuyo grado de desviación debe ser demostrada y sustentada con evidencias.

CRITERIO: Unidades de medidas o normas aplicables. Lo que debe ser. Es la norma o estándar técnico-profesional, alcanzable en el contexto evaluado, que permiten al auditor tener la convicción de que es necesario superar una determinada acción u omisión de la entidad, en procura de mejorar la gestión.

CAUSA: Razones de desviación. ¿Por qué sucedió? Es la razón fundamental por la cual ocurrió la condición, o el motivo por el que no se cumplió el criterio o norma. Su identificación requiere de la habilidad y juicio profesional del auditor y es necesaria para el desarrollo de las recomendaciones constructivas que prevenga la ocurrencia de la condición.

Las causas deben recogerse de la administración activa, de las personas o actores responsables de las operaciones que originaron la condición, y estas deben ser por escrito, a los efectos de evitar inconvenientes en el momento de la discusión del informe, en el sentido de que después puedan ser negadas por los responsables, o se diga que tales causas

fueron redactadas por el auditor actuante, sin tener un conocimiento claro y exacto de lo ocurrido.

EFEECTO: Importancia relativa del asunto, preferible en términos monetarios. La diferencia entre lo que es y lo que debe ser.

Es la consecuencia real o potencial cuantitativo o cualitativo, que ocasiona la observación, indispensable para establecer su importancia y recomendar a la administración activa que tome las acciones requeridas para corregir la condición. Siempre y cuando sea posible, el auditor debe revelar en su informe la cuantificación del efecto. (Estupiñan, 2006)

2.8. Normas de Control Interno para la Auditoría Informática

NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS

Dentro del grupo 400, subgrupo 410 y en el grupo 500, encontramos las normas para la evaluación del control interno en el área de la Informática.

410-01 Organización informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

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.

Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones

Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410-03 Plan informático estratégico de tecnología

La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario.

La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico.

El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

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 y se medirá el cumplimiento de las regulaciones y estándares definidos.

La unidad de tecnología de información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

410-05 Modelo de información organizacional

La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.

El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente.

Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos

La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.
2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.
3. La formulación de los proyectos considerará el Costo Total de Propiedad CTP; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.
4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.
5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.
6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.
7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.
8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.
9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.
10. E

El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo

La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.
2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario,

interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.
4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.
5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.
6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.
7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.
8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.
9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica

La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.
2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.
3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.
4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

410-09 Mantenimiento y control de la infraestructura tecnológica

La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.
2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
3. Control y registro de las versiones del software que ingresa a producción.
4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

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.
7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;
2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;
4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
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;
7. Consideración y disposición de sitios de procesamiento alternativos.
8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.

2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.
3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alternativo propio o de uso compartido en un data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.
4. Plan de recuperación de desastres que comprenderá:
 - Actividades previas al desastre (bitácora de operaciones)
 - Actividades durante el desastre (plan de emergencias, entrenamiento)
 - Actividades después del desastre.
5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.
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.
7. El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
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.
3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.
4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.
5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.
6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.

7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.
8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.
9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.
10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.
11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet

Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

La unidad de tecnología de información considerará el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.

410-15 Capacitación informática

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.

410-16 Comité informático

Para la creación de un comité informático institucional, se considerarán los siguientes aspectos:

- El tamaño y complejidad de la entidad y su interrelación con entidades adscritas.
- La definición clara de los objetivos que persigue la creación de un comité de informática, como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad.
- La conformación y funciones del comité, su reglamentación, la creación de grupos de trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.

410-17 Firmas electrónicas

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.

El uso de la firma electrónica en la administración pública se sujetará a las garantías, reconocimiento, efectos y validez señalados en estas disposiciones legales y su normativa secundaria de aplicación.

Las servidoras y servidores autorizados por las instituciones del sector público podrán utilizar la firma electrónica contenida en un mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público que ocupan.

Los aplicativos que incluyan firma electrónica dispondrán de mecanismos y reportes que faciliten una auditoría de los mensajes de datos firmados electrónicamente.

a) Verificación de autenticidad de la firma electrónica

Es responsabilidad de las servidoras y servidores de las entidades o dependencias del sector público verificar mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida sea emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.

b) Coordinación interinstitucional de formatos para uso de la firma electrónica

Con el propósito de que exista uniformidad y compatibilidad en el uso de la firma electrónica, las entidades del sector público sujetos a este ordenamiento coordinarán y definirán los formatos y tipos de archivo digitales que serán aplicables para facilitar su utilización. Las instituciones públicas adoptarán y aplicarán los estándares tecnológicos

para firmas electrónicas que las entidades oficiales promulguen, conforme a sus competencias y ámbitos de acción.

c) Conservación de archivos electrónicos

Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros, bajo la responsabilidad del usuario y de la entidad que los generó. Para ello se establecerán políticas internas de manejo y archivo de información digital.

d) Actualización de datos de los certificados de firmas electrónicas

Las servidoras y servidores de las entidades, organismos y dependencias del sector público titulares de un certificado notificarán a la entidad de certificación de Información sobre cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado. Cuando un servidor público deje de prestar sus servicios temporal o definitivamente y cuente con un certificado de firma electrónica en virtud de sus funciones, solicitará a la entidad de certificación de información, la revocación del mismo, además, el superior jerárquico ordenará su cancelación inmediata. El dispositivo portable seguro será considerado un bien de la entidad o dependencia pública y por tanto, a la cesación del servidor, será devuelto con la correspondiente acta de entrega recepción.

e) Seguridad de los certificados y dispositivos portables seguros

Los titulares de certificados de firma electrónica y dispositivos portables seguros serán responsables de su buen uso y protección. Las respectivas claves de acceso no serán divulgadas ni compartidas en ningún momento. El servidor solicitará la revocación de su certificado de firma electrónica cuando se presentare cualquier circunstancia que pueda comprometer su utilización.

f) Renovación del certificado de firma electrónica

El usuario solicitará la renovación del certificado de firma electrónica con la debida anticipación, para asegurar la vigencia y validez del certificado y de las actuaciones relacionadas con su uso.

g) Capacitación en el uso de las firmas electrónicas

La entidad de certificación capacitará, advertirá e informará a los solicitantes y usuarios de los servicios de certificación de información y servicios relacionados con la firma electrónica, respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados. Esta capacitación facilitará la comprensión y utilización de las firmas electrónicas, en los términos que establecen las disposiciones legales vigentes. (ESTADO, 2009)

2.9. IDEA A DEFENDER

2.9.1 Idea General

Los resultados alcanzados en la Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, período 2014; ayudara a mejorar la calidad y seguridad de la información y dar solución a los inconvenientes encontrados.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. MODALIDAD DE INVESTIGACIÓN

Método cualitativo.- tendrá como objetivo la descripción de las cualidades de un fenómeno. Busca un concepto que pueda abarcar una parte de la realidad. No se trata de probar o de medir en qué grado una cierta cualidad se encuentra en un cierto acontecimiento dado, sino de descubrir tantas cualidades como sea posible.

Método cuantitativo._ es aquel que permitirá examinar los datos de manera numérica, especialmente en el campo de la Estadística. Para que exista metodología cuantitativa se requiere que entre los elementos del problema de investigación exista una relación cuya Naturaleza sea lineal.

3.2. Tipos de Investigación

- Exploratoria.- también conocido como estudio piloto, son aquellos que se investigan por primera vez o son estudios muy pocos investigados. También se emplean para identificar una problemática.
- Descriptiva.- describirá y analizará los procesos, programas, procedimientos, técnicas y políticas de auditoría.
- Explicativa.- este tipo de estudio busca el porqué de los hechos, estableciendo relaciones de causa- efecto.

3.3. Población y Muestra

Con el fin de obtener un resultado preciso y objetivo el examen de Auditoría Informática se aplicó a todos los directores departamentos y jefes de las unidades con un total de 18 personas.

3.4. Métodos, Técnicas e Instrumentos de Investigación

- **Inductivo-Deductivo.**

Este método permitirá analizar la problemática que presenta la UTIC del GADMCG, y como la auditoría Informática permitirá mejorar el proceso de calidad y seguridad de información.

- **Entrevista**

Se realizará una entrevista a los funcionarios del área TIC para la obtención de información a través de una serie de preguntas significativas que nos darán pautas en el proceso de la auditoría informática.

- **Observación**

Es una de las técnicas más utilizadas para examinar los diferentes aspectos que intervienen en el funcionamiento del área informática.

- **Encuesta**

Se aplicará a los funcionarios del Unidad de Tecnologías de Información y Comunicación del GADM Cantón Guamote.

3.5. Resultados

A lo largo de la auditoría, se mantendrá constante comunicación entre auditor y funcionarios de la entidad, los cuales presentaran pruebas documentadas, darán información verbal de los asuntos sometidos a los exámenes.

Los resultados se consideran como la última fase de la auditoría.

Una vez recopilada la información se procederá al análisis de los datos obtenidos, los cuales serán cuantificados y representados gráficamente.

Para lo cual se efectuará las siguientes técnicas para la recolección de información:

- Entrevista
- Ficha de Observación
- Encuesta

CAPÍTULO IV: MARCO PROPOSITIVO

4.1 AUDITORÍA INFORMÁTICA A LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE, PERÍODO 2014.

ENTIDAD:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote.
TEMA:	Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, período 2014.
FECHA DE CIERRE:	Al 31 de Diciembre del 2014.

FORMALIDADES

Elaborado por:	CH.C.LE	Fecha:	15/12/2015
Revisado por:	O.E.W.V	Fecha:	15/12/2015

4.1.1.1 Orden de trabajo

ORDEN DE TRABAJO N° 0001-GADMCG

Guamote, 28 de diciembre del 2015

Sr. Luis Ernesto Chimbo Caizaguano
EGRESADO DE LA EICA
Ciudad.-

En cumplimiento del trabajo de Titulación aprobado por el Consejo Directivo de la Facultad de Administración de Empresas, Escuela de Ingeniería en Contabilidad y Auditoría CPA, sírvase proceder a efectuar la Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, cuyo alcance cubrirá el período comprendido desde el 01 de Enero al 31 de Diciembre del 2014

Se faculta al Sr, Luis Ernesto Chimbo Caizaguano que actué en calidad de Investigador-Auditor y el suscrito como Supervisor.

Terminado el Trabajo de Auditoría, se servirá presentar el respectivo informe.

Atentamente,

Ing. Oscar Omar Espíndola Lara
DIRECTOR TRABAJO DE TITULACIÓN

Ing. Wilson Antonio Velasteguí Ojeda
MIEMBRO DE TRIBUNAL

Guamote, 28 de diciembre del 2015

PARA:	Eco. Luis Ángel Chuquimarca Coro.
	ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE.
DE:	SR. Luis Ernesto Chimbo Caizaguano
	INVESTIGADOR-AUDITOR
ASUNTO:	INICIO DE AUDITORÍA INFORMÁTICA A LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE, PERÍODO 2014.

En cumplimiento a la Orden de Trabajo N°0001-GADMCG emitida por el Ing. Oscar Espíndola y el Ing. Wilson Velastigui, catedráticos de la Escuela Superior Politécnica de Chimborazo, Director y Miembro del tribunal de Trabajo de Titulación respectivamente, pongo en consideración que en esta fecha se da inicio a la práctica de *Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote*, cuyo alcance comprende el período entre el 01 de Enero al 31 de Diciembre del 2014.

Particular que le notifico para que se preste la colaboración para la información que obtendremos para nuestra auditoría.

Atentamente,

Luis Ernesto Chimbo Caizaguano
EGRESADO DE LA EICA

4.1.2. INDÍCE DEL ARCHIVO PERMANENTE

A P. 1

Cuadro No 3. Índice de archivo permanente

	ÍNDICE
AP	<u>ARCHIVO PERMANENTE</u>
AP 1	Información General
AP 2	Reseña Histórica
AP 3	Misión, Visión, Valores y Principios
AP 4	Base Legal
AP 5	Organigrama
AP 6	Nómina del Personal
AP 7	FODA
AP 8	Notificaciones.
AP 9	Referencias
AP 10	Marcas de Auditoría

Elaborado por:	CH.C.LE	Fecha:	28/12/2015
Revisado por:	O.E.W.V	Fecha:	28/12/2015

RESEÑA HISTÓRICA

Según el historiador Padre Juan de Velasco, en el actual territorio del cantón Guamote se asentaban varios cacicazgos autodenominados “Guamotis”, “Atapos”, “Pull”, “Tipines”, “Vishudes”, “Basanes”, entre otros, los mismos que formaban parte del pueblo Puruhá. De acuerdo a este historiador, el origen de Guamote es anterior a la conquista de los Incas, lo que lo ubica como un pueblo con una larga historia llena costumbres y tradiciones Puruháes. Al respecto, cabe mencionar que en la planicie del Tiocajas se desarrollaron cruentas batallas primero en contra de la conquista incásica y luego en contra de la conquista española.

Durante la vigencia de la Gran Colombia Guamote formó parte del cantón Riobamba, hasta el año de 1884, año en el que se crea el cantón Colta del cual Guamote pasa a formar parte hasta su posterior cantonización.

En 1938, a partir de la promulgación de la ley de comunas, obtienen su personería jurídica las comunidades de San José de Atillo, Chismaute Alto y Gualipite.

Guamote formaba parte del cantón Colta desde el año de 1884 (fecha de cantonización de Colta), hasta el primero de agosto de 1944, fecha en la que alcanza su cantonización, por el decreto ejecutivo No. 606 dictado por el Dr. José María Velasco Ibarra, y el 21 de Agosto del mismo año se inaugura el Ilustre Concejo Municipal de Guamote. En sus inicios el cantón se integró con las parroquias: Matriz de Guamote y Cebadas y el 7 de agosto de 1946 se decreta la anexión de la parroquia Palmira perteneciente hasta esa fecha al cantón Alauís.

Elaborado por:	CH.C.LE	Fecha:	28/12/2015
Revisado por:	O.E.W.V	Fecha:	28/12/2015

Identificación del Gobierno Autónomo descentralizado Municipal del Cantón Guamote

Figura 1. GAD Municipal de Guamote



Fuente: Gobierno Autónomo Descentralizado Municipal del Cantón Guamote
Elaborado por: Luis Ernesto chimbo Caizaguano

Provincia: Chimborazo

Cantón: Guamote

Razón Social: Gobierno Autónomo Descentralizado Municipal del Cantón Guamote

Representante Legal: Eco. Luis Chuquimarca

Dirección: 10 de Agosto y Abelardo Montalvo

Teléfonos: (+593) 32916160

Correo Página: <http://www.municipiodeguamote.gob.ec/>

Ubicación física del GAD Municipal de Guamote.

El Cantón Guamote se encuentra ubicado en la parte central del callejón interandino, al sur de Quito, a 50 Km de Riobamba, constituye el segundo cantón más extenso de los que integran la Provincia de Chimborazo.

Se encuentra a una altitud que va desde los 2600 m.s.n.m. hasta 4500 m.s.n.m., su temperatura media anual es de 13,7°C, constituyendo dos tipos de clima: invierno húmedo frío en los meses de octubre a mayo y verano, cálido, seco, ventoso de junio a septiembre. La precipitación es de 683,3 mm.

Elaborado por:	CH.C.LE	Fecha:	28/12/2015
Revisado por:	O.E.W.V	Fecha:	28/12/2015

Figura 2. Ubicación GAD Municipal de Cantón Guamote

AP 3/11



Fuente: Gobierno Autónomo Descentralizado Municipal de Cantón Guamote

Elaborado por: Luis Ernesto Chimbo Caizaguano

MISIÓN, VISIÓN, VALORES Y OBJETIVOS INSTITUCIONALES

Misión y Visión de la institución

Misión

Ser un Municipio en desarrollo permanente, sostenible, ofreciendo servicios básicos de calidad, impulsando el desarrollo local a niveles competitivos, con relaciones y trabajos socioculturales fortalecidos, conciencia ambiental y turística orientada a condiciones de vida óptima, donde la imagen del cantón, su ornato, presentación y cultura promuevan la identificación y el aprovechamiento de unidad cantonal que toma decisiones concertadas y equitativas , respetando a la pacha mama y alcanzando el buen vivir.

Visión

El Cantón Guamote para el año 2026 será el eje del desarrollo nacional con una producción agropecuaria, turística competitiva y sostenible que garantice la calidad de vida de sus habitantes, en un ambiente sano, seguro y ecológicamente equilibrado, con una economía dinámica y solidaria.

Elaborado por:	CH.C.LE	Fecha:	28/12/2015
Revisado por:	O.E.W.V	Fecha:	28/12/2015

Principales Disposiciones Legales

AP 4/11

La normativa aplicable para el GAD Municipal de Guamote:

- Constitución Política de la República del Ecuador
- Ley Orgánica de la Contraloría General del Estado
- Código Orgánico de Organización Territorial Autonomía y Descentralización
- Ley de Presupuesto del Sector Público
- Ley Orgánica de Servicio 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 / Ministerio de Finanzas
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de la Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos
- Código de Trabajo
- Ley Orgánica del Sistema Nacional de Contratación Pública.

Elaborado por:	CH.C.LE	Fecha:	28/12/2015
Revisado por:	O.E.W.V	Fecha:	28/12/2015

ESTRUCTURA ADMINISTRATIVA Y ORGANIZACIONAL

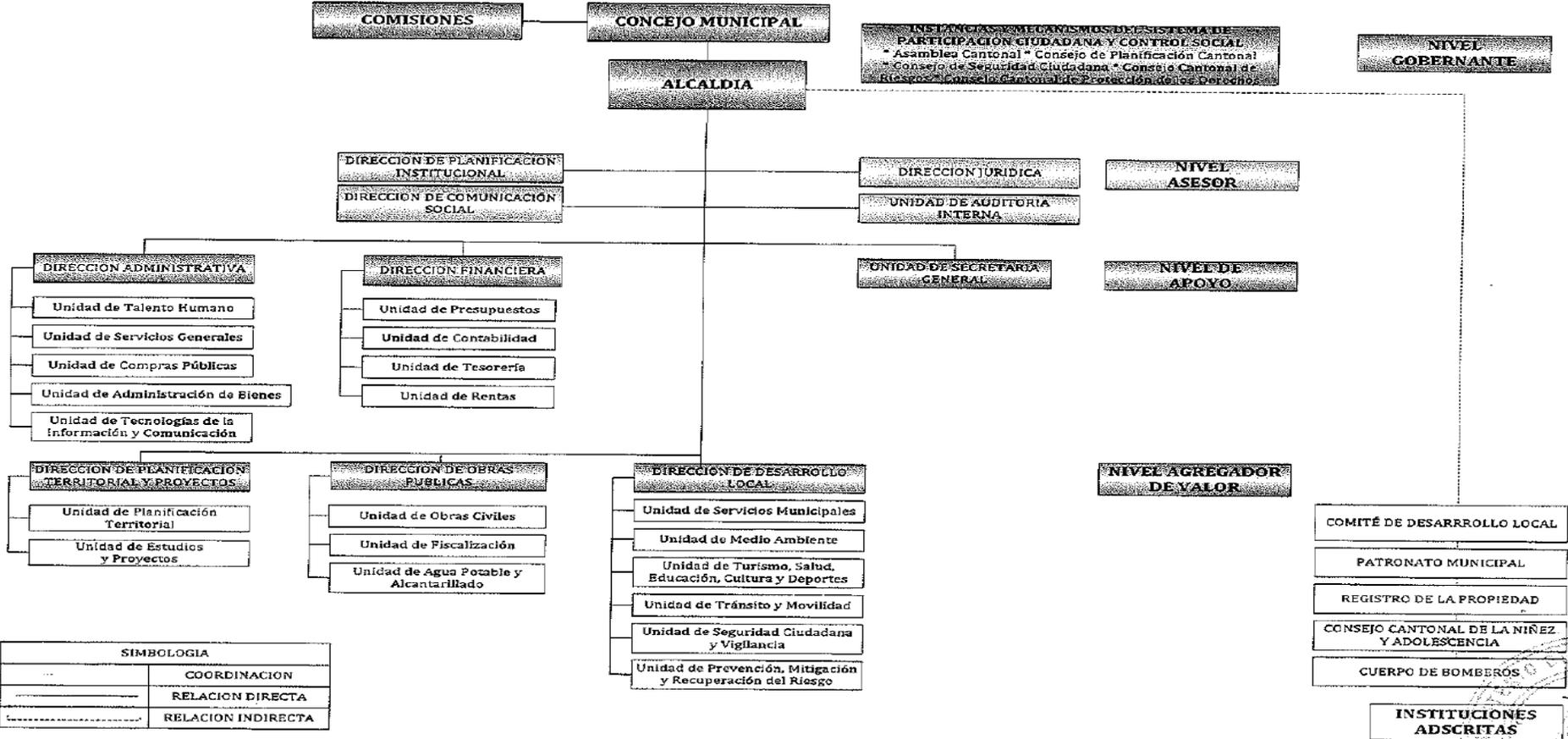


Figura 2: Organigrama Estructural Del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote.
Fuente: GADMCG
Realizado por: Luis Ernesto Chimbo Caizaguano

Cuadro No 4: NOMINA DEL PERSONAL

FUNCIONARIO	CARGO
Luis Ángel Chuquimarca Coro	Alcalde
Sayay Delgado José Manuel	Director De Gestión Administrativa
Orozco Peñafiel Luis Alfredo	Director De Gestión De Obras Publicas
Naula Yangol Luis Alfredo	Director De Gestión Financiera
Yangol Condo Pedro Vicente	Director De Gestión De Desarrollo Local
Mejía Tixi Ángel Gustavo	Director De Patronato Municipal
Avendaño Sasnalema Ángel Arnulfo	Jefe De Adquisiciones
Guambo Yuquilema Rodrigo	Jefe De Recursos Humanos
Llumaglla Añileme José Felipe	Jefe De Dispensario Medico
Yasaca Alvares Segundo Carlos	Jefe De Seguridad Ciudadana
Delgado Galarza Segundo	Jefe De Mantenimiento Mecánico
Quespaz Montoya Wandember	Jefe De Unidad TIC
Chávez López Guillermo Javier	Jefe De Agua Potable
Condo Vimos Ángel Felipe	Jefe De Planificación Estratégica
Castillo Mora Wilson Eduardo	Jefe De Avalúos Y Catastros
Chimbo Caizaguano Segundo Ángel	Jefe De Gestión Ambiental
Donoso Cajas Lucia de Lourdes	Jefe De Gestión De Desarrollo Local
Pazmiño Méndez Juan Gabriel	Jefe de Seguridad y salud ocupacional
TOTAL	18

Fuente: Gobierno Autónomo Descentralizado Municipal de Cantón Guamote

Elaborado por: Luis Ernesto Chimbo Caizaguano

Elaborado por:	CH.C.LE	Fecha:	28/12/2015
Revisado por:	O.E.W.V	Fecha:	28/12/2015

FODA	DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA UNIDAD DE TECNOLOGÍAS INFORMACIÓN Y COMUNICACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE	AP 7/11
Análisis Interno		
FORTALEZAS		DEBILIDADES
F1 personal técnico capacitado.		D1 espacio físico y ambiente de trabajo inadecuado
F2 infraestructura tecnológica adecuada		D2 carencia de plan de capacitación para usuarios de la UTIC.
F3 conexión permanente a la red		D3 carencia de un plan estratégico de TIC.
F4 existencia de la estructura orgánica municipal		D4 no cuenta con plan de mantenimiento de sistemas de información
		D5 Manejo de un software aplicativo sin licencia.
Análisis Externo		
OPORTUNIDADES		AMENAZAS
O1 Aplicación de nuevas alternativas informáticas al sector público		A1 Cortes de energía eléctricas, por los cambios de redes principales.
O2 Mejora de los procesos de seguridad física y lógica.		A2 Pérdida de la información
O3 Actualización de los equipos y software		A3 No aprobación del presupuesto presentado por la unidad en el Plan Operativo Anual
O4 Nuevas herramientas informáticas de código abierto		A4 cambios en las políticas de estado
O5 Apoyo del Gobierno		

Guamote, 04 de enero del 2016

AP 8/11

Economista

Luis Ángel Chuquimarca Coro

**ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN GUAMOTE.**

Presente.-

De mi consideración:

Reciba un cordial y atento saludo, me dirijo a usted en referencia a la solicitud enviada en meses pasados para la realización de la “Auditoría Informática a la Unidad de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, Provincia de Chimborazo, período 2014.”, la misma que fue aprobada por su persona, y en virtud de ello, informarle que una vez incluidos a los requisitos previos al inicio de este trabajo, hemos planificado empezar el desarrollo de esta actividad de este día 10 de enero del año en curso.

Al mismo tiempo de la manera más comedida solicitamos su colaboración y la colaboración del personal que labora en la institución, para acceder a la respectiva documentación e información que nos permita desarrollar con facilidad nuestro trabajo investigativo.

Para lo cual solicitamos se nos facilite la siguiente información:

- Organigrama Estructural
- Manual de Funciones
- Plan Estratégico Institucional
- Reglamento Interno de Trabajo
- Inventario de Tecnologías Información y comunicación

Seguro de contar con su valiosa colaboración, les anticipo mis agradecimientos.

Atentamente,

Luis Ernesto Chimbo Caizaguano
AUDITOR- INVESTIGADOR

Guamote, 05 de enero del 2016.

Economista

Luis Ángel Chuquimarca Coro

**ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN GUAMOTE.**

Presente.-

De nuestra consideración:

Por medio de la presente le doy a conocer el equipo de trabajo que estará encargado de la ejecución de la Auditoría Informática a la Unidad de Tecnologías Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, Provincia de Chimborazo, período 2014.

Ing. Oscar Omar Espíndola Lara SUPERVISOR 1

Ing. Wilson Antonio Velasteguí Ojeda SUPERVISOR 2

Luis Ernesto Chimbo Caizaguano AUDITOR – INVESTIGADOR

Atentamente,

Luis Ernesto Chimbo Caizaguano
AUDITOR- INVESTIGADOR

Cuadro No 6: Hoja de Referencias

AP	ARCHIVO PERMANENTE
AC	ARCHIVO CORRIENTE
PA	PROGRAMA DE AUDITORÍA
CI	CUESTIONARIO DE CONTROL INTERNO
MP	MEMORANDO DE PLANIFICACIÓN
MCR	MATRIZ DE PONDERACIÓN DE CONFIANZA Y RIESGO
MAC	MATRIZ DE ÁREAS CRÍTICAS
HH	HOJA DE HALLAZGO
OOEL	OSCAR OMAR ESPÍNDOLA LARA
WAVO	WILSON ANTONIO VELASTEGUÍ OJEDA
LECHC	LUIS ERNESTO CHIMBO CAIZAGUANO

Elaborado por:	CH.C.LE	Fecha:	05/01/2016
Revisado por:	O.E.W.V	Fecha:	05/01/2016

 <p>ASERCONP Asesoría Fiscal, Contable y Laboral</p>	HOJA DE MARCAS DE AUDITORÍA	AP 11/11
--	------------------------------------	-----------------

Cuadro 7: Marcas de Auditoría

√	=	Verificado mediante inspección física
@	=	Analizado
↕	=	Comparado
⇒	=	Determinación de hallazgo
∝	=	Cotejado con inventarios
⊗	=	Incluir en informe
≡	=	Cotejado con documentos

Elaborado por:	CH.C.LE	Fecha:	05/01/2016
Revisado por:	O.E.W.V	Fecha:	05/01/2016

ENTIDAD:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote
TEMA:	Auditoría Informática a la Unidad de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, Provincia de Chimborazo, período 2014.
FECHA DE CIERRE:	Al 31 de Diciembre del 2014.

ARCHIVO CORRIENTE

Elaborado por:	CH.C.LE	Fecha:	05/01/2016
Revisado por:	O.E.W.V	Fecha:	05/01/2016

4.2 Archivo Corriente

AC 2/2

4.2.1. INDÍCE DEL ARCHIVO CORRIENTE

Cuadro 8: GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE

	ÍNDICE
AC	<u>ARCHIVO CORRIENTE</u>
	FASE I
VP	Visita Preliminar
PA	Programa de Auditoría
CP	Carta de Presentación
EA	Entrevista al Alcalde
ET	Entrevista al Jefe de la Unidad de TIC
	FASE II
EA	Ejecución de la Auditoría
PA	Programa de Auditoría
MPL	Memorándum de Planeación
CI	Cuestionario de Control Interno
MP	Matriz de Ponderación
MAC	Matriz de Áreas Críticas
HH	Hoja de Hallazgos
	FASE III
CR	Comunicación de Resultados
PA	Programa de Auditoría
IA	Informe Final de Auditoría Informática

Elaborado por:	CH.C.LE	Fecha:	06/02/2016
Revisado por:	O.E.W.V	Fecha:	06/02/2016

**FASE I
VISITA PRELIMINAR**

 ASERCOMP <small>Asesoría Fiscal Contable y Laboral</small>	PROGRAMA DE AUDITORÍA	PA 1
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote	
Periodo	Enero - Diciembre 2014	
Objetivo:	Evaluar los resultados en base a la evidencia y determinación de hallazgos.	

Nº	PROCEDIMIENTO	REF. P/T/	RESPONSABLE	FECHA
1	Realice una carta compromiso señalando que se iniciara con la ejecución de la auditoría, con la finalidad de que se brinde las facilidades necesarias.	VP	L.E.CH.C	11/01/2016
2	Realice una entrevista al Alcalde del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote	EA	L.E.CH.C	12/01/2016
3	Aplicar entrevista al Jefe de la unidad de tecnología información y comunicación.	ET	L.E.CH.C	12/01/2016

Elaborado por:	CH.C.LE	Fecha:	11/01/2016
Revisado por:	0.E.W.V	Fecha:	12/01/2016

Guamote, 11 de enero del 2016

Economista

Luis Ángel Chuquimarca Coro

**ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN GUAMOTE.**

Presente.-

Reciba un atento y cordial saludo, a la vez deseando éxito en las funciones que se desempeña favorablemente en beneficio de nuestro cantón.

La presente tiene por objeto de pedirle de la manera más comedida la autorización para la realización de la Auditoría Informática a la Unidad de Tecnologías Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, provincia de Chimborazo, Periodo 2014, para lo cual indico a usted que la Auditoría Informática se lo desarrollará en base a las Normas de Control Interno emitidas por la Contraloría General del Estado, con el objetivo de medir el Grado de Cumplimiento de la normativa relacionado a las TIC y asegurar la calidad y seguridad de la información.

El tiempo que dispondrá para su ejecución será de 90 días laborables, contados a partir de la fecha y concluido el mismo servirá presentar el informe respectivo.

Los objetivos de la Auditoría Informática buscaran: Evaluar el grado de eficiencia y eficacia sobre el sistema de control interno establecido por la entidad ante los sistemas informáticos. Verificar el cumplimiento de las disposiciones legales, reglamentarias y normativas vigentes para su aplicación. Los resultados se harán conocer mediante el informe de auditoría que incluirá comentarios, conclusiones y recomendaciones.

Atentamente,

Luis Ernesto Chimbo Caizaguano

AUDITOR – INVESTIGADOR

Elaborado por:	CH.C.L.E	Fecha:	12/01/2016
Revisado por:	0.E.W.V	Fecha:	12/01/2016

ENTREVISTA DIRIGIDA AL ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE, REFERENTE A TECNOLOGÍAS INFORMACIÓN Y COMUNICACIÓN.

1. ¿Con que objetivo se crea la unidad de TIC en GADM Guamote?

El objetivo es brindar calidad de servicios para los usuarios, dándole comodidad y facilidad con la utilización de herramientas tecnológicas, para de esta manera puedan dar seguimiento a las gestiones en diferentes departamentos en línea.

2. ¿Existen planes de inversión periódicos en lo que corresponde a la adquisición y equipamiento de la unidad de TIC de GADM Guamote?

Se lo realiza planes de inversión anualmente de acuerdo a la necesidad de los recursos tecnológicos en cada uno de las Unidades de nuestro municipio.

3. ¿Existe personal suficiente con conocimientos y experiencia para realizar las actividades dentro de esta área?

El personal debe cumplir con el perfil establecido en el manual de funciones que dispone la unidad de talento humano de nuestra institución previa un concurso por lo tanto estamos seguros que el personal es capacitado y con mucha experiencia.

4. ¿Cree usted que la infraestructura tecnológica con la que dispone la institución es suficiente para que los servidores desempeñen sus labores?

Últimamente hemos hecho adquisición de equipos informáticos para poder mejorar el desempeño de los usuarios y también actualización de los mismos por lo tanto creo que por el momento es suficiente la infraestructura tecnológica.

5. De acuerdo a la situación actual de la Unidad de TIC. ¿cree usted que esto contribuye a la Misión y Visión del GADM Guamote?

Sin duda ya que el objetivo primordial es de optimizar recurso y el tiempo por medio de utilización de herramientas tecnológicas y también nuestro Municipio es el pionero en la protección ambiental que con la tecnología eliminamos la utilización de papeles en nuestra institución.

Elaborado por:	CH.C.L.E	Fecha:	12/01/2016
Revisado por:	O.E.W.V	Fecha:	12/01/2016

ENCUESTA AL JEFE DE LA UNIDAD DE TECNOLOGÍAS INFORMACIÓN Y COMUNICACIÓN

Ing. Wandember Quespaz

1. ¿La infraestructura física para los equipos de informática existentes son los adecuados?

SI...x..... NO.....

2. ¿La unidad dispone de planes de capacitación para el uso correcto de los equipos tecnológicos?

SI..... NO...x.....

Se realiza cuando lo necesita cada a usuario.

3. ¿Existe misión, visión, objetivos y políticas establecidas para la Unidad de TIC?

SI.....x.... NO.....

4. ¿Existen zonas WIFI para los empleados?

SI...x..... NO.....

5. ¿La cobertura WIFI tiene contraseña de acceso?

SI...x..... NO.....

6. ¿Existe manuales de políticas y procedimientos para el personal que labora dentro de esta área?

SI...x..... NO.....

7. ¿El equipo de red Data Center ha cumplido su tiempo de vida útil?

SI...x..... NO.....

Elaborado por:	CH.C.L.E	Fecha:	12/01/2016
Revisado por:	0.E.W.V	Fecha:	12/01/2016

8. ¿Considera Ud. Que existen las seguridades físicas adecuadas dentro de las instalaciones de equipos informáticos, tales como: extintores, salidas de emergencia, aire acondicionado, etc.?

SI..... NO...x.....

9. ¿Conoce el lugar que ocupa en el organigrama la Unidad de Tecnologías Información y comunicación?

SI.....x.... NO.....

10. ¿Existe planes y programas de capacitación, adiestramiento y promoción del personal de la Unidad de TIC?

SI..... NO.....x....

Elaborado por:	CH.C.LE	Fecha:	12/01/2016
Revisado por:	0.E.W.V	Fecha:	12/01/2016

FASE II PLANIFICACIÓN

		PROGRAMA DE AUDITORÍA			PA 2
Entidad:		Gobierno Autónomo Descentralizado Municipal del Cantón Guamote			
Periodo:		Enero- Diciembre 2014			
Objetivo:		Evaluar los resultados obtenidos en base a la evidencia y determinación de hallazgos.			
Nº	PROCEDIMIENTO	REF. P/T/	RESPONSABLE	FECHA	
1	Elaborar programa de Auditoría.	PA 2	CH.C.L.E	12/01/2016	
2	Elaborar Memorándum de Planificación.	MP 1/4	CH.C.L.E	12/01/2016	
3	Evaluación de control Interno	PCI	CH.C.L.E	15/01/2016	
4	Elaborar y aplicar cuestionarios de Control Interno	CI 1/21	CH.C.L.E.	15 /01/2016	
5	Elaborar la matriz de ponderación de los cuestionarios de control interno y determine el grado de confianza y riesgo.	MP 1/2	CH.C.L.E	25/01/2016	
6	Identificar debilidades de Control Interno.	DCI 1/5	CH.C.L.E	01/02/2016	
7	Determinar áreas críticas.	AC 1/1	CH.C.L.E	10/02/2016	
8	Desarrollar la hoja de hallazgos.	HH 1/11	CH.C.L.E	22/02/2016	

laborado por:	CH.C.L.E	Fecha:	13/01/2016
Revisado por:	0.E.W.V	Fecha:	13/01/2016

MEMORÁNDUM DE PLANEACIÓN

MP 1/4

ENTIDAD:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote
TIPO DE TRABAJO:	Auditoría Informática a la Unidad de Tecnología Información Y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, Período 2014.
ÁREA:	Unidad de Tecnologías Información y Comunicación
PERÍODO:	Del 01 de Enero al 31 de Diciembre del 2014
RESPONSABLE:	Chimbo Caizaguano Luis Ernesto

1. ANTECEDENTES

En el Gobierno Autónomo Descentralizado Municipal Cantón Guamote, no se ha realizado una Auditoría Informática en la unidad de tecnología información y comunicación.

La auditoría Informática en el Gobierno Autónomo Descentralizado Municipal Cantón Guamote, se efectuará de conformidad con la Orden de Trabajo N°. 0001-GADMCG emitida por el Ing. Oscar Omar Espíndola Lara, Ing. Wilson Antonio Velasteguí Ojeda, en calidad de Director y Miembro del tribunal de trabajo de titulación respectivamente.

2. MOTIVO DE LA AUDITORÍA

La ejecución de la Auditoría Informática a la unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal Cantón Guamote, se llevará a efecto conforme la Orden de Trabajo N°. 0001-GADMCG, emitida por el por Ing. Oscar Omar Espíndola Lara Ing. Wilson Antonio Velasteguí Ojeda, en calidad de Director y Miembro del tribunal de Trabajo de Titulación respectivamente; y, conforme a un trabajo práctico previo a la obtención del Título de Ingeniería en Contabilidad y Auditoría; por esta razón se efectuará la Auditoria cumpliendo con los parámetros establecidos, normas reglamentarias, procedimientos necesarios de acuerdo a las condiciones del estudio, consecutivamente medir el nivel de cumplimiento de las Normas de Control Interno Emitidas Por la Contraloría General del Estado y emitir un Informe

con conclusiones y Recomendaciones que puedan contribuir con la consecución de metas y objetivos planteados.

3. OBJETIVOS DE LA AUDITORÍA

Realizar auditoría informática a la unidad de tecnología información y comunicación del gobierno autónomo descentralizado municipal del cantón Guamote, evaluar la seguridad lógica, seguridad física, el uso y administración de las Tics, en concordancia a las Normas de Control Interno Emitidas por la Contraloría General del Estado determinando así el grado de cumplimiento de dichas normas.

4. ALCANCE DE LA AUDITORÍA

La Auditoría Informática a la Unidad de Tecnología Información y Comunicación se realizara al Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, cuyo alcance comprende el período entre el 01 de Enero al 31 de Diciembre del 2014.

5. LOCALIZACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE

El Cantón Guamote se encuentra ubicado en la parte central del callejón interandino, al sur de Quito, a 50 Km de Riobamba, constituye el segundo cantón más extenso de los que integran la Provincia de Chimborazo.

Se encuentra a una altitud que va desde los 2600 m.s.n.m. hasta 4500 m.s.n.m., su temperatura media anual es de 13,7°C, constituyendo dos tipos de clima: invierno húmedo frío en los meses de octubre a mayo y verano, cálido, seco, ventoso de junio a septiembre. La precipitación es de 683,3 mm.

MISIÓN, VISIÓN, OBJETIVOS, VALORES Y PRINCIPIOS

Misión

Ser un Municipio en desarrollo permanente, sostenible, ofreciendo servicios básicos de calidad, impulsando el desarrollo local a niveles competitivos, con relaciones y trabajos socioculturales fortalecidos, conciencia ambiental y turística orientada a condiciones de vida óptima, donde la imagen del cantón, su ornato, presentación y cultura promuevan la identificación y el aprovechamiento de unidad cantonal que

toma decisiones concertadas y equitativas , respetando a la pacha mama y alcanzando el buen vivir.

Visión

El Cantón Guamote para el año 2026 será el eje del desarrollo nacional con una producción agropecuaria, turística competitiva y sostenible que garantice la calidad de vida de sus habitantes, en un ambiente sano, seguro y ecológicamente equilibrado, con una economía dinámica y solidaria.

Objetivos

- Mejorar los servicios de salud y educación mediante la readecuación, construcción y equipamiento de los centros educativos y las unidades operativas de salud en las tres parroquias del cantón.
- Ampliar la cobertura del servicio de agua potable en la cabecera cantonal y sus comunidades hasta el año 2017.
- Disminuir las enfermedades infecto-contagiosas en el cantón mediante la construcción de las Unidades básicas de Salud en las Comunidades del Cantón Guamote.
- Ampliar la cobertura de las unidades básicas de salud en las comunidades del Cantón.
- Prevenir y mitigar la contaminación ambiental mediante la aplicación de normas estándares de manejo, disposición y tratamiento de residuos sólidos domiciliarios y hospitalarios.

Valores

- **Equidad**, en las relaciones y percepciones, en la distribución de los recursos en situaciones sociales y profesionales.
- **Compromiso**, de la institución frente a sus miembros y usuarios
- **Lealtad**, como una obligación de fidelidad que un sujeto o ciudadano le debe a la institución.
- **Integridad**, como sinónimo de rectitud, honradez en las responsabilidades asignadas que generen confianza.

Principios

El gobierno Municipal, además de los principios constitucionales, se regirá por los siguientes principios.

- **Ética del buen vivir**, considerada como la satisfacción de las necesidades básicas de la población en los territorios, a través de los procesos de generación de riqueza que resulten sostenible en el tiempo.
- **Prevalencia de interés colectivo**, pensaba como la necesidad y urgencia de crear una sociedad más justa y más libre en todos los órdenes. Ampliar fortalecer y extender la justicia social, los derechos democráticos y las bondades del desarrollo tecnológico al mayor número de seres humanos.
- **Honestidad y transparencia**, considerada como una honestidad, significa generar confianza y transparencia y expresa conciencia de las cosas para una auténtica vida comunitaria, que desecha la corrupción.
- **Responsabilidad Social**, Implica que la sociedad sea participe de los beneficios del desarrollo, que mantenga relaciones justas y solidaridad, que le permita acceder y controlar recurso, tener poder de decisión y negociación; además que recibe beneficios acordes con su dispendio, trabajo realizado y riesgo asumido.
- **Solidaridad**, es una característica de la sociabilidad que inclina al hombre a sentirse unido a sus semejantes y a la cooperación con ellos.

6. BASE LEGAL INSTITUCIONAL

En el año de 1.944 Guamote cristaliza su cantonización que desde hace mucho tiempo atrás se venía gestionando, para lo cual se conformó una directiva. Con esta ayuda la delegación, había conseguido el decreto de cantonización de Guamote, con fecha primero de agosto de 1.944. El presidente de la República Dr. José María Velasco Ibarra, mediante el decreto No 606, Art. 1., establece: "Constituyese en la Provincia de Chimborazo un nuevo cantón con el Nombre de Guamote, que comprenderá las parroquias de Guamote y Cebadas, esta última perteneciente al cantón Riobamba y de las parroquias que el nuevo cantón crease". En la actualidad el cantón Guamote está integrado por tres parroquias: La Matriz que lleva su mismo nombre y dos parroquias rurales Cebadas y Palmira.

El Gobierno Autónomo Descentralizado Municipal de Cantón Guamote se basa en las siguientes las normativas:

- Constitución Política de la República del Ecuador
- Ley Orgánica de la Contraloría General del Estado
- Código Orgánico de Organización Territorial Autonomía y Descentralización
- Ley de Presupuesto del Sector Público
- Ley Orgánica de Servicio 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 / Ministerio de Finanzas
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de la Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos
- Código de Trabajo
- Ley Orgánica del Sistema Nacional de Contratación Pública.

7. FACULTADES DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE

- Planificar el desarrollo cantonal y formular los correspondientes planes de ordenamiento territorial, de manera articulada con la planificación nacional, regional, provincial y parroquial, con el fin de regular el uso y la ocupación del suelo urbano y rural.
- Ejercer el control sobre el uso y ocupación del suelo en el cantón.
- Planificar, construir y mantener la vialidad urbana.
- Prestar los servicios públicos de agua potable, alcantarillado, depuración de aguas residuales, manejo de desechos sólidos, actividades de saneamiento ambiental y aquellos que establezca la ley.
- Crear, modificar o suprimir mediante ordenanzas, tasas y contribuciones especiales de mejoras.
- Planificar, regular y controlar el tránsito y el transporte público dentro de su territorio cantonal.

- Planificar, construir y mantener la infraestructura física y los equipamientos de salud y educación, así como los espacios públicos destinados al desarrollo social, cultural y deportivo, de acuerdo con la ley.
- Preservar, mantener y difundir el patrimonio arquitectónico, cultural y natural del cantón y construir los espacios públicos para estos fines.
- Formar y administrar los catastros inmobiliarios urbanos y rurales.
- Delimitar, regular, autorizar y controlar el uso de las playas de mar, riberas y lechos de ríos, lagos y lagunas, sin perjuicio de las limitaciones que establezca la ley.
- Gestionar los servicios de prevención, protección, socorro y extinción de incendios.
- Gestionar la cooperación internacional para el cumplimiento de sus competencias.

8. RECURSO UTILIZADO

Recurso Humano

SUPERVISOR 1	Ing. Oscar Omar Espíndola Lara
SUPERVISOR 2	Ing. Wilson Antonio Velasteguí Ojeda
AUDITOR	Luis Ernesto Chimbo Caizaguano

Recursos Materiales

- Bicolor
- Resma de Papel Bond
- Esferos gráficos
- Archivadores

Recursos Financieros

- El investigador/auditor asume el financiamiento total de la investigación.

Recurso Tecnológico

- Computador
- Internet
- Flash Memory
- Cámara Digital

9. Tiempo Estimado

La presente auditoría informática se efectuara en un período de 90 días a partir del 01 de Diciembre del 2014, en donde se realizó:

Luis Ernesto Chimbo Caizaguano
ELABORADO POR

Ing. Oscar Espíndola e Ing. Wilson Velasteguí
REVISADO POR

		CUESTIONARIO DE CONTROL INTERNO			FASE II	C.C.I 1/9
Entidad:		Gobierno Autónomo Descentralizado Municipal del Cantón Guamote				
Tipo de Auditoría:		Auditoría Informática				
Componente:		Ambiente de Control				
Objetivo:		Comprobar si el GAD Municipal de Guamote implanta un ambiente organizacional referente a procesos de integridad y valores éticos, conducta y reglas para concientizar a los funcionarios de la Institución.				
N°	Preguntas	Respuesta y Ponderación			Observación	
		Si	No	N/A		
1	¿La alta dirección, ha establecido los principios valores éticos como parte de la cultura organizacional?	✓	10			
2	¿Existe un código de ética en la entidad?			✓	10	No se ha realizado un Código de Ética.
3	¿Toma la alta dirección acciones disciplinarias apropiadas cuando existe desvío de políticas o violaciones del código de ética?	✓	10			
4	¿Se utiliza el plan presupuestario como una herramienta de control para la Unidad de TIC?	✓	10			
5	¿Se ha elaborado un plan de capacitación para el nuevo personal?			✓	10	La capacitación para el nuevo personal no se ha elaborado.
6	¿Existe delegación de autoridad y responsabilidad por escrito sobre las disposiciones legales, normativas y reglamentos vigentes?	✓	10			
7	¿Existen sistemas de información computarizada para el registro y control de las operaciones?	✓	10			
		Elaborado por:		CH.C.L.E	Fecha:	15/02/2016
		Revisado por:		O.E.W.V	Fecha:	15/02/2016

8	¿Los funcionarios tienen definido los accesos a los sistemas e información?	✓	10				
TOTAL			60		20		

NC = Nivel confianza

NR = Nivel de riesgo

CT = confianza total

PT = Ponderación Total

$NC = \frac{CT}{PT} * 100$ $NC = \frac{60}{80} * 100$ $NC = 75\%$

$NR = 100 - NC$ $NR = 100 - 75$ $NR = 25$

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO ✓
76-100	ALTO	ALTO

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente Ambiente de Control se obtiene un nivel de confianza del 75% equivalente a rango medio y un nivel de riesgo del 25% equivalente a rango bajo

Elaborado por:	CH.C.LE	Fecha:	15/02/2016
Revisado por:	O.E.W.V	Fecha:	15/02/2016

		CUESTIONARIO DE CONTROL INTERNO			FASE II	CCI 2/9
Entidad:		Gobierno Autónomo Descentralizado Municipal del Cantón Guamote				
Tipo de Auditoría:		Auditoría Informática				
Componente:		Evaluación del Riesgo				
Objetivo:		Determinar si las autoridades del GAD Municipal de Guamote ponen énfasis en controles preventivos y administrativos.				
Nº	Preguntas	Respuesta y Ponderación			Observación	
		Si	No	N/A		
1	¿El personal conoce todas las aplicaciones y el manejo del sistema?	✓ 10				
2	¿Existe un plan para disminuir el riesgo?	✓ 10				
3	¿Se encuentran identificados los riesgos internos como externos que podrían interferir en que los objetivos sean cumplidos?		✓ 10		No se tiene definidos los riesgos que afectan en el cumplimiento de los objetivos.	
4	¿Las transacciones de la entidad se respaldan con documentos originales y fotocopias?	✓ 10				
5	¿El acceso a los módulos y utilización del sistema es limitados solo a personas autorizadas?	✓ 10				
TOTAL		40	10			

NC = Nivel confianza
NR= Nivel de riesgo

CT = confianza total
PT = Ponderación Total

$$NC = \frac{CT}{PT} * 100 \quad NC = \frac{40}{50} * 100 \quad NC = 80\% \quad NR = 100 - NC \quad NR = 100 - 80 \quad NR = 20\%$$

Elaborado por:	CH.C.LE	Fecha:	15/02/2016
Revisado por:	O.E.W.V	Fecha:	15/02/2016

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO
76-100	ALTO	ALTO ✓

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente Evaluación del Riesgo se obtiene un nivel de confianza del 80% equivalente a rango alto y un nivel de riesgo del 20% equivalente a rango bajo

Elaborado por:	CH.C.L.E	Fecha:	15/02/2016
Revisado por:	O.E.W.V	Fecha:	15/02/2016

 ASERCONP <small>Asesoría Fiscal Contable y Laboral</small>	CUESTIONARIO DE CONTROL INTERNO	FASE II	C.C.I.3/9 S.L. 1
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote		
Tipo de Auditoría:	Auditoría Informática		
Componente:	Actividades para el control / Seguridad Lógica		
Objetivo:	Comprobar la existencia y aplicación de las medidas para contrarrestar las amenazas que pueda afectar la integridad de los datos e información de los equipos.		

No	Preguntas	Respuesta y Ponderación			Observaciones	
		SI	NO	N/A		
1	¿Los equipos de cómputos tienen contraseña para iniciar sus actividades?	✓	10			
2	¿La modificación de las contraseñas es de manera permanente?	✓	10			
3	¿El sistema operativo de los ordenadores cumple con las características necesarias para el desarrollo de las actividades?	✓	10			
4	¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?			✓	10	No tienen normas de seguridad física
5	¿Existen procedimientos de asignación y distribución de contraseñas?	✓	10			
6	¿Existen procedimientos de notificación y gestión de incidencias?			✓	10	No tienen procedimientos de notificación
7	¿Posee una contraseña personal para el uso del sistema de la entidad?	✓	10			
8	¿Existe el adecuado almacenamiento de respaldos con información crítica y sensible en lugares externos a la organización?	✓	10			
		Elaborado por:	CH.C.LE	Fecha:	16/02/2016	
		Revisado por:	0.E.W.V	Fecha:	16/02/2016	

9	¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos e información?			✓	10		Los usuarios desconocen la realización de copias de seguridad.
10	¿Para instalar nuevos software en los equipos de cómputos realizan con autorización?	✓	10				
11	¿Se realizan controles periódicos para verificar el cumplimiento de procesos y normas?			✓	10		No tienen controles de cumplimiento de procedimiento
12	¿Los acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones encomendada?			✓	10		No existe un control de los claves
13	¿Tiene conocimiento de todo el software instalado en los equipos de cómputo?	✓	10				
14	¿Cree que necesita una capacitación para el uso de sistemas nuevos en la entidad?	✓	10				
15	¿Se realizan auditorías a los archivos de seguridad?			✓	10		Nunca realizo auditoria
16	¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	✓	10				
TOTAL		100			60		

NC = Nivel confianza

CT = confianza total

NR= Nivel de riesgo

PT = Ponderación Total

NC= $\frac{CT}{PT} * 100$ NC= $\frac{60}{100} * 100$ NC= 60%. NR= 100 - NC NR= 100 - 60

NR=40%

Elaborado por:	CH.C.LE	Fecha:	16/02/2016
Revisado por:	O.E.W.V	Fecha:	16/02/2016

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO ✓
76-100	ALTO	ALTO

ANÁLISIS: Al aplicar cuestionario de control interno a la seguridad lógica se obtiene un nivel de confianza del 60 % equivalente a rango medio y un 40% de nivel de riesgo equivalente a un rango bajo.

Elaborado por:	CH.C.LE	Fecha:	16/02/2016
Revisado por:	O.E.W.V	Fecha:	16/02/2016

		CUESTIONARIO DE CONTROL INTERNO		FASE II	C.C.I. 4/9 S.F. 1								
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote												
Tipo de Auditoría:	Auditoría Informática												
Componente:	Actividades para el control/ Seguridad Física												
Objetivo:	Evaluar el control interno de las seguridades físicas de la UTIC del GAD Guamote, así como la evaluación de estándares y procedimientos que en él se aplica en caso de un desastre, para evitar dichas emergencias y verificar con que seguridad cuenta la información de la organización.												
No	Preguntas	Respuesta y Ponderación			Observaciones								
		SI	NO	N/A									
1	¿El departamento donde usted trabaja tiene seguridades contra desastres naturales?	✓	10										
2	¿Existe un plan de evacuación para el departamento?	✓	10										
3	¿Existe personal de vigilancia en la institución?	✓	10										
4	¿Se registra el acceso al área informática de personas ajenas a la dirección?			✓	10	No registran el acceso del personal							
5	¿El personal ajeno a operación sabe qué hacer en el caso de un incendio?	✓	10										
6	¿Existe un sistema de ventilación adecuado para los equipos e instalaciones?			✓	10	No tienen ventiladores							
7	Existen en el departamento extintores de fuego	✓	10										
8	¿Se vigilan la moral y comportamiento del personal con el fin de mantener una buena imagen y evitar un posible fraude?			✓	10	No tienen código de ética							
9	Se ha adiestrado al personal para el manejo de extintores	✓	10										
<table border="1" style="margin-left: auto;"> <tr> <td>Elaborado por:</td> <td>CH.C.LE</td> <td>Fecha:</td> <td>17/02/2016</td> </tr> <tr> <td>Revisado por:</td> <td>O.E.W.V</td> <td>Fecha:</td> <td>17/02/2016</td> </tr> </table>						Elaborado por:	CH.C.LE	Fecha:	17/02/2016	Revisado por:	O.E.W.V	Fecha:	17/02/2016
Elaborado por:	CH.C.LE	Fecha:	17/02/2016										
Revisado por:	O.E.W.V	Fecha:	17/02/2016										

10	¿Existe un inventario de los soportes existentes?	✓	10				
11	¿Dicho inventario incluye las copias de seguridad?	✓	10				
12	¿Existe salida de emergencia?			✓	10		
13	¿Se ha adiestrado a todo el personal en la forma en que se debe desalojar las instalaciones en caso de emergencia?	✓	10				
14	¿Se han tomado medidas para minimizar la posibilidad de fuego?	✓	10				
15	¿Existen procedimientos para la realización de las copias de seguridad?			✓	10		Los usuarios nunca hacen
16	¿Se hace mantenimiento periódico a los equipos de cómputo?	✓	10				
17	¿Los cables de red, switch, hubs, etc. se encuentran debidamente etiquetados?	✓	10				
18	¿Se limpia con frecuencia el polvo acumulado en lugares de difícil acceso para evitar daños a los equipos?	✓	10				
19	¿Existe una persona responsable de la seguridad informática en su departamento?	✓	10				
20	¿Hay procedimientos que aseguran la realización de copias de todos aquellos datos que han experimentado algún cambio en su contenido?	✓	10				
21	¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?	✓	10				
22	Los extintores automáticos son activados por detectores automáticos	✓	10				
				Elaborado por:	CH.C.LE	Fecha:	17/02/2016
				Revisado por:	O.E.W.V	Fecha:	17/02/2016

23	¿Los interruptores de energía eléctrica están debidamente protegidos, etiquetados, sin obstáculos para alcanzarlos?	✓	10				
24	¿Existen controles sobre el acceso físico a las copias de seguridad?	✓	10				
TOTAL			190	50			

NC = Nivel confianza

CT = confianza total

NR= Nivel de riesgo

PT = Ponderación Total

$$NC = \frac{CT}{PT} * 100 \quad NC = \frac{190}{240} * 100 \quad NC = 79\% \quad NR = 100 - NC \quad NR = 100 - 60 \quad NR = 21\%$$

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO
76-100	ALTO	ALTO ✓

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente seguridad física se obtiene un nivel de confianza del 79% equivalente a rango alto y un nivel de riesgo del 21% equivalente a rango bajo.

Elaborado por:	CH.C.LE	Fecha:	17/02/2016
Revisado por:	O.E.W.V	Fecha:	17/02/2016

 ASERCOMP <small>Asesoría Fiscal, Contable y Laboral</small>	CUESTIONARIO DE CONTROL INTERNO	FASE II	C.C.I. 5/9 T.I. 1
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote		
Tipo de Auditoría:	Auditoría Informática		
Componente:	Actividades para el control / Tecnologías de Información		
Objetivo:	Conocer aspectos relacionados a la utilización y aprovechamiento de los recursos informáticos a fin de determinar si los equipos disponibles son actualizados y si existen políticas establecidas para su utilización.		

No	Preguntas	Respuesta y Ponderación			Observaciones	
		SI	NO	N/A		
1	¿Existe un tiempo establecido para la solución de problemas presentados en los equipos informáticos?	✓	10			
2	¿Disponen de un plan logístico para el mantenimiento preventivo/correctivo para el hardware e instalaciones de los equipos?	✓	10			
3	¿Cuenta con plan logístico para el mantenimiento preventivo /correctivo del software en la entidad?	✓	10			
4	¿Se protegen con planes de limpieza adecuados a fin de evitar la acumulación de polvo en los equipos Informáticos?	✓	10			
5	¿Los planes de mantenimiento de los equipos se cumplen a cabalidad?			✓	10	Se hace cuando tiene algún problema
6	¿Existen procedimientos para reparar daños o fallas existentes en los equipos de la entidad?	✓	10			
7	¿Disponen de mobiliario suficiente para la operatividad y desenvolvimiento de los sistemas informáticos en la entidad?			✓	10	Espacio muy reducido

Elaborado por:	CH.C.LE	Fecha:	17/02/2016
Revisado por:	O.E.W.V	Fecha:	17/02/2016

8	¿Existe políticas que norme el trabajo del personal que labora en esta Unidad?	✓	10				
9	¿Disponen de políticas, manuales y procesos de utilización y uso de los equipos informáticos de la institución?			✓	10		No hay un manual de uso
10	¿La Institución cuenta con equipos suficientes para su operatividad?	✓	10				
11	¿Disponen de software utilitario que sea de ayuda y que estén disponibles para los empleados y funcionarios de la entidad?	✓	10				
12	¿Poseen normas, instrucciones y procedimientos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitios WEB en base a las disposiciones legales?			✓	10		No tienen guía de configuración
13	¿Los softwares disponibles en los ordenadores de la institución contribuyan a las actividades diarias?	✓	10				
14	¿La información transmitida por internet es controlada por la UTIC?	✓	10				
15	¿Existe software ofimática actualizado que estén disponibles para los empleados y funcionarios de la institución?	✓	10				
TOTAL			110		40		

Elaborado por:	CH.C.L.E	Fecha:	17/02/2016
Revisado por:	O.E.W.V	Fecha:	17/02/2016

NC = Nivel confianza
NR= Nivel de riesgo

CT = confianza total
PT = Ponderación Total

$$NC = \frac{CT}{PT} * 100 \quad NC = \frac{110}{150} * 100 \quad NC = 73\% \quad NR = 100 - NC \quad NR = 100 - 73 \quad NR = 27\%$$

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO ✓
76-100	ALTO	ALTO

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente tecnologías de información se obtiene un nivel de confianza del 73% equivalente a rango medio y un nivel de riesgo del 27% equivalente a rango bajo

Elaborado por:	CH.C.LE	Fecha:	17/02/2016
Revisado por:	O.E.W.V	Fecha:	17/02/2016

 ASERCOMP <small>Asesoría Fiscal Contable y Laboral</small>		CUESTIONARIO DE CONTROL INTERNO			FASE II	C.C.I.6/9 G. I. 1
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote					
Tipo de Auditoría:	Auditoría Informática					
Componente:	Actividades para el control/ Gestión Informática					
Objetivo:	Evaluar procedimientos aplicados a la gestión que se realiza la Unidad de TIC.					
No	Preguntas	Respuesta y Ponderación				Observaciones
		SI	NO	N/A		
1	¿Se desarrolla regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión, visión y metas de la institución?	✓	10			
2	¿Dispone la institución de un plan Estratégico de Tecnología de Información y comunicación?			✓	10	
3	¿Existe un comité de TIC específica?			✓	10	
4	¿Las tareas y actividades plasmadas en el plan tienen la correspondiente y adecuada asignación de recursos?	✓	10			
5	¿Existen procedimientos para la adquisición de bienes y servicios?			✓	10	Se lo hace por el portal
6	¿Disponen estándares de funcionamiento, procedimientos y descripciones de puestos de trabajo adecuados?	✓	10			
7	¿Disponen de un plan operativo anual para las TIC?			✓	10	solo el POA del municipio
8	¿Existe un cronograma de cumplimiento de metas?			✓	10	No está establecido
9	¿Cuentan con un presupuesto económico para la adquisición de nuevos bienes?	✓	10			
10	¿La unidad encargada de la tecnología información y comunicación se encuentra dentro de la estructura organizacional de la entidad?	✓	10			
		Elaborado por:	CH.C.LE	Fecha:	18/02/2016	
		Revisado por:	O.E.W.V	Fecha:	18/02/2016	

11	¿Se comprueban los resultados con datos reales?			✓	10		
12	¿Existe un organigrama con la estructura de organización del área?	✓	10				
13	¿El presupuesto está en concordancia con los objetivos a cumplir?	✓	10				
14	¿Existen procedimientos para vigilar y determinar permanentemente la normativa aplicable?			✓	10		No aplican la norma de C. I.
TOTAL			70		70		

NC = Nivel confianza

CT = confianza total

NR= Nivel de riesgo

PT = Ponderación Total

$$NC = \frac{CT}{PT} * 100 \quad NC = \frac{50}{140} * 100 \quad NC = 50\% \quad NR = 100 - NC \quad NR = 100 - 50 \quad NR = 50\%$$

RANGO	RIESGO	CONFIANZA
1-50	BAJO	BAJO
51-75	MEDIO ✓	MEDIO ✓
76-100	ALTO	ALTO

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente Gestión Informática se obtiene un nivel de confianza del 50% equivalente a rango bajo y un nivel de riesgo del 50% equivalente a rango medio.

Elaborado por:	CH.C.LE	Fecha:	18/02/2016
Revisado por:	O.E.W.V	Fecha:	18/02/2016

	CUESTIONARIO DE CONTROL INTERNO	FASE II	C.C.I.7/9 G.U. 1
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote		
Tipo de Auditoría:	Auditoría Informática / Gestión de Usuarios		
Componente:	Actividades para el control		
Objetivo:	Evaluar procedimientos aplicados a la gestión que se realiza en la Unidad de Tecnologías Información y Comunicación.		

No	Preguntas	Respuesta y Ponderación			Observaciones	
		SI	NO	N/A		
1	¿Existen procedimientos determinadas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	✓	10			
2	¿Los programas nuevos son revisados y aprobados antes de ponerlos en funcionamiento?			✓	10	No avisan antes de instalar
3	¿Cuenta con políticas de cambio de claves de acceso durante un determinado tiempo?	✓	10			
4	¿Existe las seguridades apropiadas para evitar daños o alteraciones en el sistema por terceras personas?			✓	10	
5	¿Disponen de procedimientos adecuados para mantener la documentación al día?	✓	10			
6	Por fallos de hardware, software. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	✓	10			
7	¿Al ejecutar actividades, realiza usted respaldos de la información generada?	✓	10			
8	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?			✓	10	No tienen establecido
9	¿Se aprueban solicitudes de nuevas aplicaciones por los usuarios?			✓	10	Solo cuando es necesario

Elaborado por:	CH.C.LE	Fecha:	18/02/2016
Revisado por:	O.E.W.V	Fecha:	18/02/2016

10	¿Disponen de personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?			✓	10		Los usuarios lo hacen por su cuenta
11	¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	✓	10				
TOTAL			50		60		

NC = Nivel confianza
NR= Nivel de riesgo

CT = confianza total
PT = Ponderación Total

$$NC = \frac{CT}{PT} * 100 \quad NC = \frac{50}{110} * 100 \quad NC = 45\% \quad NR = 100 - NC \quad NR = 100 - 45 \quad NR = 55\%$$

RANGO	RIESGO	CONFIANZA
1-50	BAJO	BAJO ✓
51-75	MEDIO ✓	MEDIO
76-100	ALTO	ALTO

ANÁLISIS: Una vez realizada las encuestas a los funcionarios de las diferentes unidades de GADMC Guamote se determina un nivel de confianza del 45% equivale a un rango bajo y un nivel de riesgo del 55% equivalente a un rango medio.

Elaborado por:	CH.C.L.E	Fecha:	18/02/2016
Revisado por:	O.E.W.V	Fecha:	18/02/2016

		CUESTIONARIO DE CONTROL INTERNO			FASE II	C.C.I.8/9
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote					
Tipo de Auditoría:	Auditoría Informática					
Componente:	Información y comunicación.					
Objetivo:	Analizar la seguridad y confiabilidad de la información interna y externa generada por la entidad.					
No	Preguntas	Respuesta y Ponderación			Observaciones	
		SI	NO	N/A		
1	¿La información interna y externa generada por la entidad es remitida previamente los niveles correspondientes para su aprobación?	✓	10			
2	¿El contenido de la información es el apropiado y confiable?			✓	10	Es propenso a daños
3	¿El sistema cuenta con medidas de seguridad que alcancen a las entradas de procesos, almacenamiento y salida de datos?	✓	10			
4	¿El acceso a los módulos y utilización del sistema es limitados solo a personas autorizadas?	✓	10			
TOTAL			30		10	

NC = Nivel confianza
NR= Nivel de riesgo

CT = confianza total
PT = Ponderación Total

$$NC = \frac{CT}{PT} * 100 \quad NC = \frac{30}{40} * 100 \quad NC = 75. \quad NR = 100 - NC \quad NR = 100 - 75 \quad NR = 25$$

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO ✓
76-100	ALTO	ALTO

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente Información y Comunicación se obtiene un nivel de confianza del 75% equivalente a rango medio y un nivel de riesgo del 25% equivalente a rango bajo.

Elaborado por:	CH.C.L.E	Fecha:	18/02/2016
Revisado por:	O.E.W.V	Fecha:	18/02/2016

	CUESTIONARIO DE CONTROL INTERNO	FASE II	C.C.I. 9/9
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote		
Tipo de Auditoría:	Auditoría Informática		
Componente:	Seguimiento		
Objetivo:	Determinar si las máximas autoridades ponen énfasis en el proceso de supervisión y monitoreo en la entidad.		

No	Preguntas	Respuesta y Ponderación			Observaciones
		SI	NO	N/A	
1	¿Se considera los informes provenientes de fuentes externas para valorar y mejorar el sistema de control interno?		✓	10	No lo hacen con evidencias
2	¿Se comunican las deficiencias al máximo autoridad de la entidad?	✓	10		
3	¿Se efectúa un seguimiento de cumplimiento a las recomendaciones que permita superar las deficiencias?	✓	10		
	TOTAL		20	10	

NC = Nivel confianza
NR= Nivel de riesgo

CT = confianza total
PT = Ponderación Total

NC= $\frac{CT}{PT} * 100$ NC= $\frac{20}{30} * 100$ NC= 66,67%. NR= 100 - NC NR= 100 - 66.67 NR=33,33%.

RANGO	RIESGO	CONFIANZA
1-50	BAJO ✓	BAJO
51-75	MEDIO	MEDIO ✓
76-100	ALTO	ALTO

ANÁLISIS: Realizado la ponderación del cuestionario del control interno pertinente a componente Seguimiento se obtiene un nivel de confianza del 66.67% equivalente a rango medio y un nivel de riesgo del 33.33% equivalente a rango bajo.

Elaborado por:	CH.C.LE	Fecha:	19/02/2016
Revisado por:	O.E.W.V	Fecha:	19/02/2016

		VERIFICACIÓN FÍSICA UTIC		FASE II	V.F. 10/10
Entidad:		Gobierno Autónomo Descentralizado Municipal del Cantón Guamote			
Tipo de Auditoría:		Auditoría Informática			
Objetivo:		Determinar medidas de seguridad para las TICs			
Tipologías	Complemento	Cumple		Observaciones	
		si	No		
Seguridad	Existe una persona que custodie los bienes de la unidad TIC.	✓		El guardia del municipio	
	Existe un circuito cerrado de cámaras de vigilancia.		✓		
	El espacio físico donde se encuentra la UTIC está en buenas condiciones.		✓	Espacio inadecuado	
	Existen adecuadas salidas de emergencia.		✓		
	Existen extintores contra incendios.	✓			
	Existen alarmas contra incendios y/o robos.		✓		
Accesos	Existe un adecuado control de acceso para funcionarios y trabajadores de la unidad.	✓		Solo el reloj de entrada	
	Existen restricciones a usuarios externos.		✓		
	Las puertas y ventanas cuentan con las debidas seguridades.	✓			
Sistema Eléctrico	El conjunto de cables de la institución se encuentra oculto y debidamente identificado.	✓		hay cables sin canaletas	
	Existen reguladores de voltaje que salvaguarden los equipos de la institución.	✓			
	Los puntos de iluminación son adecuados	✓			
Otros	El sistema de ventilación es adecuado		✓		
	Los equipos tecnológicos e instalaciones en general cuentan con una póliza de seguros.		✓	No se entrega contrato	
	Existen las herramientas e instalaciones para dar mantenimiento a los equipos.		✓		

Elaborado por:	C.L.C.M	Fecha:	19/02/2016
Revisado por:	A.G.I.P	Fecha:	19/02/2016

Cuadro No. 9: EVALUACIÓN DE LA CONFIANZA Y RIESGO

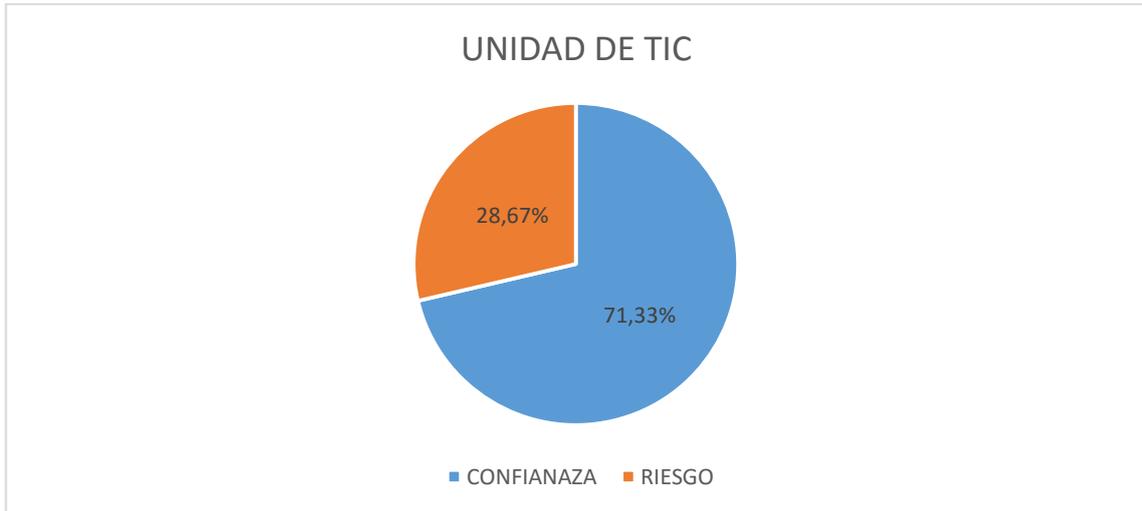
 ASERCONP <small>Asesoría Fiscal Contable y Laboral</small>		EVALUACIÓN DE LA CONFIANZA Y RIESGO		FASE II	MP 1
MATRIZ DE LA CONFIANZA Y RIESGOS DE LOS COMPONENTES DEL COSO					
COMPONENTES DEL CONTROL INTERNO COSO		NIVEL DE CONFIANZA	NIVEL DEL RIESGO		
1. AMBIENTE DE CONTROL		75%	25%		
2. EVALUACIÓN DEL RIESGO		80%	20%		
3. ACTIVIDADES DE CONTROL					
3.1	Seguridad Lógica	60%	40%		
3.2.	Seguridad Física	79%	21%		
3.3.	Tecnología de Información	73%	27%		
3.4.	Gestión Informática	42.86%	57.14%		
3.5	Gestión de Usuarios	45%	55%		
TOTAL DE CONFIANZA Y RIESGO ACTIVIDADES DE CONTROL		59,97%	40,03%		
4. INFORMACIÓN Y COMUNICACIÓN		75%	25%		
5. SEGUIMIENTO Y MONITOREO		66,67%	33,33%		
TOTAL DE CONFIANZA Y RIESGO DE LOS 5 COMPONENTES DEL COSO		71,33%	28,67%		
MATRIZ DE PONDERACIÓN DE RIESGO Y CONFIANZA					
NIVEL DE CONFIANZA PONDERADA					
BAJO		MODERADO		ALTO	
15% - 50%		51% - 75% ✓		76% - 95%	
85% - 50%		49% - 25%		24% - 5% ✓	
ALTO		MODERADO		BAJO	
NIVEL DE RIESGO PONDERADA					
CONFIANZA = 71,33% MODERADO			RIESGO= 28,67% BAJO		

Fuente: Gobierno Autónomo Descentralizado Municipal de Cantón Guamote

Elaborado por: Luis Ernesto Chimbo Caizaguano

Elaborado por:	C.L.C.M	Fecha:	19/02/2016
Revisado por:	A.G.I.P	Fecha:	19/02/2016

GRÁFICO NO 1: TABULACIÓN DE LA MATRIZ DE CONFIANZA Y RIESGO



Fuente: Gobierno Autónomo Descentralizado Municipal de Cantón Guamote

Elaborado por: Luis Ernesto Chimbo Caizaguano

INTERPRETACIÓN:

Una vez aplicadas las encuestas a los componentes de Control Interno COSO I: Ambiente de Control, Control de Riesgo, Actividades de Control con sus subcomponentes Seguridad Lógica, Seguridad Física, Gestión Informática, Tecnologías de Información y Gestión Administrativa y realizado las ponderaciones respectivas se determina un nivel de confianza para la unidad de Tecnología Información y Comunicación de 71,33% MODERADO y un nivel de riesgo del 28,67%. BAJO.

Elaborado por:	C.L.C.M	Fecha:	19/02/2016
Revisado por:	A.G.I.P	Fecha:	19/02/2016

DEBILIDADES DE CONTROL INTERNO

M.R 1/2

**EVALUACIÓN DEL CONTROL INTERNO EN BASE A LAS NORMAS DE TECNOLOGÍAS DE INFORMACIÓN
EMITIDAS POR LA CONTRALORÍA GENERAL DEL ESTADO**

TABLA 10. MATRIZ DE DEBILIDADES IDENTIFICADAS EN LOS CUESTIONARIOS DE CONTROL INTERNO COSO

componentes	debilidad	acciones recomendadas	norma relacionada
Ambiente de Control	Los funcionarios conocen sus deberes y obligaciones basados en la Ley Orgánica de Servicio Público (LOSEP), pero la UTIC del Gobierno Autónomo Descentralizado Municipal de Cantón Guamote no cuenta con un Código de Ética formalmente establecido.	El Gobierno Autónomo Descentralizado Municipal de Cantón Guamote debe establecer y socializar un código de ética el cual contenga los valores y principios institucionales.	200-01 Integridad y valores éticos.
Evaluación de Riesgo	No tiene identificado los riesgos internos y externos que podrían interferir en cumplimiento de los objetivos de la Unidad.	La unidad de TIC del Gobierno Autónomo Descentralizado Municipal de Cantón Guamote deberá identificar los posibles riesgos internos y externos para cumplir con los objetivos establecidos.	410-11 Plan de contingencias.
Actividad de Control	Inexistencia de políticas y procedimientos que regulen las actividades relacionadas con las tecnologías de información.	El funcionario encargado de esta unidad debe establecer, documentar y difundir políticas y procedimientos que den los lineamientos necesarios a las actividades propias de esta unidad.	410-04 Políticas y Procedimientos.
	Inexistencia de planes de mantenimiento tanto preventivo y/o correctivo, así como también un inventario de control de bienes informáticos.	El jefe de la unidad de TIC deberá establecer planes de mantenimiento y levantar un inventario exacto de los bienes existentes en la unidad.	410-09 Mantenimiento y control de la infraestructura tecnológica.

Actividad de Control	Ausencia de mecanismos de seguridad necesario que protejan y salvaguarden la información que se procesa mediante los sistemas informáticos de la institución.	El jefe de la unidad de TIC debe establecer los mecanismos necesarios para salvaguardar la información de la institución.	410-10 seguridades de Tecnologías de Información.
	No cuenta con planes de contingencia que describan las acciones a tomar en caso de emergencia.	El Jefe de la unidad de tic deberá implementar planes de contingencia donde se describan las acciones a tomar en caso de emergencias suscitadas.	410-11 Plan de contingencias.
	Ausencia de mecanismos, cronogramas donde se evalúe el grado de contribución al cumplimiento de metas y objetivos institucionales.	El Jefe de la unidad de TIC deberá definir y ejecutar los mecanismos necesarios para medir el grado de contribución a la consecución de metas y objetivos institucionales.	410-13 Monitoreo y evaluación de los procesos y servicios.
	No cuenta con normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad.	El Jefe de la unidad de TIC deberá implementar normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos y sitios WEB de la institución.	410-14 Sitios web, servicios de internet e intranet.
	No dispone de planes de capacitación para los usuarios de las Tics.	El Alcalde de GADM Guamote conjuntamente con el Jefe de la unidad de TIC deberá proporcionar un plan de capacitación para todos los actores y usuarios de las tecnologías de información de la institución.	410-15 Capacitación Informática.
Seguimiento	No se considera los informes provenientes de fuentes externas para valorar y mejorar el sistema de control interno	La Unidad de Tecnología Información y Comunicación deberá considerar los informes provenientes de fuentes externos para mejorar el control interno.	600-01 Seguimiento.

FUENTE: Gobierno Autónomo Descentralizado Municipal del Cantón Guamote
ELABORADO: Luis Ernesto Chimbo Caizaguano

Elaborado por:	CH.C.LE	Fecha:	19/02/2016
Revisado por:	O.E.W.V	Fecha:	19/02/2016

INEXISTENCIA DE UN CÓDIGO DE ÉTICA INSTITUCIONAL

CONDICIÓN:

La Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no cuenta con un código de ética en el que establezca principios y valores, que constituya al buen uso de los recursos públicos.

CRITERIO:

La Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote debe cumplir con la Norma de Control Interno para las Entidades, Organismos del Sector Público N° 200-01 “INTEGRIDAD Y VALORES ÉTICOS”, en la que establece: Que, La integridad y los valores éticos son elementos esenciales del ambiente de control, la administración y el monitoreo de los otros componentes del control interno. La máxima autoridad y los directivos establecerán los principios y valores éticos como parte de la cultura organizacional para que perduren frente a los cambios de las personas de libre remoción; estos valores rigen la conducta de su personal, orientando su integridad y compromiso hacia la organización.

CAUSA:

La falta de cuidado en ciertos puntos importantes dentro de la municipalidad, da como respuesta a la inexistencia de un Código de ética, esto lleva a que los funcionarios de la institución no practiquen de forma adecuada los valores y principios establecidos por la municipalidad.

EFECTO:

Esto ocasiona que el personal de la municipalidad no se comprometa a actuar con voluntad, disciplina y profesionalismo.

Elaborado por:	CH.C.L.E	Fecha:	22/02/2016
Revisado por:	O.E.W.V	Fecha:	22/02/2016

CONCLUSIÓN:

La Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, no dispone de un código de ética expresamente establecido, los funcionarios simplemente tienen conocimiento de sus deberes y obligaciones basados en la ley orgánica de servicio público (LOSEP).

RECOMENDACIÓN:

Implantar un Código de ética, y realizar la difusión pertinente para dar a conocer a los funcionarios sobre la existencia y aplicación del mismo, para contribuir al buen uso de los recursos públicos. Los responsables del control interno determinarán y fomentarán la integridad y los valores éticos, para beneficiar el desarrollo de los procesos y actividades institucionales y establecerán mecanismos que promuevan la incorporación del personal a esos valores; los procesos de reclutamiento y selección de personal se conducirán teniendo presente esos rasgos y cualidades.

Elaborado por:	CH.C.LE	Fecha:	22/02/2016
Revisado por:	O.E.W.V	Fecha:	22/02/2016

NO TIENE DEFINIDO LOS RIESGOS QUE AFECTAN AL CUMPLIMIENTO DE LOS OBJETIVOS

CONDICIÓN:

La Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote no tiene definidos los posibles riesgos que afectan al cumplimiento de los objetivos planteados por la entidad.

CRITERIO:

La Unidad de Tecnología Información y Comunicación debe tener identificados los posibles riesgos que vayan afectar el cumplimiento de objetivos.

CAUSA:

Inobservancia del entorno externo e interno.

EFECTO:

No cumplimiento de objetivos propuestos por la unidad

CONCLUSIÓN:

La Unidad de TIC del GADM Cantón Guamote no tiene definidos los posibles riesgos que pueden afectar a la ejecución de los fines propuestos.

RECOMENDACIÓN:

La Unidad de TIC del GADM Cantón Guamote debe tener determinado tanto los riesgos externos como los riesgos internos para poder cumplir con las funciones establecidas.

Elaborado por:	CH.C.LE	Fecha:	22/02/2016
Revisado por:	0.E.W.V	Fecha:	22/02/2016

FALTA DE POLÍTICAS Y PROCEDIMIENTOS.

CONDICIÓN:

No establecen políticas y procedimientos que normen las actividades que se desarrolla en esta unidad.

CRITERIO:

La máxima autoridad y el Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote deben promover y establecer políticas y procedimientos que regulen las actividades relacionadas con las Tecnologías de Información, conforme establece la Norma de Control Interno 410-04, que corresponde a “Políticas y Procedimientos”.

CAUSA:

La máxima autoridad y el Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote no acatan ni aplican la ley establecida, puntualmente a la norma de control Interno, políticas y procedimientos.

EFECTO:

Desorganización, falta de control y lineamientos dentro de todas las actividades que se desarrollan en la Unidad de Tecnologías de Información del GADM Cantón Guamote, que deja en evidencia la vulnerabilidad de los datos, información e equipos Informáticos que posee la institución.

CONCLUSIÓN:

La Unidad de Tecnologías de Información del GADM Cantón Guamote, deja en evidencia la vulnerabilidad de los datos, información e equipos Informáticos que posee la institución.

RECOMENDACIÓN:

Implantar políticas y procedimientos que normen las actividades concernientes con las Tecnologías de Información, cumpliendo y aplicando la Norma de Control Interno 410-04, que concierne a “Políticas y Procedimientos, implantando así un adecuado control y lineamientos dentro de todas las actividades que se desarrollan en la unidad de TIC.

Elaborado por:	CH.C.LE	Fecha:	22/02/2016
Revisado por:	O.E.W.V	Fecha:	22/02/2016

INEXISTENCIA DE PLANES DE MANTENIMIENTO Y CONTROL DE INVENTARIO PARA LA UTIC.

CONDICIÓN:

Inexistencia de planes de mantenimiento correctivo/preventivo, así como también el control de inventario de los bienes existentes en la unidad.

CRITERIO:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote debe definir y ejecutar planes de mantenimiento para toda la infraestructura tecnológica, así como también levantar un inventario de los bienes existentes en la institución, conforme establece la Norma de Control Interno 410-09, que concierne a “Mantenimiento y control de la infraestructura tecnológica”.

CAUSA:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote no cumple la ley establecida, puntualmente a la norma control interno, Mantenimiento y control de la infraestructura tecnológica

EFEECTO:

Daños parciales o totales de la infraestructura tecnológica, pérdida de recursos, datos erróneos e inexactos en la existencia y control de bienes de la unidad.

CONCLUSIÓN:

Inexistencia de planes de mantenimiento, así como también el control de inventario de los bienes existentes en la unidad. El Jefe de la Unidad de TIC no definió ni ejecuta planes de mantenimiento para la infraestructura tecnológica, así como también no realiza el levantamiento de inventario de los bienes existentes en la institución

RECOMENDACIÓN:

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no se elabora ni aplica Planes de mantenimiento correctivo/preventivo, así como también el control de inventario de los bienes existentes en la unidad de tecnologías de información.

Elaborado por:	CH.C.L.E	Fecha:	22/02/2016
Revisado por:	O.E.W.V	Fecha:	22/02/2016

INEXISTENCIA DE MECANISMOS DE SEGURIDAD EN LA UNIDAD.

CONDICIÓN:

No se establecen los mecanismos necesarios que salvaguarden los medios Informáticos de la institución.

CRITERIO:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote debe establecer los mecanismos necesarios para que ayuden a salvaguardar los medios Informática de la institución, conforme establece la Norma de Control Interno 410-10, que corresponde a “Seguridad de Tecnologías de Información”

CAUSA:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO:

Pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos existente en la institución.

CONCLUSIÓN:

No se establecen los mecanismos necesarios que salvaguarden los medios Informáticos, El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente

RECOMENDACIÓN:

Implantar los mecanismos de seguridad necesarios que ayuden a salvaguardar los medios Informática de la institución, acatando y aplicando la Norma de Control Interno 410-10, que compete a “Seguridad de Tecnologías de Información”, evitando así pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos existente en la institución.

Elaborado por:	CH.C.LE	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

INEXISTENCIA DE PLANES DE CONTINGENCIA PARA LA UNIDAD.

CONDICIÓN:

No define planes de contingencia para que sean ejecutados en casos de emergencias que se susciten en la institución.

CRITERIO:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote debe establecer y definir planes de contingencias donde se describan los lineamientos a seguir en caso de emergencias suscitadas dentro de la institución, conforme establece la Norma de Control Interno 410-11, que concierne a “Plan de contingencias”.

CAUSA:

El Jefe de la unidad tecnológica del GADM Cantón Guamote no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO:

Inadecuada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado, que desemboca en pérdidas de información y operatividad de la unidad.

CONCLUSIÓN:

El jefe de la Unidad de TIC, no define planes de contingencia para que sean ejecutados en casos de emergencias, conforme establece la Norma de Control Interno 410-11, que concierne a “Plan de contingencias”.

RECOMENDACIÓN:

Delimitar planes de contingencias donde se detallen los lineamientos a seguir en caso de emergencias originadas dentro de la institución, cumpliendo y aplicando la Norma de Control Interno 410-11, que concierne a “Plan de contingencias”, para una apropiada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado, que llegue a pérdidas de información y operatividad de la unidad.

Elaborado por:	CH.C.L.E	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

INEXISTENCIA DE MONITOREO Y EVALUACIÓN DE PROCESOS.

CONDICIÓN:

Inexistencia de sistemas de monitoreo y evaluación a los procesos operativos de la unidad TIC.

CRITERIO:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote debe definir y ejecutar sistemas de monitoreo y evaluación donde se determine el grado de operatividad de la unidad Tecnológica de la institución, conforme establece la Norma de Control Interno 410-13, que corresponde a “Monitoreo y evaluación de los procesos y servicios.”

CAUSA:

El Jefe de la unidad tecnológica del GADM Cantón Guamote no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO:

Faltas operativas no detectadas en la unidad TIC, las mismas que conllevan a un inadecuado aporte a la obtención de metas y objetivos planteados por la institución.

CONCLUSIÓN:

Inexistencia de sistemas de monitoreo y evaluación a los procesos operativos que determine el grado de operatividad de la unidad Tecnológica de la institución, conforme establece la Norma de Control Interno 410-13, que corresponde a “Monitoreo y evaluación de los

RECOMENDACIÓN:

Definir y ejecutar sistemas de monitoreo y evaluación donde se determine el grado de operatividad de la unidad Tecnológica de la institución, acatando y aplicando la Norma de Control Interno 410-13, que concierne a “Monitoreo y evaluación de los procesos y servicios.”, con el propósito de detectar y corregir deficiencias operativas en la unidad de tecnologías.

Elaborado por:	CH.C.LE	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

INEXISTENCIA DE CONTROL PARA SITIOS WEB.**CONDICIÓN:**

No tiene establecido normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad.

CRITERIO:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote debe establecer normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos, y sitios WEB de la entidad, conforme establece la Norma de Control Interno 410-14, que concierne a “Sitios web, servicios de internet.”

CAUSA:

El jefe de la unidad tecnología de información y comunicación no acata ni aplica la ley establecida, puntualmente a la norma referida a “Sitios web, servicios de internet.”

EFEECTO:

Uso inadecuado de los sitios de internet que pueden afectar y dañar parcial o totalmente a los equipos informáticos, así como también fuga y/o pérdida de información propia de la institución.

CONCLUSIÓN:

No tiene establecido normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad. Esto lleva a incumplimiento de la Norma de Control Interno 410-14, que concierne a “Sitios web, servicios de internet.”

RECOMENDACIÓN:

Establecer normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad, cumpliendo con la normativa de control interno 410-14, que concierne a “Sitios web, servicios de internet.”

Elaborado por:	CH.C.LE	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

INEXISTENCIA DE CAPACITACIÓN INFORMÁTICA.

CONDICIÓN:

Inexistencia de desarrollo y ejecución de planes de capacitación tanto a usuarios internos como externos de la unidad TIC.

CRITERIO:

La máxima autoridad y el Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote debe establecer y ejecutar planes de capacitación donde se integre a todos los usuarios directos e indirectos de las tecnologías de información de la institución, conforme establece la Norma de Control Interno 410-15, que concierne a “Capacitación Informática.”

CAUSA:

El Jefe de la Unidad de Tecnología Información y Comunicación del GADM Cantón Guamote no acata ni aplica la ley establecida, a la norma control Interno 410-15, que concierne a “Capacitación Informática.”

EFEECTO:

Uso inadecuado de los equipos tecnológicos que pueden comprometer el estado físico de la infraestructura tecnológica y comprometer la integridad de la información de la Institución.

CONCLUSIÓN:

Inexistencia de desarrollo y ejecución de planes de capacitación tanto a usuarios internos como externos de la unidad informática y esto ocasiona por el incumplimiento de la Norma de Control Interno 410-15, que concierne a “Capacitación Informática.”

RECOMENDACIÓN:

Implementar y ejecutar planes de capacitación tanto a usuarios internos como externos de la unidad TIC. Aplicando la norma control Interno que concierne a “Capacitación Informática.”

Elaborado por:	CH.C.LE	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

FALTA DE IDENTIFICACIONES PERSONALES A LOS USUARIOS**CONDICIÓN:**

No se incorpora los mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de protección para la utilización de todos los usuarios.

CRITERIO:

La Unidad de TIC del GADM Cantón Guamote debe basarse en la Norma de Control Interno para las Entidades, Organismos del Sector Público N° 410-12 “administración de soporte de tecnologías de información” que establece: La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad.

CAUSA:

La administración de claves personales por terceras personas para el ingreso de los equipos y sistemas informáticos.

EFEECTO:

Ausencia de 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:

No se incorpora los mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de protección para la utilización de todos los usuarios como los internos, externos

RECOMENDACIÓN:

Implementar mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de protección para la utilización de todos los usuarios, cumpliendo con la normativa 410-12 “administración de soporte de tecnologías de información”

Elaborado por:	CH.C.LE	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

NO SE CONSIDERA LOS INFORMES EXTERNOS PARA MEJORAR EL SISTEMA DE CONTROL INTERNO

CONDICIÓN:

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no toma en cuenta las recomendaciones externas.

CRITERIO:

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote debe basarse en la Norma de Control Interno para las Entidades, Organismos del Sector Público N° 600-01 Seguimiento. "La máxima autoridad, los niveles directivos y los directivos de la entidad efectuaran un seguimiento constante del ambiente interno y externo que le permita conocer y aplicar medidas oportunas sobre condiciones reales y potenciales que afecten las actividades institucionales, la ejecución de los planes y el cumplimiento de los objetivos previstos".

CAUSA:

Desinterés del jefe de la unidad de tecnología información y comunicación de GADM Guamote en tomar consideraciones a las recomendaciones provenientes de los usuarios externos.

EFECTO:

A futuro se puede ser afecto la información de la institución los mismos que pueden causar daños y pérdidas irreparables.

CONCLUSIÓN:

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no reporta a la máxima autoridad las quejas de los usuarios externos y que perjudican a la consecución de los objetivos de la institución.

RECOMENDACIÓN:

Se recomienda a La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote tomar atención a las quejas de los usuarios externos para un adecuado control interno y mejora la calidad de servicio.

Elaborado por:	CH.C.LE	Fecha:	23/02/2016
Revisado por:	O.E.W.V	Fecha:	23/02/2016

**FASE III
COMUNICACIÓN DE RESULTADOS**

		PROGRAMA DE AUDITORÍA			PA 3
Entidad:		Gobierno Autónomo Descentralizado Municipal del Cantón Guamote			
Periodo:		Enero - Diciembre 2014			
Objetivo:		Exponer las respectivas conclusiones y recomendaciones en cuanto a la aplicación de normas de control Interno Establecido para las instituciones del sector público, relacionados a las tecnologías de información.			
N°	PROCEDIMIENTO	REF. P/T/	RESPONSABLE	FECHA	
1	Informe Final de la Auditoría Informática.	-	CH.C.L.E	24-02-2016	

Elaborado por:	CH.C.L.E	Fecha:	24/02/2016
Revisado por:	O.E.W.V	Fecha:	24/02/2016



4.3.1 Informe Final de Auditores Independientes.

Guamote, 24 de Febrero 2016.

Economista

Luis Chuquimarca Coro

**ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN GUAMOTE**

Presente.-

De mi consideración:

Se ha realizado la Auditoría Informática a la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, Provincia de Chimborazo, período 2014.

El examen se efectuó en base a la evaluación del control interno mediante el Método COSO y normas de control interno emitidas por la Contraloría General del Estado en lo referente a las Tecnologías de la Información. Estas Normas requieren que el examen sea planificado y ejecutado para obtener certeza razonable de que la información y la documentación examinada no contienen exposiciones erróneas de carácter significativo, que se haya ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Los resultados encontrados en el examen se encuentran expresados en los comentarios, conclusiones y recomendaciones que consta en el presente informe.

Atentamente,

Luis Ernesto Chimbo Caizaguano
AUDITOR – INVESTIGADOR

PARTE I

INFORMACIÓN INTRODUCTORA

Motivo de la Auditoría

Realizar una Auditoría Informática a la Unidad de Tecnología Información y comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, provincia de Chimborazo, periodo 2014, para determinar las medidas y controles adecuados en la Gestión de Tecnologías de Información, con el fin de evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.

Objetivos de la Auditoría

Realizar auditoría informática a la unidad de tecnología información y comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, evaluar la seguridad lógica, seguridad física, el uso y administración de las Tics, en concordancia a las Normas de Control Interno Emitidas por la Contraloría General del Estado determinando así el grado de cumplimiento de dichas normas.

Objetivos específicos

- Verificar el cumplimiento de las disposiciones legales, reglamentarias y normativas aplicables para la ejecución de las actividades desarrolladas inherentes al Sistema de Información y Comunicación.
- Aplicar fases de auditoría informática para diagnosticar las áreas críticas y determinar la situacional real de la Unidad de TIC.
- Emitir un informe con sus respectivas conclusiones y recomendaciones proporcionando las debidas soluciones para mejorar la eficiencia y eficacia de los recursos informáticos.

Alcance del Examen

La Auditoría Informática a la Unidad de Tecnología Información y Comunicación se realizara al Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, cuyo alcance comprende el período entre el 01 de Enero al 31 de Diciembre del 2014.

PARTE II

INFORMACIÓN DE LA INSTITUCIÓN

El Cantón Guamote se encuentra ubicado en la parte central del callejón interandino, al sur de Quito, a 50 Km de Riobamba, constituye el segundo cantón más extenso de los que integran la Provincia de Chimborazo.

Se encuentra a una altitud que va desde los 2600 m.s.n.m. hasta 4500 m.s.n.m., su temperatura media anual es de 13,7°C, constituyendo dos tipos de clima: invierno húmedo frío en los meses de octubre a mayo y verano, cálido, seco, ventoso de junio a septiembre. La precipitación es de 683,3 mm.

MISIÓN, VISIÓN, OBJETIVOS, VALORES Y PRINCIPIOS

Misión

Ser un Municipio en desarrollo permanente, sostenible, ofreciendo servicios básicos de calidad, impulsando el desarrollo local a niveles competitivos, con relaciones y trabajos socioculturales fortalecidos, conciencia ambiental y turística orientada a condiciones de vida óptima, donde la imagen del cantón, su ornato, presentación y cultura promuevan la identificación y el aprovechamiento de unidad cantonal que toma decisiones concertadas y equitativas, respetando a la pacha mama y alcanzando el buen vivir.

Visión

El Cantón Guamote para el año 2026 será el eje del desarrollo nacional con una producción agropecuaria, turística competitiva y sostenible que garantice la calidad de vida de sus habitantes, en un ambiente sano, seguro y ecológicamente equilibrado, con una economía dinámica y solidaria.

Objetivos

- Mejorar los servicios de salud y educación mediante la readecuación, construcción y equipamiento de los centros educativos y las unidades operativas de salud en las tres parroquias del cantón.
- Ampliar la cobertura del servicio de agua potable en la cabecera cantonal y sus comunidades hasta el año 2017.

- Disminuir las enfermedades infecto-contagiosas en el cantón mediante la construcción de las Unidades básicas de Salud en las Comunidades del Cantón Guamote.
- Ampliar la cobertura de las unidades básicas de salud en las comunidades del Cantón.
- Prevenir y mitigar la contaminación ambiental mediante la aplicación de normas estándares de manejo, disposición y tratamiento de residuos sólidos domiciliarios y hospitalarios.

Valores

- **Equidad**, en las relaciones y percepciones, en la distribución de los recursos en situaciones sociales y profesionales.
- **Compromiso**, de la institución frente a sus miembros y usuarios
- **Lealtad**, como una obligación de fidelidad que un sujeto o ciudadano le debe a la institución.
- **Integridad**, como sinónimo de rectitud, honradez en las responsabilidades asignadas que generen confianza.

Principios

El gobierno Municipal, además de los principios constitucionales, se regirá por los siguientes principios.

- **Ética del buen vivir**, considerada como la satisfacción de las necesidades básicas de la población en los territorios, a través de los procesos de generación de riqueza que resulten sostenible en el tiempo.
- **Prevalencia de interés colectivo**, pensaba como la necesidad y urgencia de crear una sociedad más justa y más libre en todos los órdenes. Ampliar fortalecer y extender la justicia social, los derechos democráticos y las bondades del desarrollo tecnológico al mayor número de seres humanos.
- **Honestidad y transparencia**, considerada como una honestidad, significa generar confianza y transparencia y expresa conciencia de las cosas para una auténtica vida comunitaria, que desecha la corrupción.
- **Responsabilidad Social**, Implica que la sociedad sea participe de los beneficios del desarrollo, que mantenga relaciones justas y solidaridad, que le permita acceder y

controlar recurso, tener poder de decisión y negociación; además que recibe beneficios acordes con su dispendio, trabajo realizado y riesgo asumido.

- **Solidaridad**, es una característica de la sociabilidad que inclina al hombre a sentirse unido a sus semejantes y a la cooperación con ellos.

10. BASE LEGAL INSTITUCIONAL

En el año de 1.944 Guamote cristaliza su cantonización que desde hace mucho tiempo atrás se venía gestionando, para lo cual se conformó una directiva. Con esta ayuda la delegación, había conseguido el decreto de cantonización de Guamote, con fecha primero de agosto de 1.944. El presidente de la República Dr. José María Velasco Ibarra, mediante el decreto No 606, Art. 1., establece: "Constituyese en la Provincia de Chimborazo un nuevo cantón con el Nombre de Guamote, que comprenderá las parroquias de Guamote y Cebadas, esta última perteneciente al cantón Riobamba y de las parroquias que el nuevo cantón crease". En la actualidad el cantón Guamote está integrado por tres parroquias: La Matriz que lleva su mismo nombre y dos parroquias rurales Cebadas y Palmira.

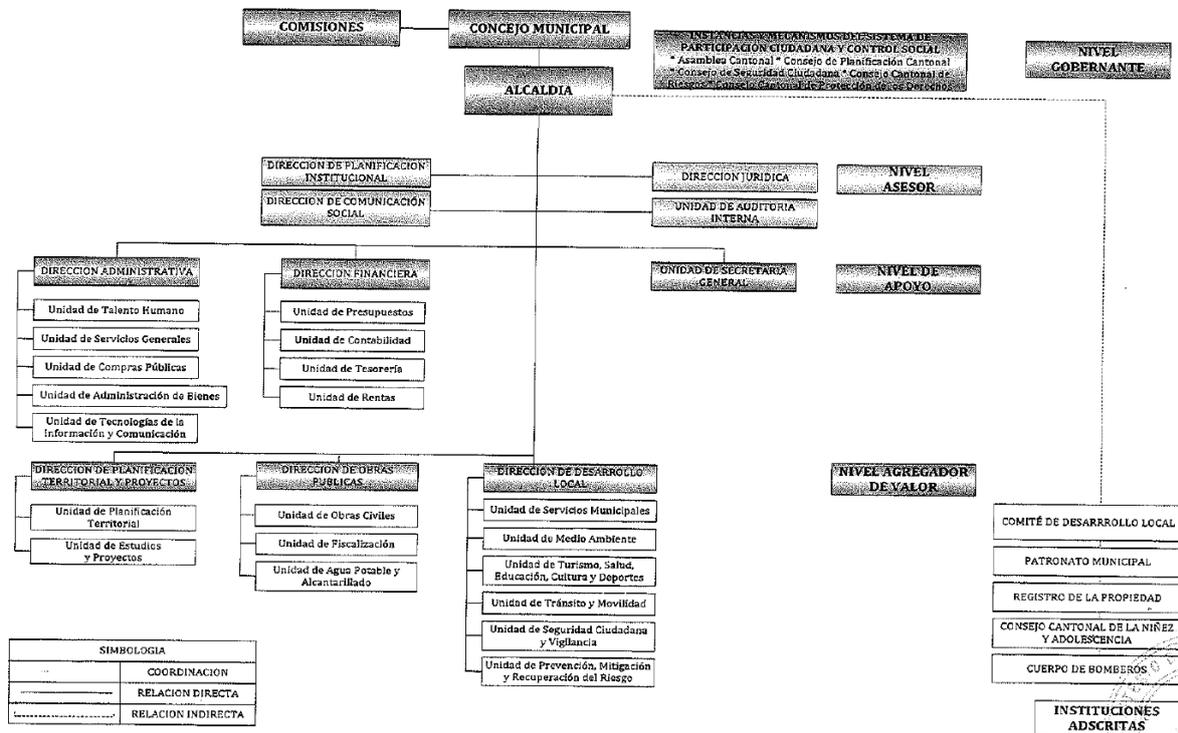
El Gobierno Autónomo Descentralizado Municipal de Cantón Guamote se basa en las siguientes las normativas:

- Constitución Política de la República del Ecuador
- Ley Orgánica de la Contraloría General del Estado
- Código Orgánico de Organización Territorial Autonomía y Descentralización
- Ley de Presupuesto del Sector Público
- Ley Orgánica de Servicio 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 / Ministerio de Finanzas
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de la Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos
- Código de Trabajo
- Ley Orgánica del Sistema Nacional de Contratación Pública.

11. FACULTADES DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE

- Planificar el desarrollo cantonal y formular los correspondientes planes de ordenamiento territorial, de manera articulada con la planificación nacional, regional, provincial y parroquial, con el fin de regular el uso y la ocupación del suelo urbano y rural.
- Ejercer el control sobre el uso y ocupación del suelo en el cantón.
- Planificar, construir y mantener la vialidad urbana.
- Prestar los servicios públicos de agua potable, alcantarillado, depuración de aguas residuales, manejo de desechos sólidos, actividades de saneamiento ambiental y aquellos que establezca la ley.
- Crear, modificar o suprimir mediante ordenanzas, tasas y contribuciones especiales de mejoras.
- Planificar, regular y controlar el tránsito y el transporte público dentro de su territorio cantonal.
- Planificar, construir y mantener la infraestructura física y los equipamientos de salud y educación, así como los espacios públicos destinados al desarrollo social, cultural y deportivo, de acuerdo con la ley.
- Preservar, mantener y difundir el patrimonio arquitectónico, cultural y natural del cantón y construir los espacios públicos para estos fines.
- Formar y administrar los catastros inmobiliarios urbanos y rurales.
- Delimitar, regular, autorizar y controlar el uso de las playas de mar, riberas y lechos de ríos, lagos y lagunas, sin perjuicio de las limitaciones que establezca la ley.

12. ORGANIGRAMA ESTRUCTURAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUAMOTE.



Fuente: GADMC Guamote
 Realizado por: Luis Ernesto Chimbo Caizaguano

RESULTADOS OBTENIDOS EN LA AUDITORÍA

COMPONENTE: AMBIENTE DE CONTROL

INEXISTENCIA DE UN CÓDIGO DE ÉTICA

El Gobierno Autónomo Descentralizado Municipal del Cantón Guamote, no cuenta con un Código de Ética en el cual se establezca principios y valores, que contribuya al buen uso de los recursos públicos, infringiendo la Norma de Control Interno para las Entidades, Organismos del Sector Público N° 200-01 “Integridad y Valores Éticos”.

RECOMENDACIÓN

AL JEFE DE PERSONAL

Elaborará un Código de Ética en donde se plasme los principios y valores éticos como parte de la cultura organizacional para que perduren frente a los cambios de las personas de libre remoción; estos valores rigen la conducta de su personal, orientando su integridad y compromiso hacia la organización.

AL ALCALDE

Aprobaran y harán cumplir el Código de Ética propuesto por el jefe de personal.

COMPONENTE: ACTIVIDADES DE CONTROL

SUBCOMPONENTE: SEGURIDAD LÓGICA

FALTA DE POLÍTICAS Y PROCEDIMIENTOS.

En la Unidad de Tecnología Información y Comunicación del Gobierno Autónomo Descentralizado del Cantón Guamote no se promueven ni se implantan políticas y procedimientos que regulen las actividades de la unidad de tecnologías de Información.

RECOMENDACIÓN:

AL ALCALDE Y AL JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN.

Promoverá e implantará políticas y procedimientos que norme las actividades concernientes con las Tecnologías de Información, cumpliendo y aplicando la Norma de Control Interno 410-04, que concierne a “Políticas y Procedimientos, implantando así un adecuado control y lineamientos dentro de todas las actividades que se desarrollan en la unidad de TIC de GADM Cantón Guamote, de este modo salvaguardar los datos, información y equipos Informáticos que tiene la institución.

FALTA DE CONTROL PARA SITIOS WEB.

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no implanta normas, procedimiento e instructivos de instalación, configuración, y uso de los servicios de internet, correos electrónicos y sitios WEB de la entidad.

RECOMENDACIÓN:

AL JEFE DE LA UNIDAD DE TECNOLOGÍAS INFORMACIÓN Y COMUNICACIÓN.

Establecerá normas, procedimientos e instructivos de instalación, configuración y uso de los servicios de internet, correos electrónicos, y sitios WEB de la entidad, cumpliendo y aplicando la Norma de Control Interno 410-14, que concierne a “Sitios web, servicios de internet e intranet.”, evitando daños parciales o totales a los equipos informáticos, así como también fuga y/o pérdida de información propia de la institución.

SUBCOMPONENTE: *SEGURIDAD FÍSICA*

INEXISTENCIA DE MECANISMOS DE SEGURIDAD.

La unidad TIC del GADM Cantón Guamote no se implantan los mecanismos necesarios que salvaguarden los medios Informáticos existentes en la misma.

ECOMENDACIÓN:

AL JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN.

Implantará los mecanismos de seguridad necesarios que ayuden a salvaguardar los medios Informática de la institución, acatando y aplicando la Norma de Control Interno 410-10, que compete a “Seguridad de Tecnologías de Información”, evitando así pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos existente en la institución.

RECOMENDACIÓN:

INEXISTENCIA DE PLANES DE CONTINGENCIA.

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote No define planes de contingencia para que sean ejecutados en casos de emergencias que se originen en la institución y afecten directa o indirectamente a la unidad de tecnologías de información.

RECOMENDACIÓN:

AL JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN.

Delimitará planes de contingencias donde se detallen los lineamientos a seguir en caso de emergencias originadas dentro de la institución, cumpliendo y aplicando la Norma de Control Interno 410-11, que concierne a “Plan de contingencias”, para una apropiada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado, que llegue a pérdidas de información y operatividad de la unidad.

SUBCOMPONENTE: *GESTIÓN INFORMÁTICA*

INEXISTENCIA DE PLANES DE MANTENIMIENTO Y CONTROL DE INVENTARIO.

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no se elabora y aplica Planes de mantenimiento

correctivo/preventivo, así como también el control de inventario de los bienes existentes en la unidad de tecnologías de información.

RECOMENDACIÓN:

AL JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACION.

Desarrollará y ejecutará planes de mantenimiento para toda la infraestructura tecnológica, así como también levantar un inventario de los bienes existentes en la institución, acatando y aplicando la Norma de Control Interno 410-09, que concierne a “Mantenimiento y control de la infraestructura tecnológica”, evitando así daños parciales o totales de la infraestructura tecnológica, pérdida de recursos, datos erróneos e inexactos en la existencia y control de bienes.

INEXISTENCIA DE MONITOREO Y EVALUACIÓN DE PROCESOS.

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no existen sistemas de monitoreo y evaluación a los procesos operativos de la unidad de tecnologías de información.

RECOMENDACIÓN:

AL JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACION.

Definirá y ejecutará sistemas de monitoreo y evaluación donde se determine el grado de operatividad de la unidad Tecnológica de la institución, acatando y aplicando la Norma de Control Interno 410-13, que concierne a “Monitoreo y evaluación de los procesos y servicios.”, con el propósito de detectar y corregir deficiencias operativas en la unidad de tecnologías de información, aportando así a la consecución de metas y objetivos planteados por la institución.

FALTA DE CAPACITACIÓN INFORMÁTICA.

En la Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no existe el debido desarrollo y ejecución de planes de capacitación tanto a usuarios internos como externos de la unidad de tecnologías de la información.

RECOMENDACIÓN:

AL ALCALDE Y JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACION.

Desarrollarán y ejecutarán planes de capacitación donde se integre a todos los usuarios directos e indirectos de las tecnologías de información de la institución, acatando y aplicando la Norma de Control Interno 410-15, que concierne a “Capacitación Informática.”, conservando así el estado físico de la infraestructura tecnológica y la integridad de la información.

COMPONENTE: SEGUIMIENTO

NO SE CONSIDERA LOS INFORMES EXTERNOS

La Unidad de Tecnología Información del Gobierno Autónomo Descentralizado Municipal del Cantón Guamote no toma en cuenta las recomendaciones externas.

RECOMENDACIÓN:

AL ALCALDE Y JEFE DE LA UNIDAD DE TECNOLOGÍA INFORMACIÓN Y COMUNICACION.

Darán debidas importancias a las quejas de los usuarios externos para mejora la calidad de servicio. Aplicando la norma de control interno N° 600-01 que concierne a Seguimiento efectuaran un seguimiento constante del ambiente interno y externo que le permita conocer y aplicar medidas oportunas sobre condiciones reales y potenciales que afecten las actividades institucionales.

CONCLUSIONES

- La Auditoría Informática es una herramienta fundamental en toda institución para comprobar si un sistema de información salvaguarda el activo de la entidad, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la municipalidad, utiliza eficientemente los recursos y cumplen con las leyes y regulaciones establecidas, el Gobierno Autónomo Descentralizado Municipal del Cantón Guamote al no haber aplicado durante su vida institucional esta herramienta de evaluación, carece del conocimiento sobre la eficiencia y eficacia en la gestión que se está llevando a cabo en la Institución con respecto al manejo y uso Tecnologías de Información.
- Las normas de control interno emitidas por la Contraloría General del Estado establecidas en el sub grupo 410, son de aplicación obligatoria para todas las instituciones y organismos del sector público, que sirven como marco de referencia para la evaluación y control de sus procesos.
- En base al análisis de riesgo y confianza se determinó que se tiene un riesgo del 28,67%, lo cual implica una confianza del 71,33%.
- Se pudo constatar que los activos informáticos que posee el GAD municipal manejan información que es de mucha importancia para los ciudadanos del cantón, esto es debido a que cada vez más, los servicios principales que presta esta dependencia dependen de los sistemas informáticos, es por eso la necesidad de una auditoria de informática, además el manejo eficiente de las TICs es uno de los principales objetivos estratégicos de la municipalidad.

RECOMENDACIONES

- Se recomienda que el personal del departamento de informática tenga capacitación en aspectos de seguridad y control de tecnología para que en base a los conocimientos obtenidos expongan nuevas estrategias adecuadas para mantener segura las tecnologías de la información, que a diario se maneja en la municipalidad
- Es menester poner en marcha las recomendaciones redactadas en el capítulo cuatro de este proyecto de titulación con el fin de mejorar el nivel de seguridad de la información y optimizar los recursos de las tecnologías de la información.
- Se recomienda que el departamento de informática con apoyo del GAD municipal de Cantón Guamote adopte como una buena práctica la planificación y realización de auditorías periódicas tomando en cuenta que los estándares van evolucionando y cambiando para asegurar que los objetivos relacionados a la seguridad de la información se estén cumpliendo.

BIBLIOGRAFÍA

- Echenique, J. A. (2001). Auditoría en informática. México: McGRAW-HILL
- Hermoso, J. J. (2013). Informática aplicada a la gestión de las empresas. México: ESIC Editorial.
- Maldonado, M. (2011). Auditoría de Gestión. Cuarta edición. Quito: Abya - Yala.
- Hernandez, E. H. (2012). Auditoría en Informática. Mexico: CECSA.
- Muñoz, C. (2002). Auditoría en Sistemas Computacionales. México: Pearson Educación.
- Muñoz, C. (2002). Auditoría de Sistemas Computacionales. México: Pearson educación.
- Piattini, M. (2001). Auditoría Informática un enfoque práctico. México: Alfa Omega.

LINKOGRAFÍA

- Contraloría, G. E. (16 de 11 de 2009). *normas de control interno para las entidades, organismos*. obtenido de 410 tecnología de la información : <http://www.contraloria.gob.ec/documentos/normatividad/ACUERDO%20039%20CG%202009%205%20Normas%20de%20Control%20Interno.pdf>
- Javier., R. (31 de agosto de 2012). *Control interno y sus 5 componentes según COSO*. . Obtenido de <http://www.gestiopolis.com/control-interno-5-componentes-segun-coso/>

ANEXOS

ANEXO 1: PAPELES DE TRABAJO

- ENCUESTA APLICADA AL ALCALDE DE GADMC GUAMOTE



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE INGENIERÍA EN CONTABILIDAD Y AUDITORIA



Encuesta al alcalde de GADMC Guamote

Objetivo: obtener información general sobre las funciones que desarrolla la unidad de TIC dentro del Municipio

- 1. ¿Con que objetivo se crea la unidad de TIC en GADM Guamote?**
Es brindar calidad de servicios por los usuarios brindando comodidad y facilidad con la Adquisición de hardware tecnológico para hacer seguimiento a los costos.
- 2. ¿Existen planes de inversión periódicos en lo que corresponde a la adquisición y equipamiento de la unidad de TIC de GADM Guamote?**
se le realiza planes de inversión constantemente de acuerdo a la necesidad de los recursos en la unidad.
- 3. ¿Existe personal suficiente con conocimientos y experiencia para realizar las actividades dentro de esta área?**
El personal debe cumplir con el perfil ya establecido en el manual de funciones para poder cumplir.
- 4. ¿Cree usted que la infraestructura tecnológica con la que dispone la institución es suficiente para que los servidores desempeñen sus labores?**
El momento hemos hecho adquisiciones de equipos nuevos para mejorar el desempeño del curso.
- 5. De acuerdo a la situación actual de la Unidad de TIC, ¿cree usted que esto contribuye a la Misión y Visión del GADM Guamote?**
se debe al optimizar los recursos y utilizarlos de manera adecuada.



ENCUESTA APLICADA AL JEFE DE LA UNIDAD DE TECNOLOGÍA
INFORMACIÓN Y COMUNICACIÓN



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE INGENIERÍA EN CONTABILIDAD Y AUDITORIA



Encuesta al Jefe de La Unidad de Tecnologías Información Y Comunicación

Objetivo: obtener información general de la unidad de TIC

1. **¿La infraestructura física para los equipos de informática existentes son los adecuados?**

SI... NO.....

2. **¿La unidad dispone de planes de capacitación para el uso correcto de los equipos tecnológicos?**

SI..... NO...

3. **¿Existe misión, visión, objetivos y políticas establecidas para la Unidad de TIC?**

SI... NO.....

4. **¿Existen zonas WIFI para los empleados?**

SI... NO.....

5. **¿La cobertura WIFI tiene contraseña de acceso?**

SI... NO.....

6. **¿Existe manuales de políticas y procedimientos para el personal que labora dentro de esta área?**

SI... NO.....

7. ¿El equipo de red Data Center ha cumplido su tiempo de vida útil?

SI........ NO.....

.....
.....

8. ¿Considera Ud. Que existen las seguridades físicas adecuadas dentro de las instalaciones de equipos informáticos, tales como: extintores, salidas de emergencia, aire acondicionado, etc.?

SI..... NO........

.....
.....

9. ¿Conoce el lugar que ocupa en el organigrama la Unidad de Tecnologías Información y comunicación?

SI........ NO.....

.....
.....

10. ¿Existe planes y programas de capacitación, adiestramiento y promoción del personal de la Unidad de TIC?

SI..... NO........

.....
.....

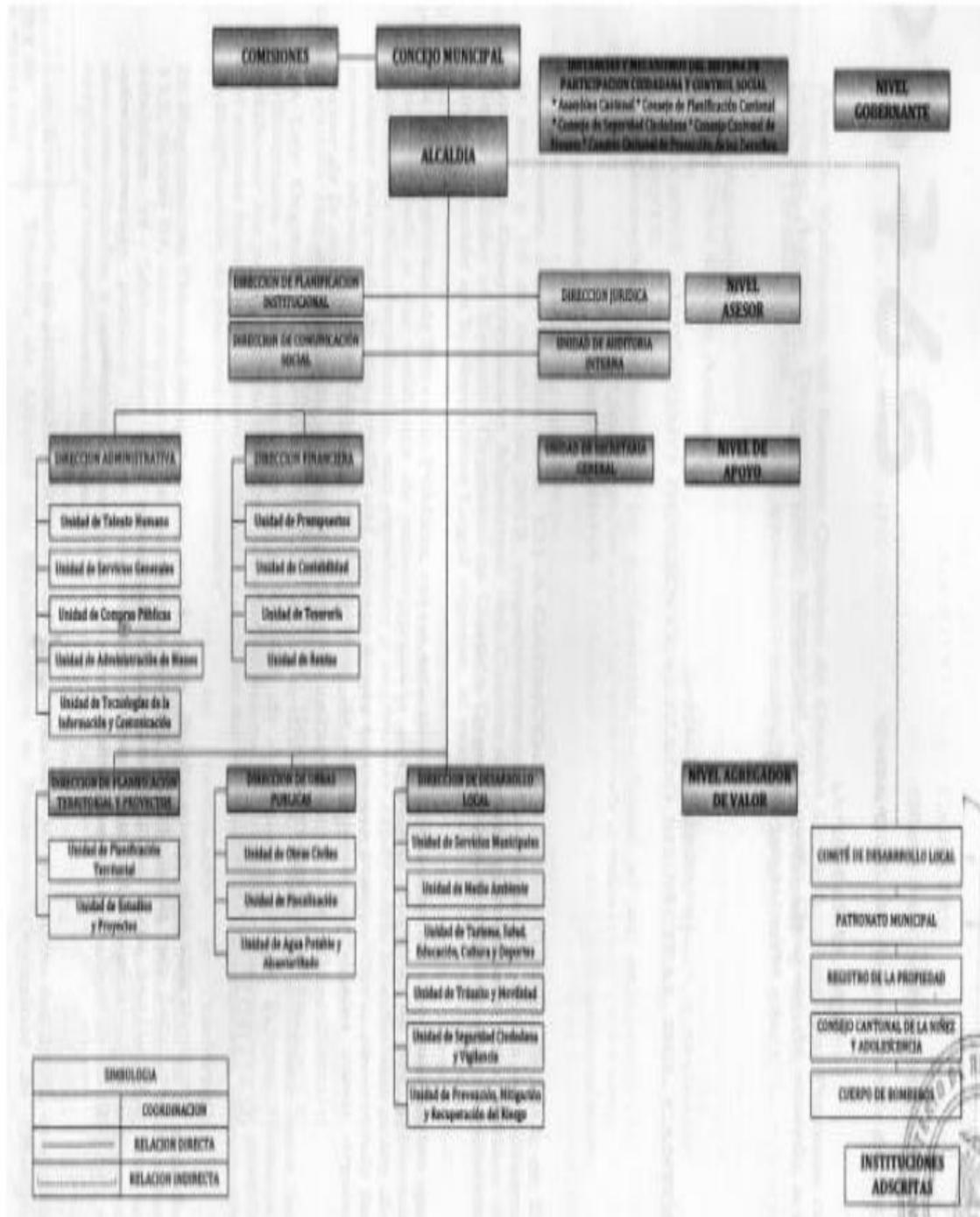


OBSERVACIÓN DIRECTA A TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN

		VERIFICACIÓN FÍSICA UTIC		FASE II	<i>U F</i>
Entidad:	Gobierno Autónomo Descentralizado Municipal del Cantón Guamote				
Tipo de Auditoría:	Auditoría Informática				
Objetivo:	Determinar medidas de seguridad para las TICs				
Tipologías	Complemento	Cumple		Observaciones	
		si	No		
Seguridad	Existe una persona que custodie los bienes de la unidad TIC.	✓		<i>Guardia por todo el GAOMB</i>	
	Existe un circuito cerrado de cámaras de vigilancia.		✓		
	El espacio físico donde se encuentra la UTIC está en buenas condiciones.		✓	<i>Espacio inadecuado</i>	
	Existen adecuadas salidas de emergencia.		✓		
	Existen extintores contra incendios.	✓	✓		
	Existen alarmas contra incendios y/o robos.		✓		
Accesos	Existe un adecuado control de acceso para funcionarios y trabajadores de la unidad.	✓		<i>solo reloj de entrada</i>	
	Existen restricciones a usuarios externos.		✓		
	Las puertas y ventanas cuentan con las debidas seguridades.	✓			
Sistema Eléctrico	El conjunto de cables de la institución se encuentra oculto y debidamente identificado.	✓		<i>hay cables sin conectarlos</i>	
	Existen reguladores de voltaje que salvaguarden los equipos de la institución.		✓		
	Los puntos de iluminación son adecuados		✓		
Otros	El sistema de ventilación es adecuado		✓		
	Los equipos tecnológicos e instalaciones en general cuentan con una póliza de seguros.		✓		
	Existen las herramientas e instalaciones para dar mantenimiento a los equipos.	✓			



ORGANIGRAMA ESTRUCTURAL



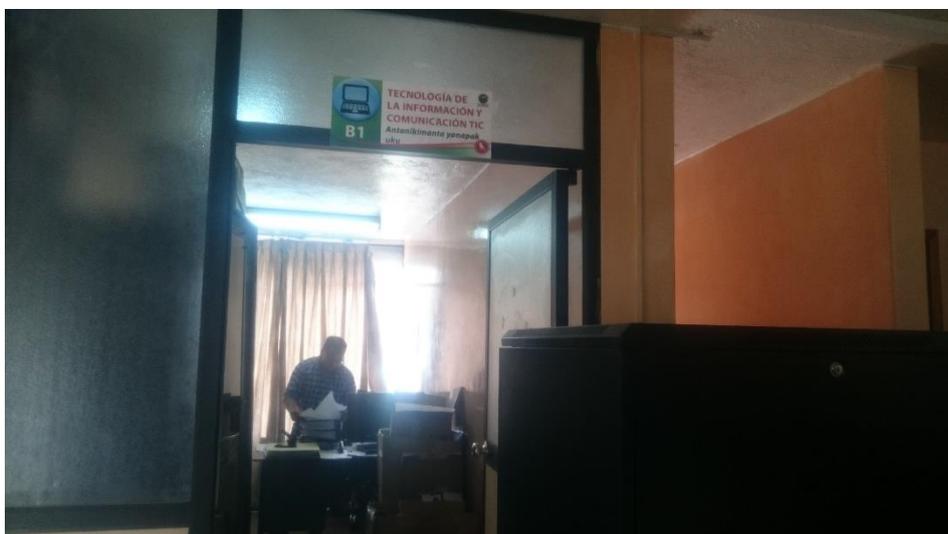
FOTOGRAFÍAS



Alcalde de GADM Cantón Guamote



Jefe de la Unidad de Tecnología Información Y Comunicación



Unidad de Tecnología Información y Comunicación