VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

I PROMOCIÓN

TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

TEMA: “GUÌA DE AUDITORÌA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN EL ÁREA DE TI EN LAS ENTIDADES PÚBLICAS DEL ECUADOR.”

AUTOR: TINOCO TINOCO, DIANA ELIZABETH

DIRECTOR: ING. AGUIRRE MANOSALVAS, HAROLD FRANCISCO

SANGOLQUÍ, 2014

CERTIFICACIÓN

El presente trabajo de tesis realizado por la Ing. Diana Elizabeth Tinoco Tinoco, cuyo tema es **"DESARROLLO DE UNA GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN EL ÁREA DE TI EN LAS ENTIDADES PÚBLICAS DEL ECUADOR",** ha sido dirigido, orientado y evaluado en todas sus fases, habiendo constatado que cumple con los requisitos exigidos por el programa de Maestría en Evaluación de Auditoría de Sistemas Tecnológicos del Nivel de Postgrados de la Universidad de las Fuerzas Armadas, en consecuencia autorizo su presentación, sustentación y defensa.

Sangolquí, enero del 2014

_____

Ing. Francisco Aguirre

DIRECTOR DE TESIS

UNIVERSIDAD DE LAS FUERZAS ARMADAS “ESPE”

TEMA: “GUÌA DE AUDITORÌA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN EL ÁREA DE TI EN LAS ENTIDADES PÚBLICAS DEL ECUADOR.”

AUTOR: Ing. Diana Elizabeth Tinoco Tinoco,

AUTORÍA DE RESPONSABILIDAD

Los conceptos, ideas y opiniones desarrolladas en el presente trabajo son de exclusiva responsabilidad de la autora.

Sangolquí, enero del 2014

_____

Ing. Diana Tinoco

AUTORIZACIÓN

Yo, Ing. Diana Elizabeth Tinoco Tinoco, aautorizó a la Universidad de las Fuerzas Armadas “ESPE”, la publicación de la tesis **“DESARROLLO DE UNA GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN EL ÁREA DE TI EN LAS ENTIDADES PÚBLICAS DEL ECUADOR“**, en la Biblioteca Virtual de la Institución, cuyo contenido, ideas y criterios son de exclusiva responsabilidad de la autora.

Sangolquí, enero del 2014

_____

Ing. Diana Tinoco

DEDICATORIA

Este trabajo lo dedico a mi familia, por su apoyo incondicional, por estar siempre a mi lado.

A mis amigos por ser la fuente de inspiración y motivación.

A todas las personas que dan sentido a nuestra vida y nos impulsan a tomar nuevos retos.

AGRADECIMIENTO

A la Universidad de las Fuerzas Armadas, a través del nivel de Postgrado con el programa de Maestría en Evaluación y Auditoría de Sistemas Tecnológicos, a sus directivos y docentes por los conocimientos impartidos en el transcurso de preparación y estudio.

Expreso el más sincero agradecimiento al director de tesis Ing. Francisco Aguirre, por su acertada guía y apoyo en el desarrollo de este proyecto

A todas y cada una de las personas que de manera directa o indirecta han contribuido en el desarrollo del presente proyecto.

ÍNDICE DE CONTENIDOS

CERTIFICACIÓN I

AUTORÍA DE RESPONSABILIDAD II

AUTORIZACIÓN..... III

DEDICATORIA IV

AGRADECIMIENTO..... V

ÍNDICE DE CONTENIDOS..... VI

ÍNDICE DE TABLAS XVI

ÍNDICE DE GRÁFICOS..... XVII

CAPITULO I 1

CONTROL INTERNO EN EL SECTOR PÚBLICO 1

1.1 JUSTIFICACIÓN E IMPORTANCIA 1

1.2 PLANTEAMIENTO DEL PROBLEMA..... 2

1.3 HIPÓTESIS 4

1.4 OBJETIVO GENERAL 5

1.5 OBJETIVOS ESPECÍFICOS..... 5

CAPITULO II 6

MARCO TEÓRICO REFERENCIAL PARA EL CONTROL INTERNO 6

2.1 MARCO TEÓRICO Y ANÁLISIS REFERENCIAL DEL ESTADO DEL ARTE 6

2.1.1 MARCO TEÓRICO 6

2.1.1.1 CONTROL INTERNO 6

2.1.2 MARCO CONCEPTUAL 8

2.1.2.1 CONTROL INTERNO 8

2.1.2.2 CONTROL INTERNO INFORMÁTICO 8

2.1.2.3 CLASIFICACIÓN DE LOS CONTROLES 9

2.1.2.4 FUNCIONES DEL CONTROL INTERNO INFORMÁTICO 11

2.1.2.5 EVALUACIÓN DE RIESGO DE TI 12

2.1.2.6 MEJORES PRÁCTICAS RELACIONADAS CON EL CONTROL INTERNO 12

2.1.3 ESTADO DEL ARTE 14

2.1.3.1 EVALUACIÓN DEL CONTROL INTERNO TECNOLÓGICO 14

2.2 METODOLOGÍAS Y TÉCNICAS DE INVESTIGACIÓN 17

2.2.1 MÉTODOS TEÓRICOS 17

2.2.1.1 MÉTODO ANALÍTICO 17

2.2.1.2 MÉTODO SINTÉTICO 17

2.2.1.3 MÉTODO DEDUCTIVO 18

2.2.2 METODOLOGÍAS CUANTITATIVAS 18

2.2.3 METODOLOGÍAS CUALITATIVAS O SUBJETIVA 19

2.2.4 METODOLOGÍAS DE ANÁLISIS DE RIESGOS 19

2.3 BASE LEGAL 20

2.3.1 CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR 20

2.3.2 CÓDIGO 22

2.3.2.1 CÓDIGO ORGÁNICO DE PLANIFICACIÓN Y FINANZAS 22

2.3.3 LEYES 23

2.3.3.1 LEY ORGÁNICA DE LA CONTRALORÍA GENERAL DEL ESTADO 23

2.3.3.2 LEY DEL SISTEMA NACIONAL DE REGISTROS DE DATOS PÚBLICOS 24

2.3.3.3 LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN……. PÚBLICA ……..25

2.3.3.4 LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS. 28

2.3.3.5 LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA. 35

2.3.4 REGLAMENTOS 42

2.3.4.1 REGLAMENTO GENERAL A LA LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA Y REFORMAS 42

2.3.4.2 REGLAMENTO GENERAL DE BIENES DEL SECTOR PÚBLICO 43

2.3.4.3 REGLAMENTO GENERAL DE LA LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA 45

2.4 NORMAS DE CONTROL INTERNO INFORMÁTICO 46

2.5 MEJORES PRÁCTICAS 49

2.5.1 PROCESOS ITIL 2011 49

2.5.1.1 ESTRATEGIA DE SERVICIO 49

2.5.1.2 ESTRATEGIA DE DISEÑO 50

2.5.1.3 TRANSICIÓN DEL SERVICIO 51

2.5.1.4 OPERACIÓN DEL SERVICIO 53

2.5.1.5 SIETE PASOS DE LA MEJORA CONTINUA 54

2.5.2 PROCESOS COBIT 5 55

2.5.2.1 EVALUAR ORIENTAR Y SUPERVISAR 55

2.5.2.2 ALINEAR, PLANIFICAR Y ORGANIZAR 55

2.5.2.3 CONSTRUIR, ADQUIRIR E IMPLEMENTAR 56

2.5.2.4 ENTREGAR DAR SERVICIO Y SOPORTE 56

2.5.2.5 SUPERVISAR EVALUAR Y VALORAR 56

2.5.3 ISO IEC 2700 56

2.6 ANÁLISIS COMPARATIVO 58

2.6.1 NORMAS DE CONTROL INTERNO VS MEJORES PRÁCTICAS DE TI 58

2.6.2 NORMAS DE CONTROL INTERNO VS LEYES Y REGLAMENTOS 64

CAPÍTULO III 66

GUÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO 66

3.1 INTRODUCCIÓN 66

3.1.1 ÁREAS A EVALUAR 66

3.1.1.1 ORGANIZACIÓN Y ADMINISTRACIÓN 66

3.1.1.2 SISTEMAS INFORMÁTICOS 74

3.1.1.3 INFRAESTRUCTURA TECNOLÓGICA 84

3.1.1.4 SEGURIDADES 89

3.1.1.5 MONITOREO Y EVALUACIÓN 92

3.2 EVALUACIÓN DE RIESGOS 93

3.2.1 IDENTIFICACIÓN DE LOS RIESGOS 93

3.2.2 ANÁLISIS DE LOS RIESGOS 94

3.2.2.1 NIVEL DE RIESGO 94

3.2.3 MAPEO DE RIESGOS 95

3.2.4 PRIORIZACIÓN DE RIESGOS 96

3.2.5 PLAN DE TRATAMIENTO DE RIESGOS 96

3.3 IDENTIFICACIÓN DE LOS CONTROLES CLAVES 100

3.3.1 PRUEBAS SUSTANTIVAS 100

3.3.2 PRUEBAS DE CUMPLIMIENTO 100

3.4 PROCEDIMIENTOS DE AUDITORÍA A SER APLICADOS 102

3.4.1 ORGANIZACIÓN Y ADMINISTRACIÓN 102

3.4.1.1 PLANES ESTRATÉGICOS Y OPERATIVOS 102

3.4.1.2 ESTRUCTURA ORGANIZACIONAL Y FUNCIONES 103

3.4.1.3 NORMAS Y POLÍTICAS 105

3.4.2 SISTEMAS INFORMÁTICOS 106

3.4.2.1 ADMINISTRACIÓN DE CAMBIOS 108

3.4.2.2 ACREDITACIÓN DE SISTEMAS 109

3.4.2.3 DOCUMENTACIÓN TÉCNICA 110

3.4.2.4 CONTROL DE ENTRADAS Y SALIDAS 110

3.4.2.5 ADMINISTRACIÓN DE BD 111

3.4.3 INFRAESTRUCTURA TECNOLÓGICA 113

3.4.3.1 MANTENIMIENTO DE HARDWARE 113

3.4.3.2 REDES Y COMUNICACIONES 114

3.4.3.3 ALMACENAMIENTO 115

3.4.3.4 MANTENIMIENTO DE HARDWARE 115

3.4.4 SEGURIDADES 116

3.4.4.1 PLAN DE CONTINGENCIAS 116

3.4.4.2 SEGURIDAD LÓGICA 118

3.4.4.3 SEGURIDAD INFORMÁTICA 119

3.4.4.4 SEGURIDAD FÍSICA 120

3.5 EL PROCESO DE LA AUDITORÍA 120

3.5.1 ORDEN DE TRABAJO 121

3.5.2 NOTIFICACIÓN DE INICIO 121

3.5.3 SOLICITUD INICIAL DE INFORMACIÓN 121

3.5.4 DIAGNÓSTICO GENERAL Y PLANIFICACIÓN.....123

3.5.5 DESARROLLO Y RECOPILACIÓN DE LA INFORMACIÓN.....124

3.5.6 COMENTARIOS, CONCLUSIONES Y RECOMENDACIONES.....124

3.5.7 COMUNICACIÓN DE RESULTADOS E INFORME FINAL.....125

3.5.8 SEGUIMIENTO 126

3.6 INDICADORES DE LA SITUACIÓN REAL DE LA EVALUACIÓN DEL CONTROL INTERNO EN LAS ENTIDADES PÚBLICAS. 126

CAPÍTULO IV 133

APLICACIÓN PRÁCTICA DE LA GUÍA DE EVALUACIÓN DE CONTROL INTERNO 133

4.1 DIAGNÓSTICO PRELIMINAR 133

4.1.1 FORTALEZAS.....133

4.1.2 OPORTUNIDADES 133

4.1.3 DEBILIDADES 133

4.1.4 AMENAZAS.....134

4.2 CUESTIONARIOS DE EVALUACIÓN DE CONTROLES.....134

4.2.1 ADMINISTRACIÓN Y ORGANIZACIÓN 135

4.2.2 SISTEMAS INFORMÁTICOS 138

4.2.3 INFRAESTRUCTURA TECNOLÓGICA.....142

4.2.4 SEGURIDADES.....144

4.2.5 MONITOREO Y EVALUACIÓN.....148

4.3 EVALUACIÓN DE RIESGOS 149

4.3.1 IDENTIFICACIÓN DE LOS RIESGOS 149

4.3.1.1 ÁREA DE DESARROLLO, ADMINISTRACIÓN Y MANTENIMIENTO DE SISTEMAS 149

4.3.1.2 ÁREA DE INFRAESTRUCTURA TECNOLÓGICA.....151

4.3.1.3 ÁREA DE ADMINISTRACIÓN Y ORGANIZACIÓN 153

4.3.1.4 ÁREA DE SOPORTE A USUARIOS Y MANTENIMIENTO DE SISTEMAS 154

4.3.2 ANÁLISIS DE LOS RIESGOS.....155

4.3.2.1 ÁREA DE DESARROLLO ADMINISTRACIÓN Y MANTENIMIENTO DE SISTEMAS 155

4.3.2.2 ÁREA DE INFRAESTRUCTURA TECNOLÓGICA.....157

4.3.2.3 ÁREA DE ADMINISTRACIÓN Y ORGANIZACIÓN 158

4.3.2.4 ÁREA DE SOPORTE Y MANTENIMIENTO A USUARIOS.....159

4.3.3 MAPA DE RIESGOS.....160

4.3.4 PRIORIZACIÓN DE RIESGOS.....161

4.3.5 TRATAMIENTO DE RIESGOS 163

4.4 COMENTARIOS DE CONTROL INTERNO 166

CAPÍTULO V 170

CONCLUSIONES Y RECOMENDACIONES 170

5.1 CONCLUSIONES 170

5.2 RECOMENDACIONES.....171

5.3 BIBLIOGRAFÍA.....173

5.4 ANEXOS..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 1 PROCESOS ITIL 2011. ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 1.1 ESTRATEGIA DE SERVICIO ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 1.2 ESTRATEGIA DE DISEÑO..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 1.3 TRANSICIÓN DEL SERVICIO ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 1.4 OPERACIÓN DEL SERVICIO ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 2 PROCESOS COBIT 5..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 2.1 EVALUAR ORIENTAR Y SUPERVISAR ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 2.2 ALINEAR, PLANIFICAR Y ORGANIZAR..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 2.3 CONSTRUIR, ADQUIRIR E IMPLEMENTAR ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 2.4 ENTREGAR DAR SERVICIO Y SOPORTE ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 2.5 SUPERVISAR EVALUAR Y VALORAR ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 3: ISO IEC 27000 – OBJETIVOS DE CONTROL Y CONTROLES.....¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 4 EVALUACIÓN DE RIESGOS..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 4.1 IDENTIFICACIÓN DE RIESGOS..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 4.2 ANÁLISIS DE RIESGOS ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 4.3 MAPEO DE RIESGOS ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 4.4 PRIORIZACIÓN DE RIESGOS ..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 4.4 TRATAMIENTO DE RIESGOS..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 5.1 ENCUESTA..... ¡ERROR! MARCADOR NO DEFINIDO.

ANEXO 5.2 TABULACIÓN DE RESULTADOS..... ¡ERROR! MARCADOR NO DEFINIDO.

ÍNDICE DE TABLAS

TABLA 1. NORMAS DE CONTROL INTERNO 46
TABLA 2. NORMAS DE CONTROL INTERNO VS MEJORES PRÁCTICAS DE TI 58
TABLA 3.- NORMAS DE CONTROL INTERNO VS LEYES Y REGLAMENTOS 64
TABLA 4.- ÁREAS DE TI 127
TABLA 5.- MANUAL DE PROCESOS 128
TABLA 6. FUNCIONES Y RESPONSABILIDADES 129
TABLA 7.- FUNCIONES Y RESPONSABILIDADES DEL PERSONAL DE TI 130
TABLA 8.- EVALUACIÓN DE CONTROL INTERNO 131
TABLA 9 ORGANIZACIÓN Y ADMINISTRACIÓN 135
TABLA 10 SISTEMAS INFORMÁTICOS 138
TABLA 11. INFRAESTRUCTURA TECNOLÓGICA 142
TABLA 12. SEGURIDADES 144
TABLA 13. MONITOREO Y EVALUACIÓN. 148
TABLA 14. IDENTIFICACIÓN DE RIESGOS – DESARROLLO DE APLICACIONES 149
TABLA 15. IDENTIFICACIÓN DE RIESGOS - MANTENIMIENTO DE SISTEMAS 150
TABLA 16. IDENTIFICACIÓN DE RIESGOS - ADMINISTRACIÓN DE SERVIDORES, REDES Y COMUNICACIONES 151
TABLA 17. IDENTIFICACIÓN DE RIESGOS – ORGANIZACIÓN Y ADMINISTRACIÓN 153
TABLA 18 IDENTIFICACIÓN DE RIESGOS – SOPORTE A USUARIOS Y MANTENIMIENTO DE EQUIPOS 154
TABLA 19. ANÁLISIS DE RIESGOS – DESARROLLO DE APLICACIONES 155
TABLA 20 ANÁLISIS DE RIESGOS – MANTENIMIENTO DE SISTEMAS 156
TABLA 21. ANÁLISIS DE RIESGOS – ADMINISTRACIÓN DE SERVIDORES, REDES Y COMUNICACIONES 157
TABLA 22 ANÁLISIS DE RIESGO–ORGANIZACIÓN Y ADMINISTRACIÓN 158
TABLA 23. SOPORTE A USUARIOS Y MANTENIMIENTO DE EQUIPOS. 159
TABLA 24.PRIORIZACIÓN DE RIESGOS. 161
TABLA 25. TRATAMIENTO DE RIESGOS 163

ÍNDICE DE GRÁFICOS

GRÁFICO 1.- ÁREAS DE TI 128
GRÁFICO 2.- MANUAL DE PROCESOS 129
GRÁFICO 3.- FUNCIONES Y RESPONSABILIDADES 129
GRÁFICO 4.- NORMAS DE CONTROL INTERNO 131
GRÁFICO 5.- EVALUACIÓN DE CONTROL INTERNO 132
GRÁFICO 6.-MAPA DE RIESGOS 160

RESUMEN

La Contraloría General del Estado dirige el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos; es por ello que se propone el desarrollo de una guía de auditoría para la evaluación del control interno en el área de TI en las entidades públicas del Ecuador. El desarrollo de una guía de auditoría para la evaluación de control interno del área informática ayudará a mejorar y optimizar la eficiencia de los recursos informáticos de las entidades públicas. Para ello se utilizará el método analítico en la etapa inicial porque se necesita separar el control interno informático en partes bien diferenciadas que ayuden al desarrollo de la guía. Método sintético, proceso que al identificar las partes del control interno informático en las áreas de tecnología de información, ayuda a la comprensión cabal de lo que conocemos en todas su partes y particularidades; y, el método deductivo utilizado para analizar las diferentes metodologías que son aplicadas para la evaluación del control interno de TI, como son la metodología cualitativa, cuantitativa y la de riesgos. Con este propósito, la guía especializada incluye el objetivo general, objetivos específicos, el marco teórico referencial, guía de evaluación del control interno, aplicación práctica de la guía del área de TI en las entidades públicas, conclusiones y recomendaciones.

Palabras Claves: control interno, tecnologías de información, riesgos, auditoría,

ABSTRACT

The General Controller's heads the administrative control system that consist in: internal audit , external audit and internal control of public and private entities that dispose of public resources; therefore proposed the development an audit guide for the evaluation of internal control in Information Technology in Public Entities.The development of an audit guide for the evaluation of internal control of information technologies helps improve efficiency and optimize computing resources in public entities. For this will be used the analytical method at the initial stage because it requires separating the IT internal control in distinct parts that support the development of the guide. Synthetic method, process to identify the parts of IT internal control in the areas of information technology that helps to understand what we know in all its parts and characteristics and the deductive method used to analyze the different methodologies that are applied for the evaluation of internal control of IT, such as qualitative, quantitative and risk methodology. For this purpose the specialized guide includes: general objective, specific objectives, theoretical framework, guide of evaluation for internal control, practical application of the guidance of the IT in public entities, conclusions and recommendations.

Keywords: Internal control, information technology, risks, audit.

PRÓLOGO

El control interno informático controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo con los procedimientos y estándares fijados por la Unidad de Tecnología, así como los requerimientos legales de la entidad, normas de control interno para el sector público y requerimientos legales para la administración pública.

Esta evaluación permite a la alta gerencia reforzar el área de tecnología, para que cumpla con sus objetivos y estrategias de la entidad, mientras que al área de tecnología le brinda la oportunidad de definir acciones preventivas y adoptar alternativas de mejora continua de los servicios.

La guía de evaluación de control interno de TI permite no solo a los auditores sino también a los servidores públicos, conocer sobre los requerimientos legales obligatorios para su cumplimiento, los controles que deben tomarse en cuenta en cada una de las áreas, así como también conocer el proceso de la auditoría.

El presente trabajo está organizado de la siguiente manera:

En la parte inicial se describen los objetivos, planteamiento del problema, justificación e importancia, e hipótesis del presente trabajo.

Seguidamente encontramos el marco teórico y conceptual, la base legal y normativa vigente en el sector público, buenas prácticas de tecnología para al finalizar realizar la comparación entre esta normativa.

A continuación se realiza la guía de auditoría para la evaluación del control interno en el área de TI en las entidades públicas del Ecuador, en la que se describe cada área a evaluar como: organización y administración, sistemas informáticos, infraestructura tecnológica, seguridades, monitoreo y evaluación.

En la parte de evaluación de riesgos se describe la metodología de evaluación de riesgos que consiste en: identificación, análisis, mapeo, priorización y el plan de tratamiento de riesgos.

En la identificación de los controles claves, se realizan pruebas sustantivas y pruebas de cumplimiento y los procedimientos de auditoría a ser aplicados de acuerdo a las áreas descritas anteriormente.

Posteriormente se describe el proceso de auditoría a ser aplicado desde la orden de trabajo hasta la comunicación de resultados e informe final.

Finalmente se detalla la aplicabilidad de la guía de auditoría la misma que consiste en: diagnóstico preliminar, cuestionarios de evaluación control interno para las diferentes áreas de acuerdo a la normativa para las entidades públicas, evaluación de riesgos y comentarios de evaluación de control interno.

Luego de haber concluido con la elaboración de la guía, se ha llegado a determinar las conclusiones y recomendaciones del presente trabajo.

CAPITULO I
CONTROL INTERNO EN EL SECTOR PÚBLICO

1.1 JUSTIFICACIÓN E IMPORTANCIA

La Contraloría General del Estado es un organismo técnico encargado del control de la utilización de los recursos estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos. (Constituyente, 2008)

Además de las competencias conferidas por la ley, la Contraloría General del Estado dirige el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos; determina responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal, relacionadas con los aspectos y gestiones sujetas a su control, sin perjuicio de las funciones que en esta materia sean propias de la Fiscalía General del Estado; expide la normativa para el cumplimiento de sus funciones y asesora a los órganos y entidades del Estado cuando se le solicite.

La Ley Orgánica de la Contraloría General del Estado, dispone a este organismo, la regulación del funcionamiento del sistema de control interno, con la adaptación, expedición, aprobación y actualización de las normas de control interno. A partir de este marco regulador, cada institución del Estado,

dictará las normas, políticas y manuales específicos que considere necesarios para su gestión.

Las normas de control interno vigentes, emitidas mediante Acuerdo N° 039-CG, promulgadas en el Registro Oficial N°78 de 1 de diciembre de 2009 incluyen: normas generales y otras específicas relacionadas con la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos, las mismas que son concordantes con el marco legal vigente y están diseñadas bajo principios administrativos, disposiciones legales y normativa técnica pertinente. (Contraloria General, 2010)

Es por ello que contar con un buen ambiente de control, que contenga un marco de control interno, que regule y asegure procesos internos eficaces, así como las políticas y procedimientos organizacionales, ayuda a que todos los miembros de la empresa que operan los sistemas informáticos sean partícipes de sus deberes y responsabilidades, de manera que su accionar sea el más adecuado para el cumplimiento de los objetivos organizacionales.

1.2 PLANTEAMIENTO DEL PROBLEMA

De la revisión a los informes aprobados en el año 2012 por la Contraloría General del Estado, se observa que existen entidades públicas

que no han implementado controles en los procesos y servicios de Tecnologías de Información como:

- ✓ Seguridades de tecnologías de información con el fin de evitar la ocurrencia de incidentes que afecten a los sistemas de información como fraudes o robos de información confidencial.
- ✓ Controles de aplicación que evalúen la integridad, cumplimiento, confiabilidad, autenticidad y segregación de funciones.
- ✓ Establecimiento de un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento para el área de TI.
- ✓ Asignación del tiempo y recursos suficientes para el establecimiento de soporte básico de TI y actividades operativas.

El uso ineficiente e inadecuado de los recursos y procesos informáticos de las entidades públicas ocasiona que no se pueda brindar una seguridad razonable del logro de la misión de la institución y de los objetivos generales, identificar y dar respuesta a los riesgos, ejecutar las operaciones de manera ordenada, ética, económica, eficiente y efectiva, satisfacer las obligaciones de responsabilidad, cumplir con las leyes y regulaciones y salvaguardar los recursos contra pérdida por desperdicio, abuso, mala administración, errores, fraude e irregularidades.

- ✓ ¿Las entidades públicas están cumpliendo con los requerimientos de información de los usuarios, políticas y procedimientos así como las leyes y reglamentaciones aplicables?
- ✓ ¿Cuáles son las áreas críticas de las entidades públicas, donde no se han efectuado controles?
- ✓ ¿Cuáles son las recomendaciones que las entidades públicas debe seguir para que sus controles sean los adecuados?

El "Desarrollo de una guía de auditoría para la evaluación de control interno del área informática en las entidades públicas del Ecuador" plantea evaluar el control interno de TI, de acuerdo a la normativa existente y actualizada, que permita determinar su nivel de fortaleza, estableciendo si existe una seguridad razonable o poco confiable de las operaciones y procesos sistematizados. Así también permita a los servidores públicos conocer las normas obligatorias para su cumplimiento.

1.3 HIPÓTESIS

El desarrollo de una guía de auditoría para la evaluación de control interno del área informática ayudará a propiciar la mejora continua de los recursos informáticos de la Unidad de Tecnología de Información de las entidades públicas.

1.4 OBJETIVO GENERAL

Desarrollar una guía de auditoría para la evaluación del control interno en el área de TI en las entidades públicas del Ecuador.

1.5 OBJETIVOS ESPECÍFICOS

- ✓ Analizar la normativa vigente para realizar el control interno del área informática en las entidades públicas.
- ✓ Proponer una metodología de análisis de riesgo con la finalidad de conocer las áreas críticas de las entidades.
- ✓ Identificar los procesos de las áreas de TI y los controles que se van a analizar dentro de la organización.
- ✓ Diseño de cuestionarios de control interno de TI

CAPITULO II
MARCO TEÓRICO REFERENCIAL PARA EL CONTROL INTERNO

2.1 MARCO TEÓRICO Y ANÁLISIS REFERENCIAL DEL ESTADO DEL ARTE

2.1.1 MARCO TEÓRICO

2.1.1.1 CONTROL INTERNO

El Control Interno es un elemento muy importante en el funcionamiento y operación de las empresas y tiene un gran efecto en la calidad, oportunidad y veracidad de la información que genera la empresa. El auditor debe realizar un estudio y evaluación del Control Interno, como parte de una revisión de estados financieros practicada conforme a las Normas de Auditoria Generalmente Aceptadas.
(Comisión de Auditoría. CCPM)

El Control Interno busca en forma general los siguientes objetivos:

- Proteger los activos
- Verificar la exactitud y confiabilidad de la información financiera
- Promover la eficiencia de las operaciones

La estructura de control interno de una entidad consiste en las políticas y procedimientos establecidos para proporcionar una seguridad razonable de poder lograr los objetivos específicos de la entidad y alcanzar los objetivos generales mencionados.

El estudio y evaluación del Control Interno debe considerar las características de la empresa y del tipo de negocio en que participa.

Los elementos de la estructura del Control Interno son:

- ✓ El Ambiente de Control
- ✓ La Evaluación de Riesgos
- ✓ Los Sistemas de Información y Comunicación
- ✓ Los Procedimientos de Control
- ✓ La Vigilancia

La división del Control Interno en cinco elementos proporciona al auditor una estructura útil para evaluar el impacto de los controles internos de una entidad en la Auditoria.

2.1.2 MARCO CONCEPTUAL

2.1.2.1 CONTROL INTERNO

El informe COSO (NETCONSULT, 2009) defina al control interno como: “Proceso diseñado para entregar seguridad en: Efectividad y eficiencia en las operaciones, seguridad en reportes financieros y cumplimiento de leyes y regulaciones.

El control, según la metodología COBIT (COBIT, 2009) se define como “Las Políticas, procedimientos, prácticas y estructura organizacional, diseñadas para promover una razonable seguridad en reportes financieros y cumplimiento de leyes y regulaciones”.

2.1.2.2 CONTROL INTERNO INFORMÁTICO

El Control Interno Informático (Pinilla) puede definirse como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

2.1.2.3 Clasificación De Los Controles

Normalmente los controles (Nava Garcia) se clasifican en las siguientes clases: preventivos, detectivos y correctivos.

Preventivos

- ✓ Detectan los problemas antes de que aparezcan.
- ✓ Controlan las operaciones y las entradas
- ✓ Intentan predecir problemas potenciales antes de que ocurran y realizan ajustes.
- ✓ Previenen un error, omisión o acto malicioso de ocurrencia

Ejemplos:

- ✓ Contratar solo personal cualificado
- ✓ Segregar responsabilidades
- ✓ Control de acceso a las instalaciones
- ✓ Uso de documentos bien diseñados
- ✓ Establecer procedimientos adecuados de autorización de transacciones
- ✓ Rutinas de validación en los programas
- ✓ Software de control de acceso para permitir que solo acceda a los ficheros personal autorizado.

Detectivos

- ✓ Detectan e informan de la ocurrencia de un error, omisión o acto malicioso.

Ejemplos:

- ✓ Totales de control
- ✓ Puntos de comprobación en los trabajos
- ✓ Controles de eco en telecomunicaciones
- ✓ Mensajes de error
- ✓ Pruebas duplicadas de cálculos
- ✓ Auditoría interna

Correctivos

- ✓ Minimizan el impacto de una amenaza
- ✓ Remedian los problemas detectados por un control detectivo
- ✓ Identifican la causa del problema
- ✓ Corrigen los errores ocasionados por un problema

Ejemplos:

- ✓ Planificación de contingencias.
- ✓ Procedimientos de respaldo.
- ✓ Procedimientos de ejecución.

2.1.2.4 FUNCIONES DEL CONTROL INTERNO INFORMÁTICO

El Control Interno Informático es una función del departamento de Informática, cuyo objetivo es el de controlar que todas las actividades relacionadas a los sistemas de información automatizados se realicen cumpliendo las normas, estándares, procedimientos y disposiciones legales establecidas interna y externamente. (Auditoria de Sistemas, 2011)

Entre sus funciones específicas están:

- ✓ Difundir y controlar el cumplimiento de las normas, estándares y procedimientos al personal de programadores, técnicos y operadores.
- ✓ Diseñar la estructura del Sistema de Control Interno de la Dirección de Informática en los siguientes aspectos:

    - Desarrollo y mantenimiento del software de aplicación.
    - Explotación de servidores principales
    - Software de Base
    - Redes de Computación
    - Seguridad Informática
    - Licencias de software
    - Relaciones contractuales con terceros

- Cultura de riesgo informático en la organización.

2.1.2.5 EVALUACIÓN DE RIESGO DE TI

El objetivo del Análisis de Riesgos TIC es identificar los riesgos en que los datos, los sistemas de información, así como las redes que los apoyan, están expuestas. Este proceso involucra la evaluación de las amenazas que podrían atacar un sistema y el impacto que un ataque exitoso tendría en la empresa. El resultado final es una evaluación individual (a veces definido como “requerimiento de seguridad”), para cada tipo de amenaza que podría afectar al sistema en cuestión. Los requerimientos de seguridad se usan para entregar una base para el proceso que sigue de “Administración de Riesgos”

2.1.2.6 MEJORES PRÁCTICAS RELACIONADAS CON EL CONTROL INTERNO

Las mejores prácticas (Merida Muñoz, 2012) corresponden a un conjunto coherente de acciones que han sido implementadas por algunas organizaciones y que han rendido eficazmente lo esperado, e incluso que han demostrado que son factibles de imitar entregando similares resultados.

- ✓ **IT Governance** Estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la

empresa y añadir valor mientras se balancean los riesgos versus el retorno sobre TI y sus procesos.

- ✓ **COBIT:** Es una herramienta de gobierno de TI, que vincula las tecnologías informáticas y prácticas de control agrupadas en cuatro Dominios.

- ✓ **ITIL:** es una colección de las mejores prácticas observadas en la industria de TI. Es un conjunto de libros en los cuales se encuentran documentados todos los procesos referentes a la provisión de servicios de tecnología de información hacia las organizaciones.

- ✓ **Norma ISO 27000** Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información, su objetivo es proporcionar una base común para desarrollar normas de seguridad dentro de la organización.

2.1.3 Estado Del Arte

2.1.3.1 Evaluación Del Control Interno Tecnológico

El auditor debe evaluar (OLACEFs, 2011) y supervisar los controles de TIC que son parte integral del entorno de control interno de la organización, proponiendo al Área de Tecnología de Información y Comunicaciones consejos con respecto al diseño, implementación, operación y mejora de controles de TIC.

El control interno del Área de tecnología de información y comunicaciones está comprendido por controles generales (CPD, organización, implementación, seguridad de programas y datos, operación del computador, seguridad de comunicaciones y sistema operativo) diseñados para asegurar que los aplicativos os funcionan adecuadamente y controles de aplicación (Control de acceso, origen, entrada, proceso y salida de información) procedimientos diseñados para asegurar que las transacciones sean administradas de acuerdo con los objetivos específicos de control; que la información conserve todos sus atributos y características, y que los sistemas informáticos cumplan con los objetivos para los cuales fueron creados.

El auditor debe asegurarse que los controles internos diseñados por la institución, mitiguen en gran medida los riesgos residuales obtenidos en el análisis de riesgos, siendo factible y con menor

inversión la administración de éstos, valor agregado que podrá denotar el auditor de TIC.

La evaluación del control interno aporta a la entidad elementos de medición de la gestión informática y de la cultura informática; al área de TIC le brinda indicadores de satisfacción de usuarios, tanto por las aplicaciones, como por el nivel de servicio que proporciona de la seguridad lógica y administración de plataformas tecnológicas, que los alerta sobre las posibles fallas de seguridad y le brinda retroalimentación sobre políticas y medidas de control, que podrían mejorar el funcionamiento de los equipos.

Esta revisión permite a la alta gerencia reforzar el área de Tecnología de Información y Comunicaciones, para que cumpla sus objetivos y soporte, las estrategias del negocio, mientras que al área de Tecnología de Información y Comunicaciones le brinda la oportunidad de definir acciones preventivas y adoptar alternativas de mejora continua de sus servicios.

El factor crítico en el proceso de la auditoría es el conocimiento y evaluación del Control Interno Tecnológico y la elaboración de los programas de auditoría, por tal motivo es importante que el auditor informático, realice una revisión y evaluación detallada del control

interno en las Tecnologías de Información y Comunicaciones (TIC) de las entidades públicas, en los siguientes puntos de control:

- ✓ Gerenciales.
- ✓ Desarrollo y Mantenimiento de Sistemas Informáticos.
- ✓ Operación.
- ✓ Aplicaciones.
- ✓ Tecnología.
- ✓ Continuidad y Oportunidad del Servicio.
- ✓ Cumplimiento de Objetivos estratégicos y operativos

Se deberá realizar una revisión y evaluación de las condiciones de seguridad lógica y física, que garanticen que las medidas de seguridad en las plataformas tecnológicas estén siendo administradas de tal forma que cumplan con los propósitos para lo cual fueron diseñadas y gestión adecuada de los procesos sustantivos sistematizados de la entidad y las metas de la organización y los objetivos de los proyectos tecnológicos implementados.

Esta evaluación tiene un enfoque técnico y es recomendable como medida preventiva, para reducir el riesgo de los ataques externos e internos hacia la información de la entidad, que puede afectar la continuidad de las operaciones.

El auditor debe asegurarse que el control interno haya sido implementado por la administración de la entidad y monitoreado periódicamente como medida preventiva, para anticiparse a situaciones que pongan en peligro la información o la continuidad de las operaciones de las entidades públicas; así como para identificar a tiempo oportunidades de mejora o desviaciones de las estrategias de TIC.

2.2 METODOLOGÍAS Y TÉCNICAS DE INVESTIGACIÓN

2.2.1 MÉTODOS TEÓRICOS

2.2.1.1 MÉTODO ANALÍTICO

Este procedimiento permitirá de un todo complejo, descomponerlo en sus partes, se lo utilizará en la etapa inicial porque se necesita separar el control interno informático en partes bien diferenciadas que ayuden al desarrollo de la guía.

2.2.1.2 MÉTODO SINTÉTICO

Este método se lo aplicará para el desarrollo de la guía, ya que una vez identificadas las partes del control interno informático, podremos emplear en cada una de las áreas de tecnología de información.

2.2.1.3 MÉTODO DEDUCTIVO

Se utilizará el método deductivo para analizar las diferentes metodologías que son aplicadas para la evaluación del control interno de TI para de esta manera llegar a conclusiones que sea útiles para nuestro trabajo.

2.2.2 METODOLOGÍAS CUANTITATIVAS

Están diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos o de planes de contingencias son datos de probabilidad de ocurrencia (riesgo) de un evento que se debe extraer de un registro de incidencias donde el número de ellas sea suficientemente grande.

Esto no pasa en la práctica, y se aproxima ese valor de forma subjetiva restando, así, rigor científico al cálculo pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas podríamos aceptarlo.

En general, podemos observar con claridad dos grandes inconvenientes que presentan estas metodologías. Por una parte, la debilidad de los datos de la probabilidad de ocurrencia por los pocos

registros y la poca significación de los mismos a nivel mundial; y por otro, la imposibilidad o dificultad de evaluar económicamente todos los impactos que pueden acaecer frente a la ventaja de poder usar un modelo matemático para el análisis.

Todas las metodologías (Roberto Sobrinos Sánchez, Planificación y Gestión de Sistemas de Información 1999) existentes, desarrolladas y utilizadas en la auditoría y el control informáticos, se pueden agrupar en:

2.2.3 METODOLOGÍAS CUALITATIVAS O SUBJETIVA

Están basadas en métodos estadísticos y lógica difusa (humana, no matemática FUZZY LOGIC). Precisan de la colaboración de un profesional experimentado, pero requieren menos recursos humanos/tiempo que las metodologías cuantitativas.

2.2.4 METODOLOGÍAS DE ANÁLISIS DE RIESGOS

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. En base a unos cuestionarios, se identifican vulnerabilidades y riesgos, y se evalúa el impacto para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante, pues mediante un juego de simulación (que llamaremos 'Que pasa sí?') analizamos el efecto de las

distintas contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad) que compondrá el informe final de la evaluación.

Esquema

- ✓ Etapa 1: Cuestionarios.
- ✓ Etapa 2: Identificación de riesgos
- ✓ Etapa 3: Calcular el impacto
- ✓ Etapa 4: Identificar las contramedidas y el coste.
- ✓ Etapa 5: Simulaciones.
- ✓ Etapa 6: Creación de los informes.

2.3 BASE LEGAL

2.3.1 CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

De conformidad con los artículos 211 y 212 de la Constitución de la República del Ecuador (Constitución de la Republica del Ecuador, 2008) la Contraloría General es un organismo técnico que cumple las siguientes funciones:

Art. 211.- La Contraloría General del Estado es un organismo técnico encargado del control de la utilización de los recursos estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos.

Art. 212.- Serán funciones de la Contraloría General del Estado, además de las que determine la ley:

1. Dirigir el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos.

2. Determinar responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal, relacionadas con los aspectos y gestiones sujetas a su control, sin perjuicio de las funciones que en esta materia sean propias de la Fiscalía General del Estado.

3. Expedir la normativa para el cumplimiento de sus funciones.

4. Asesorar a los órganos y entidades del Estado cuando se le solicite.

Art. 226. – Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal, ejercerán solamente las competencias y facultades, que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de derechos reconocidos en la Constitución.

Art.- 280.- El Plan Nacional de Desarrollo es el instrumento al que se sujetarán las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto del Estado; y la inversión y la asignación de los recursos públicos; y coordinar las competencias exclusivas entre el Estado Central y los Gobiernos Autónomos Descentralizados. Su observancia será de carácter obligatorio para el sector público e indicativo para los demás sectores.

2.3.2 CÓDIGO

2.3.2.1 CÓDIGO ORGÁNICO DE PLANIFICACIÓN Y FINANZAS

Art. 87.- Planificación fiscal plurianual y anual

La programación fiscal del Sector Público no Financiero será plurianual y anual y, servirá como marco obligatorio para la formulación y ejecución del Presupuesto General del estado y la Programación Presupuestaria Cuatrianual y referencial para otros presupuestos del Sector Público.

Art. 97.- Contenido y finalidadFase del ciclo presupuestario en la que, en base de los objetivos determinados por la planificación y las disponibilidades presupuestarias coherentes con el escenario fiscal esperado, se definen los programas, proyectos y actividades a incorporar en el presupuesto, con la identificación de las metas, los recursos necesarios, los impactos o resultados esperados de su entrega a la sociedad; y los plazos para su ejecución.

Las entidades sujetas al presente código(Codigo Organico de Planificación y Finanzas Públicas , 2010)efectuarán la programación de sus presupuestos en concordancia con lo previsto en el Plan Nacional de Desarrollo, las directrices presupuestarias y la planificación institucional.

2.3.3 LEYES

2.3.3.1 LEY ORGÁNICA DE LA CONTRALORÍA GENERAL DEL ESTADO

Art. 9.- Concepto y elementos del control interno.- El control interno constituye un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución, que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales. Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, los riesgos institucionales en el logro de tales objetivos y las medidas adoptadas para afrontarlos, el sistema de información, el cumplimiento de las normas jurídicas y técnicas; y, la corrección oportuna de las deficiencias de control.

El control interno será responsabilidad de cada institución del Estado y tendrá como finalidad primordial crear las condiciones para el ejercicio del control externo a cargo de la Contraloría General del Estado(Ley Orgánica de la Contraloría General del Estado, 2002)

2.3.3.2 LEY DEL SISTEMA NACIONAL DE REGISTROS DE DATOS PÚBLICOS

Art 23.- Sistema Informático.- El sistema informático tiene como objetivo, la tecnificación y modernización de los registros, empleando tecnologías de información bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive, codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados.

El sistema informático utilizado para el funcionamiento e interconexión de los registros y entidades, es de propiedad estatal y del mismo se podrán conceder licencias de uso limitadas a las entidades públicas y privadas que correspondan, con las limitaciones previstas en la Ley y el Reglamento.

Art 26.- Seguridad Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública.(Ley del sistema nacional de registro de datos publicos, 2010)

2.3.3.3 LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

Art.7.- Difusión de la Información Por la transparencia en la gestión administrativa que están obligadas a observar todas las instituciones del Estado que conforman al sector público en los términos del artículo 118 de la Constitución Política de la República y demás entes señalados en el artículo 1 de la presente Ley, difundirá a través de un portal de información o página web, así como de los medios necesarios a disposición del público, implementados en la misma institución, la siguiente información mínima actualizada, que para efectos de esta Ley, se considera de naturaleza obligatoria:

a) Estructura orgánica funcional, base legal que la rige, regulaciones y procedimientos internos aplicables a la entidad; las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos;
b) El directorio completo de la institución, así como el distributivo del personal;
c) La remuneración mensual por puesto y todo ingreso adicional, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;
d) Los servicios que ofrece y las formas de acceder a ellos, horarios de atención y demás indicaciones necesarias, para que la

ciudadanía pueda ejercer sus derechos y cumplir sus obligaciones;

e) Texto íntegro de todos los contratos colectivos vigentes en la institución; así como sus anexos y reformas;

f) Se publicarán los formularios o formatos de solicitudes que requieran para los trámites inherentes a su campo de acción;

g) Información total sobre el presupuesto anual que administra la institución, especificando ingresos, gastos, financiamiento y resultados operativos de conformidad con los clasificadores presupuestales, así como liquidación del presupuesto, especificando destinatarios de la entrega de recursos públicos;

h) Los resultados de las auditorías internas y gubernamentales al ejercicio presupuestal;

i) Información completa y detallada sobre los procesos precontractuales, contractuales, de adjudicación y liquidación, de las contrataciones de obras, adquisición de bienes , prestación de servicios, arrendamientos mercantiles, etc…, celebrados por la institución con personas naturales o jurídicas, incluidos concesiones, permisos o autorizaciones;

j) Un listado de las empresas y personas que han incumplido contratos con dicha institución;

k) Planes y programas de la institución en ejecución;

l) El detalle de los contratos de crédito externos o internos; se señalará la fuente de los fondos con los que se pagarán esos

créditos. Cuando se trata de préstamos o contratos de financiamiento, se hará constar, como lo prevé la Ley Orgánica de la Contraloría General del Estado y la Ley Orgánica de Responsabilidad y Transparencia Fiscal, las operaciones y contratos de crédito, los montos, plazo, costos financieros o tipos de interés;

m) Mecanismos de rendición de cuentas a la ciudadanía, tales como metas e informes de gestión e indicadores de desempeño;

n) Los viáticos, informes de trabajo y justificativos de movilización nacional o internacional de las autoridades, dignatarios y funcionarios públicos;

o) El nombre, dirección de la oficina, apartado postal y dirección electrónica del responsable de atenderá la información pública de que trata esta Ley;

p) La Función Judicial y el Tribunal Constitucional, adicionalmente publicarán el texto íntegro de las sentencias ejecutoriadas , producidas en todas sus jurisdicciones ;

q) Los organismos de control del estado, adicionalmente, publicarán el texto íntegro de las resoluciones ejecutoriadas, así como sus informes, producidos en todas sus jurisdicciones;

r) El Banco Central, adicionalmente, publicará los indicadores e información relevante de su competencia de modo asequible y de fácil comprensión para la población en general.

s) Los organismos seccionales, informarán oportunamente a la ciudadanía de las resoluciones que adoptaren , mediante la publicación de las actas de las respectivas sesiones de estos cuerpos colegiados, así como sus planes de desarrollo local; y,

t) El Tribunal de lo Contencioso Administrativo, adicionalmente publicará un texto íntegro de sus sentencias ejecutoriadas, producidas en todas sus jurisdicciones.

La información deberá ser publicada, organizándola por temas, ítems, orden secuencial o cronológico, etc. sin agrupar o generalizar, de tal manera que el ciudadano pueda ser informado correctamente y sin confusiones.(Ley organica de transparencia y acceso a la información pública , 2004)

2.3.3.4 LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

Art. 13.- Firma electrónica Son los datos en forma electrónica, consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma apruebe y reconoce la información contenida en el mensaje de datos.

Art. 14.- Efectos de la firma electrónica La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que una firma

manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Art 15.- Requisitos de la firma electrónica Para su validez, la firma electrónica, reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;

b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;

c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;

d) Que al momento de creación de firma electrónica los datos con los que se creare se hallen bajo el control exclusivo, del signatario, y;

e) Que la firma sea controlada por la persona a quien pertenece.

Art 16.- La firma electrónica en el mensaje de datos Cuando se fijare la firma electrónica en un mensaje de datos, aquella deberá enviarse, en un mismo acto como parte integrante, del mensaje de datos, o lógicamente asociada a éste.

Art. 17.- Obligaciones del titular de la firma electrónica

El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;

b) Actuar con la debida diligencia tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;

c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;

d) Verificar la exactitud de sus declaraciones;

e) Responder por las obligaciones derivadas del uno no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;

f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,

g) Las demás señaladas en la ley y sus reglamentos.

Art.18.- Duración de la firma electrónica Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica La firma electrónica se extinguirá por:

a) Voluntad de su titular;

b) Fallecimiento o incapacidad de su titular;

c) Disolución o liquidación de la persona jurídica, titular de la firma; y,

d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso

Art. 20.- Certificado de firma electrónica Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad

Art. 21.- Uso del certificado de firma electrónica El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta ley y su reglamento.

Art. 22.- Requisitos del certificado de firma electrónica El certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información;

b) Domicilio legal de la entidad de certificación de información;

c) Los datos del titular del certificado que permitan su ubicación e identificación;

d) El método de verificación de la firma del titular del certificado;

e) Las fechas de emisión y expiración del certificado;

f) El número único de serie que identifica el certificado;

g) La firma electrónica de la entidad de certificación de información.

h) Las limitaciones o restricciones para los usos del certificado e,

i) Los demás señalados en esta ley y los reglamentos

Art. 23.- Duración del certificado de firma electrónica Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta ley.

Art. 24.- Extinción del certificado de firma electrónica Los certificados de firma electrónica, se extinguen por las siguientes causas:

a) Solicitud de su titular;

b) Extinción de la firma electrónica de conformidad con lo establecido en el artículo 19 de esta ley; y,

c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Art.25.- Suspensión del certificado de firma electrónica La entidad de certificación de información, podrá suspender temporalmente, el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley;

b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,

c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica. La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar una suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso la entidad de certificación de la información, está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Art.26.- Revocatoria del certificado de firma electrónica El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes, no sean asumidos por otra entidad de certificación; y,

b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Art. 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efecto desde el momento de su comunicación, con relación a su titular; y respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular

del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Art. 28.- Reconocimiento internacional de certificados de firma electrónica Los certificados electrónicos emitidos por entidades de certificación extranjeras que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrá el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez, en el Ecuador se someterán a lo previsto en esta ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática , la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de

estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.(Ley de comercio electrónico, firmas electrónicas y mensajes de datos., 2002)

2.3.3.5 LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA

Art 22.- Plan anual de contratación las entidades contratantes, para cumplir con los objetivos del Plan Nacional de Desarrollo, sus objetivos y necesidades institucionales, formularán el Plan Anual de contratación con el presupuesto correspondiente, de conformidad a la planificación plurianual de la Institución, asociados al Plan Nacional de Desarrollo y a los presupuestos del Estado.

El plan será publicado obligatoriamente en la página Web de la Entidad Contratante dentro de los 15 días del mes de enero de cada año e interoperará con el portal de compras públicas. De existir reformas al Plan Anual de contratación, estas serán publicadas, siguiendo los mismos mecanismos previstos en este inciso.

Art 23.- Estudios Antes de iniciar un procedimiento precontractual, de acuerdo a la naturaleza de la contratación, la entidad deberá contar con los estudios y diseños completos, definitivos y actualizados, planos y cálculos, especificaciones técnicas, debidamente aprobados por las instancias correspondientes, vinculados al Plan Anual de Contratación de la entidad.

Los estudios y diseños incluirán obligatoriamente como condición previa a su aprobación e inicio del proceso contractual, el análisis de desagregación tecnológica o de Compra de Inclusión, según corresponda, los que determinarán la proporción mínima de participación nacional o local de acuerdo a la metodología y parámetros determinados por el Instituto Nacional de Contratación Pública.

La máxima autoridad de la Entidad Contratante y los funcionarios que hubieren participado en la elaboración de los estudios, en la época en que éstos se contrataron y aprobaron, tendrán responsabilidad solidaria junto con los consultores o contratistas, si fuere del caso, por la validez de sus resultados y por los eventuales perjuicios que pudieran ocasionarse en su posterior aplicación.

Art 24.- Presupuesto Las entidades previamente a la convocatoria, deberán certificar la disponibilidad presupuestaria y la existencia presente o futura de recursos suficientes para cubrir las obligaciones derivadas de la contratación.

El Reglamento establecerá las formas en que se conferirán las certificaciones o los mecanismos electrónicos para la verificación a que se refiere el inciso anterior.

Art. 69.- Suscripción de contratos Los contratos que por su naturaleza o expreso mandato de la Ley lo requieran se formalizarán en escritura pública dentro del término de quince (15) días desde la notificación de la adjudicación. Los contratos cuya cuantía sea igual o superior a la base

prevista para la licitación se protocolizarán ante Notario Público. Los gastos derivados del otorgamiento del contrato son de cuenta del contratista.

Las contrataciones que se realicen por el sistema de catálogo se formalizarán con la orden de compra y el acta de entrega.

Las contrataciones de menor cuantía se instrumentarán con la factura correspondiente, sin perjuicio de que se puedan elaborar documentos que contengan las obligaciones particulares que asuman las partes.

Los demás contratos se otorgarán por documento suscrito entre las partes sin necesidad de escritura pública.

Para la suscripción del contrato, será requisito previo la rendición de las garantías correspondientes.

Cuando por causas imputables al adjudicatario no se suscriba el contrato dentro del término correspondiente, la entidad deberá declararlo como adjudicatario fallido y disponer su suspensión del RUP. De existir ofertas habilitadas, la entidad, de convenir a sus intereses, adjudicará el contrato al oferente que hubiera presentado la siguiente oferta de mejor costo.

Si el contrato no se celebrare por causas imputables a la Entidad Contratante, el adjudicatario podrá demandar la correspondiente indemnización de los daños y perjuicios o reclamar administrativamente los gastos en que ha incurrido, siempre que se encuentren debida y legalmente comprobados. La entidad a su vez deberá repetir contra el o los funcionarios o empleados responsables.

En ningún caso se podrá iniciar la ejecución del contrato sin la previa celebración o formalización de los instrumentos expuestos en este artículo.

Art 70.- **Administración del contrato** Los contratos contendrán estipulaciones específicas relacionadas con las funciones y deberes de los administradores del contrato, así como de quienes ejercerán la supervisión o fiscalización.

En el expediente se hará constar todo hecho relevante que se presente en la ejecución del contrato, de conformidad a lo que se determine en el Reglamento. Especialmente se referirán a los hechos, actuaciones y documentación relacionados con pagos; contratos complementarios; terminación del contrato; ejecución de garantías; aplicación de multas y sanciones; y, recepciones.

Art 73.- Formas de garantía En los contratos a que se refiere esta Ley, los contratistas podrán rendir cualquiera de las siguientes garantías:

1. Garantía incondicional, irrevocable y de cobro inmediato, otorgada por un banco o institución financiera establecidos en el país o por intermedio de ellos;

2. Fianza instrumentada en una póliza de seguros, incondicional e irrevocable, de cobro inmediato, emitida por una compañía de seguros establecida en el país;

3. Primera hipoteca de bienes raíces, siempre que el monto de la garantía no exceda del sesenta (60%) por ciento del valor del inmueble hipotecado, según el correspondiente avalúo catastral correspondiente;

4. Depósitos de bonos del Estado, de las municipalidades y de otras instituciones del Estado, certificaciones de la Tesorería General de la Nación, cédulas hipotecarias, bonos de prenda, Notas de crédito otorgadas

por el Servicio de Rentas Internas, o valores fiduciarios que hayan sido calificados por el Directorio del Banco Central del Ecuador. Su valor se computará de acuerdo con su cotización en las bolsas de valores del país, al momento de constituir la garantía. Los intereses que produzcan pertenecerán al proveedor; y,

5. Certificados de depósito a plazo, emitidos por una institución financiera establecida en el país, endosados por valor en garantía a la orden de la Entidad Contratante y cuyo plazo de vigencia sea mayor al estimado para la ejecución del contrato.

No se exigirán las garantías establecidas por la presente Ley para los contratos referidos en el número 8 del artículo 2 de esta Ley.

Para hacer efectiva la garantía, la Entidad Contratante tendrá preferencia sobre cualquier otro acreedor, sea cual fuere la naturaleza del mismo y el título en que se funde su pretensión.

Las garantías otorgadas por bancos o instituciones financieras y las pólizas de seguros establecidas en los numerales 1 y 2 del presente artículo, no admitirán cláusula alguna que establezca trámite administrativo previo, bastando para su ejecución, el requerimiento por escrito de la entidad beneficiaria de la garantía. Cualquier cláusula en contrario, se entenderá como no escrita.

Art 74.- Para seguridad del cumplimiento del contrato y para responder por las obligaciones que contrajeren a favor de terceros, relacionadas con el contrato, el adjudicatario, antes o al momento de la firma del contrato, rendirá garantías por un monto equivalente al cinco (5%) por ciento del valor

de aquel. En los contratos de obra, así como en los contratos integrales por precio fijo, esta garantía se constituirá para garantizar el cumplimiento del contrato y las obligaciones contraídas a favor de terceros y para asegurar la debida ejecución de la obra y la buena calidad de los materiales, asegurando con ello las reparaciones o cambios de aquellas partes de la obra en la que se descubran defectos de construcción, mala calidad o incumplimiento de las especificaciones, imputables al proveedor.

En los contratos de obra o en la contratación de servicios no normalizados, si la oferta económica corregida fuese inferior al presupuesto referencial en un porcentaje igual o superior al diez (10%) por ciento de éste, la garantía de fiel cumplimiento deberá incrementarse en un monto equivalente al veinte (20%) por ciento de la diferencia entre el presupuesto referencial y la cuantía del contrato.

Tales cauciones podrán constituirse mediante la entrega de las garantías contempladas en los números: 1, 2; y, 5 del artículo 73 de esta Ley.

No se exigirá este tipo de garantía en los contratos de compraventa de bienes inmuebles y de adquisición de bienes muebles que se entreguen al momento de efectuarse el pago.

Tampoco se exigirá esta garantía en los contratos cuya cuantía sea menor a multiplicar el coeficiente 0.000003 por el Presupuesto Inicial del Estado del correspondiente ejercicio económico.

Con cargo a la garantía de fiel cumplimiento se podrá efectivizar las multas que le fueren impuestas al contratista.

Art 75.- Garantía por anticipo Si por la forma de pago establecida en el contrato, la Entidad Contratante debiera otorgar anticipos de cualquier naturaleza, sea en dinero, giros a la vista u otra forma de pago, el contratista para recibir el anticipo, deberá rendir previamente garantías por igual valor del anticipo, que se reducirán en la proporción que se vaya amortizando aquél o se reciban provisionalmente las obras, bienes o servicios. Las cartas de crédito no se considerarán anticipo si su pago está condicionado a la entrega - recepción de los bienes u obras materia del contrato.

El monto del anticipo lo regulará la Entidad Contratante en consideración de la naturaleza de la contratación.

Art. 99.- En todos los procedimientos precontractuales previstos en esta Ley, los oferentes participarán a su riesgo.

Los miembros de la asociación o consorcio contratista serán responsables solidaria e indivisiblemente por el cumplimiento de las obligaciones derivadas de la oferta y del contrato, indistintamente del plazo de duración de la asociación. La ejecución del contrato es indivisible y completa para los asociados, a efectos de determinar su experiencia y cumplimiento.

La máxima autoridad de la entidad, así como los funcionarios o servidores de la misma que hubieren intervenido en cualquiera de las etapas de los procedimientos precontractuales de preparación, selección, contratación así como en la ejecución misma de los contratos serán personal y pecuniariamente responsables por el cumplimiento de las disposiciones de esta Ley, sin perjuicio, de ser el caso, de la responsabilidad penal a que hubiere lugar.

Los contratistas o proveedores podrán demandar o recurrir contra el o los funcionarios o empleados por cuya acción u omisión, la entidad incumplió sus obligaciones contractuales.

(Ley orgánica del sistema nacional de contratación pública , 2008)

2.3.4 REGLAMENTOS

2.3.4.1 REGLAMENTO GENERAL A LA LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA Y REFORMAS

Art. 6.- Obligatoriedad Todas las instituciones que se encuentran sometidas al ámbito de la Ley de Transparencia y acceso a la Información, difundirá en forma, obligatoria, permanente, a través de su página web, la información mínima actualizada prevista en el artículo 7 de dicho cuerpo legal.

Esta información será organizada por temas, en orden secuencial o cronológico de manera q facilite el acceso¨

(Reglamento general a la ley orgánica de transparencia y acceso a la información pública y reformas, 2005)

2.3.4.2 REGLAMENTO GENERAL DE BIENES DEL SECTOR PÚBLICO

Art. 95.- Plan de Mantenimiento Todas las entidades públicas deberán, deberán tener un Plan Anual de Mantenimiento de Equipos Informáticos , el mismo que debe contar con cronogramas, y financiamiento y estar aprobado por las máximas autoridades

Art. 96.- Mantenimiento El mantenimiento de equipos informáticos estará a cargo de la Unidad responsable de esta actividad en cada institución. En las entidades que no dispongan de esta unidad, se deberán contratar los servicios externos para el efecto, de acuerdo a los procedimientos internos de cada entidad y en atención a las normas vigentes sobre la materia.

Art. 97.- Control Corresponde a la unidad responsable de cada entidad independientemente del inventario que mantenga la Unidad de Activos Fijos, mantener un listado actualizado de los equipos que conforman el parque informático de la institución. El registro deberá contener los datos básicos de cada equipo, como son: Código de activo fijo, número de serie, marca, ubicación del bien, características principales, fecha de compra, período de garantía, proveedor del equipo y estado del equipo, de manera que permita conocer sus características . Con la finalidad de mantener actualizada la información, las unidades administrativas, darán a conocer a la unidad responsable las novedades de movilización efectuadas.

Adicionalmente, la unidad responsable deberá mantener un historial de los trabajos efectuados.

La unidad responsable de cada entidad deberá mantener también un registro actualizado del licenciamiento del software adquirido, el mismo que comprenderá el código de activo fijo, identificación del producto, descripción del contenido, número de versión, número de serie, nombre del proveedor, fecha de adquisición y otros datos que sean necesarios.

Art 98.- Reparación de talleres particulares Cuando los equipos de la entidad u organismo deban ser reparados en talleres particulares, previamente a su salida se debe, se debe contar con la autorización y conocimiento de las correspondientes unidades administrativas y del Guardalmacén de la entidad, y con los documentos de respaldo de la persona que ha entregado el equipo y del taller que lo recibió.

Art 99.- Clases de mantenimiento El término mantenimiento se entenderá como:

Mantenimiento correctivo, que es el conjunto de procedimientos utilizados para reparar una máquina o equipos ya deteriorados. Mediante el mantenimiento correctivo no solo ser repara maquinaria ya deteriorada sino que se realizan ajustes de equipos cuyos procesos evidentemente tienen fallas.

Mantenimiento preventivo, que es la inspección periódica de máquinas y equipos, para evaluar su estado de funcionamiento, identificar fallas, prevenir y poner en condiciones el equipo, para su óptimo funcionamiento, limpieza, lubricación y ajuste. Es también en este tipo de mantenimiento, en el que se remplazan piezas, para las cuales el fabricante del equipo, ha identificado que tiene un número específico de horas de servicio.

Mantenimiento predictivo, que consiste en el monitorio continuo de máquinas y equipos con el propósito de detectar y evaluar, cualquier pequeña variación en su funcionamiento, antes de que se produzca una falla.

(Reglamento General de Bienes del Sector Público, 2006)

2.3.4.3 REGLAMENTO GENERAL DE LA LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA

Art.121.- Administrador del contrato En todo contrato, la entidad contratante designará de manera expresa, un administrador del mismo, quien velará por el aval y oportuno cumplimiento de todas y cada una de las obligaciones derivadas del contrato. Adoptará las acciones que sean necesarias para evitar retrasos injustificados e impondrá las multas y sanciones a que hubiere lugar

Si el contrato es de ejecución de obras, prevé y requiere de los servicios de fiscalización, el administrador del contrato velará porque está actúe de acuerdo a las especificaciones constantes en los pliegos o en el propio contrato.

Art 124.- Contenido de las actas Las actas de recepción provisional, parcial, total y definitivas serán suscritas por el contratistas y los integrantes de la Comisión designada por la máxima autoridad de la entidad contratante o su delegado conformada por el administrador del contrato y un técnico que no haya intervenido en el proceso de ejecución del contrato.

Las actas contendrán los antecedentes, condiciones generales de la ejecución, condiciones operativas, liquidación económica, liquidación de plazos, constancia de la recepción, cumplimiento de las obligaciones contractuales, reajustes de precios pagados, o pendientes de pago, o cualquier otra circunstancia que se estime necesaria.

En las recepciones provisionales parciales, se hará constar como antecedente, los datos relacionados con la recepción precedente. La última recepción provisional incluirá la información sumaria de todas las anteriores. (Reglamento general a la ley orgánica del sistema nacional de contratación publica, 2009)

2.4 NORMAS DE CONTROL INTERNO INFORMÁTICO

Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos y reforma (Normas de aplicación obligatoria para las entidades del sector público ecuatoriano expedidas por la Contraloría General del Estado , 2009)

TABLA 1. NORMAS DE CONTROL INTERNO

410 TECNOLOGÍA DE LA INFORMACIÓN	
410-01 Organización Informática	Las entidades y organismos del sector público deben estar acopladas a 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.
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.
410-03 Plan informático estratégico de tecnología	La unidad de tecnología de 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.
410-04 Políticas y procedimientos	La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología necesaria
410-05 Modelo de información organizacional	La unidad de tecnología de información definirá el modelo de información 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.
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.
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.
410-08 Adquisiciones de infraestructura	La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización
410-09 Mantenimiento y control de 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
410-10 Seguridad de tecnología de información	La unidad de tecnología de información, establecerá mecanismo que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos
410-11 Plan de contingencias	Corresponde a la unidad de tecnología de información la definición, aprobación e implantación 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
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

Continúa

	tecnológicos que se ofrecen
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.
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.
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, los 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 instituciones.
410-16 Comité informático	Para la creación de un comité informático institucional, se considerará los siguientes aspectos: - El tamaño y la complejidad de la entidad y su interrelación con entidades adscritas. – Definición clara de los objetivos q persigue la creación de un comité de informática…..- 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.

Fuente: Normas de Control Interno, Contraloría General del Estado

2.5 MEJORES PRÁCTICAS

2.5.1 PROCESOS ITIL 2011

2.5.1.1 ESTRATEGIA DE SERVICIO

El objetivo es hacer que los proveedores del servicio IT, piensen estratégicamente y consigan objetivos usando activos estratégicos. (**Anexo 1.1** Estrategia de servicio)

PRINCIPIOS CLAVES

- ✓ Ciclo de vida del servicio
- ✓ Generación de valor
- ✓ Funcionalidad y garantía
- ✓ Activos del servicio
- ✓ Recursos y capacidades
- ✓ Sistemas, procesos, roles, unidades y funciones.
- ✓ Tipos de proveedores de servicios.

DOCUMENTOS CLAVES

- ✓ Objetivos del servicio,
- ✓ Estratégicas, políticas y planes.
- ✓ Definición de servicios, clasificación y visualización.

- ✓ Modelos de servicio
- ✓ Business Case
- ✓ Patrones de actividad del negocio
- ✓ Perfiles de usuario (UP)
- ✓ Paquetes de servicios (SP)
- ✓ Paquetes de nivel de servicios (SLP)

2.5.1.2 ESTRATEGIA DE DISEÑO

El objetivo es proporcionar una guía al diseño y despliegue de servicios y los procesos de Gestión del Servicio. (**Anexo 1.2** Estrategia de diseño)

PRINCIPIOS CLAVES

5 Aspectos

- ✓ Definición de requerimientos y diseño de soluciones de servicio.
- ✓ Arquitectura tecnológica y de gestión
- ✓ Diseño de procesos
- ✓ Sistema y herramientas.- portafolio de servicios
- ✓ Métricas y métodos de medición

4P .- Son las herramientas que utiliza la empresa pata implementar las estrategias de mercado y alcanzar los objetivos establecidos

- ✓ Gente

- ✓ Procesos
- ✓ Productos
- ✓ Aliados

DOCUMENTOS CLAVES

- ✓ Políticas y planes del diseño del servicio
- ✓ Criterios de aceptación
- ✓ Niveles de requerimientos de servicios (SLR)
- ✓ Políticas de niveles de servicio, planes y reportes.
- ✓ Acuerdos de niveles de servicio (SLAs-OLAs)
- ✓ Planes de mejora del servicio (SIP)
- ✓ Políticas de disponibilidad
- ✓ Políticas de capacidad
- ✓ Políticas de continuidad del negocio
- ✓ Políticas de proveedores.

2.5.1.3 TRANSICIÓN DEL SERVICIO

Proporciona guiado para la transición de operaciones de nuevos servicios o servicios cambiados. (**Anexo 1.3** Transición del servicio)

PRINCIPIOS CLAVES

- ✓ Políticas de la transición del servicio

- ✓ Administración de comunicaciones y compromisos.
- ✓ Administración de cambios organizacionales
- ✓ Gestión de stakeholders.
- ✓ Big band vs phased
- ✓ Push vs pull
- ✓ Automatización vs. Manual
- ✓ Modelo V del Servicio
- ✓ Sabiduría (Wisdom)

DOCUMENTOS CLAVES

- ✓ Políticas y planes de la transición del servicio
- ✓ Paquete del diseño de servicios
- ✓ Criterio de aceptación de servicios
- ✓ Políticas, planes y reportes de configuración y cambios
- ✓ Programación de cambios
- ✓ Agenda del CAB y Actas
- ✓ Modelo de configuración
- ✓ Líneas de referencia en la configuración
- ✓ Informes de estado
- ✓ Liberación de políticas, planes, paquetes y documentación
- ✓ Políticas de calidad del servicio, políticas de riesgo, estrategias, modelo de pruebas, planes e informes de pruebas
- ✓ Construcción de planes y documentación

- ✓ Planes y reportes de evaluación
- ✓ Planes y reportes de la implementación
- ✓ Informe de cierre de la transición
- ✓ Estrategia de la gestión de conocimiento

2.5.1.4 OPERACIÓN DEL SERVICIO

Lleva a cabo las actividades y procesos que gestionan y ofrecen servicios en los niveles acordados con los usuarios del negocio y los clientes. Gestiona la tecnología utilizada para prestar los servicios y recoger la información del rendimiento y las métricas. (**Anexo 1.4** Operación del servicio)

PRINCIPIOS CLAVES

- ✓ Vista Interna de TI vs vista externa del negocio
- ✓ Estabilidad vs responsabilidad
- ✓ Calidad vs costo
- ✓ Reactivo vs proactivo
- ✓ Comunicaciones
- ✓ Bases de datos de errores conocidos
- ✓ Modelo de prioridades

DOCUMENTOS CLAVES

- ✓ Políticas y planes de la operación del servicio
- ✓ Políticas, planes, reportes de gestión de eventos
- ✓ Políticas, planes y reportes de gestión de incidentes
- ✓ Modelo de incidentes
- ✓ Procedimiento de incidentes principales
- ✓ Políticas, planes y reportes de gestión de requerimientos
- ✓ Modelo de requerimiento
- ✓ Políticas planes y reportes de gestión de problemas
- ✓ Modelo de problemas
- ✓ Manual de procesos
- ✓ Documentación técnica
- ✓ Procedimientos operaciones e instrucciones
- ✓ Documentación funcional
- ✓ Guías de usuario

2.5.1.5 SIETE PASOS DE LA MEJORA CONTINUA

Identifica puntos de mejora en los servicios IT que apoya a los procesos de negocio, asegurándose que se mantienen alineados con los cambios necesarios en la organización. Está vigente a lo largo de todo el ciclo de vida.

1. Identificar la estrategia de mejora.
2. Definir lo que se medirá

3. Capturar los datos
4. Procesar los datos
5. Analizar la información
6. Presentar y utilizar la información
7. Implementar las mejoras

2.5.2 PROCESOS COBIT 5

2.5.2.1 EVALUAR ORIENTAR Y SUPERVISAR

Corresponde al gobierno que asegura que los objetivos de la empresa se logren mediante la evaluación de las necesidades de las partes interesadas, las condiciones y opciones, estableciendo la dirección a través de la priorización y decisión, y monitoreando el desempeño, el cumplimiento y el progreso contra acordaron dirección y objetivos.(**Anexo 2.1** Evaluar Orientar y Supervisar)

2.5.2.2 ALINEAR, PLANIFICAR Y ORGANIZAR

Proporciona dirección para la entrega de soluciones y la entrega de servicio. (**Anexo 2.2** Alinear, Planificar y Organizar)

2.5.2.3 CONSTRUIR, ADQUIRIR E IMPLEMENTAR

Proporciona las soluciones y las pasa para convertirlas en servicios. (**Anexo 2.3** Construir, adquirir e implementar)

2.5.2.4 ENTREGAR DAR SERVICIO Y SOPORTE

Recibe las soluciones y las hace utilizables por los usuarios finales. (**Anexo 2.4** Entregar dar servicio y soporte)

2.5.2.5 SUPERVISAR EVALUAR Y VALORAR

Monitorear todos los procesos para asegurar que se sigue la dirección provista (**Anexo 2.5** Supervisar, evaluar y valorar)

2.5.3 ISO IEC 2700

Este Estándar Internacional abarca todos los tipos de organizaciones como: empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro.

Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad

de la Información documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella. (**Anexo 3** ISO IEC 27000)

2.6 ANÁLISIS COMPARATIVO

2.6.1 NORMAS DE CONTROL INTERNO VS MEJORES PRÁCTICAS DE TI

TABLA 2. NORMAS DE CONTROL INTERNO VS MEJORES PRÁCTICAS DE TI

410 TECNOLOGÍA DE LA INFORMACIÓN	PROCESOS COBIT 4.1	PROCESOS COBIT 5.0		ISO IEC 27001	ITIL
		Primario	Secundario		
410-01 Organización Informática	P04	APO01	APO07/ APO11/ DSS06	A.6.1.3, A.6.1.4, A.6.1.6, A.6.1.7 A.8.1.1, A.8.1.2 A.8.1.3, A.8.2.1 A.8.2.2	2.5, 4.5, 5.1
410-02 Segregación de funciones	P04	APO01	APO07/ APO11/ DSS06	A.6.1.3, A.6.1.4 A.6.1.5, A.6.1.6	2.5, 4.5, 5.1
			APO01	A.8.1.1, A.8.1.2 A.8.1.3, A.8.2.1	
	PO7	APO07		A.8.2.2, A.8.2.3 A.8.3.1, A.8.3.2 A.8.3.3, A.10.1.3	
410-03 Plan informático estratégico de tecnología	P01	APO02	EDM02 /APO05		1.1, 1.2, 2.2
410-04 Políticas y procedimientos	P02	APO03	APO01	4.2	2.5, 2.6, 2.7, 3.2, 3.3, 3.4, 3.7, 4.1, 4.2, 4.3, 4.5, 5.1
	P04	APO01	APO07/ APO11/ DSS06	A.5.1.1, A.5.1.2	
			EDM03	A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4 A.6.1.5, A.6.1.6, A.6.1.8, A.6.2.1	
			APO01	A.6.2.2, A.6.2.3	
	P06	APO01	-	A.7.1.1, A.7.1.2, A.7.1.3, A.8.1.1	
	PO7	APO07	EDM03/ APO01	A.8.1.2, A.8.1.3	

Continúa

PO8	APO11	BAI05	A.8.2.1, A.8.2.2
PO9	APO12	BAI03	A.8.2.3, A.8.3.1
		-	A.8.3.2, A.8.3.3
AI4	BAI08	APO13	A.9.1.1, A.9.1.2
AI5	APO10	-	A.9.1.3, A.9.1.4
AI6	BAI06	DS002	A.9.1.5, A.9.2.1
DS5	DSS05	-	A.9.2.2, A.9.2.3
DS8	DSS03	DSS02/	A.9.2.4, A.9.2.5
DS9	EAI10	DSS05/	A.9.2.6, A.9.2.7
DS10	DS003	DSS06	A.10.1.1, A.10.1.2
DS11	DSS04	-	A.10.1.3, A.10.1.4
			A.10.2.2, A.10.3.2
		DSS05/	A.10.5.1, A.10.6.1, A.10.6.2, A.10.7.1
DS12	DSS01/ DSS05	EAI09	A.10.7.3, A.10.7.4
	DSS01	-	A.10.8.1, A.10.8.2
DS13			A.10.8.3, A.10.8.5
	MEA02		A.10.9.3, A.10.10.2
ME2			A.10.10.4, A.11.1.1
			A.11.2.1, A.11.2.2 A.11.2.3, A.11.2.4
			A.11.3.1, A.11.3.2, A.11.3.3, A.11.4.3
			A.11.5.4, A.12.3.1
			A.12.4.1, , A.12.4.2
			A.12.4.3, A.12.5.1
			A.12.5.5, A.13.1.1
			A.13.1.2, A.13.2.1
			A.13.2.2, A.13.2.3
			A.14.1.1, A.14.1.2
			A.14.1.4, A.15.1.1
			A.15.1.2, A.15.1.3
			A.15.1.4, A.15.1.5
			A.15.1.6, A.15.2.1
			A.15.2.2, A.15.3.1

Continúa

				A.15.3.2,	
10-05 Modelo de información organizacional	P02	APO03	APO01	A.7.1.1, A.7.2.1 A.10.8.1, A.10.8.2 A.11.1.1,	5.1
10-06 Administración de proyectos tecnológicos	PO10	BAI01	-	A.8.2.2,	2.1
10-07 Desarrollo y adquisición de software aplicativo	P05	APO06	APO05	A.6.1.4, A.6.1.5 A.6.1.6, A.6.2.1	1.2, 1.3, 2,1
	AI1	BAI02	-	A.6.2.3, A.7.1.1 A.7.1.2, A.7.2.1 A.7.2.2, A.8.1.2	2.2, 2.3, 2.7,
	AI2	BAI03	-	A.8.1.3, A.10.1.1 A.10.1.4, A.10.2.1	2.8, 3.1, 3.3,
	AI5	AP010	BAI03	A.10.2.2, A.10.2.3	3.4, 3.5, 3.6,
	AI7	BAI07	BAI05	A.10.3.2, A.10.7.4 A.10.8.2, A.10.10.1 A.10.10.5, A.11.4.3 A.11.6.2, A.12.1.1 A.12.2.1, A.12.2.2 A.12.2.3, A.12.2.4 A.12.3.1, A.12.4.1 A.12.4.2, A.12.4.3 A.12.5.1, A.12.5.2 A.12.5.3, A.12.5.4 A.12.5.5, A.12.6.1 A.13.2.2, A.13.2.3 A.15.1.1, A.15.1.4 A.15.1.5, A.15.3.1 A.15.3.2	4.2, 4.3, 5.1
	DS2	APO10	-		
	DS9	EAI10	DSS02		
	ME3	MEA03	-		
	P03	AP002/ AP004	EDM01/ AP003/ AP001	A.6.1.5, A.6.1.6	1.1, 1.2, 1.3, 2.2, 2.4, 2.5, 2.7, 4.2, 4.3,
			APO05	A.6.2.3, A.9.1.5	5.1
10-08 Adquisiciones de infraestructura		APO06	DSS02	A.9.2.4, A.10.3.1	
	P05	BAI03	BAI03	A.10.3.1, A.10.8.2	
	AI3	APO10	-	A.12.1.1, A.12.4.2	
	AI5	BAI04	-	A.12.5.2, A.12.6.1	
	DS3	MEA03		A.14.1.1, A.14.1.5	
	ME3			A.15.1.1, A.15.1.8	
10-09 Mantenimiento y control de infraestructura	AI3	BAI03	DSS02	A.7.1.1, A.8.3.2 A.9.1.5, A.9.2.4	3.2, 4.2, 4.3
	AI4	BAI08	BAI05	A.10.1.1, A.10.1.2	
	AI6	BAI06	-	A.10.1.4, A.10.3.2	
				A.10.7.4, A.11.5.4	

Continúa

tecnológica				A.12.1.1, A.12.4.2	
				A.12.5.1, A.12.5.2	
				A.12.5.3, A.12.6.1	
				A.13.2.2,	
	DS4	DSS04	-	A.6.1.6, A.6.1.7	2.6, 2.7, 4.1,
	DS11	DSS04	DSS01/ DSS05/	A.6.2.1, A.9.1.1	4.5
			DS006	A.9.1.2, A.9.1.3	
			-	A.9.1.4, A.9.1.5	
	DS12	DSS01/ DSS05		A.9.1.6, A.9.2.1	
				A.9.2.2, A.9.2.3	
				A.9.2.4, A.9.2.5	
10-10 Seguridad de tecnología de información				A.9.2.6, A.9.2.7	
				A.10.5.1, A.10.7.1	
				A.10.7.2, A.10.7.3	
				A.10.8.1, A.10.8.3	
				A.10.8.4, A.10.8.5	
				A.12.4.2, A.12.4.3	
				A.14.1.1, A.14.1.2	
				A.14.1.3, A.14.1.4	
				A.14.1.5, A.15.1.3	
	DS4	DSS04	-	A.6.1.6, A.6.1.7	2.6
				A.14.1.1, A.14.1.2	
10-11 Plan de contingencias				A.14.1.3, A.14.1.4	
				A.14.1.5	
	DS1	APO09	-	A.6.1.1, A.6.1.2, A.6.1.4, A.6.1.5, A.6.1.8, A.6.2.1	1.2, 1.4, 2.2,
	DS3	BAI04	-	A.6.2.2, A.6.2.3	2.3, 2.4, 2.5,
10-12 Administración de soporte de tecnología de información	DS5	DSS05	AP013	A.7.1.1, A.7.1.2	2.7, 3.3, 3.4,
	DS8	DSS02	-	A.7.2.2, A.8.1.1	4.2, 4.3, 5.2
	DS9	EAI10	DSS02	A.8.2.2, A.8.3.1	
	DS10	DSS03	-	A.8.3.3, A.9.1.6	
				A.9.2.1, A.9.2.3	

Continúa

				A.10.1.3, A.10.2.1	
				A.10.2.2, A.10.2.3	
				A.10.4.1, A.10.4.2	
				A.10.6.1, A.10.6.2	
				A.10.7.4, A.10.8.4	
				A.10.9.1, A.10.10.2	
				A.10.10.3, A.10.10.4	
				A.10.10.5, A.11.1.1	
				A.11.2.1, A.11.2.2 A.11.2.3, A.11.2.4	
				A.11.3.1, A.11.3.2 A.11.3.3, A.11.4.1	
				A.11.4.2, A.11.4.3	
				A.11.4.4, A.11.4.5 A.11.4.6, A.11.4.7	
				A.11.5.1, A.11.5.2	
				A.11.5.3, A.11.5.4, A.11.5.5, A.11.5.6	
				A.11.6.1, A.11.6.2	
				A.12.2.3, A.12.3.1	
				A.12.3.2, A.12.4.1	
				A.12.4.2, A.12.5.1	
				A.12.5.3, A.12.5.5	
				A.12.6.1, A.13.1.1	
				A.13.1.2, A.13.2.1	
				A.13.2.2, A.13.2.3	
				A.14.1.1, A.14.1.4	
				A.15.1.5, A.15.1.6	
				A.15.2.2, A.15.3.1	
				A.15.3.2,	
10-13 Monitoreo y evaluación de los procesos y servicios	ME1 ME2	MEA01 MEA02		A.5.1.1, A.5.1.2, A.6.1.8, A.6.2.3, A.10.2.2, A.10.10.2 A.10.10.4, A.15.2.1 A.15.2.2, A.15.3.1	5.1, 5.2
10-14 Sitio web,					

Continúa

servicios de internet e intranet				
10-15 Capacitación Informática	DS7	APO07	A.8.2.2	2.5
10-16 Comité informático **10-17 Firmas Electrónicas**	ME4	EDM01/EDM02/ EDM03/EDM04/MEA02	A.6.1.8	1.2, 1.4

2.6.2 NORMAS DE CONTROL INTERNO VS LEYES Y REGLAMENTOS

TABLA 3.- NORMAS DE CONTROL INTERNO VS LEYES Y REGLAMENTOS

410 TECNOLOGÍA DE LA INFORMACIÓN	LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICAS	LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA	REGLAMENTO GENERAL DE LA LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA Y REFORMAS	LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.	REGLAMENTO GENERAL DE BIENES DEL SECTOR PÚBLICO	LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA	REGLAMENTO GENERAL DE LA LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA
410-01 Organización Informática							
410-02 Segregación de funciones							
410-03 Plan informático estratégico de tecnología							
410-04 Políticas y procedimientos							
410-05 Modelo de información organizacional							
410-06 Administración de proyectos tecnológicos							
410-07 Desarrollo y adquisición de software aplicativo	Art.23					Art 22, Art 23 Art 24, Art. 69 Art 70, Art 73 Art 74, Art 75 Art 99	Art.121,Art 124
410-08 Adquisiciones de infraestructura						Art 22, Art 23 Art 24, Art.	Art.121,Art 124

Continúa

						69
						Art 70, Art 73
						Art 74, Art 75
						Art 99
410-09 Mantenimiento y control de infraestructura tecnológica					Art. 95	
					Art. 96	
					Art. 97	
					Art 98	
					Art 99	
410-10 Seguridad de tecnología de información	Art.26					
410-11 Plan de contingencias						
410-12 Administración de soporte de tecnología de información						
410-13 Monitoreo y evaluación de los procesos y servicios						
410-14 Sitio web, servicios de internet e intranet		Art.7	Art. 6			
410-15 Capacitación Informática						
410-16 Comité informático						
410-17 Firmas Electrónicas				Art. 13, Art. 14		
				Art.15, Art 16		
				Art 17, Art.18		
				Art. 19, Art. 20		
				Art. 21, Art. 22		
				Art. 23, Art. 24		
				Art.25, Art.26		
				Art.27, Art. 28		

CAPÍTULO III
GUÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO

3.1 INTRODUCCIÓN

De acuerdo al análisis de la estructura organizacional de la Unidad de Tecnología diferentes entidades públicas y de acuerdo a las Normas de Control Interno se identificaron las siguientes áreas e identificamos los medios de verificación para su cumplimiento.

3.1.1 ÁREAS A EVALUAR

3.1.1.1 ORGANIZACIÓN Y ADMINISTRACIÓN

a) Estructura Organizacional

- ✓ La estructura organizacional de la Unidad de Tecnología de Información se encontrará en un nivel que permita realizar actividades de asesoría y apoyo a la alta dirección y unidades usuarias.
- ✓ Debe reflejar las necesidades institucionales, garantizar independencia con las otras áreas y que la cobertura del servicio se brinde a todas las unidades de la entidad.
- ✓ Revisar de forma periódica para actualizar de acuerdo a las estrategias internas, objetivos planteados y avances tecnológicos.

ESQUEMA MÍNIMO

Proyectos Tecnológicos

Infraestructuras Tecnológicas

Soporte Interno

MEDIOS DE VERIFICACIÓN

- ✓ Organigrama de la Unidad de Tecnología de Información y Comunicación.
- ✓ Orgánico funcional aprobado.

b) Segregación de Funciones

- ✓ Asignar funciones y responsabilidades considerando que no se presente funciones incompatibles
- ✓ Supervisar roles y funciones del personal en cada una de las áreas.
- ✓ Evaluar las posibilidades de reubicación e incorporación de nuevo personal.
- ✓ Evaluar el desempeño en base a la descripción documentada.

MEDIOS DE VERIFICACIÓN

- ✓ Descripción documentada y aprobada de los puestos de trabajo del área de tecnología que contenga: Deberes, responsabilidades, habilidades y experiencia considerando procedimientos que eliminen la dependencia de personal clave.
- ✓ Resultados de la evaluación de desempeño.

c) Plan Estratégico y Tecnología

- ✓ Elaborar e implementar un plan informático estratégico alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.
- ✓ El plan informático estratégico tendrá un nivel de detalle suficiente que permita la definición de planes operativos.
- ✓ Los planes operativos deberán estar alineados al plan estratégico informático y a los objetivos estratégicos de la institución.
- ✓ Actualizar, monitorear y evaluar de forma trimestral el grado de ejecución.

MEDIOS DE VERIFICACIÓN

- ✓ El Plan estratégico y operativo de tecnología de información y su presupuesto analizados y aprobados por la máxima autoridad de la entidad y que al menos incluya:

El Plan Informático estratégico:

- Análisis de la Situación Actual
- Propuestas de mejora de todas las áreas
- Estructura Interna
- Procesos
    - Infraestructura
    - Comunicaciones
    - Aplicaciones y Servicios
- Definición de Estrategias
- Riesgos
- Cronograma.
- Presupuesto de Inversión y Operativo
- Fuentes de Financiamiento
- Requerimientos Legales y Regulatorios

Los planes operativos incluirán:

- Portafolio de proyectos y de servicios
- Arquitectura y dirección tecnológica
- Estrategias de migración
- Contingencia de infraestructura
- Consideraciones para incorporación de nuevas tecnologías.

d) Políticas y Procedimientos

- ✓ Definir, documentar y difundir las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicación.
- ✓ Alinear a las leyes afines y estándares de tecnología de información.
- ✓ Actualizar permanentemente e incluir las tareas, responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento, el control de los procesos y las sanciones en el caso de que no se cumpliera.
- ✓ Promover y establecer convenios.

MEDIOS DE VERIFICACIÓN

- ✓ Políticas y procedimientos aprobados por la máxima autoridad y difundidos en temas como:
    - Calidad
    - Seguridad
    - Confidencialidad
    - Controles Internos
    - Propiedad Intelectual
    - Firmas electrónicas y mensajería de datos
    - Legalidad del software
    - Sistema de aseguramiento de la calidad

- Gestión de riesgos
- Supervisión de funciones, e indicadores de desempeño el permitan medir el cumplimiento de las regulaciones y estándares.

e) Modelo de Información Organizacional

- ✓ Definir un modelo de información de la organización que facilite y garantice su creación, uso, compartición, disponibilidad, integridad, exactitud y seguridad en base a los procesos y procedimientos correspondientes
- ✓ Diccionario de datos corporativo documentado y actualizado permanentemente
- ✓ Reglas de validación y controles de integridad y consistencia
- ✓ Identificación de los módulos y las relaciones que ayudan en las aplicaciones y procesos institucionales
- ✓ Clasificación de datos para aplicar niveles de seguridad y propiedad.

MEDIOS DE VERIFICACIÓN

- ✓ Diccionario de datos
- ✓ Modelo entidad – relación
- ✓ Modelo físico

f) Proyectos Tecnológicos

- ✓ Descripción de la naturaleza, objetivos y alcance y de ser el caso exista relación con otros proyectos institucionales con la debida aceptación de los usuarios interesados
- ✓ Cronograma de actividades que incluya: talento humano, tecnológicos, financiero, planes de prueba y capacitación.
- ✓ Presupuesto referencial en el que incluya aspectos de uso y mantenimiento, capacitación para el personal de soporte y usuarios.
- ✓ Nombrar un servidor responsable para la ejecución del proyecto con la descripción de sus funciones y responsabilidades.
- ✓ El proyecto debe contener al menos las siguientes etapas: inicio, planeación, ejecución, control, monitoreo, cierre. Las etapas importantes serán aprobadas y comunicadas a los interesados.
- ✓ Análisis de riesgos.
- ✓ Monitoreo y control del avance del proyecto
- ✓ El cierre del proyecto incluirá aceptación formal y pruebas que certifiquen la calidad y cumplimiento de los objetivos planteados.

MEDIOS DE VERIFICACIÓN

- ✓ Documentos entregables con sus respectivas aprobaciones, documentos formales como actas o documentos electrónicos legalizados.

- ✓ Plan de control de cambios aprobado
- ✓ Plan de aseguramiento de la calidad aprobado

g) Capacitación

- ✓ Necesidades de capacitación identificadas para el personal de tecnología como para los usuarios que utilizan los servicios de información.
- ✓ El plan de capacitación estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

MEDIOS DE VERIFICACIÓN

- ✓ Plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.

h) Comité Informático

- ✓ Para la conformación de un comité informático institucional, se tomará en cuenta lo siguiente:
- ✓ El tamaño y complejidad de la entidad y su interrelación con entidades adscritas.
- ✓ Objetivos claros para la creación de un comité de informática, con el propósito de definir, conducir y evaluar las políticas internas, la

calidad de los servicios informáticos, y apoyar 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.

MEDIOS DE VERIFICACIÓN

- ✓ Resolución de la entidad en donde se encuentre:
  - Creación y Objetivos
  - Integración
  - Funciones
  - Sesiones
  - Subcomisiones de apoyo

3.1.1.2 SISTEMAS INFORMÁTICOS

a) Políticas de Software

- ✓ Regular los procesos de desarrollo, adquisición de software con lineamientos metodologías y procedimientos.
- ✓ Políticas públicas y estándares internacionales para:
  - Codificación de software

- Nomenclatura,
- Interfaz de usuario
- Interoperabilidad
- Eficiencia en el desempeño del sistema,
- Escalabilidad,
- Validación contra requerimientos,
- Planes de pruebas unitarias y de integración.

✓ Procesos de desarrollo, mantenimiento o adquisición

- Estándares de desarrollo
- Documentación
- Calidad
- Diseño Lógico y Físico
- Controles para prevenir, detectar, corregir errores e irregularidades del procesamiento con el objeto de que sea exacto, oportuno, aprobado y auditable
- Mecanismos de autorización
- Integridad de la información
- Control de acceso
- Respaldos
- Diseño de Implementación de pistas de auditoria
- Requerimientos de seguridad
- Especificación del diseño: arquitecturas tecnológicas y de información definidas en la organización

MEDIOS DE VERIFICACIÓN

- ✓ Políticas y estándares de software aprobados y difundidos.
- ✓ Metodologías y procedimientos definidos en el desarrollo de software.

b) Adquisición de Software

- ✓ Verificar que esta adquisición sean parte de:
  - Portafolio de proyectos y servicios priorizados en los planes estratégicos y operativos aprobados.
  - Constar en el Plan Anual de Contrataciones de la Institución
  - Autorizadas por la máxima autoridad previa justificación técnica documentada.
- ✓ Criterios para la aceptación del requerimiento de software
  - Definición de las necesidades.
  - Factibilidad tecnológica y económica.
  - Análisis de riesgo.
  - Costo beneficio.
  - Estrategia de compra del software y así como los procesos de emergencia de ser el caso.
- ✓ Especificaciones técnicas constantes en los pliegos.
- ✓ En los contratos debe constar:

- Mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos solicitados.
- Procedimientos de recepción de productos, documentación en general, garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.
- Para el caso de software adquirido, el detalle suficiente q garantice la obtención de licencias de uso y servicios.
- Para el caso de software desarrollado a la medida los derechos de autor que será de la entidad contratante y el contratista entregará el código fuente, el mismo que será registrado de acuerdo a las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.

✓ La implementación del software incluirá:

- Procedimientos de configuración, aceptación y pruebas personalizados e implantados.
- Validación contra los términos contractuales
- Arquitectura de la información de la organización
- Aplicaciones existentes
- Interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos
- Eficiencia en el desempeño del sistema
- Manuales de integración y planes de prueba del sistema.

- ✓ Actas de aceptación formalizadas por parte de los usuarios desde el ambiente de desarrollo/ prueba al de producción de los sistemas probados y aprobados y su revisión en la post implantación.
- ✓ Elaboración de los manuales técnicos, instalación, configuración, usuario que se encuentre difundidos publicados y actualizados de manera permanente

MEDIOS DE VERIFICACIÓN

- ✓ Plan Anual de Compras de la Institución.
- ✓ Portafolio de proyectos.
- ✓ Documento que se solicita el requerimiento, la necesidad.
- ✓ Pliegos
- ✓ Contrato
- ✓ Actas entrega-recepción.

Procedimiento Precontractual

- Estudios, diseños o proyectos
- Certificación presupuestaria para el objeto de contratación correspondiente.
- Convocatoria o invitación a participar en el proceso según el caso.
- Pliego

- Resolución de aprobación del pliego e inicio del proceso.
- Preguntas, respuestas y aclaraciones correspondientes al proceso.
- Acta de apertura de ofertas presentadas por el oferente.
- Acta de los detalles de errores de forma de las ofertas y por la cual se solicita convalidación de errores presentados, así como el acta por el cual se han convalidado esos errores de ser el caso.
- Informe de evaluación de las ofertas realizadas por las subcomisiones de apoyo a la comisión técnica y/o por la comisión técnica de ser el caso.
- Cuadro resumen de calificación de las ofertas presentadas.
- Informe de la comisión técnica en el que se recomienda a la máxima autoridad o su delegado, la adjudicación o declaratoria de desierto según sea el caso de contratación.
- Acta de Negociación
- Resolución de Adjudicación
- Garantías presentadas antes de la firma del contrato.
- Resoluciones de cancelación o declaratoria de desierto de los procesos, según el caso de existir.

Procedimiento contractual y de ejecución.

- Contrato suscrito entre la entidad contratante y la empresa contratista, así como los documentos habilitantes de ser el caso.

- Contratos modificatorios en caso de que sea necesario enmendar errores.
- Contratos complementarios en caso de haberse celebrado.
- Notificación de disponibilidad del anticipo, cuando su pago implica que a partir de ese hecho corren los plazos de cumplimiento de las obligaciones por parte del contratista.
- Garantías presentadas a la firma del contrato.
- Informe provisional y final o actas de recepción provisional, parcial, total o definitiva, debidamente suscritas según el caso.
- Comunicaciones al contratista respecto de aplicación de multas y otras sanciones.
- Actos administrativos de sanción y multas.

c) Desarrollo de Software

- ✓ Verificar que este desarrollo sean parte de:
  - Portafolio de proyectos y servicios priorizados en los planes estratégicos y operativos aprobados.
- ✓ Criterios para la aceptación del requerimiento de software
  - Definición de las necesidades.
  - Factibilidad tecnológica y económica.
  - Análisis de riesgo.
  - Costo beneficio.
  - Estrategia de desarrollo del software.

- ✓ Requerimientos funcionales y técnicos:
  - Tipos de usuarios
  - Requerimientos de entrada
  - Definición de interfaces, archivo, procesamiento, salida, control, seguridad
  - Plan de pruebas
  - Trazabilidad
  - Pistas de auditoría donde se aplique, con la participación y aprobación de las unidades usuarias.
- ✓ Actas de aceptación formalizadas por parte de los usuarios desde el ambiente de desarrollo/ prueba al de producción de los sistemas probados y aprobados y su revisión en la post implantación.
- ✓ La implementación del software incluirá:
  - Procedimientos de configuración, aceptación y pruebas personalizados e implantados.
  - Validación contra los términos contractuales
  - Arquitectura de la información de la organización
  - Aplicaciones existentes
  - Interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos
  - Eficiencia en el desempeño del sistema
  - Manuales de integración y planes de prueba del sistema.

- ✓ Elaboración de los manuales técnicos, instalación, configuración, usuario que se encuentre difundidos publicados y actualizados de manera permanente.

MEDIOS DE VERIFICACIÓN

- ✓ Portafolio de proyectos y servicios.
- ✓ Requerimientos funcionales y técnicos
- ✓ Actas de aceptación por parte de los usuarios.
- ✓ Manuales técnicos, instalación, configuración, y de usuario.

d) Mantenimiento de Software

- ✓ Procedimientos para mantenimiento y liberación de software de aplicación por:
  - Planeación
  - Cambios a disposiciones legales y normativas.
  - Corrección y mejoramiento de los mismos.
  - Requerimientos de los usuarios.
- ✓ Los cambios deben estar:
  - Registrados, evaluados y autorizados previa su implementación, con la finalidad de disminuir los riesgos de integridad del ambiente de producción.

- Registrados en la bitácora e informar a todos los actores, y usuarios finales relacionados, adjuntando las respectivas evidencias.

✓ Control y registro de versiones del software que entran a producción.

✓ Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, para luego difundirlos y publicarlos.

✓ Ambientes de desarrollo prueba y producción independientes

✓ 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.

✓ Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

MEDIOS DE VERIFICACIÓN

✓ Procedimientos para el mantenimiento y liberación del software de aplicación.

✓ Registro del control de cambios.

✓ Registro de control de versiones.

✓ Manuales técnicos y de usuarios actualizados.

✓ Verificar si existe ambientes de desarrollo, prueba y producción.

✓ Diagramas y configuraciones de hardware y software

e) Aplicaciones y Servicios

- ✓ Elaborar normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad,
- ✓ Desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites institucionales y ciudadanos en general.

MEDIOS DE VERIFICACIÓN

- ✓ Instructivos de instalación, configuración y uso de los servicios de intranet, internet y correo electrónico.

3.1.1.3 INFRAESTRUCTURA TECNOLÓGICA

- ✓ Definir, justificar, implementar y actualizar la infraestructura tecnológica

a) Administración de la Infraestructura

- ✓ Planificar el incremento de las capacidades
- ✓ Evaluar los riesgos tecnológicos, costos y vida útil de la inversión para futuras actualizaciones; considerando carga de trabajo, almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos.

- ✓ Costo-Beneficio para el uso compartido de Data Center con otras entidades del sector público optimar los recursos invertidos.

b) Adquisición de la Infraestructura

- ✓ Se debe realizar en base a un portafolio de proyectos y servicios priorizados en los planes estratégicos y operativos, aprobados, principios de calidad de servicio. Constará en el plan anual de contrataciones aprobado de la institución, caso contrario autorizadas por la máxima autoridad previa justificación técnica documentada.
- ✓ Contratos tendrán el detalle suficiente de las características técnicas de los principales componentes tales como:
  - marca,
  - modelo,
  - número de serie,
  - capacidades,
  - unidades de entrada y salida,
  - garantías ofrecidas, entre otros.
- ✓ Contratos de proveedores de servicios incluirán:
  - Acuerdos de nivel de servicio que contenga:
    - confidencialidad
    - seguridad de la información y otros requerimientos legales que se apliquen.

MEDIOS DE VERIFICACIÓN

- ✓ Plan Anual de Compras de la Institución.
- ✓ Portafolio de proyectos.
- ✓ Documento que se solicita el requerimiento, la necesidad.
- ✓ Pliegos
- ✓ Contrato
- ✓ Actas entrega-recepción.
- ✓ Los mismos procedimientos precontractuales y contractuales aplicados en la adquisición de software.
- ✓ Determinar la correspondencia de las características técnicas entre los equipos adquiridos, especificaciones técnicos y requerimientos establecidos en las fases precontractual, contractual y confirmado en las actas entregas recepción.

c) Mantenimiento y Soporte de la Infraestructura.

- ✓ Implementar medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos para garantizar la integridad, disponibilidad, confiabilidad y seguridad.
- ✓ Plan de Mantenimiento preventivo y correctivo de la infraestructura tecnológica

- ✓ Inventario de bienes Informáticos actualizado y detallado de las características y responsables a cargo conciliado con los registros contables.
- ✓ Los bienes en garantía serán proporcionados por el proveedor, sin costo adicional.
- ✓ Niveles de servicio y de operación para todos los procesos críticos de tecnología de información.
- ✓ Revisión, monitoreo y notificación de la efectividad y cumplimiento de los servicios claves de tecnologías de información.
- ✓ 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.
- ✓ 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.

MEDIOS DE VERIFICACIÓN

- ✓ Políticas y procedimientos emitidos para el mantenimiento de la infraestructura tecnológica.

- ✓ Plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica, sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales:
  - Estrategias de actualización de hardware y software
  - Riesgos
  - Evaluación de vulnerabilidades.
  - Requerimientos de seguridad.
- ✓ Inventario de bienes informáticos que permita realizar el mantenimiento y control a través de la siguiente información.
  - Código de activo fijo.
  - Número de serie
  - Marca
  - Ubicación del bien
  - Características principales.
  - Fecha de compra
  - Periodo de garantía
  - Proveedor del equipo
  - Estado del equipo
- ✓ Acuerdos de nivel de Servicio
- ✓ Reporte de incidentes.

3.1.1.4 SEGURIDADES

- ✓ Mecanismos que protejan y salvaguarden contra pérdidas y fuga de medios físicos e información que se procesa mediante sistemas informáticos.
- ✓ Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: desarrollo y bibliotecas;
- ✓ Procedimientos de obtención periódica de respaldos en base a un cronograma definido y aprobado.
- ✓ En caso de actualización de tecnologías de soporte se migrará la información a los medios físicos con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación
- ✓ Almacenamiento de respaldos de información crítica o sensible en lugares externos a la organización
- ✓ Implementación y administración de seguridades a nivel de hardware y software sobre las vulnerabilidades o incidentes de seguridad identificados, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas.
- ✓ Instalaciones físicas adecuadas:
    - Mecanismos, dispositivos y equipo especializado para controlar el fuego
    - Mantener el ambiente con temperatura y humedad relativa del aire controlado.

- Energía acondicionada esto es estabilizada y polarizada

✓ Sitios de procesamiento alternativos.

✓ Procedimientos de seguridad para el personal que trabaja en turnos por la noche o fin de semana.

✓ Plan de Contingencia que describa acciones a tomar en caso de emergencia o suspensión en el procesamiento de la información.

✓ Identificación única de los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.

✓ Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.

✓ Revisiones periódicas a las cuentas de usuarios y los privilegios asociados por parte los responsables y administradores de los sistemas de tecnología de información.

✓ Medidas de prevención, detección y corrección de software malicioso y virus informáticos.

✓ 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.

✓ Firmas electrónicas.- Las servidoras y servidores autorizados por las instituciones públicas podrán utilizar la firma electrónica en un mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público.

- Verificación de la autenticidad de la firma electrónica.
- Coordinación interinstitucional de formatos para uso de firma electrónica.
- Conservación de archivos electrónicos.
- Actualización de datos de los certificados de firmas electrónicas.
- Seguridad de los certificados y dispositivos portables seguros
- Renovación del certificado de firma electrónica
- Capacitación en el uso de firmas electrónicas.

MEDIOS DE VERIFICACIÓN

- ✓ Políticas y procedimientos aprobados y difundidos para proteger y salvaguardar los bienes y la información.
- ✓ Constatación física de la ubicación e instalaciones físicas de la Unidad de Tecnología de Información y del Centro de Datos.
- ✓ Políticas y procedimientos para la obtención de respaldos.
- ✓ Plan de Contingencia aprobado e implementado que contenga por lo menos los siguientes aspectos:
  - Plan de respuesta a riesgos
  - Definición y ejecución de procedimientos de control de cambios
  - Plan de continuidad de operaciones

- Plan de recuperación de desastres
- Comité de roles específicos y nombres de los encargados.

3.1.1.5 MONITOREO Y EVALUACIÓN

a) Procesos y Servicios.

- ✓ Marco de trabajo de monitoreo y el alcance.
- ✓ Metodología y proceso a seguir para monitorear la contribución y el impacto de las tecnologías de información.
- ✓ Definir indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos necesarios.
- ✓ Definir y ejecutar procedimientos para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.
- ✓ Informes periódicos de gestión a la alta dirección, para verificar el cumplimiento y se identifiquen e implanten acciones correctivas.

MEDIOS DE VERIFICACIÓN

- ✓ Indicadores de desempeño definidos
- ✓ Medidas o procedimientos definidos para el análisis de satisfacción al cliente
- ✓ Informes de gestión
- ✓ Metodologías utilizadas para la evaluación y monitoreo.

3.2 EVALUACIÓN DE RIESGOS

La evaluación de riesgos comprende su identificación, análisis, mapeo y priorización. (31000, 2009)

3.2.1 IDENTIFICACIÓN DE LOS RIESGOS

- ✓ Identificar los procesos de la unidad que está evaluando, podría haber uno o más procesos. Los procesos están detallados en el Reglamento Orgánico Funcional/ Estatuto de procesos de la entidad. En el caso de no existir definición por procesos identificar las áreas.
- ✓ Definir el objetivo de cada proceso en un enunciado
- ✓ Señalar las fuentes de riesgos o eventos que pueden dificultar o impedir la consecución del objetivo propuesto. Cuáles son los eventos o circunstancias que podrían afectar o impedir la consecución del objetivo de este proceso?
- ✓ Identificar las causas de cada fuente de riesgo. Cuál es la causa de este evento o circunstancia?
- ✓ Definir las consecuencias potenciales de no alcanzar o cumplir el objetivo del área o proceso
- ✓ Redactar el enunciado del riesgo identificando:

- **Fuentes de riesgo** + PODRIAN OCASIONAR + que no se cumpla con el **objetivo del área. (Anexo 4.1.** Identificación de los riesgos.)

3.2.2 Análisis De Los Riesgos

3.2.2.1 Nivel De Riesgo

- ✓ Con los riesgos identificados
- ✓ Identificar los controles existentes para el cumplimiento del objetivo del área. Un control puede ser proceso, política, dispositivo, práctica, u otras acciones que contribuyan al cumplimiento del objetivo de la actividad analizada. La siguiente pregunta puede ayudar: *¿Cuáles son los controles existentes en este proceso?*
- ✓ Definir la efectividad de los controles eligiendo un rango que va desde bueno hasta deficiente. No se trata de emitir un criterio sobre el funcionamiento teórico del control sino de medir su efectividad en la realidad.
- ✓ Definir la probabilidad de ocurrencia de los riesgos identificados. Escogiendo un rango de la siguiente escala:
  - 5 Casi cierta
  - 4 Probable
  - 3 Posible

- 2 Poco probable
- Rara

La pregunta es Que tan probable es que el riesgo identificado ocurra?

✓ Definir el impacto que podría generarse si el riesgo identificado se hace realidad. Escogiendo un rango de la siguiente escala.

- 5: Grave.
- 4. Daños mayores.
- 3. Mediano.
- 2. Leve.
- 1. Muy leve.

La pregunta es Cual sería el impacto para la entidad si el riesgo identificado ocurre?

Para obtener el nivel de riesgo, se debe multiplicar el valor definido en el impacto por el valor de la probabilidad. **(Anexo 4.2.** Análisis de riesgos.)

3.2.3 MAPEO DE RIESGOS

Una vez que se ha definido la probabilidad y el impacto de cada riesgo identificado se procede a ubicarlos gráficamente en el mapa de riesgos. La probabilidad se ubica en el eje vertical (y), y el impacto en el eje horizontal x. (**Anexo 4.3** Mapeo de riesgos.)

Los riesgos identificados con un nivel de riesgo en el rango de 16 a 25 son considerados “altos”, de 9 a 15 “moderados”, y de 1 a 8 “bajos”.

3.2.4 PRIORIZACIÓN DE RIESGOS

El propósito de la priorización de riesgos es asistir en la toma de decisiones, con base en los resultados del análisis de riesgos, sobre los riesgos que necesitan prioridad para su tratamiento.

- ✓ Transcribir el nivel de riesgos y el nivel exposición.
- ✓ Definir el criterio de riesgo, de acuerdo a la siguiente escala:
  - Podemos tolerar este riesgo
  - Es un riesgo medianamente tolerable.
  - No podemos tolerar este riesgo
- ✓ Riesgos a tratar, marcar con una x los riesgos que tanto por su nivel o criterio previamente definido requieren ser tratados
- ✓ Asignar la prioridad década riesgo identificado en forma ordinal. (**Anexo 4.4** Priorización de riesgos.)

3.2.5 PLAN DE TRATAMIENTO DE RIESGOS

El tratamiento de los riesgos involucra seleccionar una o más acciones para implementarlas y mitigar los riesgos identificados.

a) Transcribir los riesgos identificados en el orden de prioridad establecido.

b) Definir las acciones que deben cumplirse para mitigar (de ser posible) el riesgo identificado.

Las opciones/acciones para el tratamiento del riesgo pueden ser:

- (E) Evitar el riesgo: es decidir no empezar o continuar con la actividad que genera el riesgo; implica descontinuar las actividades que los originan.
- (R) Reducir el riesgo: incluye los métodos y técnicas específicas para tratar los riesgos, identificándolos y proveyendo acciones para la reducción de su probabilidad e impacto.
- (C) Compartir el riesgo: reduce la probabilidad y el impacto mediante la transferencia u otra manera de compartir una parte del riesgo con terceros.
- (A) Aceptar el riesgo: no se realiza acción alguna para afectar la probabilidad e impacto.

c) Definir un indicador de desempeño para la administración de riesgos, por cada acción propuesta.

Los indicadores de desempeño o de gestión para la administración de riesgos son variables o parámetros que permiten medir de forma cuantitativa y cualitativa el grado de cumplimiento que deberán tener las acciones propuestas (opciones de tratamiento) para reducir, compartir y aceptar el

riesgo, en términos de eficiencia, economía, efectividad e impacto. Un indicador es la fuente de medición de cualquier objetivo, meta o proceso y permite medir el grado de avance en la ruta para alcanzarlos.

Los indicadores son concebidos como frases, que luego de su aplicación se transforman en cifras.

- Parámetros semánticos en la construcción de indicadores-

Uno de los problemas comunes en la redacción de indicadores, es la forma muy general en que se presentan. Se sugiere la siguiente metodología en su redacción:

1) Agregación más preposición

- 4 (cantidad de)……
- 90% (porcentaje de)……
- Un (Total de)……

2) Sustantivo plural (variable)

- carreteras……
- cuentas por cobrar……
- plan de mantenimiento vehicular……

Ejemplos adicionales de variables de indicadores: póliza de seguro, reglamento de salud y seguridad ocupacional, anteproyectos de ley, servidores, etc.

3) Verbo en participio pasado (acción)

mantenidas……

recuperadas……

implementado……

4) Adjetivo

De acuerdo a las normas y procedimientos de mantenimiento vial……

dentro del plazo de cobro ……

en cumplimiento de las especificaciones y manuales técnicos de cada vehículo ……

5) Complemento circunstancial (tiempo, lugar, etc.)

por la Dirección de Obras Públicas en el 2013.

por la Dirección Financiera a diciembre del 2013.

por la Dirección de Administración General en el 2013.

Estos requisitos semánticos, procuran definir el indicador y adecuarlo a las circunstancias que requiere la medición.

Señalar quien es responsable del cumplimiento (cargo y unidad en la que presta sus servicios) en el casillero 16.

Señalar la fecha en la se estima cumplir con la acción propuesta, en el casillero 17.(**Anexo 4.5** Tratamiento de riesgos.)

3.3 IDENTIFICACIÓN DE LOS CONTROLES CLAVES

3.3.1 PRUEBAS SUSTANTIVAS

El objetivo de las pruebas sustantivas es obtener la suficiente evidencia para que el auditor pueda juzgar si ha habido pérdidas materiales o podrían ocurrir en el ambiente de procesamiento de datos.

Pruebas sustantivas que pueden ser usadas.

a) Pruebas para identificar procesos erróneos.
b) Pruebas para evaluar la calidad de los datos.
c) Pruebas para identificar datos inconsistentes.
d) Pruebas para comparar datos con conteos físicos.
e) Confirmación de datos con fuentes externas.

3.3.2 PRUEBAS DE CUMPLIMIENTO

El objetivo de las pruebas de cumplimiento es determinar si el control es adecuado y si está funcionando en la forma que se planeó en el área informática.

Las pruebas de cumplimiento deben apoyarse en el alcance que se determinó, pudiendo soportarlo a través de:

a) Documentación

b) Manuales de usuario, técnicos y procedimientos.

c) Cambios en los programas

d) Solicitud por escrito.

e) Pruebas por parte de los usuarios.

f) Actualización de los manuales técnicos y de usuarios.

g) Verificar que los cambios en los programas sean realizados por el personal de informática o por el proveedor de la aplicación.

h) Copias de respaldo y de recuperación.

i) Contenido de las copias

j) Periodicidad de las copias.

k) Persona responsable

l) Custodia, almacenamiento, inventario.

m) Acceso a datos y programas.

n) Verificar la lista de usuarios que tiene acceso.

o) Revisar el procedimiento para otorgar y eliminar los accesos.

p) Analizar la periodicidad de los cambios de claves.

q) Capacitación de los usuarios

r) Controles en la entrada, proceso y salida.

3.4 PROCEDIMIENTOS DE AUDITORÍA A SER APLICADOS

Procedimientos que permitirán al auditor de sistemas guiarlo sobre los puntos importantes a evaluar dentro de la organización, no obstante la experiencia de este podrá hacer la ampliación o reducción del mismo, estando sujeto a su responsabilidad y objetividad. (Manual de Auditoria de Sistemas, s.f.)

3.4.1 ORGANIZACIÓN Y ADMINISTRACIÓN

3.4.1.1 PLANES ESTRATÉGICOS Y OPERATIVOS

- ✓ Verificar si en el plan estratégico institucional se encuentra incluido el plan estratégico de TI.
- ✓ Verificar si las actividades y metas del plan estratégico de TI están alineados, con los objetivos estratégicos institucionales y dar seguimiento al cumplimiento de los proyectos a largo plazo.
- ✓ Verificar la existencia de un plan operativo de TI para dar seguimiento al cumplimiento de metas de los proyectos a corto plazo.
- ✓ Verificar las actividades, períodos, grado de avance y responsables de ejecución de las actividades del plan estratégico.

- ✓ Verificar que el plan estratégico de TI sea traducido periódicamente en planes a corto plazo.

3.4.1.2 ESTRUCTURA ORGANIZACIONAL Y FUNCIONES

- ✓ Solicitar el organigrama de la institución e identificar la ubicación de TI, analizar su estructura jerárquica y que esté conforme a la situación actual. Así mismo verificar su vigencia y aprobación.
- ✓ Verificar si la estructura actual está encaminada a los logros de los objetivos del área de TI.
- ✓ Verificar si los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área de TI.
- ✓ Verificar si se consideran adecuados los departamentos y áreas en que está dividida la estructura de TI.
- ✓ Solicitar los manuales de puestos del área de TI y verificar que las funciones descritas correspondan con las que ejecuta cada empleado de TI.
- ✓ Evaluar el manual de puestos, su claridad en la delegación de autoridades, y que deben ir acompañadas de definiciones de las habilidades técnicas necesarias, para utilizarse como base para la evaluación del desempeño.

  Verificar si los puestos actuales son adecuados a la necesidad que tiene el área para cumplir con sus funciones.

- ✓ Identificar las causas de incumplimiento de las funciones y objetivos previstos por la Administración, como por ejemplo: falta de personal, personal no capacitado, cargas de trabajo excesivas, realización de otras actividades, planificación y la forma en que se desarrollan.
- ✓ Verificar que la posición de la unidad de tecnología esté en un nivel suficientemente alto para garantizar su independencia de los departamentos usuarios.
- ✓ Verificar que exista una separación adecuada de tareas entre los operadores de la computadora, los programadores de la aplicación y los analistas de sistemas.
- ✓ Verificar que exista un plan de capacitación y que éste responda a las necesidades de la institución en cumplimiento al plan estratégico de TI.
- ✓ Verificar que todo el personal tome un mínimo de cinco días consecutivos de vacaciones, de manera que alguien más pueda ejecutar las funciones específicas de un puesto determinado.
- ✓ Verificar que exista una política o norma apropiada para la separación de funciones y esta sea auditada.
- ✓ Revisar las descripciones de los puestos por cada departamento o unidad, de tal manera asegurar que cada una de ellas está conforme al cargo.

3.4.1.3 NORMAS Y POLÍTICAS

- ✓ Solicitar las políticas y normas establecidas para TI.
- ✓ Verificar que la Unidad de TI sea responsable de la formulación, desarrollo, documentación, divulgación y el control de las políticas; y que todas ellas estén por escrito y debidamente autorizadas y actualizadas.
- ✓ Verificar que la Unidad de TI haya creado mecanismos de divulgación que permitan asegurar que las políticas sean comunicadas y comprendidas por todo el personal involucrado directa o indirectamente con el área de TI.
- ✓ Verificar que las políticas o normas emitidas sean actualizadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional, para garantizar que sean funcionales y aplicables.
- ✓ Verificar si las políticas o normas son del conocimiento del personal de TI.
- ✓ Verificar la existencia de políticas o normas sobre reserva y confidencialidad de información.
- ✓ Verificar que las normas y políticas estén aprobadas por la máxima autoridad y que presenten fecha de vigencia.

3.4.2 SISTEMAS INFORMÁTICOS

- ✓ Verificar si existe un inventario de software aplicativo en el que se detalle la versión, el proveedor y la vigencia de la licencia, etc.
- ✓ Verificar el inventario de software contra las licencias, con el objeto de evitar sanciones por la Ley de propiedad intelectual.
- ✓ Verificar que no se permita a los programadores de las aplicaciones, modificar y ejecutar directamente programas en ambiente de producción.
- ✓ Verificar que existan controles sobre recursos compartidos en los equipos informáticos como: discos duros, carpetas o archivos.
- ✓ Verificar si el diseño de las nuevas aplicaciones o de las modificaciones a los módulos puestos en producción, son aprobados o revisados por el jefe de la Unidad de Tecnología.
- ✓ Verificar si existen procedimientos definidos, estándares para las etapas de desarrollo de un nuevo sistema o cambios a los ya existentes.
- ✓ Verificar si cuenta con mecanismos de seguridad para identificar los requerimientos de seguridad y control interno para cada proyecto de desarrollo y modificación de sistemas de información previo a su desarrollo.
- ✓ Verificar e identificar si se incluye en el diseño de nuevas aplicaciones o en las modificaciones de los sistemas de

información controles de aplicación que garanticen que los datos de entrada y salida estén completos.

- ✓ Verificar si consideran aspectos básicos de seguridad y control interno del módulo a ser desarrollado y modificado, y estos son evaluados junto con el diseño conceptual del mismo.
- ✓ Identificar si existe una metodología estándar, para el desarrollo de un plan de pruebas, en donde se incluyan pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga para cada módulo.
- ✓ Verificar si la formulación del procedimiento de prueba, y los datos de prueba son revisados y aprobados.
- ✓ Verificar si se aplican adecuadas medidas de seguridad para prevenir divulgación de información sensitiva durante las pruebas.
- ✓ Verificar que los resultados de las pruebas son revisados y aprobados por el usuario.
- ✓ Verificar que exista un archivo lógico o bitácora, que permita identificar los errores de ejecución de aplicaciones, sistema operativo y BD.
- ✓ Verificar que exista una persona responsable en el área de TI de revisar periódicamente los archivos logs o bitácoras del sistema.
- ✓ Verificar que la entidad cuente con un servidor de desarrollo que sea de uso de los programadores para el desarrollo y pruebas de aplicaciones internas.

- ✓ Verificar que los programadores no tengan acceso a la línea de comandos en los servidores de producción y acceso a estos para consulta.
- ✓ Verificar si existe una persona responsable dentro del área de tecnología encargada de ejecutar programas de diagnóstico de la red institucional.
- ✓ Verificar el reporte de caídas al sistema, medir la frecuencia y magnitud de los mismos.

3.4.2.1 ADMINISTRACIÓN DE CAMBIOS

- ✓ Verificar si existe un sistema para el control de requerimientos de usuarios que afecten la estructura de los sistemas de información.
- ✓ Verificar el o los tipos de formularios utilizados para el control de cambios.
- ✓ Verificar si existen procedimientos definidos para determinar el estatus de cada solicitud de cambios realizados.
- ✓ Verificar el procedimiento de solicitudes identificadas como urgentes.
- ✓ Verificar que exista un procedimiento de control de cambios de los programas y del traslado del ambiente de desarrollo a producción.
- ✓ Verificar si se mantiene un registro de cambios en los programas, que indique, a fin de proveer el orden cronológico exacto del

sistema. Así mismo identificar el responsable de realizar el cambio.

- ✓ Verificar si se requiere de la aprobación y autorización por escrito del responsable de la Unidad de Tecnología, para todas las modificaciones antes de hacer los cambios.
- ✓ Verificar si los cambios al sistema operacional o programas aplicativos, sus pruebas y resultados son revisados por el responsable de la programación técnica o quien hace sus funciones.

3.4.2.2 ACREDITACIÓN DE SISTEMAS

- ✓ Verificar si se planifica la migración de los datos, y se define responsabilidades.
- ✓ Verificar si las pruebas a los nuevos sistemas o a las modificaciones a los nuevos sistemas son llevadas a cabo por un grupo de prueba independiente, diferente a los desarrolladores.
- ✓ Verificar si cuentan con procedimientos establecidos para asegurar que las pruebas piloto, o en paralelo sean llevadas a cabo con planes pre establecidos.
- ✓ Verificar si se incluye como parte de la instalación y acreditación del sistema pruebas de aceptación por parte de los usuarios finales de los sistemas nuevos o de las modificaciones a los sistemas de información.

- ✓ Verificar como certifican los usuarios finales la aceptación final de los nuevos sistemas.
- ✓ Verificar el proceso utilizado para el traslado de las nuevas aplicaciones o modificaciones al sistema de producción.

3.4.2.3 DOCUMENTACIÓN TÉCNICA

- ✓ Verificar la existencia y disponibilidad de diagramas entidad-relación.
- ✓ Verificar la existencia de manuales de usuario de los aplicativos puestos en producción
- ✓ Verificar si los manuales de usuario, se encuentran autorizados y disponen de fecha de vigencia, con la finalidad de identificar su actualización.
- ✓ Verificar la existencia de diccionario de datos, de las tablas, o archivos que conforman los sistemas puestos en producción.

3.4.2.4 CONTROL DE ENTRADAS Y SALIDAS

- ✓ Verificar si existe un control a nivel de perfil de usuario, que ingresan datos, para evitar ingreso para usuarios no autorizados
- ✓ Verificar que existan controles sobre los documentos de propiedad con número de serie secuenciales, y el ingreso de dichos números al sistema para crear la relación entre ambos.

- ✓ Verificar que exista un registro de la fecha de proceso y la fecha de transacción para las transacciones de entrada.
- ✓ Comprobar que el control utilizado para demostrar que la información a ingresar se encuentra autorizada
- ✓ Verificar que procedimientos existen para el manejo de errores con el fin de proporcionar al personal usuario instrucciones sobre la corrección de errores en los documentos fuentes.
- ✓ Revisar los tipos de errores y las razones y su ocurrencia con el fin de determinar si los problemas son ocasionados por el programa o por el ingreso incorrecto de los datos.
- ✓ Verificar si se obtiene una copia del log, que registra el sistema en relación a las entradas de datos.

3.4.2.5 ADMINISTRACIÓN DE BD

- ✓ Verificar que mecanismos y herramientas usa, el administrador de la base de datos (DBA), para administrar y supervisar la base de datos.
- ✓ Verificar el procedimiento utilizado para definir el nivel de acceso a los usuarios.
- ✓ Verificar que únicamente el administrador de la base de datos tiene privilegios a nivel de administrador para hacer cambios a la base de datos.

- ✓ Verificar los diferentes tipos de usuarios que tienen acceso a la base de datos e identificar su clasificación por medio de la siguiente segmentación: usuarios operativos, técnicos, usuarios que modifican los datos, usuarios que modifican la estructura.
- ✓ Verificar que el administrador de la base de datos disponga de procedimientos escritos para la restauración de la base de datos, en caso de una destrucción total o parcial.
- ✓ Verificar que el usuario y la clave del DBA se registre en un sobre lacrado y este se resguarde en un lugar seguro.
- ✓ Verificar que el Administrador de la base de datos sea el responsable de la integridad de la base de datos y desarrolle reglas de validación y acceso.
- ✓ Verificar que el administrador de la Base de Datos documente cualquier cambio que se realice en la base de datos.
- ✓ Verificar que el administrador de la base de datos administra el diccionario de datos.
- ✓ Verificar que el administrador de la base de datos es el responsable de la seguridad global de la base de datos.
- ✓ Verificar que el administrador de la base de datos tiene el control para que no se realicen prueba de base de datos de producción, sino que se dispongan de diferentes ambientes para este fin.
- ✓ Verificar que los usuarios no tengan acceso directo a la base de datos, sino que el acceso sea a través del servidor de aplicaciones.

- ✓ Verificar que solo el usuario administrador tenga el privilegio de acceso a las tablas usuarias y contraseñas.
- ✓ Verificar si el software de base de datos utilizado, cuenta con registros de auditoría para registrar los eventos que tienen registros.
- ✓ Verificar en las tablas de registros de auditoría de las bases de datos, las acciones de intentos de conexión, acceso a los objetos y acceso a las bases.
- ✓ Verificar las acciones que el administrador de la base de datos realiza con las tablas de registros de auditoría de la base, para corregir posibles fallas o accesos no autorizados.
- ✓ Verificar el parámetro para permitir auditoría a la Base de Datos, tenga el valor que equivale o permita auditoría.

3.4.3 INFRAESTRUCTURA TECNOLÓGICA

3.4.3.1 MANTENIMIENTO DE HARDWARE

- ✓ Verificar que existan contratos de mantenimiento preventivo y correctivo para el equipo informático de la institución.
- ✓ Verificar si existen informes sobre el mantenimiento a nivel físico y de parámetros efectuados por el proveedor a los servidores principales de la institución.

3.4.3.2 REDES Y COMUNICACIONES

- ✓ Verificar la existencia de un inventario de direcciones IP, asignadas a los usuarios, con la información general asociada a cada IP.
- ✓ Verificar la existencia de un inventario actualizado de equipo de comunicaciones: módems, hubs, terminales, routers, firewalls, etc.
- ✓ Verificar el software instalado en la red, por ejemplo sistema operativo, lenguaje, programas, paqueterías, utilerías.
- ✓ Verificar el diagrama de red para identificar las interconexiones internas y externas.
- ✓ Verificar la existencia de servicios de Intranet, internet y sitio web.
- ✓ Verificar la existencia de procedimientos de autorización para conectar nuevo equipo en la red.
- ✓ Verificar si el plan de contingencias considera el respaldo y recuperación de los sistemas de comunicaciones.
- ✓ Verificar si existe el control y monitoreo de las conexiones a fin de deshabilitar aquellas que no estén en uso.
- ✓ Verificar que exista software de monitoreo de las conexiones remotas, de forma que se documenten los incidentes o interrupción del servicio de comunicación.
- ✓ Verificar si disponen de reportes de incidentes contingencias y circunstancias que afecten el funcionamiento de la red, conforme a la bitácora.

3.4.3.3 ALMACENAMIENTO

- ✓ Verificar si la cintoteca se encuentra ubicada en el mismo edificio o en otro.
- ✓ Verificar que procedimientos utilizan para copiar: documentos, datos, programas, reportes, etc y si estos están documentados.
- ✓ Verificar si el proceso de copiado de la información, utiliza procesos de encriptación y autenticación.
- ✓ Verificar la periodicidad con la que realizan pruebas de restauración con los medios magnéticos, con la finalidad de asegurar la recuperación.

3.4.3.4 MANTENIMIENTO DE HARDWARE

- ✓ Verificar que exista contratos de mantenimiento preventivo y correctivo para los equipos informáticos de la entidad.
- ✓ Verificar si el mantenimiento otorgado por el proveedor es conforme a lo establecido en el contrato.
- ✓ Verificar la programación del mantenimiento preventivo y correctivo con la finalidad de reducir la frecuencia y el impacto de fallas de rendimiento.
- ✓ Verificar cual es el proceso de notificación de fallas del equipo informático y como se documenta dicho proceso.

- ✓ Verificar si existen informes sobre el mantenimiento a nivel físico y de parámetros efectuados por el proveedor a los servidores principales de la institución.

3.4.4 SEGURIDADES

3.4.4.1 PLAN DE CONTINGENCIAS

- ✓ Identificar la existencia del plan de contingencias y obtener una copia, que contenga la fecha de vigencia, última actualización y el funcionario responsable de la autorización.
- ✓ Verificar que el plan hace referencia a normas y políticas dictadas por tecnología.
- ✓ Verificar si el plan está orientado a superar procesos críticos e imprevistos en el menor tiempo posible.
- ✓ Verificar que en el plan se encuentren definidas las tareas a realizar para cada una de las personas involucradas en el plan.
- ✓ Verificar que en el plan se hayan considerado pruebas para los distintos escenarios y los mecanismos para la solución, por ejemplo fallas en los servidores centrales y de servicios, en los suministros eléctricos, fallas en los enlaces de comunicación, falta de insumos, respaldos actualizados, etc.
- ✓ Identificar si el plan incluye o describe la participación de un comité de administración de desastres o del equipo de

emergencia, el mismo que se encargará de ejecutar las actividades previas durante y después del desastre, contenidas en el plan de desastres.

- ✓ Verificar si existe un servidor de contingencia para todas las aplicaciones críticas.
- ✓ Verificar que el plan disponga un anexo con los nombres del personal de soporte, administrativo y proveedores de servicio, el cargo, número telefónico fijo y móvil.
- ✓ Realizar llamadas telefónicas a parte del personal involucrado en el plan con la finalidad que los números son correctos y están actualizados.
- ✓ Verificar que el plan haya sido probado al menos dos veces al año.
- ✓ Entrevistar al personal para identificar si conocen las responsabilidades que tienen asignadas en una situación de desastre.
- ✓ Verificar si existen procedimientos definidos para actualizar el manual. Así mismo si aplican y distribuyen las actualizaciones a los usuarios involucrados.
- ✓ Verificar que el plan contenga los planos del centro de cómputo, diagramas de cableado eléctrico, diagramas de red, diagramas de ducto e inventarios de hardware.

- ✓ Comprobar que exista una copia de datos actualizada, programas y documentación técnica del sistema, que se almacene en un lugar externo a la empresa.
- ✓ Verificar que el personal involucrado tiene el conocimiento de los procedimientos establecidos para la continuidad de las operaciones en caso de desastres.

3.4.4.2 SEGURIDAD LÓGICA

- ✓ Verificar que el software de comunicaciones, exige código de usuario y contraseña para su acceso.
- ✓ Verificar que los usuarios no pueden acceder a ningún sistema sin antes haberse autenticado correctamente a la red de la entidad
- ✓ Verificar si se inhabilita al usuario después de ingresar la contraseña, después de un número determinado de intentos fallidos.
- ✓ Verificar que el sistema operativo obliga a cambiar la contraseña periódicamente.
- ✓ Verificar que la contraseña no sea menor a 8 caracteres y que sea una combinación de números y letras, entre ellos mayúsculas y minúsculas.
- ✓ Verificar que las contraseñas no son mostradas cuando se ingresan.

3.4.4.3 SEGURIDAD INFORMÁTICA

- ✓ Verificar que existan políticas de seguridad definidas y aprobadas.
- ✓ Verificar que las políticas de seguridad contengan elementos como: confidencialidad, integridad y disponibilidad.
- ✓ Verificar que las políticas contengan mecanismos para medir: riesgos y amenazas, análisis de riesgos, plan de seguridad, controles preventivos y correctivos, plan de contingencia, biometría, firma electrónica, protección y defensa.
- ✓ Identificar información, que mecanismos utilizan para no revelar la información a personas no autorizadas, acceso a información confidencial y protección de datos.
- ✓ Verificar como controlan las amenazas externas las amenazas como hackers o espías.
- ✓ Verificar que controles lógicos y físicos se utilizan para asegurar que solo el personal autorizado pueda acceder a la información, dentro de los niveles de atención.
- ✓ Verificar como monitorean y rastrean la actividad de los usuarios administrativos y operativos a fin de detectar y corregir desviaciones en el uso correcto de la información, o en el cumplimiento de las normas y procedimientos asociados a la seguridad de la información.

- ✓ Verificar si las firmas digitales son emitidas, manejadas, y/o certificadas por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.

3.4.4.4 SEGURIDAD FÍSICA

- ✓ Verificar el cumplimiento de lo establecido en las normas de seguridad de acceso, al centro de cómputo implementadas por TI.
- ✓ Verificar que exista formulario de registro para el ingreso, al centro de cómputo, para el personal externo al área.
- ✓ Verificar que exista un sistema automático de extinción de fuego en el centro de cómputo.
- ✓ Verificar la existencia de detectores de fuego y humo tanto en el área de techo y piso falso.
- ✓ Verificar si el personal se encuentra capacitado para el uso y manejo de extintores.
- ✓ Verificar si existe vigilancia en el área de TI las 24 horas.
- ✓ Verificar si se registran las acciones de las operadoras

3.5 EL PROCESO DE LA AUDITORÍA

El proceso de auditoría en las entidades públicas es el mismo en todo tipo de auditorías es por ello que se tomó como referencia la guía de Auditoría Ambiental.(Contraloria General, Guia de auditoria Ambiental, 2013)

3.5.1 ORDEN DE TRABAJO

Los Directores de las Unidades de Control emite la orden de trabajo, documento que determina: el tipo y nombre de la acción de control, la institución responsable de la ejecución o manejo del proyecto, las instituciones relacionadas, el alcance, el periodo a hacer examinado, los objetivos, la conformación del equipo de trabajo, la distribución de las responsabilidades y el tiempo asignado.

3.5.2 NOTIFICACIÓN DE INICIO

De manera simultánea a la emisión de la orden de trabajo, el Director de la Unidad de Control o Delegado Provincial pertinente comunica el inicio de la acción de control a la máxima autoridad de la entidad auditada, incluyendo los contenidos establecidos en el artículo 20 del Reglamento a la Ley Orgánica de la Contraloría General del Estado.

3.5.3 SOLICITUD INICIAL DE INFORMACIÓN

Luego de la emisión de la orden de trabajo y las notificaciones de inicio a las máximas autoridades de la entidad auditada y de las instituciones relacionadas, se emite las solicitudes iniciales de información con los siguientes objetivos:

- ✓ Recopilar información básica, que permita al equipo auditor alcanzar un nivel de conocimiento general de la entidad a ser auditada.
- ✓ Identificar aspectos significativos relevantes y sensibles, que pasarán a constituir las áreas críticas
- ✓ Ayudará a elaborar la planificación.

Las solicitudes iniciales de información son elaboradas por el jefe de equipo, relacionadas para nuestro caso información sobre el control interno, como por ejemplo:

- ✓ Listado de leyes, reglamentos, ordenanzas de las entidades auditadas.
- ✓ Planificación estratégica y operativa
- ✓ Organigramas y manual de funciones
- ✓ Políticas y procedimientos, etc.

En el oficio se determinará el plazo de 10 días, desde la fecha de recepción del requerimiento, para emitir la respuesta correspondiente, de conformidad con lo establecido en los artículos 76 y 88 de la Ley Orgánica de la Contraloría General del Estado y 7 de su Reglamento de aplicación.

3.5.4 DIAGNÓSTICO GENERAL Y PLANIFICACIÓN

A más de la documentación de la información recibida y recopilada, es necesario realizar reuniones de trabajo con las personas vinculadas con la auditoría, y de ser el caso inspecciones de campo a las instalaciones de la entidad, a las diferentes áreas a evaluar.

El equipo de auditoría debe cumplir con lo siguiente:

- ✓ Revisar la información general disponible.
- ✓ Visualizar la naturaleza de la entidad.
- ✓ Definir el marco regulatorio informático aplicable: leyes, reglamentos, ordenanzas, acuerdos particulares de la institución, entre otros, con el fin de establecer puntos de control.
- ✓ Identificar las funciones de las unidades y personas responsables del diseño, ejecución y control del área de informática. Elaborar un listado de funcionarios y autoridades relacionados con la auditoria a ser notificados.
- ✓ Elaborar y distribuir las notificaciones de inicio de la auditoría, de conformidad con las disposiciones establecidas en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 21 de su Reglamento.

En la planificación se establece, el enfoque propuesto para la auditoría, detallando las actividades a desarrollar, la estrategia a emplear, las fechas necesarias y los recursos necesarios.

3.5.5 DESARROLLO Y RECOPILACIÓN DE LA INFORMACIÓN

En esta etapa comprende el desarrollo de los cuestionarios de control interno y la evaluación de riesgos con la finalidad de identificar las áreas críticas.

Luego de ser identificadas las áreas críticas, y aplicar los procedimientos de auditoría, y si es necesario solicitar información como evidencia de los hallazgos realizados, se los puede solicitar.

3.5.6 COMENTARIOS, CONCLUSIONES Y RECOMENDACIONES

Los comentarios consisten en la exposición de condición, criterio, causa y efecto de los hallazgos obtenidos en la ejecución de la acción de control.

Las conclusiones representan los pronunciamientos profesionales del auditor sobre el análisis del control interno, se sustentan en el análisis de la evidencia de la auditoría, identificando los responsables de las inobservancias de carácter técnico, legal o económico, describiendo la norma que inobservó y las consecuencias y efectos para la institución.

Las recomendaciones son las acciones que se requiere para corregir los incumplimientos detectados. En las recomendaciones se puede tomar como base la aplicación de buenas prácticas de TI.

3.5.7 COMUNICACIÓN DE RESULTADOS E INFORME FINAL

En cumplimiento a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, los auditores en el desarrollo de la acción de control deben mantener la comunicación con los servidores de la organización auditada y demás personas relacionadas con las actividades relacionadas.

La comunicación de resultados provisionales, se realizará al finalizar el trabajo de campo mediante un documento escrito en el que se incluirá los comentarios y conclusiones referentes a los hallazgos significativos detectados.

No se incluirán las recomendaciones con la finalidad de cumplir con el debido proceso y dar oportunidad a los auditados de presentar documentos que aclaren o desvirtúen los hallazgos.

El borrador del informe revisado por el supervisor del equipo de control, se da a conocer en la conferencia final.

El informe final está sujeto a los procesos de control de calidad institucionales, cuyo objetivo fundamental es la descripción jerárquica de los hallazgos, identificados por el equipo de auditoría para establecer las acciones que permitan corregir los incumplimientos.

La estructura general del informe deberá sujetarse a lo establecido en el Reglamento para elaboración y trámite de informes de auditoría.

3.5.8 SEGUIMIENTO

Una vez receptado el informe final aprobado por la Contraloría General del Estado, las entidades auditadas, deberán elaborar un plan que permita aplicar las recomendaciones emitidas, en el cual se determinará las actividades necesarias como: recursos, responsables y tiempos.

La Contraloría General del Estado puedo evaluar, la efectividad de las recomendaciones emitidas a través del seguimiento.

3.6 INDICADORES DE LA SITUACIÓN REAL DE LA EVALUACIÓN DEL CONTROL INTERNO EN LAS ENTIDADES PÚBLICAS.

Con la finalidad de conocer la estructura organizacional de las entidades del sector público, el manejo de procesos así como también el

conocimiento de la normas de control interno, se realizó la encuesta a 15 entidades. (**Anexo 5.1** Encuestas).

Se efectuaron las siguientes preguntas y se obtuvo los siguientes resultados. (**Anexo 5.2** Tabulación de resultados)

- ✓ La pregunta 1, da a conocer las áreas de TI que son parte de la estructura de organizacional implementada en las diferentes instituciones. Las áreas que se encuentran en todas las instituciones son infraestructura tecnológica y soporte técnico con un 33%, seguido de desarrollo y mantenimiento de sistemas con un 20%, con un 8% se encuentran las instituciones que solo realizan mantenimiento de sistemas, el 4% le corresponde al área de seguridad y en último lugar se encuentra otros con 2%.

TABLA 4.- ÁREAS DE TI

Nro.	Pregunta	Opciones de respuesta	Código respuesta	%	Ponderado
1	Cuál de las siguientes áreas de TI, son parte de la estructura de organizacional implementada en su Institución?	Infraestructura Tecnológica	1.1	100	33
		Desarrollo y Mantenimiento de Sistemas	1.2	60	20
		Mantenimiento de Sistemas	1.3	27	8
		Soporte Técnico	1.4	100	33
		Seguridades	1.5	13	4
		Ninguna	1.6	0	0
		Otros	1.7	7	2
				307	

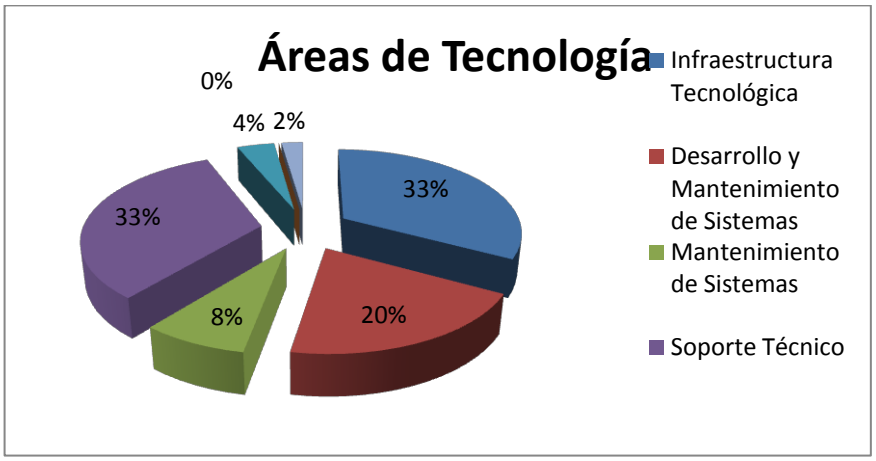

GRÁFICO 1.- ÁREAS DE TI

- ✓ La pregunta 2, da a conocer si existe un manual de procesos en el área de TI. El 87% de los encuestados indicaron que no tienen definido los procesos mientras que el 37% si lo tiene.

TABLA 5.- MANUAL DE PROCESOS

Nro.	Pregunta	Opciones de respuesta	Código respuesta	%	Ponderado
2	¿Cuenta con un manual de procesos para el área de TI?	Si	2.1	13%	13%
		No	2.2	87%	87%
				100%	

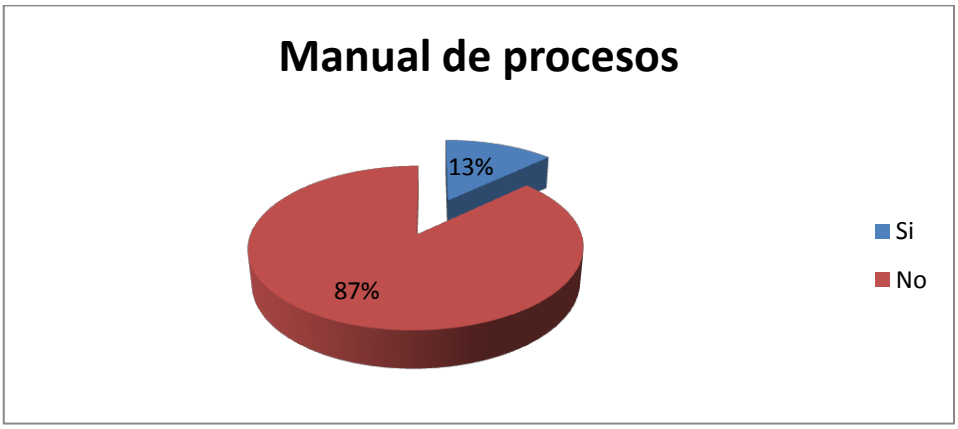

GRÁFICO 2.- MANUAL DE PROCESOS

✓ La pregunta 3, da a conocer si se han asignado funciones y responsabilidades en el área de TI. El 73% de los encuestados indicaron que no se han definido mientras que el 27% si lo tiene.

TABLA 6. FUNCIONES Y RESPONSABILIDADES

Nro.	Pregunta	Opciones de respuesta	Código respuesta	%	Ponderado
3	¿Se le han asignado funciones y responsabilidades al persona de tecnología?	Si	3.1	27%	27%
		No	3.2	73%	73%
				100%	

GRÁFICO 3.- FUNCIONES Y RESPONSABILIDADES

✓ La pregunta 4, hace referencia al conocimiento de las normas de control interno emitidas por la Contraloría General del Estado. El 73% de los encuestados indicaron que no tiene conocimiento, mientras que el 27% si las conoce.

TABLA 7.- FUNCIONES Y RESPONSABILIDADES DEL PERSONAL DE TI

Nro.	Pregunta	Opciones de respuesta	Código respuesta	%	Ponderado
4	¿Tiene conocimiento de las normas de control interno emitidas por la Contraloría General del Estado?	Si	4.1	27%	27%
		No	4.2	73%	73%
				100%	

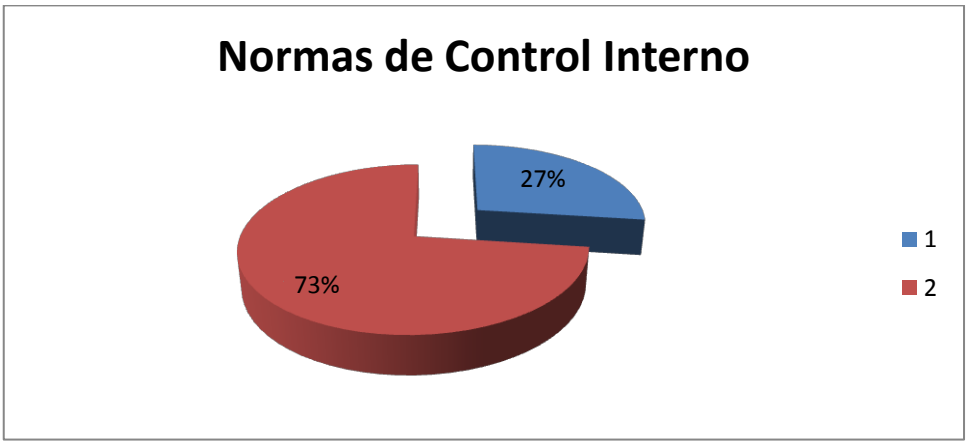

GRÁFICO 4.- NORMAS DE CONTROL INTERNO

- ✓ La pregunta 5, hace referencia a la frecuencia en que las entidades realizan la evaluación del control interno. El 73% de los encuestados indicaron que no tiene conocimiento, mientras que el 27% si las conoce.

TABLA 8.- EVALUACIÓN DE CONTROL INTERNO

Nro.	Pregunta	Opciones de respuesta	Código respuesta	%	Ponderado
5	¿Con qué frecuencia realiza evaluaciones de control interno?	Anual	5.1	7	7
		Semestral	5.2	7	7
		Trimestral	5.3	0	0
		Mensual	5.4	0	0
		Semanal	5.5	0	0
		Diario	5.6	0	0
		Ninguno	5.7	87	86
				101	100

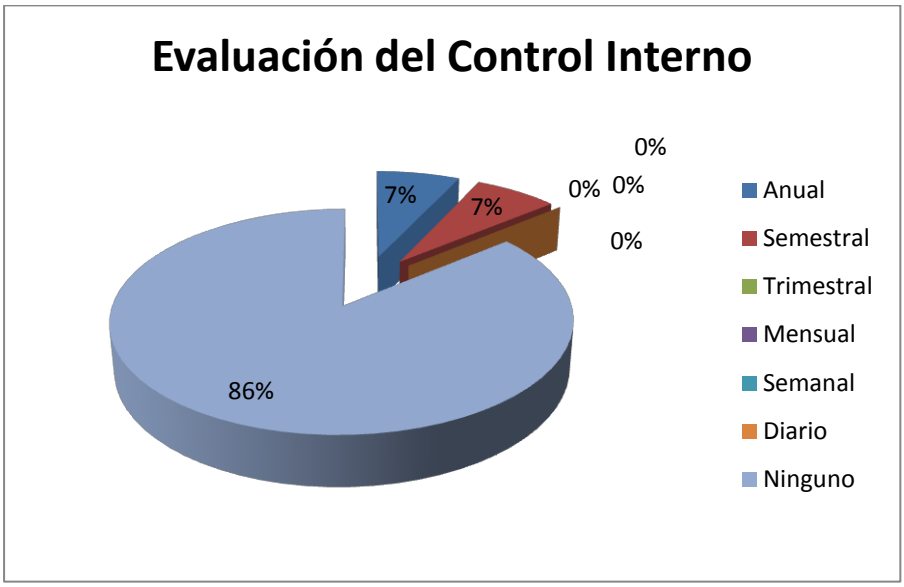

GRÁFICO 5.- EVALUACIÓN DE CONTROL INTERNO

CAPÍTULO IV
APLICACIÓN PRÁCTICA DE LA GUÍA DE EVALUACIÓN DE CONTROL INTERNO

4.1 DIAGNÓSTICO PRELIMINAR

4.1.1 FORTALEZAS

- ✓ Aplicaciones con estándares abiertos.
- ✓ Conocimiento y profesionalismo del personal del área de tecnología.
- ✓ Posicionamiento de la institución como referente en el uso de software libre en el sector público.
- ✓ Plataforma tecnológica.

4.1.2 OPORTUNIDADES

- ✓ Aplicar tecnología de punta en los procesos que se realizan manualmente.
- ✓ Políticas públicas que apalancan el desarrollo del software libre o de código abierto.
- ✓ Establecer alianzas estratégicas para la gestión de TIC con entidades públicas similares en Latinoamérica.

4.1.3 DEBILIDADES

- ✓ Falta de soluciones tecnológicas que soporten los procesos.

- ✓ Falta de un comité que procese, valide y apalanque los proyectos tecnológicos.
- ✓ Insuficiente personal capacitado.
- ✓ Salida de personal técnico capacitado en áreas críticas.
- ✓ Mantener enlaces de comunicación alternos.

4.1.4 AMENAZAS

- ✓ Agitación social.
- ✓ Vulnerabilidad en el acceso a la Institución.
- ✓ Posibles ataques a la infraestructura tecnológica por hackers.

4.2 CUESTIONARIOS DE EVALUACIÓN DE CONTROLES

Consiste en un conjunto amplio de preguntas, que están orientadas a comprobar el cumplimiento de políticas, planes, programas, normas, procedimientos y funciones tanto generales como específicas relacionados con algún aspecto en particular. Las preguntas debe ser sencillas, directas, concisas, y orientadas hacia los diferentes niveles jerárquicos de la entidad objeto de la auditoria.

4.2.1 ADMINISTRACIÓN Y ORGANIZACIÓN

TABLA 9 ORGANIZACIÓN Y ADMINISTRACIÓN

PREGUNTAS	SI	NO	OBSERVACIONES
Existe algún documento que contiene las funciones que son competencia de la Coordinación General de Servicios Tecnológicos, está aprobado y se respeta?	√		El Reglamento Orgánico Funcional se encuentra aprobado
Existe un organigrama con la estructura de organización del área de TI adecuada para el tamaño y las actividades de sus operaciones? Con que áreas cuenta?	√		
Se revisa y modifica periódicamente la estructura organizacional, con la finalidad de reflejar los cambios en la unidad o coordinación de servicios tecnológicos?	√		
El marco de trabajo para los procesos de tecnología de información permite la definición y seguimiento de los objetivos de los procesos que han sido definidos e implementados, así como formalmente documentados y aprobados?		√	
Las funciones y responsabilidades del personal han sido, correctamente establecidos, formalizados, documentados y satisfacen los requisitos del área. Son ejecutados por el personal con la suficiente formación y experiencia en la materia?	√		Falta asignar funciones al nuevo personal que ingresó.
Existe un manual de funciones? Existe un orgánico funcional?		√	
Se realizan evaluaciones periódicas de desempeño a los servidores?		√	
Existe un Plan Informático Estratégico y Tecnológico, alineado al Plan Estratégico Institucional, Plan Nacional de Desarrollo y a las políticas públicas aprobados por la máxima autoridad?		√	Existe un plan estratégico de tecnología para el año 2012-2016 no aprobado. En este momento se está realizando la Planificación Estratégica Institucional 2013-2017

Continúa

Existen Planes operativos de tecnología de información alineados con el plan estratégico informático y objetivos estratégicos de la institución aprobados por la máxima autoridad?		√	Plan operativo 2013 no aprobado.
El Plan Estratégico y planes operativos se revisa y actualiza de manera permanente?. Se monitorea y evalúa de forma trimestral?		√	
Existen políticas, estándares y procedimientos aprobados y difundidos por la máxima autoridad, que permitan regular las actividades del área de TI?		√	Solo existe las políticas de utilización de software libre No existen políticas para las demás áreas.
Están definidas métricas de calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas, mensajería de datos, legalidad del software entre otros, alineados con leyes conexas, y estándares de TI?		√	Se están realizando evaluaciones de control interno, implementando firmas electrónicas, Falta calidad, seguridad, propiedad intelectual, mensajería de datos.
Se tiene incorporado la gestión de riesgos e indicadores de gestión de desempeño?		√	
Existe un diccionario de datos con las reglas de sintaxis de la organización, el esquema de clasificación de datos y sus niveles de seguridad correspondientes, actualizado y documentado de forma permanente?		√	
Se garantiza la consistencia y seguridad de la información de los SI con los recursos proporcionales y dicha información se alinea con la estrategia y objetivos de la institución.	√		Grabaciones de información Control de acceso a los sistemas y al Data Center. Cumplimiento del Reglamento Interno.
Cuentan con un modelo entidad-relación, modelo físico, modelo conceptual?		√	No todos los sistemas cuentan con los modelos entidad-relación.
En los proyectos se realiza la descripción de la naturaleza, objetivos, alcance, relación con otros proyectos institucionales, cronograma de actividades, presupuesto referencial, servidor responsable, participación y aceptación de los usuarios interesados?	√		
Se ha descrito y dimensionado el proyecto según las normas establecidas?	√		
Se han evaluado los riesgos asociados al proyecto?	√		
Existe documentación formal de los entregables, aprobaciones compromisos formales mediante el uso de	√		

Continúa

actas o documentos electrónicos legalizados en las diferentes etapas del proyecto inicio, planeación, ejecución control, monitoreo y cierre del proyecto.		
Se registran, monitorea y controlan el avance de los proyectos, así como los recursos invertidos en los mismos.	√	
En la parte del cierre de los proyectos se realiza la aceptación formal de las pruebas que certifican con el cumplimiento de los objetivos planteados?	√	
Se tiene aprobado un plan de capacitación para el personal de tecnología y para los usuarios que utilizan los servicios de información, formulado conjuntamente con el área de talento humano?	√	
Cuentan con un comité informático?. Se encuentra definido sus objetivos, integración, funciones entre otros aspectos.		√

4.2.2 SISTEMAS INFORMÁTICOS

TABLA 10 SISTEMAS INFORMÁTICOS

PREGUNTAS	SI	NO	OBSERVACIONES
Se han adoptado y difundido políticas y estándares para codificación de software, nomenclaturas, interfaz de usuario, eficiencia del desempeño de sistemas, planes de pruebas, entre otros?		√	
Hay un estándar general para toda la documentación generada incluyendo documentación técnica (análisis, diseño, documentación de los programas), manuales de usuario, etc		√	No se tiene estándares definidos, existen algunos formatos como el de control de cambios.
Están definidas las prácticas de análisis y diseño e incluye las técnicas y herramientas a usar. Así como también hay una guía o prácticas de programación para cada uno de los lenguajes homologados?		√	
Definición de procedimientos para mantenimiento y liberación de software de aplicación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento o por requerimientos de los usuarios.	√		Se tiene documentación en excel y en el sistema mantis
Se cuenta con políticas y procedimientos relacionados con la captura, actualización, procesamiento, almacenamiento y salida de datos, que aseguren que los mismos sean completos, precisos, confiables y válidos?		√	
Políticas y procedimientos actualizados, relacionados con la instalación, administración, migración, mantenimiento y seguridad de la base de datos?		√	
Las adquisiciones de software o las soluciones tecnológicas son ejecutadas de acuerdo al portafolio de servicios, a los planes estratégicos y operativos, al plan de compras aprobados?	√		
En los contratos para la adquisición de software contienen el detalle suficiente como: aspectos técnicos, licencias de uso	√		

Continúa

y servicio, procedimientos de recepción del producto, garantías de soporte, mantenimiento y actualización?			
Existe un documento que recoge la descripción general de la necesidad planteada por el usuario y los objetivos generales, así como las posibles restricciones técnicas operativas y económicas.	√		
Se ha determinado formalmente, el grupo de usuarios que participará en el proyecto identificándose sus perfiles, dejando claro sus tareas y responsabilidades.		√	
Se ha realizado un plan detallado de entrevistas, con el grupo de usuarios y con los responsables de las unidades afectadas que permitan conocer como valoran el sistema actual y lo que esperan del nuevo sistema	√		Si se realizan entrevistas con las unidades requirientes, con los usuarios no.
Existe un catálogo de requisitos? Que requisitos incluyen? Cada requisito tiene una prioridad y está clasificado en funcional y no funcional		√	
El catálogo de requisitos ha sido revisado y aprobado por el grupo de usuarios y responsables?		√	
Las especificaciones del sistema incluye requisitos de: tipos de usuario, definición de interfaces, entradas, procesamiento, salidas, control, seguridad, trazabilidad o pistas de auditoria?	√		Para algunos sistemas existen para otros no
Se han descrito con suficiente detalle, las interfaces: pantallas a través de las cuales el usuario navegará por la aplicación, incluyendo todos los campos significativos, menús, botones, etc, así como informes y formularios asociados si existen. Si hay normas de diseño o estilo de pantallas, informes, formularios, etc. En el área se verificará que se respeta.	√		Para algunos sistemas existen para otros no
Existen controles permanentes que permiten prevenir, detectar y corregir inconsistencias ocurridas durante el procesamiento de datos?		√	Faltan controles en algunos sistemas
Se han definido los requisitos del entorno de pruebas y el alcance de las pruebas?		√	
Se ha elaborado el plan de pruebas de aceptación del sistema, este es coherente con el catálogo de requisitos, la		√	

Continúa

especificación funcional del sistema y contempla todos los recursos necesarios para llevarlos a efecto ?			
Los usuarios ratifican, que los requisitos especificados en el catálogo de requisitos, asi como los casos de uso son válidos, consistentes y completos?	√		Para algunos sistemas si se realizaron las aprobaciones con los usuarios
Cualquier petición de cambio de los requisitos que pueda surgir posteriormente debe ser evaluada y aprobada.	√		
Están definidos todos los elementos que configuran el entorno tecnológico esto es (servidores, PC, periféricos, conexiones de red, sistemas gestores de base de datos), junto con su planificación de capacidades y sus requisitos de operación, administración, seguridad y control de acceso?		√	Se encuentra definido falta documentar
El modelo de datos tiene en cuenta el entorno tecnológico y los requisitos de rendimiento para los volúmenes y frecuencias de acceso estimados, migración de datos?		√	
Se tiene en cuenta el criterio de los usuarios de la aplicación durante las diferentes etapas del ciclo de vida del sistema? Se formalizan con actas de aceptación por parte de los usuarios?	√		
Están definidos los distintos perfiles de usuario requeridos para la formación y explotación del nuevo sistema?	√		
En la fase de implementación del software aplicativo se consideran procedimientos de configuración, aceptación y prueba?		√	Falta documentar el procedimiento.
Existen controles adecuados cuando se están probando nuevas versiones del software o cuando se están aplicando programas de diagnóstico?	√		Para el sistema financiero se realiza respaldo de la versión anterior Procedimientos manuales en el sistema de recursos humanos
Existe un registro de aquellos problemas que se presentan en el software?		√	No se lleva registro
Los cambios y mejoras del software están debidamente justificados?. Se lleva un registro de cambios en los programas? Son evaluados ya autorizados de forma previa a su implantación?	√		
Son autorizadas y probadas las correcciones de programas	√		

Continúa

antes de puesta en marcha?			
Están adecuadamente documentados y probados los nuevos programas?			Los sistemas si se encuentran probados, lo que no se encuentra es documentado.
Existe un mecanismo especial para reportar las dificultades e inconsistencias?		√	
Está totalmente legalizado el software utilizado en la entidad?	√		Si se encuentra el software legalizado, la mayor parte del software es libre.
Tiene el software adquirido contrato de mantenimiento?	√		Si durante el contrato, se da mantemienot durante un año, luego el mantenimiento del software se lo realiza en la entidad
El software en funcionamiento contiene módulos de auditoría?	√		Existen algunos sistemas q tienen y otros no.
Existe un repositorio con los diagramas y configuraciones de hardware y software actualizado?		√	
Existe documentación del software del sistema. Las aplicaciones tienen manuales técnico, de operación y de usuario? Estos manuales se encuentran actualizados?		√	No todos los sistemas cuentan con esa información
Existen actas de aceptación por parte de los usuarios del paso de los sistemas probados y aprobados desde el ambiente de desarrollo y pruebas al de producción y su revisión en el de post-implementación?	√		
Existe un plan de mantenimiento de las aplicaciones?		√	
Se establecen ambientes de desarrollo, pruebas y de producción independientes? Qué tipo de seguridades se implementan?			NO presentan las seguridades adecuadas como la asignación de usuarios con claves únicas para cada servidor
Políticas y procedimientos para la utilización del correo electrónico?		√	

4.2.3 INFRAESTRUCTURA TECNOLÓGICA

TABLA 11. INFRAESTRUCTURA TECNOLÓGICA

PREGUNTAS	SI	NO	OBSERVACIONES
Existen políticas y procedimientos para la instalación y mantenimiento del hardware y su configuración base		√	Falta documentar
Existen políticas y procedimientos para la ubicación, protección y mantenimiento de los puntos de red y switches		√	Constantes cambios y reubicación y puntos de red,
Existen políticas y procedimientos para la comunicación al cliente sobre el uso adecuado de las estaciones de trabajo y sistemas lógicos.		√	
Las adquisiciones de infraestructura tecnológica son ejecutadas de acuerdo al portafolio de servicios, a los planes estratégicos y operativos, al plan de compras aprobados?	√		
Existe una planificación del incremento de las capacidades, evaluación de riesgos tecnológicos, costos, vida útil para inversiones futura?	√		
Al realizar las adquisiciones de hardware los contratos contienen el detalle de los principales componentes como: marca. Modelo, número de serie, capacidades, unidades de entrada y salida, garantías, entre otros.	√		
Se valida que las especificaciones técnicas establecidas en las fases precontractual (pliegos), contractual (contrato), y las actas entrega recepción son las mismas?	√		
En el caso de contratos de servicios, se realiza acuerdos de nivel de servicios puntualizando la seguridad y confiabilidad de la información?	√		
Existe un Plan de mantenimiento de la infraestructura tecnológica?			Se tiene un plan de mantenimiento que no se encuentra aprobado ni formalizado
Como se controla el mantenimiento a los equipos de computación?			Con los contratos de mantenimiento que se dan a los equipos.
Se lleva un registro del mantenimiento de los ups?			Este mantenimiento no está a cargo de la unidad de servicios tecnológicos.

Continúa

Son atendidas oportunamente las quejas, reclamos y sugerencias formuladas por los usuarios?	√	Se lo realiza a través de la mesa de ayuda
Se cuenta con un inventario de equipos tecnológicos	√	
Que información contienen los inventarios?	√	Serie, código, ubicación, responsable….
Que mecanismos se han utilizado para que las redes instaladas ya sean eléctricas de voz o de datos, cumplan con los requerimientos mínimos vigentes de cableado estructurado? (documentación, etiquetados, ductos y el aterrizamiento del mismo)	√	Se cuenta solo en los lugares que se tiene realizada la planificación previa de la red
¿Cómo se realiza la administración de incidentes, requerimientos de servicio, solicitudes de información, cambios que demandan los usuarios?	√	A través del sistema, llamadas telefónicas, o pedido personal

4.2.4 SEGURIDADES

TABLA 12. SEGURIDADES

PREGUNTAS	SI	NO	OBSERVACIONES
Se han adoptado medidas de seguridad en el departamento de sistemas de información, tiene una ubicación adecuada, control de acceso físico? En especial a las áreas de servidores, desarrollo y biblioteca. La ubicación es la adecuada?	√		Cuenta con registro de tarjetaselectrónicas
Procedimientos de obtención periódica de respaldos. Cronograma definido y aprobado?		√	
Se almacenan los respaldos de la información crítica y/o sensibles en lugares externos a la organización?	√		El sitio alterno se encuentra en Cuenca
Existe documentación escrita relacionada con el respaldo y recuperación de la base de datos en caso de presentarse destrucción total o parcial de esta?		√	
Que seguridades tiene implementada a nivel de software y hardware? Que pruebas realiza y que acciones correctivas realiza?	√		Firewall, IPs, se ha realizado la contratación de equipos de seguridad.
Las instalaciones del Data Center cuenta con equipos y dispositivos para monitorear y controlar el fuego, mantener ambiente de temperatura y humedad relativa del aire controlado, energía acondicionada?	√		Netboss el software de monitoreo
Cuenta con un sitio de procesamiento alterno?	√		
Se han establecido políticas, procedimientos, que permitan identificar, autentificar y autorizar a los sistemas de información, sistemas de base de datos, y sistemas operativos?		√	
Se ha estandarizado la identificación, autenticación y autorización de los usuarios así como la administración de sus cuentas?	√		Si esta, pero no está reglamentado.
Con que frecuencia se revisan las cuentas de los usuarios y	√		3 veces al año a los usuarios, a los administradores, no se

Continúa

los privilegios asociados; asi como a los administradores de los sistemas?			les revisa que privilegios tienen.
Identificación única a los usuarios internos, externos y temporales que interactúan con los sistemas y servicios tecnológicos?	√		
Existe control sobre las claves de acceso al sistema?	√		Zimbraencriptada
Son verificados los accesos y restricciones a las tablas que autorizan las contraseñas a los usuarios?		√	No está a nivel de base de datos sino de tablas
Se llevan reseñas de estadísticas o reseñas de fraudes cometidos con respecto al software del sistema?		√	
Con que periodicidad se saca los back-up (copia de seguridad) a la aplicación?		√	No se están realizando los backups, no se tiene el storage
Pueden los operadores o usuarios modificar los programas fuente de la aplicación?		√	
Existe control sobre el ingreso de los funcionarios a la entidad?	√		Mediante las tarjetas
Se permite el uso de la computadora a personas extrañas a la dependencia?		√	Para las personas que no se encuentran laborando en el Edificio Central se han instalado computadoras para que utilicen
Existe un plan de contingencia aprobado?		√	
El Plan de Contingencias se encuentra probado y actualizado?		√	
Existen un plan de seguridad?		√	
Hay información de carácter confidencial o privada relacionada con la aplicación?	√		Información privada de los funcionarios
Existen procedimientos formales que garanticen la seguridad física y lógica de los datos en la red, de tal manera que garanticen la oportunidad, totalidad y exactitud?		√	
Brinda el sistema de administración de base de datos una adecuada protección a la información y datos almacenados?		√	Por la naturaleza de la base de datos (Postgres y Mysql) no permite tener toda la seguridad, se lo realiza restricciones a las tablas.
Se revisa la bitácora de la base de datos?		√	
Se realizan revisiones periódicas de los recursos tecnológicos (hardware y líneas de comunicación) que permitan determinar de forma oportuna las necesidades de ampliación de	√		

Continúa

capacidades o actualizaciones de los equipos.			
Se han establecido políticas y procedimientos de prevención, detección y corrección de virus?		√	
Q medidas de prevención, detección y corrección se han implementado para proteger los sistemas y tecnologías de la entidad contra software malicioso y virus?	√		Servidor de antivirus (Northon) y para el servidor de correo se tiene un antivirus. PCS Kaspersky.
Se han diseñado lineamientos de tal manera que todas las transacciones efectuadas por los usuarios de los sistemas posean huellas o pistas de auditoría que permitan rastrear a los responsables de ingresar, eliminar o modificar, los registros de la base de datos.	√		Algunos sistemas, si contienen pistas de auditoria.
Qué mecanismos de seguridad física y lógica se han implementado para que se proteja la integridad y privacidad de la información sensible cuando el canal de transmisión era internet	√		Se ha implementado VPN. Encriptación de conexiones
Qué procedimientos se han establecido para el uso de internet y correo electrónico?	√		Administrador del Ancho de Banda (Políticas), conjunto de sitios restringidos de acuerdo a los perfiles
Qué mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico, entrega de información y de mensajes sensitivos: así como la protección y conservación de la información utilizada para la encriptación y autenticación?	√		Segmentación de red en VLAN. Autenticación para conexión y autorización de acuerdo a los perfiles
Se cuenta con dispositivos de firma electrónica?		√	Se encuentra en proceso de contratación
Los aplicativos que incluyen firma electrónica, contienen mecanismos y reportes que facilitan la auditoría de los mensajes firmados electrónicamente?			No aplica
El certificado recibido de firma electrónica es emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente?	√		
Se han establecido políticas internas de manejo y archivo de información digital?			No aplica
Los titulares del certificado notifican a la entidad de certificación sobre algún cambio , modificación o variación de los datos que proporciona la emisión del certificado			No aplica
Cuando el servidor público deja de prestar sus servicios			No aplica

Continúa

temporal o definitivamente y cuenta con un certificado de firma electrónica. **El servidor solicita a la entidad de certificación la revocación del mismo?** **El superior jerárquico ordena la cancelación del mismo?**	
El dispositivo portable se lo considera como un bien?. Es entregado y devuelto con alta entrega recepción?	No aplica
Los usuarios conocen de que son responsables de su buen uso y protección que no deben divulgar sus claves?	No aplica
Que se realiza en el caso de alguna circunstancia que comprometa su utilización?	No aplica
Quien y como se realiza la renovación del certificado de la firma electrónica?	No aplica
Se recibió capacitación en el uso de firmas electrónicas?	No aplica

4.2.5 MONITOREO Y EVALUACIÓN

TABLA 13. MONITOREO Y EVALUACIÓN.

PREGUNTAS	SI	NO	OBSERVACIONES
Se han definido indicadores de desempeño y métricas del proceso para monitorear gestión y tomar los correctivos que se requieran?		√	
Q procedimientos y mecanismos se utilizan para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos?	√		Se realiza a través del Módulo de Encuestas de Satisfacción.
Con que frecuencia la Unidad de Tecnologías de Información presenta informes de gestión a la alta dirección	√		

4.3 Evaluación De Riesgos

4.3.1 Identificación de los riesgos

4.3.1.1 Área De Desarrollo, Administración y Mantenimiento de sistemas

1. Desarrollo de aplicaciones

Tabla 14. Identificación de riesgos – desarrollo de aplicaciones

OBJETIVOS DEL ÁREA	FUENTES DE RIESGO	CAUSAS	CONSECUENCIAS POTENCIALES	RIESGOS IDENTIFICADOS
Desarrollar aplicaciones que sirvan de apoyo a las unidades requirentes para el logro de los objetivos institucionales	Falta de involucramiento de las unidades requirentes	Temor de automatizar procesos. Falta de interés. Temor al cambio	Se extienden los tiempos en el desarrollo.	La falta de involucramiento de las unidades requirentes, alta rotación del personal, falta de formalidad en el manejo de los procesos y metodologías de trabajo y la no disponibilidad de equipamiento tecnológico suficiente PODRIA OCASIONAR que las aplicaciones desarrolladas no cumplan con la funcionalidad requerida por los clientes internos.
	Alta rotación del personal con conocimiento	Personal con contrato ocasional	Perdida del know-how y de la experiencia de los técnicos	
	Falta de planificación en el levantamiento de la información.	Falta de tiempo del usuario final	La funcionalidad no se adapta a lo que requiere el usuario	
	No existen procesos definidos	No se ha realizado el levantamiento de la información	No se realice un control adecuado a los procesos	
	Falta de estandarización de la metodología y tecnología de trabajo.	No existen procesos de estándares definidos	El mantenimiento del sistema es más complicado.	
	No disponibilidad de equipo tecnológico y espacio de trabajo	Departamento de activos fijos no cuenta con los recursos tecnológicos.	No se pueda trabajar con equipos de características necesarias para el desarrollo	
	No existe ambientes de desarrollo prueba y producción independiente	No se cuenta con los equipos.	No se puede garantizar el buen funcionamiento de la aplicación.	

Mantenimiento de sistemas

TABLA 15. IDENTIFICACIÓN DE RIESGOS - MANTENIMIENTO DE SISTEMAS

OBJETIVOS DEL ÁREA	FUENTES DE RIESGO	CAUSAS	CONSECUENCIAS POTENCIALES	RIESGOS IDENTIFICADOS
Mantener las aplicaciones institucionales operativas y actualizadas	Falta de recursos de la infraestructura en los servidores	Falta de asignación de recursos para la Unidad de Tecnología	Deje de funcionar los sistemas	La falta de recursos de la infraestructura en los servidores, que el personal que utiliza los sistemas no esté capacitado, el no poder dar soluciones de mantenimiento, ni realizar actualizaciones a los sistemas PODRIAN OCASIONAR que no se mantengan las aplicaciones institucionales operativas y actualizadas.
	No poder dar soluciones de mantenimiento por petición del usuario	No existe documentación del sistema. No existe el código fuente.	El tiempo para dar solución a los requerimientos del usuario aumenta.	
	No poder realizar actualizaciones en los sistemas	Tecnología obsoleta, desactualizada.	Limita, el rendimiento, realizar cambios, a enfocarse a solo un versionamiento de las herramientas de desarrollo	
	El personal que utiliza los sistemas no están capacitados	Desinterés Alta rotación del personal	No utilizan los sistemas Realizan procesos erróneos	
	Falta de una bitácora de los soportes realizados a los usuarios	Falta de definición de procedimientos y políticas.	No se conozca y se mantengan estadísticas de los problemas comunes q tengan los usuarios.	

4.3.1.2 ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

2. Administración de Servidores, Redes y Comunicaciones

TABLA 16. IDENTIFICACIÓN DE RIESGOS - ADMINISTRACIÓN DE SERVIDORES, REDES Y COMUNICACIONES

OBJETIVOS DEL ÁREA	FUENTES DE RIESGO	CAUSAS	CONSECUENCIAS POTENCIALES	RIESGOS IDENTIFICADOS
Garantizar que los servicios estén disponibles, seguros y confiables para el usuario final.	1. Falla en la energía eléctrica para el Data Center	Falla de los equipos por tiempo de vida útil	Se apagan los equipos y no se da el servicio	La falla de componentes que conforman el centro de datos, el acceso no autorizado a los equipos y a la información, el ingreso de personas no autorizadas al Data Center, falta de ambientes de desarrollo, prueba y producción y de almacenamiento, el mal uso de los servicio por parte de los usuarios y la falta de procedimientos definidos PODRIAN OCASIONAR que no se garantice que los servicios estén disponibles, seguros y confiables para el usuario final.
	2. Falla en el sistema de refrigeración	Falta de mantenimiento de los equipos	Daño e inoperabilidad de los equipos	
	3. Ingreso de personas no autorizadas al Data Center y a los cuartos de comunicación.	Pared de gypsum Pérdida de tarjetas	Desconecte los equipos. Perdida de información	
	4. Daño de los componentes de los equipos en el Data Center	Vida útil Fallas de fabricación Eléctrico.	Perdida de los servicios	
	5. Acceso no autorizado a los equipos	No contar con las seguridades perimetrales adecuadas. Ataques de fuerza bruta.	Alteración de información Denegación de servicios. Perdida de información.	
	6. Falta de ambientes de desarrollo, prueba y producción.	Falta de infraestructura física	Perdida de servicios No se garantiza la integridad y disponibilidad de la información	
	7. Falta de espacio para el almacenamiento de la información	Falta de infraestructura tecnológica No hay planificación del	Perdida de información.	

Continúa

		crecimiento de las capacidades de la infraestructura	
	8. Mal uso de los servicios por parte de los usuarios.	Instalan software malicioso No existen políticas para el usuario No cuidan las claves	Mandar a listas negras Envían spam
	9. Acceso a la Información de los equipos de los usuarios finales	No existe control de acceso al equipo mediante clave personalizada, se maneja con una sola clave para todos los equipos. No existen políticas para asignación de perfiles a los usuarios	Pérdida de Información
	10. Falta de procedimientos definidos para mantener la continuidad de los servicios	No existe un plan de contingencias y de seguridades.	Perdida de servicios por tiempo indefinido.

4.3.1.3 ÁREA DE ADMINISTRACIÓN Y ORGANIZACIÓN

3. Organización y Administración.

TABLA 17. IDENTIFICACIÓN DE RIESGOS – ORGANIZACIÓN Y ADMINISTRACIÓN

OBJETIVOS DEL ÁREA	FUENTES DE RIESGO	CAUSAS	CONSECUENCIAS POTENCIALES	RIESGOS IDENTIFICADOS
Planificar y administrar los Recursos Tecnológicos y de Talento Humano en cada una de las áreas de la Unidad de Tecnología.	Alta rotación del personal	Cambios políticos Personal sin nombramiento	Perdida del know-how y experiencia de los técnicos	La alta rotación del personal, alta depreciación y caducidad del soporte y mantenimiento de la infraestructura tecnológica y que los proyectos elaborados no puedan tener su curso normal para su ejecución, PODRIAN OCASIONAR que no se planifique y administre adecuadamente los recursos tecnológicos de la institución.
	Alta depreciación de la infraestructura tecnológica y caducidad del soporte y mantenimiento de la Infraestructura	Falta de la Planificación de las TIC en la Institución.	No pueden operar los servicios.	
	Los proyectos elaborados no puedan tener su curso normal para la ejecución	Demora en el proceso en la obtención de los recursos	Fracaso del proyecto en el tiempo adecuado.	

4.3.1.4 ÁREA DE SOPORTE A USUARIOS Y MANTENIMIENTO DE SISTEMAS

4. Soporte a usuarios y mantenimiento de equipos.

TABLA 18 IDENTIFICACIÓN DE RIESGOS – SOPORTE A USUARIOS Y MANTENIMIENTO DE EQUIPOS

OBJETIVOS DEL ÁREA	FUENTES DE RIESGO	CAUSAS	CONSECUENCIAS POTENCIALES	RIESGOS IDENTIFICADOS
Brindar oportunamente ayuda técnica a los usuarios y capacitar sobre el uso de manejo de las herramientas tecnológicas q dispone la institución. Anticipar a futuros daños en equipos de la Institución.	Que el personal técnico no esté actualizado en sus conocimientos	Falta de planificación Constante evolución tecnológica.	No se pueda operativizar los equipos. No se pueda capacitar al usuario eficientemente.	La falta de planificación de los trabajos, que el personal técnico no esté actualizado en sus conocimientos, alta rotación de usuario final, el no contar con los recursos tecnológicos necesarios PODRIA OCASIONAR que no se pueda dar una ayuda técnica y capacitación oportuna y eficiente al usuario final, así también mantener los equipos en buen estado.
	Falta de planificación del trabajo.	Falta de control y seguimiento	Acumulación de trabajo por equipos inactivos	
	Alta rotación de personal contratado por los usuarios finales	Compromisos políticos	Aumento de requerimientos técnicos y de capacitaciones	
	No contar con los recursos tecnológicos necesarios	No tener un diagnóstico técnico de los equipos.	No atender eficientemente los requerimientos de los usuarios finales	

4.3.2 Análisis De Los Riesgos

4.3.2.1 Área De Desarrollo Administración y Mantenimiento De Sistemas

1. Desarrollo de aplicaciones

+Probabilidad	++Impacto
5. Casi cierta	5. Grave
4. Probable	4. Daños mayores
3. Posible	3. Mediano
2. Poco probable	2. Leve
1. Rara	1. Muy leve

TABLA 19. ANÁLISIS DE RIESGOS – DESARROLLO DE APLICACIONES

RIESGOS IDENTIFICADOS	CONTROLES EXISTENTES	EFECTIVIDAD DE LOS CONTROLES (BUENO, MEDIANO Y DEFICIENTE)	PROBABILIDAD (1 AL 5)	IMPACTO (1 AL 5)	NIVEL DE RIESGO (I X P)
La falta de involucramiento de las unidades requirentes, alta rotación del personal, falta de formalidad en el manejo de los procesos y metodologías de trabajo y la no disponibilidad de equipamiento tecnológico suficiente PODRIA OCASIONAR que las aplicaciones desarrolladas no cumplan con la funcionalidad requerida por los clientes internos.	• Elaboración de flujos con la aprobación del solicitante • A través del sistema mantis se asignan los requerimientos de los programadores. • Formato de control de cambios aprobado	• Deficiente. • Bueno • Bueno	3	5	15

2. Mantenimiento de sistema

TABLA 20 ANÁLISIS DE RIESGOS – MANTENIMIENTO DE SISTEMAS

RIESGOS IDENTIFICADOS	CONTROLES EXISTENTES	EFECTIVIDAD DE LOS CONTROLES (BUENA, MEDIANA Y DEFICIENTE)	PROBABILIDAD (1 AL 5)	IMPACTO (1 AL 5)	NIVEL DE RIESGO (I X P)
La falta de recursos de la infraestructura en los servidores, que el personal que utiliza los sistemas no esté capacitado, el no poder dar soluciones de mantenimiento, ni realizar actualizaciones a los sistemas PODRIAN OCASIONAR que no se mantengan las aplicaciones institucionales operativas y actualizadas.	• Monitoreo de los recursos, como espacio en disco. • Se realiza capacitaciones permanentes • Formulario de control de cambios para las solicitudes de los usuarios. • SVN. Sistema de Versiones de código fuente	• Deficiente. • Bueno. • Bueno. • Bueno.	4	3	12

4.3.2.2 ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

3. Administración de Servidores, Redes y Comunicaciones

TABLA 21. ANÁLISIS DE RIESGOS – ADMINISTRACIÓN DE SERVIDORES, REDES Y COMUNICACIONES

RIESGOS IDENTIFICADOS	CONTROLES EXISTENTES	EFECTIVIDAD DE LOS CONTROLES (BUENO, MEDIANO Y DEFICIENTE)	PROBABILIDAD (1 AL 5)	IMPACTO (1 AL 5)	NIVEL DE RIESGO (I X P)
La falla de componentes que conforman el centro de datos, el acceso no autorizado a los equipos y a la información, el ingreso de personas no autorizadas al Data Center, falta de ambientes de desarrollo, prueba y producción y de almacenamiento, el mal uso de los servicio por parte de los usuarios y la falta de procedimientos definidos PODRIAN OCASIONAR que no se garantice que los servicios estén disponibles, seguros y confiables para el usuario final.	• Ingreso al Data Center con tarjeta y huella digital para (5) personas. • NetBotz software que notifica novedades en el ambiente del centro de datos. • Multímetro panel de distribución en el Centro de Datos. • IPS • Whatsup (Sistema de monitoreo de pérdida de enlaces con equipamiento activo de la red). • PRTG (Monitorea el ancho de banda, grafica el tráfico) • Karty (Monitorea los enlaces a nivel nacional.) • Llaves de acceso solo tienen las personas autorizadas	• Bueno • Bueno • Bueno • Mediano • Bueno • Bueno • Deficiente • Bueno	4	4	16

4.3.2.3 ÁREA DE ADMINISTRACIÓN Y ORGANIZACIÓN

4. Organización y Administración

TABLA 22 ANÁLISIS DE RIESGO–ORGANIZACIÓN Y ADMINISTRACIÓN

RIESGOS IDENTIFICADOS	CONTROLES EXISTENTES	EFECTIVIDAD DE LOS CONTROLES (BUENO, MEDIANO Y DEFICIENTE)	PROBABILIDAD (1 AL 5)	IMPACTO (1 AL 5)	NIVEL DE RIESGO (I X P)
La alta rotación del personal, alta depreciación y caducidad del soporte y mantenimiento de la infraestructura tecnológica y que los proyectos elaborados no puedan tener su curso normal para su ejecución, PODRIAN OCASIONAR que no se planifique y administre adecuadamente los recursos tecnológicos de la institución.	• Renovación de los contratos al personal. • Definición de funciones a los funcionarios. • Políticas de utilización de software libare • Elaboración del PAC • Reporte de actividades mensuales de los servidores	• Bueno. • Bueno. • Bueno. • Bueno. • Bueno.	4	5	20

4.3.2.4 ÁREA DE SOPORTE Y MANTENIMIENTO A USUARIOS.

5. Soporte a usuarios y mantenimiento de sus equipos

TABLA 23. SOPORTE A USUARIOS Y MANTENIMIENTO DE EQUIPOS.

RIESGOS IDENTIFICADOS	CONTROLES EXISTENTES	EFECTIVIDAD DE LOS CONTROLES (BUENO, MEDIANO Y DEFICIENTE)	PROBABILIDAD (1 AL 5)	IMPACTO (1 AL 5)	NIVEL DE RIESGO (I X P)
La falta de planificación de los trabajos, que el personal técnico no esté actualizado en sus conocimientos, alta rotación de usuario final, el no contar con los recursos tecnológicos necesarios PODRIA OCASIONAR que no se pueda dar una ayuda técnica y capacitación oportuna y eficiente al usuario final, así también mantener los equipos en buen estado.	• Plan Anual de Mantenimiento. • Registro de requerimientos de los usuarios; control y registro de actividades del personal técnico mediante el sistema (GLPI) • Capacitaciones a los usuarios finales. • Inventario de Recursos Tecnológicos. • Reporte mensual de las actividades de los técnicos. • Horarios de Ingreso y rotación del personal a los diferentes edificios de la institución.	• Mediano • Bueno • Mediano • Bueno • Bueno • Bueno		4	16

4.3.3 Mapa De Riesgos

Enunciado del riesgo identificado. (Probabilidad x Impacto = Nivel de riesgo)

Clasificación del riesgo
Alto
Moderado
Bajo

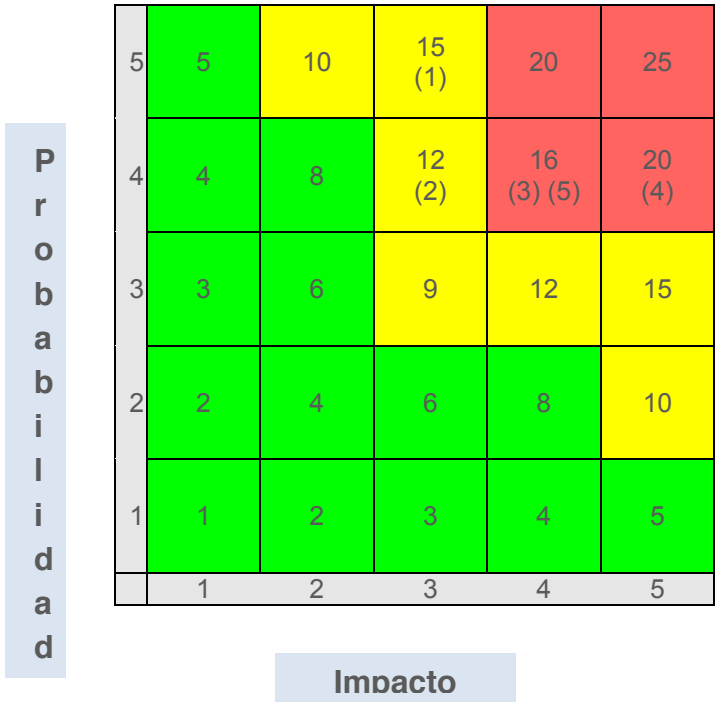

Gráfico 6.-mapa de riesgos

AREAS

1.- Desarrollo de aplicaciones

2.- Mantenimiento de sistemas.

3.- Administración de servidores, redes y comunicaciones.

4.- Organización y administración.

5.- Soporte a usuarios y mantenimiento de equipos.

4.3.4 Priorización De Riesgos

Tabla 24.Priorización de riesgos.

RIESGOS IDENTIFICADOS	NIVEL DE RIESGOS (I X P)	CRITERIO DEL RIESGO* (1, 2 O 3)	RIESGOS QUE REQUIEREN SER TRATADOS (MARCAR CON UNA X)	PRIORIDAD PARA EL TRATAMIENTO DEL RIESGO (ORDINAL)
1. La falta de involucramiento de las unidades requirientes, alta rotación del personal, falta de formalidad en el manejo de los procesos y metodologías de trabajo y la no disponibilidad de equipamiento tecnológico suficiente PODRIA OCASIONAR que las aplicaciones desarrolladas no cumplan con la funcionalidad requerida por los clientes internos.	15	2		3
2. La falta de recursos de la infraestructura en los servidores, que el personal que utiliza los sistemas no esté capacitado, el no poder dar soluciones de mantenimiento, ni realizar actualizaciones a los sistemas PODRIAN OCASIONAR que no se mantengan las aplicaciones institucionales operativas y actualizadas.	12	1	X	2
3. La falla de componentes que conforman el centro de datos, el acceso no autorizado a los equipos y a la información, el ingreso de personas no autorizadas al Data Center, falta de ambientes de desarrollo, prueba y producción y de almacenamiento, el mal uso de los servicio por parte de los usuarios y la falta de procedimientos definidos PODRIAN OCASIONAR que no se garantice que los servicios estén disponibles, seguros y confiables para el usuario final.	16	1	X	1
4. La alta rotación del personal, alta depreciación y caducidad del soporte y mantenimiento de la infraestructura tecnológica y que los proyectos elaborados no puedan tener su curso normal	20	2		5

Continúa

para su ejecución, PODRIAN OCASIONAR que no se planifique y administre adecuadamente los recursos tecnológicos de la institución.			
5. La falta de planificación de los trabajos, que el personal técnico no esté actualizado en sus conocimientos, alta rotación de usuario final, el no contar con los recursos tecnológicos necesarios PODRIA OCASIONAR que no se pueda dar una ayuda técnica y capacitación oportuna y eficiente al usuario final, así también mantener los equipos en buen estado.	16	2	4

*(1) No podemos tolerar este riesgo.

(2) Es un riesgo medianamente tolerable.

(3) Podemos tolerar este riesgo.

4.3.5 TRATAMIENTO DE RIESGOS

TABLA 25. TRATAMIENTO DE RIESGOS

RIESGOS IDENTIFICADOS (EN ORDEN DE PRIORIDAD)	ACCIONES PROPUESTAS (OPCIONES DE TRATAMIENTO)*	INDICADORES DE DESEMPEÑO PARA LA ADMINISTRACIÓN DE RIESGOS	RESPONSABLE	FECHA DE CUMPLIMIENTO
1. La falla de componentes que conforman el centro de datos, el acceso no autorizado a los equipos y a la información, el ingreso de personas no autorizadas al Data Center, falta de ambientes de desarrollo, prueba y producción y de almacenamiento, el mal uso de los servicio por parte de los usuarios y la falta de procedimientos definidos PODRIAN OCASIONAR que no se garantice que los servicios estén disponibles, seguros y confiables para el usuario final.	Reducir	• Cantidad de usuarios que mal utilizaron los servicios de TI en entidad • Número de procedimientos definidos de acuerdo a las Normas de Control Interno por la Unidad de Tecnología en el 2014. • Porcentaje de componentes que fallaron fuera del periodo de garantía en el Centro de Datos de la entidad. • Total de personal que ingresa en el centro de datos de acuerdo a las restricciones definidas por la Unidad de Tecnología. • Número de ambientes implementados para el Desarrollo, Pruebas y Producción por el área de Infraestructura.	Líder de Infraestructura Tecnológica	Primer Trimestre 2014

Continúa

2. La falta de recursos de la infraestructura en los servidores, que el personal que utiliza los sistemas no esté capacitado, el no poder dar soluciones de mantenimiento, ni realizar actualizaciones a los sistemas PODRIAN OCASIONAR que no se mantengan las aplicaciones institucionales operativas y actualizadas.	Reducir	• Cantidad de equipos adquiridos de acuerdo a las especificaciones técnicas requeridas por la Unidad de Tecnología a julio del 2014. • Número de capacitaciones realizadas a los usuarios finales que utilizan los sistemas por la Unidad de Tecnología a julio de 2014. • Número de actualizaciones y mantenimientos realizados a los sistemas a julio de 2014	. Líder de Infraestructura Tecnológica	Primer Semestre 2014
3. La falta de involucramiento de las unidades requirentes, alta rotación del personal, falta de formalidad en el manejo de los procesos y metodologías de trabajo y la no disponibilidad de equipamiento tecnológico suficiente PODRIA OCASIONAR que las aplicaciones desarrolladas no cumplan con la funcionalidad requerida por los clientes internos.	Compartir	• Cantidad de actas de trabajo efectuadas entre las unidades requirentes y la Unidad de Tecnología dentro del desarrollo de la aplicación • Cantidad del personal de desarrollo que renunció a la Unidad de Tecnología en el 2014. • Número de procesos y metodologías implementadas por el área de desarrollo en el 2014. • Porcentaje de equipos tecnológicos que ingresaron a la Coordinación General de Servicios Tecnológicos en el 2014.	Líder de Desarrollo y Mantenimiento de Sistemas.	Anual

Continúa

4. La falta de planificación de los trabajos, que el personal técnico no esté actualizado en sus conocimientos, alta rotación de usuario final, el no contar con los recursos tecnológicos necesarios PODRIA OCASIONAR que no se pueda dar una ayuda técnica y capacitación oportuna y eficiente al usuario final, así también mantener los equipos en buen estado.	Reducir	• Número de planificaciones realizadas por las áreas de Tecnología en el 2014. • Cantidad de capacitaciones realizadas al personal de soporte técnico de la Unidad de Tecnología en el 2014 • Porcentaje de personal que salieron de la Institución a marzo del 2014. • Número de adquisiciones realizadas para dar soporte y mantenimiento a los equipos de la institución.	Director de la Unidad de Tecnología	Trimestral
5. La alta rotación del personal, alta depreciación y caducidad del soporte y mantenimiento de la infraestructura tecnológica y que los proyectos elaborados no puedan tener su curso normal para su ejecución, PODRIAN OCASIONAR que no se planifique y administre adecuadamente los recursos tecnológicos de la institución.	• Reducir	• Cantidad del personal de la Coordinación General de Servicios Tecnológicos que renunció en el 2014. • Número de adquisiciones y mantenimiento realizados a los equipos informáticos en el 2014. • Estado de los proyectos que contrató la Coordinación General de Servicios Tecnológicos en el 2014.	Líder de Soporte Técnico	

(E) Evitar el riesgo: es decidir no empezar o continuar con la actividad que genera el riesgo; implica descontinuar las actividades que los originan.
(R) Reducir el riesgo: incluye los métodos y técnicas específicas para tratar los riesgos, identificándolos y proveyendo acciones para la reducción de su probabilidad e impacto.
(C) Compartir el riesgo: reduce la probabilidad y el impacto mediante la transferencia u otra manera de compartir una parte del riesgo con terceros.
(A) Aceptar el riesgo: no se realiza acción alguna para afectar la probabilidad e impacto.

4.4 COMENTARIOS DE CONTROL INTERNO

Registro de información incompleto del inventario de equipos informáticos y licenciamiento de software

Con oficio (número de oficio) (fecha) se requirió al Director de Tecnología y Desarrollo la entrega del Inventario del equipamiento informático por unidad administrativa y dependencias de la entidad a nivel nacional.

Con oficio (número de oficio) (fecha) el Director de Tecnología contestó y adjuntó la información solicitada. De la revisión a la información se identificó que no se mantiene un registro completo con la información de los equipos informáticos, pues no dispone de las características principales, fecha de compra, período de garantía, proveedor del equipo, para el caso del software adquirido no consta el código de activo fijo, fecha de adquisición, serie, nombre del proveedor; y, para el software de propiedad de la institución, no consta su registro en el Instituto Ecuatoriano de Propiedad Intelectual.

Por lo que el Director de Tecnología inobservó el artículo 97 del Reglamento General Sustitutivo para el Manejo y Administración de Bienes del Sector Público, mantenimiento y control de equipos informáticos, del Estatuto Orgánico de Gestión por Proceso de la entidad, emitido mediante

(resolución), (fecha); y la NCI 400-02 "Plan Informático, adquisición o actualización del sistema".

Conclusión

La entidad no cuenta con un registro completo de los equipos informáticos y software, lo que ocasiona que no se tenga un control sobre estos bienes, que facilite su administración como requerimientos para adquisición y mantenimiento de estos recursos.

Recomendación

A los Directores Administrativo y de Tecnología

Elaborarán de manera coordinada un inventario completo y pormenorizado de todos los activos informáticos a nivel nacional, mismo que contendrá entre otros los siguientes aspectos: descripción del bien, código de activo fijo, serie, modelo, tipo, estado, proveedor, año de fabricación, si está en garantía, ubicación, custodio, etc. Para el software adquirido, registrará el código de activo fijo, identificación del producto, descripción del contenido, número de versión, número de serie, nombre del proveedor, fecha de adquisición y otros datos necesarios; y, para el software creado por la entidad, harán constar su registro en el Instituto Ecuatoriano de Propiedad Intelectual.

Plan Integral Informático Incompleto

El Director de Tecnología, como parte de la documentación entregada con (oficio) de (fecha), adjuntó el "Plan Estratégico de Tecnología de Información", del 2013, documento sin fecha de presentación y aprobación.

El plan no contenía: la estimación de recursos financieros, humanos, materiales y tecnológicos; así como, la definición de fechas tentativas de inicio y terminación de las actividades, productos a obtener, responsables e indicadores de cumplimiento.

Por lo expuesto, el Director Ejecutivo y Director de Tecnología y Desarrollo inobservaron el (numeral) del Estatuto Orgánico de Gestión por Proceso de la entidad, emitido (documento)(fecha); y, la NCI 400-02 "Plan Informático, adquisición o actualización del sistema".

Conclusión

La entidad no contó con Plan Estratégico de Tecnología de la Información aprobado, con la definición de los proyectos tecnológicos a desarrollarse a corto y mediano plazo; así como, la estimación de recursos necesarios para su ejecución e indicadores que permitan medir su cumplimiento.

Recomendaciones

Al Director Administrativo.

Dispondrá al responsable de planificación que en coordinación con el Director de Tecnología, definan la metodología para la formulación del Plan Estratégico de Tecnología de la Información, la que contendrá entre otros aspectos: las estrategias, inventario de soluciones tecnológicas e infraestructura actual, estructura organizacional requerida, proyectos tecnológicos con sus respectivos cronogramas de actividades a

desarrollarse para la ejecución del plan a corto y mediano plazo, con la estimación de los recursos humanos, materiales, tecnológicos y financieros necesarios para su cumplimiento, responsables, indicadores y productos a obtenerse.

Dispondrá al Director de Tecnología formule los Planes Informático Estratégico, aplicando la metodología definida.

Aprobará el Plan Informático Estratégico, dispondrá su difusión y ejecución y gestionar la asignación de recursos financieros necesarios para su cumplimiento.

Al Director de Tecnología

Elaborará el Plan Informático Estratégico con la participación de los coordinadores de las áreas tecnológicas y usuarios de las áreas respectivas, en el que constará el portafolio de proyectos de infraestructura de comunicaciones, sistemas y servicios encaminados a mejorar las actividades que realizan las diferentes unidades usuarias y clientes externos. Los proyectos deberán contar con la cuantificación de recursos humanos, materiales y tecnológicos con sus respectivos cronogramas de ejecución e indicadores.

Presentará al Director Administrativo, el Plan Informático Estratégico para su aprobación.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- ✓ Se ha elaborado una guía de auditoría para la evaluación del control interno del área de TI en las entidades públicas del Ecuador cuyo resultado ha servido para determinar: la normativa vigente, los controles y medios de verificación, metodología de riesgos y cuestionarios de control interno que hay que considerar en la evaluación del control interno y la identificación de las áreas críticas.

- ✓ De acuerdo a las encuestas realizadas se concluye que existe un gran desconocimiento de las normas de control interno por parte de los servidores públicos, que hace que no estén familiarizados con los controles que deben implementar, sin embargo está vigente el principio jurídico que dice el desconocimiento de la ley no justifica la culpa.

- ✓ El 87% de las instituciones públicas encuestadas indicaron que no tienen definidos los procesos del TI, es por ello que para el diseño de la presente guía de auditoría se efectuó por áreas.

- ✓ No existen controles permanentes, ya que de acuerdo a la encuesta realizada el 86% de las instituciones públicas indicaron que no se realizan evaluaciones de control interno en el área de TI.

- ✓ De la aplicación de la metodología de riesgos se obtuvo que las áreas con mayor nivel de riesgos son: la de organización y administración, seguida por la administración de servidores, redes y comunicaciones y la de soporte a usuarios y mantenimiento a equipos.

- ✓ Se desarrolló e implementó cuestionarios de control interno para cada área de TI, incluyendo preguntas de acuerdo a las Normas de Control Interno para las entidades públicas.

- ✓ Los medios de verificación o controles identificados en las diferentes áreas, ayudan en el proceso de solicitud de información, que de no ser presentados, sirven de evidencia por incumplimiento de los mismos.

5.2 RECOMENDACIONES.

- ✓ Socializar los contenidos de las legislaciones pertinentes con la finalidad que se den cumplimiento.
- ✓ Aplicar los cuestionarios de control interno de acuerdo a la estructura organizacional de la institución.

- ✓ Se recomienda que en las instituciones públicas se haga el levantamiento de procesos del área de TI.
- ✓ Realizar evaluaciones periódicas de control interno con la finalidad de evitar riesgos y tener una mejora continua en los procesos.
- ✓ En la fase de evaluación de riesgos, se recomiendan realizar reuniones de trabajo con las diferentes áreas con la finalidad de conocer las deficiencias que presenta cada una de ellas.
- ✓ Al realizar el pedido de información es importante tomar en cuenta los medios de verificación de la presente guía.
- ✓ Realizar el tratamiento de los riesgos con la finalidad de minimizar la probabilidad de ocurrencia y el impacto que estos generan.

5.3 BIBLIOGRAFÍA.

31000, I. O. (2009). *ISO 31000.*

AUDITORIA DE SISTEMAS. (s.f.). Recuperado el 17 de 12 de 2013, de wwwisis.ufg.edu.sv/wwwisis/.../TE/004.../004-C146m-Capitulo%20IV.p...

Auditoria de Sistemas. (10 de 06 de 2011). Obtenido de Blog: http://noris14.wordpress.com/2011/06/10/control-interno-informatico

COBIT. (2009). *The Cobit Framework*. Obtenido de http://isaca.org/Content/NavagationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Cobit4_Español.pdf

Codigo Organico de Planificación y Finanzas Públicas . (2010). Registro Oficial 306 del 22 de octubre del 2010.

Comisión de Auditoría. CCPM. (s.f.). *Colegio de Contadores Públicos de México.* Obtenido de CCPM: http://www.ccpm.org.mx/avisos/boletines/boletinauditoria3.pdf

Constitución de la Republica del Ecuador. (2008). Registro oficial 449 del 20 de octubre del 2008.

Constituyente, A. (2008). *Constitución de la Republica del Ecuador.*

Contraloria General, d. (2010). *Normas de Control Interno.* Quito.

Contraloria General, d. (2013). *Guia de auditoria Ambiental.* Quito: Acuerdo 037-CG-2013.

Ley de comercio electrónico, firmas electrónicas y mensajes de datos. (2002). Registro Oficial 557 del 17 de abril del 2002.

Ley del sistema nacional de registro de datos publicos. (2010). Resgistro oficial 162, 31 de marzo del 2010.

Ley Orgánica de la Contraloría General del Estado. (2002). Registro Oficial 595 del 16 de junio del 2002.

Ley organica de transparencia y acceso a la información pública . (2004). Registro oficial 337 del 18 de mayo del 2004.

Ley orgánica del sistema nacional de contratación pública . (2008). Registro oficial 395 del 4 de agosto del 2008.

Manual de Auditoria de Sistemas. (s.f.). Obtenido de CAPITULO IV: http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CCsQFjAB&url=http%3A%2F%2Fwwwisis.ufg.edu.sv%2Fwwwisis%2Fdocumentos%2FTE%2F004-C146m%2F004-C146m-Capitulo%2520IV.pdf&ei=x50PU7XqNou3kAev74HYBw&usg=AFQjCNE9y1j5HqtO_Cg9Iq55wu8gq

Merida Muñoz, J. (2012). Guia del Participante, Curso de Auditoría de Tecnologías de Información.

Nava Garcia , F. (s.f.). Apuntes de Auditoria Informatica.

NETCONSULT. (2009). *Nuevos conceptos de control interno: Informe Coso*. Obtenido de http://netconsul.com/tecnicas/index.php?ver=coso

Normas de aplicación obligatoria para las entidades del sector público ecuatoriano expedidas por la Contraloría General del Estado . (2009). Acuerdo 039-CG Registros Oficiales 78 y Suplemento 87 del 1 y 14 de diciembre del 2009.

OLACEFs. (2011). Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

Pinilla, J. D. (s.f.). *Auditoriá Informática - Aplicaciones en Producción.*

Reglamento general a la ley orgánica de transparencia y acceso a la información pública y reformas. (2005). Registro oficial 507 del 19 de enero del 2005.

Reglamento general a la ley orgánica del sistema nacional de contratación publica. (2009). Registro Oficial 588 del 8 de mayo del 2009.

Reglamento General de Bienes del Sector Público. (2006). Registro oficial 378 del 17 de octubre del 2006.

ABREVIATURAS Y ACRÓNIMOS

IT. Tecnologías de Información y comunicación.

NCI.- Normas de Control Interno.

Art.- Artículo.

CPD.- Centro de Proceso de Datos.

TIC.- Tecnologías de Información y Comunicaciones.

COBIT**.-** Objetivos de Control para las Tecnologías de Información

ITIL.-Biblioteca de Infraestructura de Tecnologías de Información.

OLACEFS.- Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores.

CAB.- Comité Asesor de Cambios.

BD.- Base de Datos.

DBA.- Administrador de la Base de Datos.

SIP.- Planes de Mejoras de Servicio

SLAs.- Acuerdos de Nivel de Servicio

OLAs.- Acuerdos de Nivel Operativo

UP.- Perfiles de Usuario.

SP.- Paquetes de Servicio

SLP.- Paquetes de Niveles de Servicio.

SLR.- Niveles de Requerimiento de Servicio.