UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE LICENCIADO (A) EN CONTABILIDAD Y AUDITORÍA

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

AUDITORÍA INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN APLICADOS POR EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA, PROVINCIA BOLÍVAR, 2021.

AUTORES:

JHONATHAN PAÚL CHIMBO VALENCIA

BETTY FERNANDA NARVÁEZ QUINDE

DIRECTORA:

ING. MERCEDES ANABEL MONAR VERDEZOTO

PARES ACADÉMICOS

ING. RENATO PAREDES ING. OSCAR TANQUEÑO

GUARANDA – ECUADOR

2022

TEMA DEL PROYECTO DEL TRABAJO DE TITULACIÓN

AUDITORÍA INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN APLICADOS POR EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA, PROVINCIA BOLÍVAR,2021.

AGRADECIMIENTO

Agradecemos a Dios por darnos la sabiduría, paciencia y fortaleza, permitiéndonos lograr una de las metas que nos hemos propuesto alcanzar en nuestra vida profesional.

A nuestros padres por darnos amor y el apoyo incondicional en cada etapa de nuestras vidas, que nos han sabido orientar en nuestro camino hasta poder llegar a nuestras metas.

A mis compañeros, amigos y familiares por brindarnos su amistad, apoyo a lo largo de nuestra etapa como estudiantes.

A nuestra directora del proyecto de investigación Ing. Anabel Monar quien nos tuvo mucha paciencia nos brindó sus conocimientos y ser guía para desarrollar con éxito el proyecto de investigación.

Jhonathan & Fernanda

DEDICATORIA

El presente trabajo de investigación lo dedico infinitamente a Dios, quien me ha dado la oportunidad de culminar una etapa más de mi vida.

A mis padres Carmen y Hugo que son una bendición en mi vida, por todo el sacrificio y esfuerzo que han realizado para darme la educación, a mis hermanos Álvaro y Mateo por estar siempre junto a mí, y a toda mi familia que de una u otra me apoyaron para seguir adelante.

Jhonathan Paul Chimbo Valencia

El presente trabajo está dedicado en primer lugar a Dios por haberme brindado la vida, la oportunidad de estudiar.

A mis padres Gladis y Nolverto por haber forjado como la persona que soy en la actualidad, muchos de mis logros se los debo a ustedes. A mi madre que ha sido un pilar fundamental en mi vida, la persona que ha creído en mí, me ha brindado su amor y su apoyo incondicional, mostrándome que todo lo que me propongo lo puedo lograr con esfuerzo y dedicación, que me ha inculcado valores y principios guiando mi camino para ser una persona de bien y una profesional exitosa. A mi padre que me brindo su amor, su cariño incondicional, aunque no este físicamente conmigo, desde el cielo siempre me cuidas. A mi familia por darme el apoyo incondicional y moral durante mi etapa como estudiante.

Betty Fernanda Narváez Quinde

CERTIFICADO DE VALIDACIÓN

UNIVERSIDAD ESTATAL DE BOLÍVAR

UNIDAD DE INTEGRACIÓN CURRICULAR
CARRERA DE CONTABILIDAD Y AUDITORIA

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Mercedes Anabel Monar Verdezoto e Ing. Renato Estuardo Paredes Cruz, Ing. Oscar Paúl Tanqueño Colcha, en su orden Directora y Par Académico del Trabajo de Integración Curricular "AUDITORÍA INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN APLICADOS POR EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA, PROVINCIA BOLÍVAR,2021" desarrollado por el señor y señorita CHIMBO VALENCIA JHONTHAN PAÚL y BETTY FERNANDA NARVÁEZ QUINDE

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera CONTABILIDAD Y AUDITORIA, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 7 de Octubre del 2022

MERCEDES ANABEL MONAR VERDEZOTO

Ing. Anabel Monar
Directora

RENATO ESTUARDO PAREDES CRUZ

Ing. Renato Paredes
Par Académico

OSCAR PAUL TANQUENO COLCHA

Ing.Oscar Tanqueño
Par Académico

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

DERECHOS DE AUTORÍA NOTARIZADA

DERECHOS DE AUTOR

Nosotros **Chimbo Valencia Jhonathan Paul** y **Narváez Quinde Betty Fernanda** portador/res de la Cédula de Identidad No **1805338736** y **1724120207** en calidad de autor/res y titular/ es de los derechos morales y patrimoniales del Trabajo de Titulación: **Auditoría Informática a los Sistemas de Información aplicados por el Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar, 2021**, modalidad **presencial**, de conformidad con el Art. 114 **del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN**, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
JHONATHAN PAUL CHIMBO VALENCIA

Jhonathan Paul Chimbo Valencia

CI: 1805338736

Firmado electrónicamente por:
BETTY FERNANDA NARVAEZ QUINDE

Betty Fernanda Narváez Quinde

CI: 1724120207

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

El uso de las tecnologías de la información y comunicación ha formado parte de nuestra vida cotidiana mejorando nuestro estilo de vida convirtiéndose en algo necesario e indispensable la seguridad de los sistemas informáticos, lo que nos trae efecto positivos y negativos. Las instituciones publica o privadas deben salvaguardar la seguridad Informática considerándose como un activo muy importante, por la cual se debe proteger la integridad de la información ya que es confidencial, la principal prioridad es el mantenimiento de los equipos informáticos para el desarrollo de las Actividades Laborales.

El presente proyecto de investigación se lo menciona como Auditoría Informática a los Sistemas de Información aplicados por el gobierno autónomo descentralizado del Cantón Guaranda, provincia Bolívar,2021, tiene como objetivo evaluar la eficiencia y eficacia del uso de los recursos informáticos su desarrollo se detallará a continuación:

CAPITULO I: Contiene la formulación general del proyecto donde se analiza los antecedentes formulación, objetivos y la justificación que sustenta el desarrollo de la presente investigación

CAPITULO II: Comprende el Marco teórico es decir antecedentes investigativos que fueron considerado para el desarrollo del proyecto de investigación, donde se investiga conceptos, variable, leyes que nos ayudan para el análisis de la Auditoría Informática aplicados a los sistemas de información referente al COBIT 4.0.

CAPITULO III: Se refiere al Marco Metodológico, el tipo de investigación, los métodos técnicos de recolección de información, instrumentos que se utilizados para el desarrollo del proyecto de investigación.

CAPITULO IV: Se refiere a Resultados y Discusión donde se aplica la metodología y se obtiene resultados de las encuestas aplicadas de Control Interno.

CAPITULO V: Denominado Propuesta, que concierne al desarrollo de la Auditoría Informática en sus cuatro fases Planificación Preliminar, Evaluación del sistema interno, Análisis de áreas Críticas, Redacción de informe y comunicación de resultados, para obtener el producto final que es el informe de Auditoría Informática.

RESUMEN

El presente proyecto de investigación, se realizó al Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar período 2021; con el fin de medir el grado de eficiencia y eficacia del manejo y uso adecuado de los equipos informáticos y seguridad con los que el personal a cargo de los sistemas informáticos maneja los equipos informáticos y la información que brinda a la ciudadanía se espera ayudar a la institución en la búsqueda de falencias que pueden tener los diversos procesos que se realizan diariamente en la institución, problemas con recursos humanos y tecnológicos utilizados en los departamentos, áreas del Municipio.

La metodología utilizada dentro de la investigación fue cualitativa y cuantitativa para el desarrollo de la auditoría Informática que consta de cuatro fases de acuerdo con el programa de Auditoría.

El marco metodológico de COBIT se emplea para identificar las fuentes generadoras de fallos y riesgos en sistemas de información, seguridad de la información y control interno de la institución mediante los niveles de madures de cada uno de los procesos seleccionados de COBIT.

Se realizo evaluaciones del sistema de control interno informático aplicando el COSO II o ERM con la finalidad de hacer un análisis de cada componente en base de la matriz de riesgo y confianza, un análisis general en base a la misma con los cuestionarios realizados con un análisis por componente.

Se elaboro indicadores de eficiencia, eficacia y seguridad de la unidad de Informática se encontró hallazgos lo que permitió, elaborar un informe de Auditoría con las falencias y hallazgos encontrados.

Se recomienda al señor alcalde, a las autoridades pertinentes dar una mayor participación a la unidad de Informática brindándole un espacio de capacitación de las Normas de Control de la Contraloría General del Estado específicamente la Norma 410 Tecnología de la Información.

ABSTRACT

The present research project was carried out to the Decentralized Autonomous Government of the Guaranda Canton, Bolívar province, period 2021; In order to measure the degree of efficiency and effectiveness of the management and proper use of computer equipment and security with which the personnel in charge of computer systems manage computer equipment and the information provided to citizens, it is expected to help the institution in search of shortcomings that may have the various processes that are carried out daily in the institution, problems with human and technological resources used in the departments, areas of the Municipality.

The methodology used was qualitative and quantitative for the development of the IT audit consisting of four phases in accordance with the Audit program.

The COBIT methodological framework is used to identify the sources of failures and risks in information systems, information security and internal control of the institution through the levels of maturity of each of the selected COBIT processes.

Evaluations of the computerized internal control system were carried out applying the COSO II or ERM in order to make an analysis of each component based on the risk and trust matrix, a general analysis based on it with the questionnaires carried out with an analysis per component.

Efficiency, effectiveness and safety indicators of the Informatics unit were developed, findings were found, which allowed the preparation of an Audit report with the shortcomings and findings found.

It is recommended to the mayor, to the pertinent authorities, to give a greater participation to the Informatics unit, providing them with a space for training on the Control Norms of the State Comptroller General's Office, specifically Norm 410 Information Technology.

CAPÍTULO I

1. FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

La Auditoría Informática es el análisis integro de los sistemas informáticos con el propósito de identificar o detectar y describir los distintos peligros que puedan presentarse. Se establece como un conjunto de procedimientos y técnicas que permite en una organización: evaluar, parcial o totalmente la categoría de protección de sus activos, recursos y control internos asociados a los sistemas informáticos para la obtención de eficacia, requerida en la organización.

La expansión de los requisitos relacionados con la revisión de los ordenadores obliga a los municipios a disponer de controles, estrategias y técnicas que garanticen la correcta utilización de los sistemas financieros, para que se salvaguarden de forma satisfactoria la información, dando así una mejor atención dentro del municipio.

A nivel mundial, los sistemas de información son atacados, creando altos peligros en sus datos, que son vitales para los usuarios y el municipio, ya que pueden provenir de números, planes estratégicos, información de encuestas, desarrollos de nuevos servicios, entre otros.

En nuestro país se establece que son pocos los municipios que pueden enfrentar problemas informáticos por la falta de una Auditoría Informática, para ello existen empresas que se dedican a ofrecer servicios que cuiden la integridad de la información del software sin interferencia. Por lo tanto, se debe realizar Auditorías constantes para el mejor desenvolvimiento y desarrollo de las empresas de nuestro país.

Estas dificultades pueden ser de diversa índole, desde el compromiso de hacer frente a las responsabilidades legales, por ejemplo, (daño grave a la información, condena civil u otros en general), lo que puede provocar un desmoronamiento crítico de la imagen del GAD, el proceso de servicios del municipio no puede ser capaz de implementar un sistema de calidad adecuado para los usuarios.

La finalidad de la Auditoría es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información, lo cual permitiría el cumplimiento de las funciones, actividades y operaciones de los funcionarios, empleados y usuarios involucrados en los servicios que proporcionan en los sistemas computacionales del Gobierno Autónomo Descentralizado del Cantón Guaranda.

1.2. Formulación del problema

Como evaluar la eficiencia y eficacia en el uso adecuado de la información y de los equipos informáticos a través de la Auditoría Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar, 2021.

1.3. Preguntas de Investigación

- ¿Qué técnicas de Auditoría se usarán para la obtención de información necesaria de cada área?

- ¿Cómo se detectarán errores y falencias en los procesos manejados por los sistemas de información?

- ¿De qué manera se controlará la integridad del software que maneja la institución y el uso que se le da al mismo?

- ¿Mediante qué indicadores se establecerá el grado de satisfacción de las necesidades y requerimientos en relación a la calidad, integridad y confidencialidad de información?

- ¿De qué manera verificamos la seguridad física y digital del procesamiento de la información?

1.4. Justificación

La presente investigación permitirá diagnosticar el uso, control y seguridad de la infraestructura tecnológica adoptando medidas de control preventivas y correctivas, con el fin de asegurar la confidencialidad de los usuarios.

Los conocimientos obtenidos en la Universidad se reflejarán en este proyecto de investigación a través de la Auditoría Informática que deben tener los municipios para una correcta recaudación de datos e información por parte del GAD de Guaranda, lo que le permitirá ofrecer una mejor atención al usuario.

Este proyecto es factible ya que cuenta con la oportunidad suficiente para fomentarla, el acceso directo a las fuentes de datos, la posibilidad de aplicar algunos instrumentos de exploración, y más aún, la voluntad de atender la problemática actual en el GAD de Guaranda.

La Auditoría Informática que se realizará será de extraordinaria ayuda para el GAD de Guaranda ya que mejorara las deficiencias que se han observado durante la investigación, de esta manera se tratará de que los conocimientos obtenidos en la Universidad, sea de gran ayuda para el personal del Municipio lo que ayudará a evitar contratiempos en la institución.

El resultado de esta investigación se reflejará en los resultados obtenidos en el trabajo de investigación dentro del GAD de Guaranda que será de extraordinaria ayuda en el departamento de informática, la misma que conducirá a la eficiencia y eficacia, esto permitirá llevar a cumplir con los objetivos y metas de la institución.

El impacto social al realizar la presente investigación permite identificar oportunidades de mejora, mediante el análisis de información aplicados por el Gobierno Autónomo Descentralizado del cantón Guaranda, de carácter positivo el manejo adecuado de los activos informáticos de manera eficiente, eficaz y segura, así como el servicio que brinda para la ciudadanía, puesto que la información entregada será confiable y veraz, estará disponible tanto para los funcionarios y la ciudadanía.

1.5. Objetivos: General y Especifico

1.5.1. Objetivo General

- Realizar una Auditoría Informática a los sistemas de información aplicados al Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar,2021 que permita evaluar la eficiencia y eficacia del uso adecuando de los recursos de informáticos.

1.5.2. Objetivos Específicos

- Elaborar el marco teórico mediante la revisión de fuentes bibliográficas y científicas para que sirva de apoyo para emprender la Auditoría Informática.

- Establecer el marco metodológico respectivo con la determinación de los métodos técnicas e instrumentos de investigación que permita recabar información veraz, oportuna y confiable con la finalidad de realizar una apropiada Auditoría Informática.

- Ejecutar un informe de conclusiones y recomendaciones para mejorar los sistemas de información con el cumplimiento de los objetivos y metas institucionales.

1.6. Idea a Defender

- Con la realización de la Auditoría Informática al Gobierno Autónomo Descentralizado de Cantón Guaranda, provincia de Bolívar, 2021. Permitirá determinará la eficiencia y eficacia en el uso de los recursos informáticos y de los sistemas de información.

1.7. Variables

1.7.1. Variable independiente

- Auditoría Informática

1.7.2. Variable dependiente

- Eficiencia y eficacia del uso adecuando de los recursos informáticos.

1.7.3. Operacionalización de variables

Cuadro 1. Operacionalización variable independiente

Variable	**Auditoría Informática**
Tipo	Independiente
Definición conceptual	Es el proceso ejecutado por especialistas del Área de Auditoría y de Informática, que se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de Informática en la organización que se lleva a cabo de una manera oportuna y eficiente.
Dimensión	Auditoría
Indicadores	• Eficiencia de información. • Usabilidad de la Auditoría. • Complejidad de la información.

Cuadro 2. Operacionalización variable dependiente

Variable	Eficiencia y eficacia del uso adecuando de los recursos informáticos.
Tipo	Dependiente
Definición conceptual	El análisis y determinación de la mejor metodología ayudara con un buen control del sistema y del personal del GAD del Cantón Guaranda permitiendo tener una mayor eficacia y rapidez en los procesos que se realizan en el GAD y evitar errores futuros. Por lo tanto, el objetivo será maximizar la eficiencia en el desarrollo de una Auditoría Informática en el GAD.
Dimensión	• Eficacia de equipos e instalaciones. • Análisis de resultados.
Indicadores	• Tiempo en la implementación. • Disponibilidad de información. • Políticas de Seguridad. • Gestión de incidentes de seguridad de la información.

CAPÍTULO II

2. MARCO TEORICO

2.1. Antecedentes Investigativos

La presente investigación está basada en los siguientes antecedentes investigativos obtenido mediante fuentes bibliográficas:

"El concepto de Auditoría Informática ha estado siempre ligado al de Auditoría en general y al de Auditoría interna en particular, y este ha estado unido desde tiempos históricos al de contabilidad, control, veracidad de operaciones, etc. En tiempo de los egipcios y se hablaba de contabilidad y de control de los registros y de las operaciones. Aún algunos historiadores fijan el nacimiento de la escritura como consecuencia de la necesidad de registrar y controlar operaciones". (Piattini Mario & Del Peso Emilio, 2008)

La Auditoría Informática nace de la necesidad de saber si la institución está logrando las metas institucionales propuestas, mostrando como una herramienta efectiva que permite conocer el manejo de los recursos informáticos así para lograr una eficacia y eficiencia en el uso de la misma.

"El concepto de la función de la Auditoría Informática, en algunos casos llamada función de control informático y en ocasiones, llamada y conocidas por ambos términos, arranca en su corta historia, cuando en los años cincuenta las

organizaciones empezaron a desarrollar aplicaciones Informáticas. Posteriormente, en función de que las organizaciones empezaron con sistemas cada vez más complejos, se hizo necesario que parte del trabajo de Auditoría empezara a tratar con sistemas que utilizaban sistemas informáticos".

"En este momento, los equipos de Auditoría, tanto externos como internos, empezaron a ser mixtos, con involucración de auditores informáticos junto con auditores financieros, fue entonces cuando se comenzaron a utilizar dos tipos de enfoques diferentes que en algunos casos convergían".

"Trabajos en los que el equipo de Auditoría Informática trabajaba bajo un programa propio, aunque entroncando sus objetivos con los de la Auditoría financiera; este era el caso de trabajos en los que se revisaban controles generales de las instalación y controles específicos de las aplicaciones bajo conceptos de riesgo, pero siempre unido al hecho de que el equipo de Auditoría financiera utilizaría este trabajo para sus conclusiones generales sobre el componente financiero determinado".

"Revisiones en las que la Auditoría Informática consistía en la extracción de información para el equipo de Auditoría financiera. En este caso el equipo o función de Auditoría interna era un exponente de la necesidad de las organizaciones y departamentos de Auditoría de utilizar expertos en información para proveer al personal de dicho departamento de información extraída de los sistemas

informáticos cuando la información al auditar estaba empezando a ser voluminosa y se estaba perdiendo la pista como se había creado."

"El futuro de la Auditoría Informática estará en la capacidad de cubrir adecuadamente en cuanto a experiencia y especialización, todas las áreas de los sistemas informáticos y de información de una empresa y adecuarse a los cambios que sucedan en la tecnología de la información. Para adecuarse a estos cambios, el auditor informático, tendrá que autogenerar su propia filosofía de gestión del cambio." (Piattini Mario & Del Peso Emilio, 2008)

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencia para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la Auditoría Informática sustenta y confirma la consecución de los objetivos tradicionales de la Auditoría:

- Objetivos de protección de activos e integridad de datos

- Objetivos de gestión que abarca, no solamente los de protección de activos, sino también los de eficiencia y eficacia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de Auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifica datos, por lo que se deberá emplear software de Auditoría y otras técnicas por ordenador.

El auditor es responsable de revisar e informar a la Dirección de Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada. (Piattini Mario, 2015)

2.2. Científico

2.2.1. Definición de Auditoría

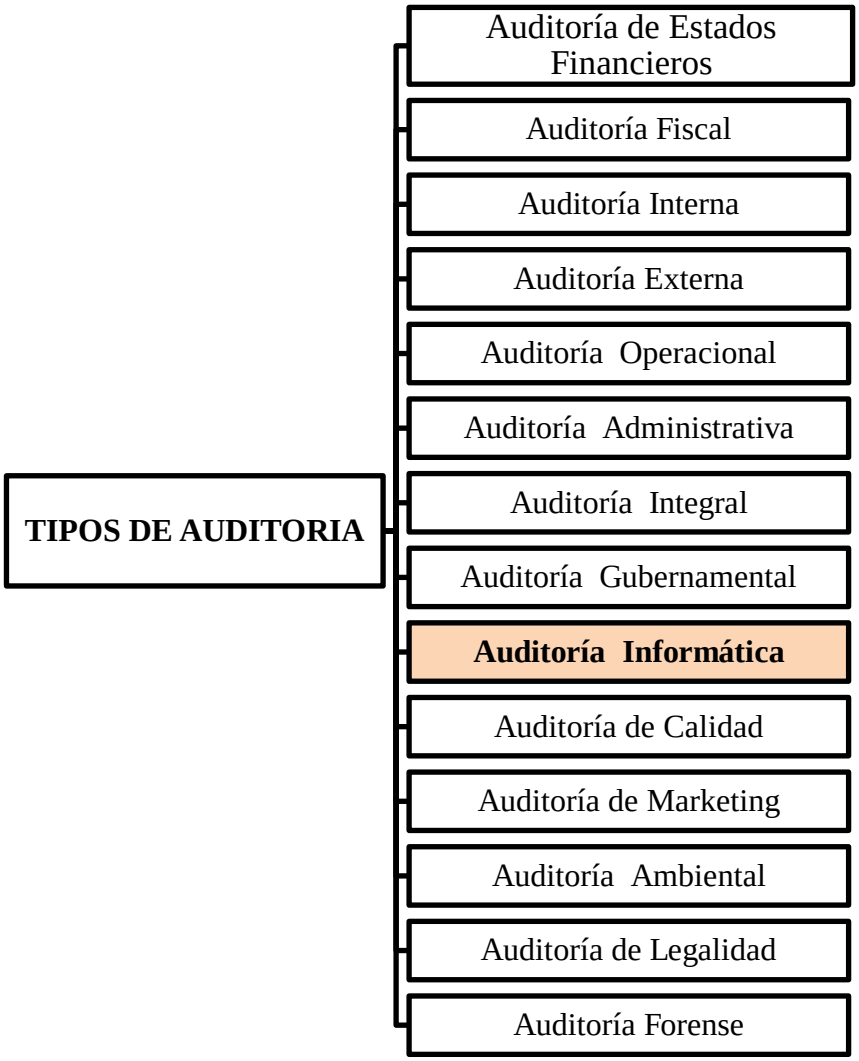
"La Auditoría es la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados a fin de evaluar el cumplimiento de las funciones actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación" (Muñoz, 2002).

El vocablo auditorio es sinónimo de examinar, verificar, investigar, consultar, revisar, comprobar y obtener evidencias sobre informaciones, registros, procesos, circuitos, etc. Hoy en día, la palabra auditoría se encuentra relacionada

con diversos procesos de revisión y verificación que, aunque todos ellos tienen en común el estar de una u otra forma vinculados a la empresa, pueden diferenciarse en función de su finalidad económica inmediata, de tal manera que según este criterio podemos establecer una primera gran clasificación de la auditoría diferenciando entre auditorías económicas y auditorías especiales (De la Peña, 2011).

2.2.2. Tipos de Auditoría

Figura 1. Tipos de Auditoría



La Auditoría constituye una herramienta de control y supervisión que constituye a la creación de una cultura de la disciplina de la organización, y permite descubrir fallas en las estructuras o vulnerabilidad existen en la organización (Placencia , 2019).

2.2.2.1. Auditoría de Estados Financieros

De acuerdo con (Delgado, 2019) una auditoría de estados financieros implica para el auditor la emisión de una opinión sobre si esos estados financieros preparados de acuerdo con una base contable determinada se presentan razonablemente de acuerdo con dicha base, para poder emitir una opinión el auditor debe haber realizado su trabajo de acuerdo con la Normas Internacionales de Auditoría y Aseguramiento, NIAA.

2.2.2.2. Auditoría Fiscal

Según (Nuño, 2017) la Auditoría fiscal consiste en verificar el correcto y oportuno pago de los diferentes impuestos y obligaciones de los contribuyentes, desde el punto de vista fiscal, de las direcciones o tesorería de hacienda estatales o tesorerías municipales.

2.2.2.3. Auditoría Interna

Es una modalidad de Auditoría basada en el control y la vigilancia interna de una empresa o Institución. Su realización busca la identificación de puntos de mejora y el correcto funcionamiento dentro de un marco normativo determinado, ayudando a una organización a cumplir con sus objetivos, aportando un enfoque sistemático y disciplinario para evaluar y mejorar la eficiencia de los procesos de gestión de riesgo, control y gobierno (Sánchez, 2022).

2.2.2.4. Auditoría Externa

Es una práctica común ejecutada por un profesional auditor externo a la empresa e instituciones donde se realiza un examen o verificación de las transacciones, cuentas informaciones o estados financieros, correspondientes a un periodo, evaluando la conformidad o el cumplimiento de las disposiciones legales o internas, vigentes en el sistema de control interno contable (Universidad Católica San Pablo, 2021).

2.2.2.5. Auditoría Operacional

Es la valoración independiente de todas las operaciones de una entidad, en forma analítica, objetiva y sistemática, para determinar si se llevan a cabo políticas y procedimientos aceptables, si se siguen las normas establecidas y si se utilizan los recursos de manera eficaz y eficiente (EUROINNOVA, 2021).

2.2.2.6.Auditoría Administrativa

Se puede considerar como un examen integral de la estructura de una organización, ya sea una empresa, institución o departamento gubernamental o cualquier otra entidad, son evaluados los métodos de control, los medios de operación y el empleo de sus recursos humanos y materiales; es un examen complejo y constructivo de la estructura organizativa (CONEXIÓN EXAN, 2017).

2.2.2.7. Auditoría Integral

Es la evaluación multidisciplinaria, independiente y con enfoque de sistemas de grado y forma de cumplimientos de los objetivos de una organización y de las relaciones con su entorno, así como de sus operaciones, con el objeto de proponer alternativas para el logro más adecuado de sus fines y el mejor aprovechamiento de sus recursos (Bautista, 2009).

2.2.2.8.Auditoría Gubernamental

La Auditoría gubernamental es un proceso mediante el cual la Autoridad vigila el uso de los recursos públicos (económicos, humanos y materiales), con objetivo de revisar la eficiencia, eficacia y la economía de la planeación, organización y ejecución de la administración pública (Dextre, 2016).

2.2.2.9. Auditoría Informática

Es la revisión y la evaluación de los controles, sistema y procedimientos de Informática de los equipos de cómputo, su utilización, eficiencia y seguridad en la organización, los cuales participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativo se logre una utilización más eficiente y segura de la información, que servirá para una adecuada toma de decisiones (Arcentales & Caycedo, 2017).

2.2.2.10. Auditoría de Calidad

Es una parte importante del sistema de administración de calidad de una entidad, y es un elemento fundamental para la obtención de la norma ISO 90001.

2.2.2.11. Auditoría de Marketing

Se define como un examen completo, sistemático independiente y periódico del entorno del marketing, objetivo, estrategias y actividades comerciales de una entidad o de una unidad de negociación, con la intención de determinar amenazas y oportunidades para recomendar un plan de acción y mejorar sus actuaciones en materia de marketing (Alvarez, 2007) .

2.2.2.12. Auditoría ambiental

Es el proceso de investigación realizado por un Auditor independiente, dirigido a determinar el grado de eficiencia empresarial, dirigido a determinar el grado de eficiencia empresarial, en relación con el grado de satisfacción experimentado por la comunidad y sus habitad, señalando en su informe de Auditoría a los agentes degradantes de medio ambiente y la magnitud de la degradación producida (Tapia, Mendoza , Castillo , & Guevara, 2019).

2.2.2.13. Auditoría de Legalidad

Este tipo de Auditoría tiene como finalidad revisar si la dependencia o entidad, en el desarrollo de sus actividades ha observado el cumplimiento de las disposiciones legales que sean aplicables a: leyes, reglamentos, decretos, circulares, etc. (Alcívar, 2021).

2.2.2.14. Auditoría Forense

La Auditoría Forense es una revisión especializada que se enfoca en la prevención y detección del fraude financiero, por medio de los siguientes enfoques:

- **Auditoría forense preventiva:** Orientada a proporcionar aseguramiento (evaluación) o asesoría a las organizaciones, respeto a su capacidad para disuadir, prevenir (evitar), detectar y reaccionar ante fraudes financieros; incluye trabajos de consultoría para implementar programas y controles antifraudes, esquemas de alerta temprana de irregularidades y sistemas de Administración de denuncias. Este enfoque es proactivo por cuanto implica tomar acciones y decisiones en el presente para evitar fraudes en el futuro (Hernández, Gallego, Ordoñez, & Alvarez , 2021).

- **Auditoría forense detectiva:** Orientada a identificar la existencia de fraudes financieros mediante la investigación profunda de estos, llegando a establecer entre otros aspectos los siguientes: cuantía del fraude, efectos directos e indirectos, posible, tipificación (según la normativa penal aplicable), presuntos autores, cómplices y encubridores; en muchas ocasiones, los resultados de un trabajo de Auditoría forense detective son puestos a consideración de la justicia que se encargara de analizar, juzgar y dictar la sentencia respectiva. (Tapia Carmen, 2016)

2.2.3. Definición de Auditoría Informática

Es el proceso forma ejecutado por especialistas del Área de Auditoría y de Informática, que se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de Informática en la organización se lleven a cabo de una manera oportuna y eficiente. (Nunñez, 2022)

2.2.3.1.Concepto de Informática

Son aquellas áreas de la tecnología de información orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya en las organizaciones (entidades internas y externas de los negocios) de manera oportuna, veraz y confiable (Rodríguez, López, Fernández, & Organista, 2021).

2.2.3.2.Objetivos de la Auditoría Informática

Según (Piattini, 2003)sostiene que la Auditoría Informática confirma la consecución de los objetivos tradicionales de la Auditoría: objetos de protección de activos e integridad de datos; y objetivos de gestión, que abarca no solamente los de protección de activos, sino también los de eficiencia y eficacia.

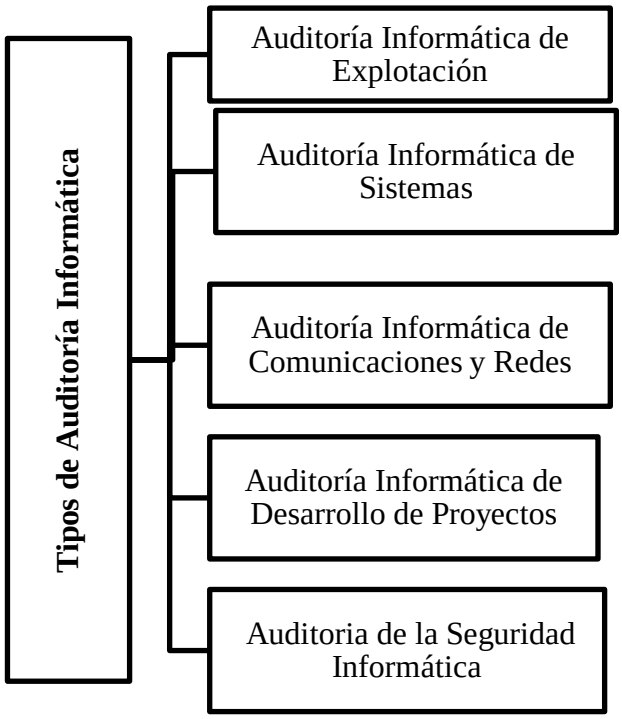
Según (Simon, 2006) en sus apuntes de Auditoría Informática cita a Ron (Weber, 1982) quien separa los objetivos en cuatro grupos: Objetivos de salvaguardar de bienes; objetivos de integridad de datos; objetivos de efectividad del sistema y objetivos de eficiencia del sistema.

2.2.3.3. Importancia de la Auditoría Informática

Según (Rivas, 200) "La tecnología Informática (hardware, software, redes, bases de datos, etc.) es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a los negocios frente a otros negocios similares en el mercado, pero puede originar costos y desventajas si no es bien administrada por el personal encargado."

2.2.4. Tipos de Auditoría Informática

Figura 2. Tipos de auditoría Informática



Auditoría Informática de Explotación

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos magnéticos para otros informáticos, órdenes automatizadas para lanzar o modificar procesos industriales, etc. Para realizar la Explotación Informática se dispone de materia prima los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso Informático, el cual está dirigido por programas. Obtenido el producto final, los resultados son sometidos a controles

de calidad, y finalmente son distribuidos al cliente, al usuario. En ocasiones, el propio cliente realiza funciones de reelaboración del producto terminado.

1. **Auditoría Informática de Sistemas**

Se ocupa de analizar la actividad propia de lo que se conoce como "Técnica de Sistemas" en todas sus facetas. En la actualidad, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones Informáticas, se auditen por separado, aunque formen parte del entorno general de "Sistemas".

2. **Auditoría Informática de Comunicaciones y Redes**

Se trata de un proceso empresarial, en el cual intervienen de manera conjunta los responsables del área de informática, administradores, contadores, auditores generales y coordinadores del resto de procesos ejecutados en la organización.

La importancia de este tipo de auditoría radica en que permite determinar las fortalezas y debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la adecuación de la configuración de la plataforma informática, el nivel de calidad de los servicios prestados por la unidad encargada y la situación de los contratos con proveedores de productos y

servicios, entre otros aspectos, todo ello en el ámbito del uso y aplicación de las TIC´s en la organización.

Esto con la finalidad de brindar recomendaciones y propuestas de solución y mejoramiento orientadas a lograr que las mismas brinden un apoyo optimo a los procesos de negocio y, por ende, ayuden a alcanzar los objetivos establecidos (Layedra, 2022).

3. Auditoría Informática de Desarrollo de Proyectos

El área de Desarrollo de Proyectos o de Aplicaciones es objeto frecuente de la Auditoría Informática.

Indicando inmediatamente que la función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones, término presente en los últimos años. La función Desarrollo engloba a su vez muchas áreas, tantas como sectores informáticos tiene la empresa.

Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario (único o plural), y del entorno.
- Análisis funcional.
- Análisis orgánico. (Pre programación y Programación).
- Pruebas.
- Entrega a Explotación y alta para el Proceso.

4. Auditoría de la Seguridad Informática

La seguridad en la Informática abarca los conceptos de seguridad física y seguridad lógica.

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

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

Se ha tratado con anterioridad la doble condición de la Seguridad Informática: Como Área General y como Área Específica (seguridad de Explotación, seguridad de las Aplicaciones, etc.).

Así, podrán efectuarse Auditorías de la seguridad global de una Instalación Informática- Seguridad General-, y Auditorías de la Seguridad de un área Informática de terminada- Seguridad Específica.

Las agresiones a instalaciones Informáticas ocurridas en Europa y América durante los últimos años, han originado acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida.

Tal estudio comporta con frecuencia la elaboración de "Matrices de Riesgo" en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y de los "Impactos" que aquellas pueden causar cuando se presentan.

Las matrices de riesgo se presentan en cuadros de doble entrada "Amenazas\Impacto", en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz. (Hernandez, Auditoría Informática , 2004)

2.2.5. Control Interno Informático

El control interno informático controla diariamente que todas las actividades del sistema de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la Organización y/o la Dirección de la Informática, así como los requerimientos legales.

La misión del control interno informático es asegurarse de que las medidas que se obtiene de los mecanismos implantados por cada responsable sean correctas y validas. (Piattini, 2003)

2.2.5.1. Objetivos del control interno informático

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijadas, evaluar su bondad y asegurarse del cumplimento de las normas legales.
- Asesorar sobre el conocimiento de las normas

- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las Auditorías externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático, lo cual no debe considerarse como que la implantación del mecanismo de medida y la responsabilidad de logro de esos niveles se ubique exclusivamente en la función de control interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de implantación de los medios adecuados. (Piattini, 2003)

2.2.5.2. Clases de Control interno Informático

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

- **Controles detectives:** cuando falla los preventivos para tratar de reconocer cuanto antes el evento. Por ejemplo, el registro de intensos de accesos no autorizados, el registro de la actividad diría para detectar errores u omisiones, etc.

- **Controles correctivos:** facilitan la vuelta la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad. (Piattini, 2003)

2.2.6. Seguridad de la información

Uno de los activos más valiosos para cualquier empresa es la información que maneja. La información es el conjunto de datos que da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la misma ruina.

La seguridad de la información es el conjunto de medidas y procedimientos, tantos humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información:

- **Integridad:** certificando que tanto la información como sus métodos de procesos son exactos y completos.
- **Confidencialidad:** Asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados.
- **Disponibilidad:** permitiendo que la información esté disponible cuando los usuarios la necesiten. (Escrivá Gasco, 2013)

2.2.7. Seguridad Informática

La seguridad Informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura

Informática y de telecomunicaciones para ser almacenada o trasmitida. Podemos distinguir los siguientes tipos:

En función de lo que se quiere proteger:

- **Seguridad física**: se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.

- **Seguridad**: lógica: mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.

En función del momento en que tiene lugar la protección:

- **Seguridad activa:** se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas). Por ejemplo, utilización de contraseñas.

- **Seguridad pasiva:** comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Por ejemplo, las copias de seguridad. (Escrivá Gasco, 2013)

2.2.8. Elementos vulnerables en sistema informático

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPU, terminales, cableado, medios de almacenamiento secundario (cintas, CD- ROM, disquetes o tarjetas de red).

Por software entendemos el conjunto de programas lógicos que hacen funcionar el hardware, tantos sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de un base de datos. (Costas Santos, 2015)

2.2.9. Amenazas de un sistema informático

Las amenazas a un sistema informático puedan provenir desde un hacker remoto que entra en nuestro sistema, pasando por un programa gratuito e incluso por una seguridad débil a continuación se detallan las amenazas del sistema informático.

- **Personas.** Las personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se divide en dos grandes grupos: los atacantes pasivos aquellos que fisgonean por el sistema, pero no lo modifican o destruyen, y los activos aquellos que dañan el objetivo atacado, o lo modifican en su favor.

- **Amenazas lógicas.** Encontramos todo tipo de programa que de una forma u otra puede dañar a nuestros sistemas, creados de forma intencional el software malicioso que pueden causar daños a los sistemas informáticos

- **Amenazas físicas:** Las amenazas físicas que pueden afectar a la seguridad y al funcionamiento de los sistemas.

  - Robos, sabotajes, destrucción de sistemas.

  - Cortes, subidas y bajadas brusca de suministro eléctrico.

  - Condiciones atmosféricas adversas. Humedad relativa excesiva o temperaturas extremas que afectan al comportamiento normal de los componentes informáticos. (Costas Santos, 2015)

2.2.10. Seguridad Física

Según (Escrivá Gasco, 2013) define la seguridad como "El conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenado de ellos."

Los riesgos externos a los que están sujetos los sistemas informáticos y las medidas preventivas que se pueden adoptar son los siguientes

- **Fenómenos naturales,** como inundaciones, tormentas, terremotos, etc.

  Se pueden adoptar medidas preventivas como la instalación de los equipos en ubicaciones adecuadas dotadas de las oportunas medidas de protección.

- **Riesgos humanos,** como actos involuntarios, actos vandálicos y sabotajes. Entre las medidas preventivas estarían: control de acceso a datos confidenciales, formación a usuarios en materia de seguridad, etc.

2.2.10.1. Elemento de la seguridad Física

Instalación eléctrica adecuada: los equipos informáticos funcionan gracias a la energía eléctrica que les llega a través de sus conexiones.

- **Protecciones eléctricas adecuadas.** Los enchufes deben constar con Tomás de tierra y la corriente suministrada debe ser lo más estable posible para evitar picos de tensión.

- **Mantenimiento del suministro eléctrico.** La corriente eléctrica está sometida anomalías, como apagones, caídas de tensión, etc. Hay que tomar las medidas necesarias para minimizar el riesgo de estas anomalías, así como para disminuir sus consecuencias negativas. Para prevenir las averías que estas anomalías pudieran producir a los equipos informáticos se desarrollaron los sistemas de alimentación interrumpida (SAI). Un SAI es un dispositivo que tiene por finalidad proporcionar alimentación a los equipos conectados a él cuándo se produce un corte en la corriente eléctrica, dando tiempo a que los equipos se apaguen de forma adecuada y no se produzca ninguna perdida de información.

Instalaciones de red adecuada. Los equipos conectados a una red de datos y esta a su vez a una red general. En primer término, hay que proteger esta red de acceso físico no deseados. Además, normalmente la red está configurada por cable, por lo que habrá que vigilar que el tipo de cable es correcto, así como que su estado de conservación es el adecuado al entorno (los cables pueden estar expuestos a la humedad, afectados por radiaciones electromagnéticas, etc.).

Control de acceso. Tanto si el ordenador está en una oficina, como si está en una sala especialmente destinada a su uso, habrá que controlar el acceso a ese lugar. Además, deberá asegurarse la entrada en el equipo en si mediante el establecimiento de claves.

Protección frente a incendios.

- **Sistema de prevención:** son los más eficaces, pues van encaminados a que no se produzcan el incendio. Por ejemplo, instalaciones de detectores de humo y alarmas, mantenimiento del orden y la limpieza para evitar la acumulación de materiales combustibles, etc.

- **Sistemas de protección:** son los que se ponen en marcha en caso de que se haya producido un incendio. Los más comunes son la colación de barreras para aislar el incendio, la delimitación clara de las vías de evacuación y salidas de emergencia y la instalación de sistemas de extinción. (Escrivá Gasco, 2013)

2.2.11. Control Interno

"El control interno comprende el plan de organización y el conjunto de métodos y procedimiento que aseguren que los activos estén debidamente protegidos, que los registros contables, son fidedignos y que la actividad de la entidad se desarrolla eficazmente según las directrices marcadas por la administración" (Estupiñan Gaitan, 2006)

2.2.11.1. Objetivos del Control Interno

- Proteger los activos y salvaguardar los bienes de la institución.
- Verificar la razonabilidad y confiabilidad de los informes contables y administrativos.
- Promover la adhesión a las políticas administrativas establecidas.
- Lograr el cumplimiento de las metas y objetivos programados. (Estupiñan Gaitan, 2006).

2.3. COBIT 4.0

Es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios. (Arturo Ocampo Lopez, 2015)

2.3.1. COBIT (objetivos de control para tecnologías de información y tecnología de información y tecnología relacionadas)

COBIT se aplica en los sistemas de información de toda empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. Brindando una efectividad a través de trabajos basados en procesos, y presenta las actividades de una estructura manejable y lógica. Las practicas del COBIT están enfocadas fuertemente en el control y no en la ejecución.

2.3.2. Distribución de los dominios y procesos de COBIT

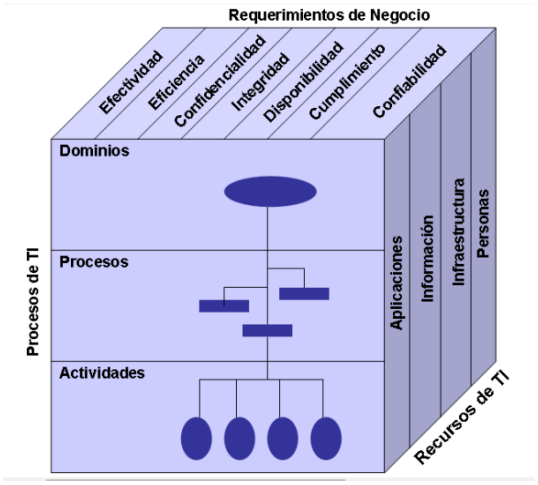
La estructura del estándar COBIT se divide en dominios, que son agrupaciones de procesos correspondientes a responsabilidades individuales. Un proceso es una secuencia de actividades asociadas con límites de control o puntos de corte, y los objetivos de control o actividades requeridas para lograr resultados medibles.

Se definen 34 objetivos generales de control, uno para cada proceso TI. Estos procesos se agrupan en cuatro grandes áreas, cuyos procesos se describen a continuación, junto con una descripción general de las actividades en cada área.

Cuadro 3 ***Dominios de COBIT***

DOMINIOS
Planeación y organización (PO): Cubriendo la estrategia y las tácticas, se ocupa de determinar cómo la tecnología de la información puede contribuir mejor al logro de las metas de la organización. La realización de la visión estratégica debe planificarse, comunicarse y gestionarse desde diferentes perspectivas, y debe establecerse la organización técnica y la infraestructura adecuadas.
Adquisición e Implementación (IA) Para ejecutar una estrategia de TI, las soluciones de TI deben identificarse, desarrollarse o adquirirse, implementarse e integrarse en los procesos comerciales. Además, este dominio incluye cambios y mantenimiento a los sistemas existentes.
Servicio y Soporte (DS) En esta área se hace referencia a la entrega de los servicios requeridos, que van desde las operaciones tradicionales hasta la capacitación, incluyendo aspectos de seguridad y continuidad. Para brindar el servicio, se deben implementar los procesos de soporte necesarios. Este dominio incluye el procesamiento de datos por parte de los sistemas de aplicaciones y generalmente se clasifica como control de aplicaciones.
MONITOREO (M) Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad.

Figura 3 Cubo de COBIT 4.0



Para satisfacer los objetivos de la entidad, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

- **Requerimientos de Seguridad. –** Calidad, Costo Entrega o Distribución (de servicio).
- **Requerimientos Fiduciarios. -** Efectividad y eficiencia de las operaciones, Confiabilidad de la información Cumplimiento de las leyes y regulaciones
- **Requerimientos de Seguridad.** - Confidencialidad, Integridad, Disponibilidad.

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave se encontró

que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas. A continuación, se muestran las definiciones utilizadas por COBIT:

- Efectividad
- Eficiencia
- Confidencialidad
- Integridad
- Disponibilidad
- Cumplimiento
- Confidencialidad

2.3.3. La misión del COBIT

Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

Los recursos de TI identificados en COBIT pueden explicarse/definirse como se muestra a continuación:

Datos. - Son objetos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Sistemas de aplicación. - Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Tecnología. - La tecnología cubre hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Instalaciones. - Recursos para alojar y dar soporte a los sistemas de información.

Personal. - Habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información. (IT GOVERNANCE INSTITUTE, 2009)

2.3.4. PRINCIPIOS COBIT

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

El marco de referencia Cobit 4.0 provee todos los procesos y actividades necesarios para permitir la creación de valor del negocio mediante el uso de TI y apoyado de herramientas propias del marco de referencia, permitiendo la consecución de beneficios y reduciendo el riesgo y uso de recursos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

COBIT 4 permite cubrir la empresa de extremo a extremo, cubriendo todos los procesos de la empresa, incluyendo todas las áreas funcionales, de TI, personal interno y externo, todo lo que sea relevante para el gobierno y la gestión de las TI relacionadas. La función de TI es considerada como un activo más de la empresa no se enfoca solo en la función que realiza

Principio 3: Aplicar un Marco de Referencia único integrado

El marco de referencia Cobit 4.0 aplica un marco de referencia único integrando estándares, marcos de trabajo y buenas prácticas relacionadas con TI y con la finalidad de ser un marco principal para el gobierno y gestión de las TI de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico

El marco de referencia Cobit 4.0 define distintas herramientas para apoyar la implementación de un sistema de gobierno y gestión para las TI de la empresa, todo esto basado en principios, políticas, marcos de trabajo, procesos, estructuras organizativas, cultura, ética, comportamiento, información, servicios, infraestructuras, aplicaciones, personas, habilidades y competencias.

Principio 5: Separar el Gobierno de la Gestión

El marco de referencia COBIT 4 divide claramente al gobierno y la gestión, ya que cada uno de estos conceptos involucra diferentes estructuras y propósitos organizacionales diferentes.

2.3.5. Metas de COBIT 4.O

COBIT 4.0 a través de la definición de metas permite traducir las necesidades de las partes interesadas de cada empresa en metas corporativas y relacionadas con metas de TI específicas para el tipo de negocio, industria, cultura que tiene una determinada empresa. Esta definición de metas se aplica y abarca a todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas.

Metas Corporativas de Negocio

COBIT 4 define 17 objetivos genéricos o metas corporativas de negocio enfocados en cuatro áreas principales como son financiera, cliente, interna, aprendizaje y conocimiento.

Metas Corporativas a Metas Relacionadas con las TI

Cobit 4.0 define 17 metas relacionadas con las TI, y cada una de estas son mapeadas con las metas corporativas de negocio usando los siguientes términos: 'P' que significa principal, una importante relación, es decir, las metas relacionadas con TI que son fundamentales para conseguir los objetivos de la empresa. 'S' que significa secundario, cuando las metas relacionadas con TI son un soporte secundario para los objetivos de la empresa. (Gualsaqui, 2013)

2.4.Coso II o ERM

"Es un proceso efectuado por la junta de directores, la administración y otro personal de la entidad, aplicando en la definición de las estrategias y a través del emprendimiento, diseñado para identificar los eventos potenciales que pueden afectar la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, para proveer seguridad razonable en relación con el logro del objetivo de la entidad." (Gaitán, 2016)

2.4.1. Fundamentos del Coso II o ERM

Las empresas con ánimo o sin ánimo de lucro deben propender a crear valor a sus protectores dueños o accionistas, así como la de enfrentar y superar las incertidumbres, desafiándolas con preparación suficiente, para poder proveer una estructura conceptual, así la gerencia trate de manera efectiva la incertidumbre que representan los riesgos y oportunidades, y así enriquecer su capacidad para generar valor. (Gaitán, 2016)

2.4.2. Beneficios del Coso o ERM

Ninguna organización con ánimo o sin ánimo de lucro opera en un entorno libre de riesgo, y el ERM, no crea tal entorno, sin embargo. Si representa beneficios importantes para operar más efectivamente en entornos llenos de riesgos, representando capacidad enriquecida para:

a) Alinear el apetito por el riesgo y la estrategia.

b) Vincular crecimiento, riesgo y retorno.

c) Enriquecer las decisiones de respuesta frente al riesgo.

d) Minimizar sorpresas y perdidas operacionales.

e) Identificar y administrar los riesgos de los impactos.

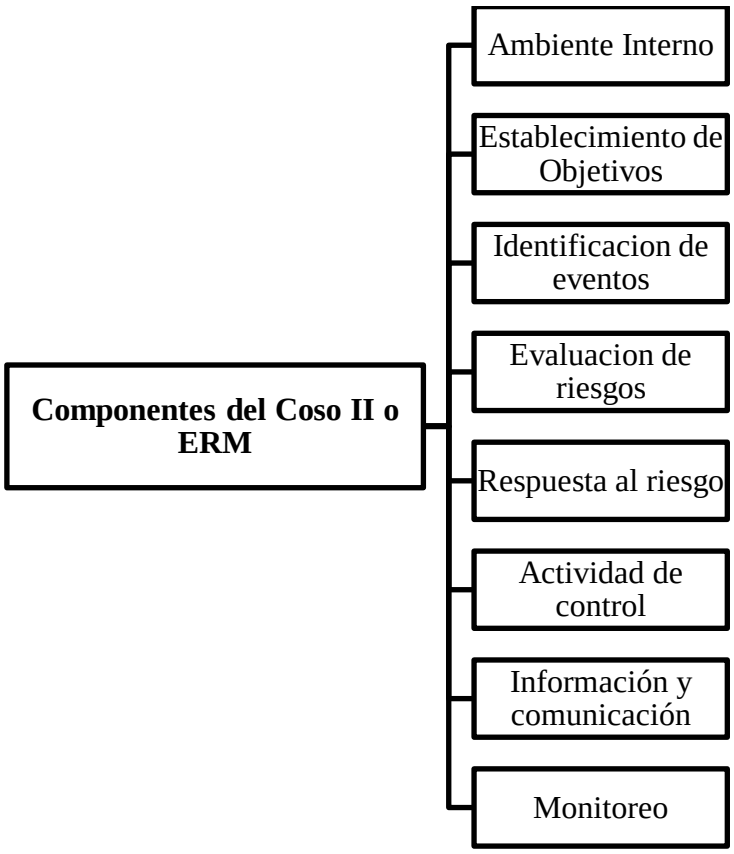
f) Proveer respuestas integradas para los riesgos múltiples.

g) Sopesar oportunidades.

h) Racionalizar el capital (Gaitán, 2016)

2.4.3. Componentes del Coso II o ERM

Figura 4. Componentes del Coso II o ERM



1. **Ambiente Interno**

Dentro de una organización el ambiente interno establece las bases sobre las cuales el riesgo es percibido y posteriormente entregado al personal de la entidad, incluyendo así la filosofía de administración del riesgo y el apetito por el riesgo, la integridad, los valores éticos y el ambiente en el que operan. (Becerra Efraín, 2016)

2. **Establecimiento de objetivos**

Es importante que los objetivos de la organización se establezcan antes que la administración pueda identificar los eventos potenciales que puedan afectar el logro. El COSO ERM, Afirma que la compañía puede administrar el correcto funcionamiento de los procesos para establecer objetivos y que estos, planteados con anterioridad, apoyan y están alineados con la visión/misión de la entidad y a su vez son consistentes con su apetito por el riesgo. (Becerra Efraín, 2016)

3. **Identificación de eventos**

Se deberá identificar todos aquellos eventos internos y externos los cuales afecten a la entidad, mediante el cual se puede clasificar entre eventos y oportunidades. Las oportunidades serán canalizadas hacia la estrategia de la administración o hacia el alcance de los objetivos. (Becerra Efraín, 2016)

4. **Evaluación de riesgos**

Al momento de identificar los riesgos, estos deben de ser analizados y teniendo en cuenta el impacto y probabilidad de que ocurran, siendo así la base para determinar cómo se debe administrar. Los riesgos se valoran sobre una base inherente y una base residual. (Becerra Efraín, 2016)

5. **Respuestas al riesgo**

La administración selecciona las respuestas a los riesgos identificados los cuales son: evitar, aceptar, reducir, o compartir el riesgo – desarrollando un conjunto de acciones que permitan a los riesgos alinearse con la tolerancia y con el apetito al riesgo que tiene la entidad. (Becerra Efraín, 2016)

6. **Actividades de control**

Se establecen e implementan políticas y procedimientos para ayudar a asegurar que se están ejecutando de manera apropiada las respuestas al riesgo, hacen parte del proceso mediante el cual una empresa intenta lograr sus objetivos de negocios. (Gaitán, 2016)

7. **Información y comunicación**

Identificar, captura y comunica información de fuentes internas y externas, en una forma y en una franja de tiempo que le permite al personal llevar a cabo sus

responsabilidades. La comunicación efectiva también ocurre en un sentido amplio, hacia abajo o a través y hacia arriba en la entidad. En todos los niveles se requiere información para identificar, valorar y responder a los riegos, así como para operar y lograr los objetivos. (Gaitán, 2016)

8. Monitoreo

Es un proceso que valora tanto la presencia como el funcionamiento de sus componentes y la calidad de su desempeño en el tiempo. Sé puede realizar mediante actividades de ongoing o través de evaluaciones separadas, los dos aseguran que la administración de riesgos continúa aplicándose en todos los niveles de una evaluación continua y periódica que hace la gerencia de la eficacia del diseño y operación de la estructura de control interno, para logra una adecuada identificación del riego, de acuerdo a lo planificado, modificando los procedimientos cuando se los requiera.

Para un adecuado monitoreo el COSO II estableció las siguientes reglas de monitoreo:

1. Obtención de la evidencia de que existe una cultura a la identificación del riesgo.
2. Si las comunicaciones externas corroboran las internas.
3. Si se hacen comparaciones periódicas
4. Si se revisan y se hacen cumplir las recomendaciones de los auditores.
5. Si las capacitaciones proporcionan realidad de lograr una cultura del riesgo.

6. Si el personal cumple las normas y procedimientos y es cuestionado
7. Si son confiables y efectivas las actividades de la Auditoría interna y externa. (Gaitán, 2016)

2.4.4. Normas de Control Interno

Norma de Control Interno de la Contraloría General del Estado

100 Normas Generales

El control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrá como finalidad crearlas condiciones para el ejercicio y control.

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos. Constituyen componentes de control interno el ambiente de control. La evaluación de riesgo, las actividades de control, los sistemas de información y comunicación y el seguimiento. Está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control.

200 Ambiente de Control

El ambiente control constituye un conjunto de circunstancias y conductas que enmarca el accionar de una entidad desde la perspectiva del control interno. También se define como el establecimiento de un entorno organizacional favorable al ejercicio de prácticas, valores, conductas y reglas apropiadas para sensibilizar a los miembros de la entidad y general una cultura de control interno.

300 Evaluación del Riesgo

La máxima autoridad establecerá los mecanismos necesarios que permitan la identificación, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos.

El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o a su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificaran, analizaran y trataran los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos.

400 Actividades de control

La máxima autoridad de la entidad y los servidoras y servidores responsables del control interno de acuerdo a sus competencias, establecerán políticas y procedimientos para manejar los riesgos en la consecución de los objetivos institucionales, proteger y conservar los activos y establecer los controles de acceso a los sistemas de información.

Las actividades de control se dan en toda la organización, en todos los niveles y en todas las funciones. Incluyen una diversidad de acciones de control de detección y prevención, tales como: separación de funciones incompatible, procedimientos de aprobación y autorización, verificaciones, controles sobre el acceso a recursos y archivos, revisión del desempeño de operaciones, segregación de responsabilidades de autorización ejecución, registro y comprobación de transacciones, revisión de procesos y acciones correctivas cuando se detectan desviaciones e incumplimientos.

410 Tecnología de la Información

410-01 Organización Informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la trasparencia 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 la información elabora 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 este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

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

410- 04 Políticas y procedimientos

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

410-05 Modelos de información organizacional

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

El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentación de forma permanente, incluirá las reglas de validación y los controles de integridad y constancia, con la identificación de los sistemas o módulos que lo conforman, sus

relaciones y los objetivos estratégicos a lo que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente.

410-06 Administración de proyectos tecnológicos

La unidad de tecnología de información definirá mecanismo 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 regulara los procesos de desarrollo y adquisición de software aplicativo con lineamiento, metodología y procedimientos.

410-08 Adquisición de infraestructura de tecnología

La unidad de tecnología de información definirá, justificará, implantará y actualizará la estructura tecnológica de la organización. Además, se evalúan los riesgos tecnológicos, el costo y la vida útil de la inversión para futuros actualizaciones.

Para la adquisición de hardware se realizará un detalle de las características técnicas como: marcas, modelo, numero de series, capacidades, con la finalidad de los equipos para la adquisición de las fases contractuales.

410 -09 Mantenimiento y control de la infraestructura tecnológica

Se elabora un plan de mantenimiento preventivo y/ o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estratégicas de actualización de hardware y software, riesgos, evaluaciones de vulnerabilidades y requerimientos de seguridad.

410-10 Seguridad de tecnología de información

Implementación y administración de seguridad a nivel de software y hardware, que se realizara con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre la vulnerabilidad o incidentes de seguridad identificados.

410-11 Plan de contingencias

Corresponde a la Unidad de tecnología de información de 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, aprobara y difundiría procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de

los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Revisiones periódicas para determinar si la capacidad y desempeño actual y futuro de los recursos tecnológicos son suficiente para cubrir los niveles de servicios acordados con los usuarios.

410-13 Monitoreo y evaluación de los procesos y servicios

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

410-14 Sitio web, servicios de internet a intranet

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

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

410-15 Capacitación Informática

Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constaran en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y las necesidades de conocimiento especifico en determinadas en las evaluaciones de desempeño institucionales.

410-16 Comité informático

Para la creación de un comité informático institucional, se consideran los siguientes aspectos: el tamaño y complejidad de la entidad y su interrelación con entidades adscritas. La definición de los objetivos que persiguen la creación de un comité de Informática como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforma la entidad.

410-17 Firmas electrónicas

Las entidades, organismos y dependencia del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustaran sus procedimientos y operaciones e incorporaran los medios técnicos necesarios, para

permitir el uso de la firma electrónica de conformidad con la ley de comercio electrónico, firmas y mensajes de datos y su reglamento.

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

500 información y comunicación

El sistema de información y comunicación, está constituido por los métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones técnicas, administrativas y financieras de una entidad. La calidad de la información que brinda el sistema facilita a la máxima autoridad adoptar decisiones adecuadas que permitan controlar las actividades de la entidad y preparar información confiable.

500-01 Controles sobre sistemas de información

Los sistemas de información contaran con controles adecuados para garantizar confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles.

La utilización de sistemas automatizados para procesar la información implica varios riesgos que necesitan ser considerados por la administración de la entidad. Estos riesgos están asociados especialmente con los cambios tecnológicos por lo que se deben establecer controles generales, de aplicación y operación que garanticen la protección de la información según su grado de sensibilidad y confiablidad, así como su disponibilidad, accesibilidad y oportunidad.

500- 02 Canales de comunicación abiertos

Se establecerán canales de comunicación abiertos, que permitan trasladar la información de manera segura, correcta y oportuna a los destinatarios dentro y fuera de la institución.

Una política de comunicación interna debe permitir las diferentes interacciones entre las servidoras y servidoras, cualesquiera sean el rol que desempeñen, así como entre las distintas unidades administrativas de la institución.

600 seguimiento

La máxima autoridad y los directivos de la entidad, establecerán procedimientos de seguimiento continuo, evaluaciones periódicas o combinación de ambas para asegurar la eficacia del sistema del control interno.

Seguimiento es el proceso que evalúa la calidad del funcionamiento de control interno en el tiempo y permite al sistema reaccionar en forma dinámica, cambiando cuando las circunstancia así lo requieran. Se orientará a la identificación de controles débiles o insuficientes para promover su reforzamiento, así como asegurar que las medidas producto de hallazgos de Auditoría y los resultados orientados de otras revisiones, se atiende de manera efectiva y con prontitud. (Contraloria General del Estado, 2014)

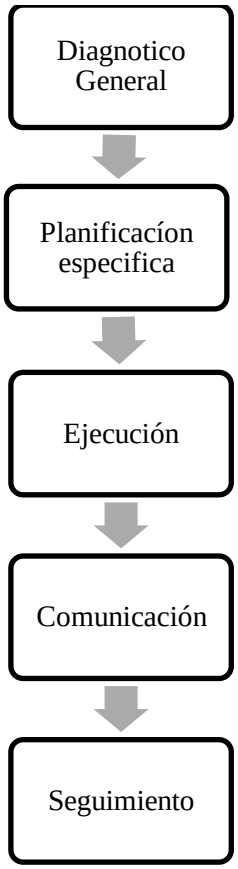
2.4.5. Normas ISO 27001

Las ISO 27001 es una norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la información en una empresa. La última revisión se denomina ISO/IEC 27001:2013. (27001 Academy, s.f.)

La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un **sistema de gestión de seguridad de la información** (SGSI) que permita evaluar todo tipo de riesgo o a menazas susceptibles de poner en peligro la información de una organización de una organización tanto propia como datos de terceros. (EXCELLENCE)

2.4.6. Procesos de Auditoría

Figura 5. Procesos de la Auditoría



El proceso de auditoría es sistemático porque hay una interrelación indudable entre las diferentes fases que lo conforman, las mismas que son cincos:

1. **Diagnostico General:** Conocimiento de la organización de la empresa
2. **Planificación:**
    - **Preliminar:** Principales actividades, metas y objetivos.
    - **Especifica:** Enfoque por componente

3. **Ejecución del Trabajo:** Aplicación de programa de trabajo y obtención de evidencia.

4. **Comunicación de resultado:** Los hallazgos de Auditoría y el informe

5. **Monitoreo:** Seguimiento de aplicación de recomendaciones

2.4.7. Papeles de Trabajo

Son el conjunto de cedulas y documentación fecha que contiene los datos e información obtenidos por el auditor en sus exámenes, así como la descripción de las pruebas realizadas y los resultados de las mismas sobre los cuales sustenta la opinión que emite al suscribir su informe. (ZAMARRÓN, 2009)

"El auditor externo deberá documentar los asuntos que son importantes para apoyar la opinión de Auditoría y dar evidencia de que la auditoría se llevó a cabo de acuerdo con las Normas Internacionales de Auditoría."

Los papeles de trabajo

a) Auxilia en la planeación y desempeño de la auditoría.
b) Auxilian en la supervisión y revisión del trabajo en auditoría.

c) Registran la evidencia de auditoría resultante del trabajo de auditoría desempeñado, para apoyar la opinión del auditor externo" (Estupiñán Gaitán, 2014)

2.4.7.1. Objetivos de los papeles de trabajo

Los papeles de trabajo constituyen una compilación de toda evidencia obtenida por el auditor y cumplen los siguientes objetivos fundamentales:

- Facilitar la preparación del informe de Auditoría y revisión fiscal.
- Comprobar y explicar en detalle las opiniones y conclusiones resumidas en el informe
- Proporcionar información para la preparación de las declaraciones de impuestos y documentos de registro para la Comisión Nacional de Valores y otros organismos de control y vigilancia del estado.
- Coordinar y organizar todas las fases de trabajo de la auditoría.
- Prever un registro histórico permanente de la información examinada y los procedimientos de la Auditoría aplicados.
- Servir de Guía en exámenes subsecuentes.

Estos objetivos son aplicables en el caso de los papeles de trabajo preparados para la auditorías y revisorías fiscales anuales recurrentes y

adaptables, tanto para auditoría no recurrentes como para investigaciones especiales. (Estupiñán Gaitán, 2014)

2.4.7.2.Documentación de los papeles de trabajo

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

- Recogen la evidencia obtenida a lo largo del trabajo.
- Ayudan al auditor en el desarrollo de su trabajo.
- Ofrecen un soporte del trabajo realizado para, así, poder utilizarlo en auditorías sucesivas.
- Permiten que el trabajo pueda ser revisado por terceros. (Piattini Velthuis, 2015)

2.4.8. Archivo permanente

El archivo permanente contiene todos aquellos papeles que tiene un interés, una validez plurianual, tales como:

- Características de los equipos y de las aplicaciones.
- Manuales de equipos.
- Descripción del control interno.
- Organigramas de la empresa en general.
- Organigramas del Servicio de Información y división de funciones.
- Cuadro de planificación plurianual de Auditoría.
- Escritura y contratos
- Consideraciones sobre el negocio
- Consideraciones sobre el sector.
- En general toda aquella información que puede tener importancia para auditorías posteriores. (Piattini Velthuis, Mario, 2015)

2.4.9. Archivo Corriente

En este archivo, a su vez, se suele dividir en archivo general y en archivo de áreas o de procesos.

a) Archivo general

Los documentos que se suelen archivar aquí son aquellos que no tienen cabido especifico en alaguna de las áreas/ Procesos en que hemos dividió el trabajo de Auditoría, tales como:

- El informe de Auditor.
- La Carta de recomendaciones.
- Los Acontecimientos posteriores.
- El cuadro de planificación de auditoría corriente.

- La Correspondencia que se ha mantenido con la dirección de la empresa.
- El tiempo que cada persona del equipo ha empleado en cada una de las áreas/ procesos.

b) Archivo por áreas/ procesos

Se debe preparara un archivo para cada de las áreas o procesos en que hayamos dividido el trabajo e incluir en cada archivo todos los documentos que hayamos necesitado para realizar el trabajo de esta área/procesos concretos. Al menos deberán incluirse los siguientes documentos:

- Programa de Auditoría de cada una de las áreas/ procesos.
- Conclusiones del área/procesos en cuestión.
- Conclusiones del procedimiento en cuestión. (Piattini Velthuis, Mario, 2015)

2.4.10. Evidencia de Auditoría

Es toda la información que utiliza el auditor para llegar a la conclusión que se basa su opinión. Esta información incluye tanto registros de los estados financieros, como otros tipos de información.

"Es toda la información que utiliza el auditor para llegar a la conclusión en que se basa su opinión. Esta información incluye tanto los registros de los estados financieros, como de otro tipo de información." (Espino García, 2015)

- **Suficiente**

  Medida cualitativa, referida a la cantidad de evidencia obtenida.

- **Apropiada**

  Medida cuantitativa, referida a la relevancia, fiabilidad y legalmente valida. (Velásquez, 2015)

2.4.11. Tipos de evidencia

1. **Sistemas de información contable**
2. **Evidencia documental.**
   a) Evidencias documentales creada fuera de la empresa y transmitida directamente a los auditores (estado de cuenta bancaria);
   b) Evidencias de fuera de la empresa y conservada por ellos. Ejemplo: factura de un proveedor, declaración de impuestos.
   c) Evidencias documental creada y conservada por el cliente. Ejemplo: cheque pagado
3. **Declaraciones de terceros**
   a) Confirmaciones;
   b) Cartas de abogados:

c) Informes de especialistas (peritos)

4. **Evidencia física, Inventarios de mercancías y de activos fijos.**

a) Cálculos de la depreciación o de ganancia por acciones;

b) Interrelaciones de datos. Costo de ventas, costo de producción;

c) Declaraciones de los clientes. Orales y escritas.

2.4.12. Riesgo de Auditoría

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

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

- Del tipo de negocio
- De su medio ambiente
- Del tipo de transacción

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

Riesgo de no detección: Es el riesgo de que un error u omisión significativa existen no sea detectado, por ultima, por el propio proceso de Auditoría. El nivel de riesgo de no detección está directamente relacionado con los procedimientos de Auditoría debido al:

- La ineficacia de los procedimientos de Auditoría aplicados.
- La inadecuada aplicación de dichos procedimientos.
- Al deficiente alcance y oportunidad de los procedimientos seleccionados.
- A la inapropiada interpretación de resultados de los procedimientos.

El riesgo de Auditoría se determina a partir de la siguiente formula:

$$RA = RI \times RC \times RD$$

RA= Riesgo de Auditoría

RI= Riesgo Inherente

RC= Riesgo de control

RD= Riesgo de Detección (Guitierrez, 2011)

2.4.13. Hallazgos de Auditoría

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

Es toda la información que a juicio del auditor le permite identificar hechos o circunstancias importantes que inciden en la gestión de recursos en la organización, programa o proyecto bajo examen que merecen ser comunicados en el informe. (Tabón, 2016)

2.4.14. Requisitos principales de un Hallazgo de Auditoría

Los requisitos que deben reunir un hallazgo de auditoría son:

- Importancia relativa que amerite ser comunicado
- Basado en hechos y evidencias precisas que figuran en los papeles de trabajo
- Objetivo. (obrar con objetividad, equidad realismo)
- Convincente para una persona que ha participado en la auditoría

2.4.15. Elementos del Hallazgo de Auditoría

Para que los hallazgos de auditoría puedan cumplir con los objetivos que persiguen el auditor, deben estar adecuadamente redactadas, es decir deben incluir los elementos o características. (Tabón, 2016)

Cuadro 4. ***Elementos de hallazgos de Auditoría***

Condición	**Constituida por la condición actual encontrada (Lo que es)**
Criterio	Representado por la norma o la unidad de medida que se compara con la condición o "Lo que debe ser"
Efecto	Consecuencia o impacto posible pasado o futuro (cuando se le aplicativo). (Diferencia entre lo que es y lo que debe ser)
Causa	Razón o las razones por la que ocurrió la condición. (Quien, o que lo origino)

2.4.16. Informe de Auditoría

El producto de la tercera fase de la auditoría es desarrollar un informe con los comentarios, conclusiones y recomendaciones, actividad concluyente de la fase de comunicación, cuando se efectúa la homologación de resultados.

La comunicación en el proceso de auditoría es permanente, por lo tanto, los resultados son discutidos apenas se generan. Estos hallazgos son sometidos a un

proceso de constante revisión. Con estos resultados estamos en capacidad de expresar una opinión que incluye en el informe de Auditoría.

Las comunicaciones por escrito se realizarán una vez que el auditor haya identificado el problema o deficiencia, se somete a pruebas y a evaluaciones para obtener evidencias suficientes que sustenten criterios. (Arcenegui Rodrigo, 2003)

2.5. Conceptual

Activos Informáticos

"Un activo se define como aquel recurso del sistema (Informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y deba ser protegido frente a un eventual percance, ya sea intencionado o no". (Gascó)

Auditor

El término "Auditor" es utilizado para referirse a la persona que conducen la Auditoría, por lo general es el socio u otro integrante del equipo de trabajo o, en su casa, la firma. (Tapia Carmen, 2016)

Auditoría

"Es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como

establecer si dichos informes se han elaborado observando los principios establecidos para el caso" (Tapia Carmen, 2016)

Auditoría Informática

"Conjunto de procedimientos y técnicas que permiten en una entidad: evaluar, total o parcialmente, el grado en que se cumplen la observancia de los controles internos asociados al Sistema informático; determina el grado de protección de sus activos y recursos; verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa Informática y general existentes en la entidad, y para conseguir la eficacia exigida en el arco de la organización correspondiente. (Lazaro, 2008)

D

Datos

"Constituye el núcleo de toda organización, hasta tal punto que se tiende a con a considera que el resto de actividades están en el servicio de la producción de datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo." (Arturo Ocampo Lopez, 2015)

E

Eficacia

"El logro de los objetivos mediante los recursos disponible" (Chiavenato, 1999)

Eficiencia

"Utilización adecuada de los recursos disponibles" (Chiavenato, 1999)

H

Hardware

"Es el elemento físico de una computadora, es decir es la parte tangible como el CPU, lo cables, etc.". (Arturo Ocampo Lopez, 2015)

I

Información

"Todo aquel elemento que contenga datos almacenados en cualquier tipo de soporte. Como, por ejemplo, documentos, libros, patentes, correspondencia, estudios de mercado, datos de los empleados manuales de usuarios, etc.". (Gascó)

Informática

"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores."
(Fernández, 2006)

S

Seguridad Informática

"Es el conjunto de medidas y procedimientos tantos humanos como técnicos que permiten proteger la integridad, confidencialidad y disponibilidad de la información" (Gascó)

Sistemas de Información

"Un sistema de información está formado por todos los componentes que colaboran para procesar los datos y producir información. Casi todos los sistemas de información empresarial están integrados por muchos subsistemas con metas secundarios, todas las cuales contribuyen a la meta principal de la organización". (Oz, 2008)

Software

"Constituido por los sistemas operativos y el conjunto de aplicación instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido". (Gascó)

2.6. Legal

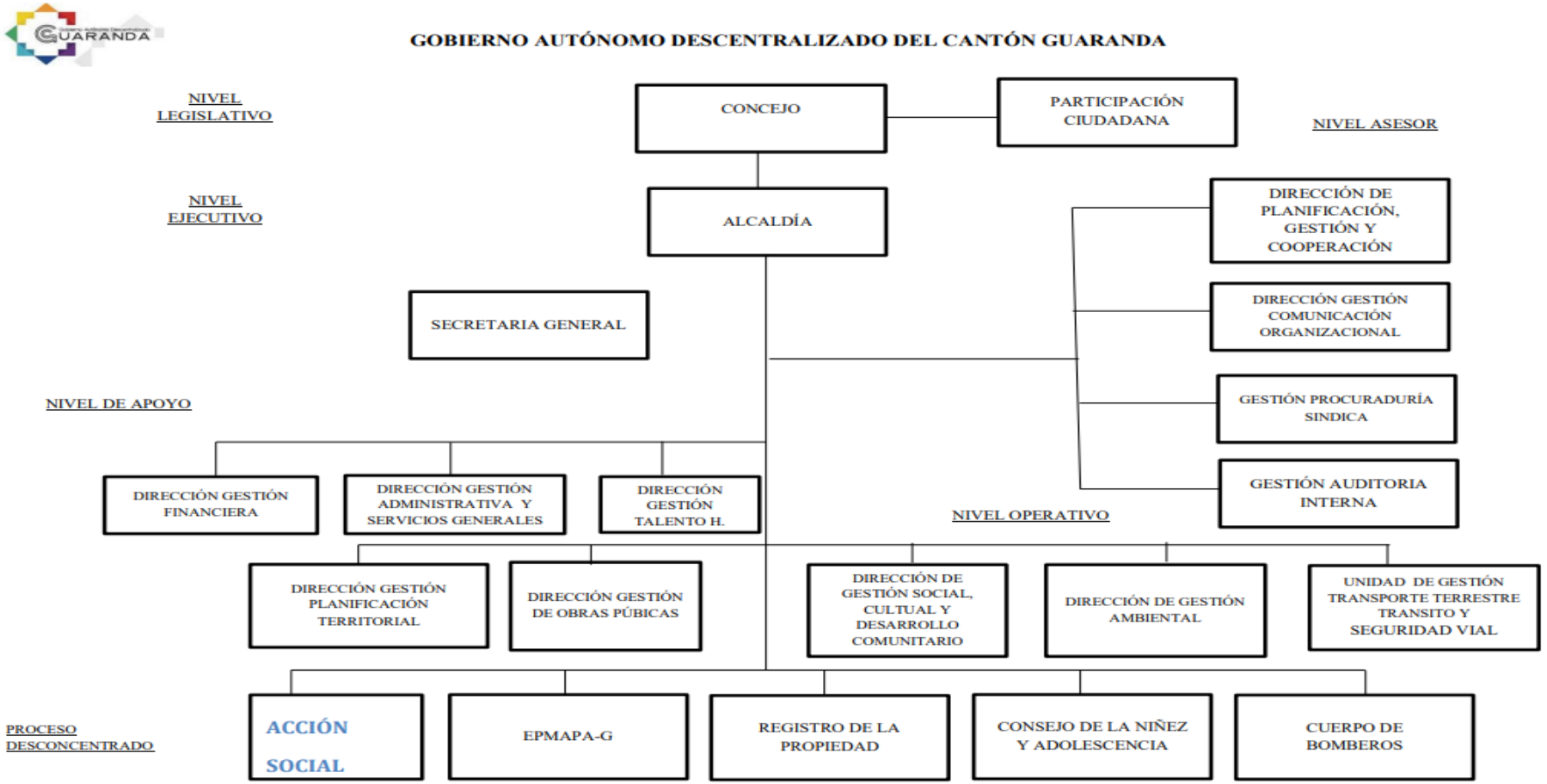
2.6.1. Base Legal

- Constitución Política de la República del Ecuador
- Ley orgánica de la contraloría General del estado
- Ley de presupuesto del sector publico
- Ley orgánica de Régimen Municipal
- Ley Orgánica de Régimen Tributario Interno
- Ley Orgánica del Sistema Nacional de Contratación Publica
- Ley Orgánica de servicio Civil Y Carrera Administrativa y Unificación Homologación de Remuneraciones del sector publico

- Código Orgánico de Organización Territorial Autonomía y Descentralización (COOTAD)
- Código de Trabajo
- Código de Procedimiento Civil
- Código Orgánico Integral Penal, COIP
- Código Orgánico de la Función Judicial
- Codificación de la Ley de Aguas
- Ley Orgánica de Participación Ciudadana
- Ley Orgánica de Defensa del Consumidor
- Ley de Arbitraje y Mediación
- Ley de la Jurisdicción Contencioso Administrativa
- Ley Orgánica del sistema Nacional de Contratación Pública (LOSNCP)
- Reglamento General a la LOSEP
- Reglamento de Talento Humano
- Reglamento General Sustitutivos de Bienes del Sector Publico
- Reglamento para el pago de Viáticos para la Movilización y Subsistencias en el Exterior para Servidores y Obreros Públicos
- Normativa de Contabilidad Gubernamental del Ministerio de Finanzas
- Estatuto Orgánico por proceso institucional
- Normas de Control interno de la Contraloría General de Estado

2.6.2. Estructura Organizacional

Figura 6. Estructura organizacional del GAD Municipal del Cantón Guaranda



2.7. Georreferencial

2.7.1. Ubicación Geográfica

El Gobierno Autónomo Descentralizado del Cantón Guaranda se encuentra localizada en las calles García Moreno y convención 1884 frente al parque central de la cuidad de la Provincia Bolívar.

Figura 7. Ubicación del GAD Municipal del Cantón Guaranda

CAPÍTULO III

2.8. METODOLOGÍA

2.9. Tipo de Investigación

La investigación se realizará mediante los siguientes tipos:

- **Bibliográfica:** Investigación documental (revistas, libros, internet). Se aplica para la elaboración del marco teórico.

- **Descriptiva:** En la investigación se describirá eventos, procesos y situaciones reales sobre la información y los equipos informáticos del Gobierno Autónomo Descentralizado del Cantón Guaranda con el objetivo de medir el grado de eficiencia y eficacia y el uso adecuado de los recursos informáticos.

- **Correlacionales:** La relación entre la variable independiente y variable dependientes que se determinara en la investigación, es decir la relación entre la Auditoría Informática y el grado de eficiencia y eficacia de los sistemas aplicados por el Gobierno Autónomo Descentralizado del Cantón Guaranda y el uso adecuado de los recursos informáticos.

2.10. Enfoques de la Investigación

Los tipos de investigación que se aplicara en el actual trabajo es la modalidad Cualitativa que permite describir eventos mediante técnica como la observación, y la cuantitativa analiza los datos recolectados de manera numérica y oportuno y es decir es una modalidad combinada.

Cualitativa. -Se realiza descripciones detalladas del manejo y seguridad de la información y de los equipos informáticos existentes en el Gobierno Autónomo Descentralizado del Cantón Guaranda.

Cuantitativa. -La información que se va obtener mediante encuestas que se va a realizar al personal del Gobierno Autónomo Descentralizado del Cantón Guaranda ya que tienen bajo custodia los equipos informáticos y la información almacenada.

2.11. Métodos de Investigación

Métodos Deductivos. -Tipo de razonamiento que lleva de lo general a lo particular o de lo complejo a lo simple, este método se utilizó para el planteamiento del problema donde se detallará indicadores mundiales hasta llegar a información particular del Gobierno Autónomo Descentralizado del Cantón Guaranda.

Método Inductivo. – Los casos particulares, eleva conocimientos generales, en este método se utilizará el análisis para el cumplimiento de las Normas de control Interno, de la Contraloría General del Estado por parte del Gobierno Autónomo Descentralizado del Cantón Guaranda es decir todas las entidades del sector público debe acatar dichas normas.

2.12. Técnicas e Instrumentos de Recopilación de Datos

Observación Directa. – Se formalizarán visitas frecuentes al Municipio de Guaranda, con el objetivo de recolectar información relevante y apreciar directamente el manejo de la información y de los equipos computacionales o informáticos por parte de los empleados públicos.

Encuestas. – Las encuestas que se van a realizar a los directivos y al personal del Municipio de Guaranda servirán de manera oportuna para la recolección de información sobre la eficacia y eficiencia del uso de los recursos informáticos.

Entrevistas. -Posteriormente se realizará una entrevista al señor alcalde para obtener información y evidencia que sustente los hallazgos que se va encontrar en el área de Informática.

2.12.1. Instrumentos de Recopilación de Datos

Cuestionario. – Se recolectará información mediante el estudio de preguntas cerradas y abiertas dirigidas al técnico de sistemas informáticos con relación a la administración de la información y de los equipos informáticos.

Checklists. - Se realizará preguntas adicionales al personal del Municipio de Guaranda para terminar la elaboración de la investigación.

2.13. Universo

El universo del Gobierno Autónomo Descentralizado del Cantón Guaranda está constituido por 59 funcionarios a nivel del Municipio de todos los departamentos.

2.13.1. Población y Muestra

La población de los sistemas Informáticos del Gobierno Autónomo Descentralizado del Cantón Guaranda está constituida por 11 personas por la razón no es necesario determinar la muestra consecuentemente se trabajará con toda la población.

En el área de los sistemas informáticos están constituido de la siguiente manera:

Cuadro 5. Sistemas informáticos del GAD Municipal del Cantón Guaranda

UNIDAD ADMINISTRATIVA	CARGO	FUNCIONARIOS
DIRECCIÓN	**DIRECTOR ADMINISTRATIVOS**	Lic. Rodrigo Castillo
SECRETARÍA	**SECRETARIA DE DIRECCIÓN**	Lcda. Blanca Purcachi
SERVICIOS INST. Y MUNICIPALES	**SERVICIOS INSTITUCIONALES**	Zumi Vallejo
CEMENTARIO GENERAL	**ADMINISTRACIÓNDE CEMENTERIO**	Lcda. Segundo Llumiguano
TERMINAL TERRESTRE	**ADMINISTRACIÓN**	Ing. Iván Mora
SISTEMAS INFORMATICOS	**JEFATURA**	Ing. Roy Olalla
PLAZA DE ANIMALES	**ADMINISTRACIÓN**	Dr. Roberto Mejía
ADQUISIONES	**JEFATURA**	Martha Rea
COMPRAS PÚBLICAS	**ANALISTA**	Ab. Bryan Santamaría
COMISARIA MUNICIPAL	**COMISARIO**	Fernando Agualongo
BODEGA	**GUARDALMACEN**	Ab. Ramiro Pazos

Nota: Elaboración propia en base a la información del Gobierno Autónomo Descentralizado del Cantón Guaranda

2.14. Procesamiento de la información

Después de haber obtenido la información suficiente se realizará hacer un análisis de todos los datos obtenidos los cuales son de suma importancia para la propuesta. Los Datos recolectados serán cuantificados y representados gráficamente de esta forma se podrá obtener las pertinencias conclusiones y recomendaciones de la misma.

CAPÍTULO IV

2.15. RESULTADO Y DISCUSIÓN

2.16. Análisis, Interpretación y Discusión de Resultados

1.- ¿El gobierno Descentralizado del Cantón Guaranda cuenta con un departamento de Informática?

Tabla 1. ***Departamento de Informática***

Departamento de informática	Frecuencia	%
SI	49	48,51
NO	52	51,49
TOTAL	101	100,00

Gráfico 1. ***Departamento de Informática***

Nota: De las encuestas realizadas a los directivos y al personal del GAD Municipal del Cantón Guaranda, el 51% respondió que no cuenta con un departamento de Informática mientras que el 49% respondió que, si cuenta con uno, de lo que se puede concluir, que este porcentaje desconoce la existencia del departamento de Informática.

2.- ¿Se ha realizado alguna Auditoría Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda?

Tabla 2. ***Auditoría Informática***

Auditoría informática	Frecuencia	%
SI	23	22,77
NO	78	77,23
TOTAL	101	100,00

Gráfico 2. ***Auditoría Informática***

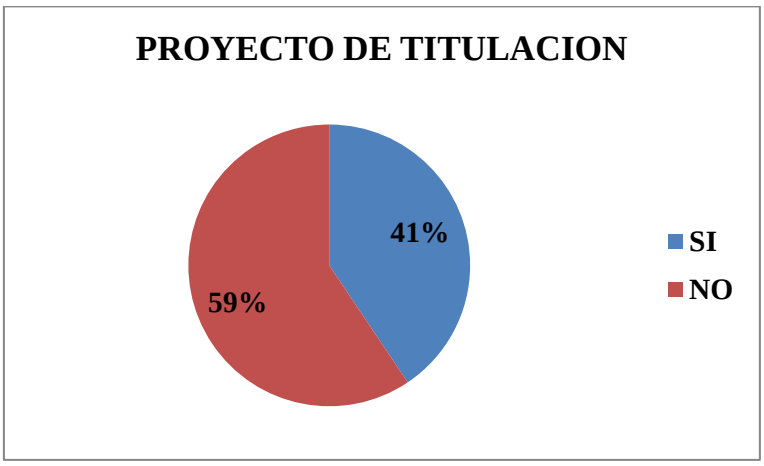
Nota: Según los resultados de la encuesta realizada un77% contesto que no se ha elaborado una Auditoría Informática dentro del GAD Municipal del Cantón Guaranda mientras que el 23% respondió que, si se ha realizado, se puede concluir que existe desconocimiento si se ha realizado algún tipo de Auditoría.

3.- ¿Dentro del Municipio cuenta con un plan de contingencia para minimizar los riesgos informáticos?

Tabla 3. ***Plan de Contingencia para minimizar los riesgos informáticos***

Plan de contingencia	Frecuencia	%
SI	41	40,59
NO	60	59,41
TOTAL	101	100,00

Gráfico 3. ***Plan de Contingencia para minimizar los riesgos informáticos***



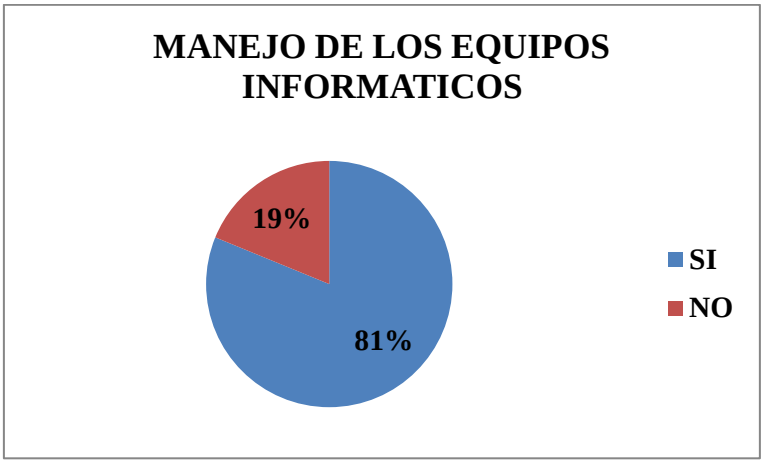
Nota: De las encuestas realizadas un 59% afirmo que el GAD Municipal de Guaranda no cuenta con un plan de contingencia que permita mitigar los riesgos informáticos mientras que el 41% del personal dijo que si cuenta con un plan de contingencia. Se puede concluir que existe falta de conocimiento del plan de contingencia informático.

4.- ¿Cree usted que el personal del Municipio maneja la información y los equipos informáticos de una manera adecuada?

Tabla 4. ***Manejo de los Equipos Informáticos***

Manejo adecuado de la información	Frecuencia	%
SI	82	81,19
NO	19	18,81
TOTAL	101	100,00

Gráfico 4. ***Manejo de los Equipos Informáticos***



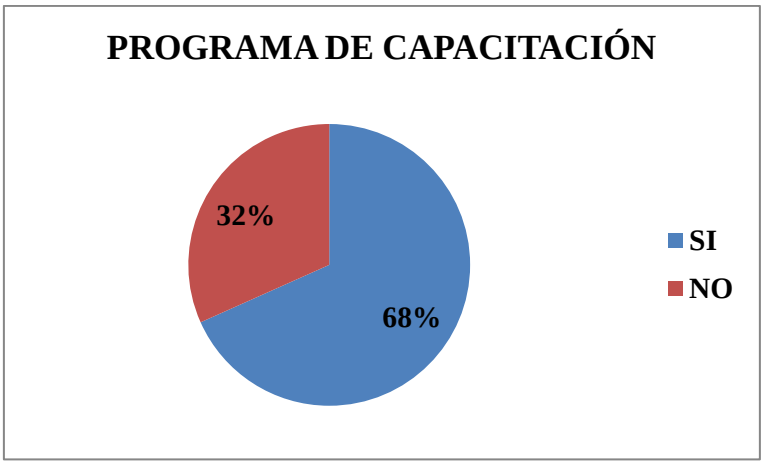
Nota: Según los resultados de las encuestas un 81% de los encuestados afirmo que el personal del GAD Municipal de Guaranda maneja la información de una manera apropiada mientras que el 19 % respondió que no se utiliza de manera correcta, se puede concluir que no todos los funcionarios de municipio manejan la información y los equipos informáticos de modo adecuado.

5.- ¿El personal del Gobierno Autónomo Descentralizado del Cantón Guaranda cuenta con programas de capacitación relacionado al ingreso al sistema de la entidad?

Tabla 5. ***Programas de Capacitación***

Programas de capacitación	**Frecuencia**	**%**
SI	69	68,32
NO	32	31,68
TOTAL	101	100,00

Gráfico 5. ***Programas de Capacitación***



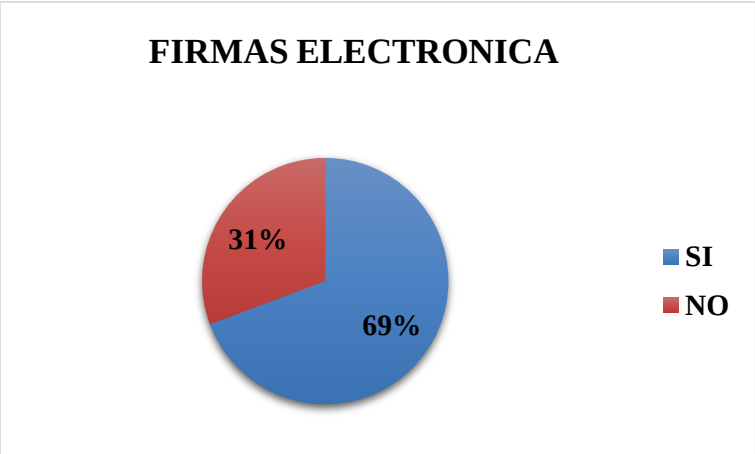
Nota: De las encuestas realizadas el 68% de los funcionarios manifiesta que, si existe un programa de capacitación sobre el ingreso hacia el sistema de la entidad, mientras que el 32% afirma que no existe una capacitación dentro de la entidad. Se puede concluir que si existe una capacitación básica al ingreso de los sistemas de la entidad.

6.- ¿Se utiliza firmas electrónicas para enviar o recibir información del Gobierno Autónomo Descentralizado del Cantón Guaranda?

Tabla 6. ***Firmas Electrónicas***

Firma electrónica	Frecuencia	%
SI	70	69,31
NO	31	30,69
TOTAL	101	100,00

Gráfico 6. ***Firmas Electrónicas***



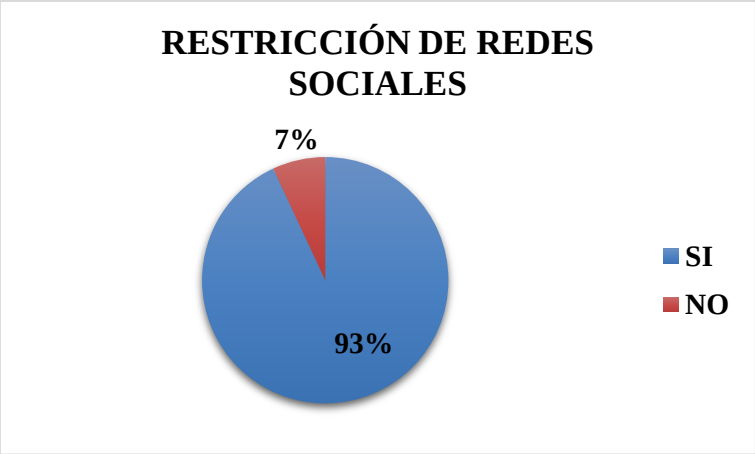
Nota: Según los resultados obtenidos de la encuesta realizada al personal del GAD Municipal de Guaranda un 69% afirma que si cuenta con firmas electrónicas mientras el 31% no cuenta con una firma electrónica. Se puede concluir que es necesario tener firma electrónica, ya que la normativa vigente obliga a los funcionarios públicos emitir firma electrónica o de lo contrario serán sancionados.

7.- ¿Se restringe el uso de páginas web como redes sociales, entre otras páginas que no tienen relación con el trabajo del municipio?

Tabla 7. ***Restricción de Redes Sociales***

Restricción de páginas web que no tienen relación con el GAD	**Frecuencia**	**%**
SI	94	93,07
NO	7	6,93
TOTAL	101	100,00

Gráfico 7. ***Restricción de Redes Sociales***



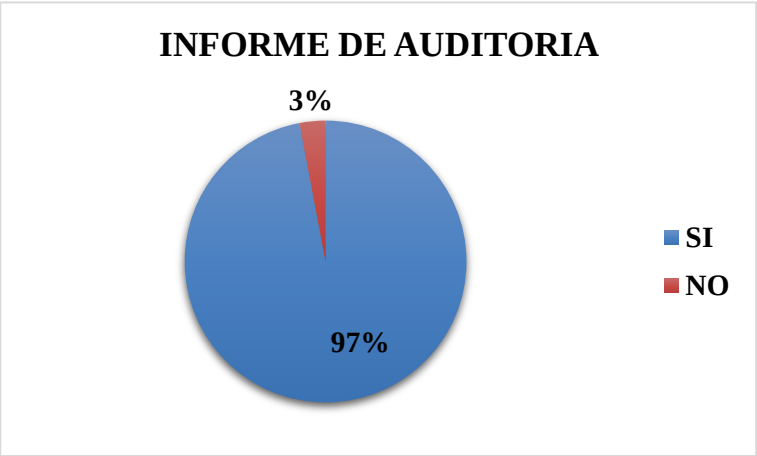
Nota: De las encuestas realizadas el 93% manifiesta que, si se restringe el uso de ciertas páginas web que no tienen relación con el trabajo que realizan dentro del Municipio, mientras que el 7% contesto que no se les restringe dichas páginas, se puede concluir que se restringen el acceso a páginas que no tiene relación con el trabajo del municipio.

8.- ¿Considera usted que el informe de una Auditoría Informática es un instrumento que permite a los directivos del Gobierno Autónomo Descentralizado del Cantón Guaranda tomar mejores decisiones?

Tabla 8. ***Informe de Auditoría***

Informe de auditoría para la toma de decisiones	Frecuencia	%
SI	98	97,03
NO	3	2,97
TOTAL	101	100,00

Gráfico 8. ***Informe de Auditoría***



Análisis: según los resultados obtenido de la encuesta realizada un 97% de los encuestados considera que el informe de Auditoría es una herramienta de suma

importancia ya que esto permitirá un mejor manejo de la información y de los equipos informáticos del Municipio mientras que el 3% no le considera importante que se realice una Auditoría Informática.

9.- ¿Se realizan copias de seguridad de la información que tiene el Gobierno Autónomo Descentralizado del Cantón Guaranda en la finalidad de salvaguardarla la información?

Tabla 9. ***Realización de Copias de seguridad del GAD***

Copias de seguridad para salvaguardar la información	**Frecuencia**	**%**
SI	96	95,05
NO	5	4,95
TOTAL	101	100,00

Gráfico 9. ***Realización de Copias de seguridad del GAD***

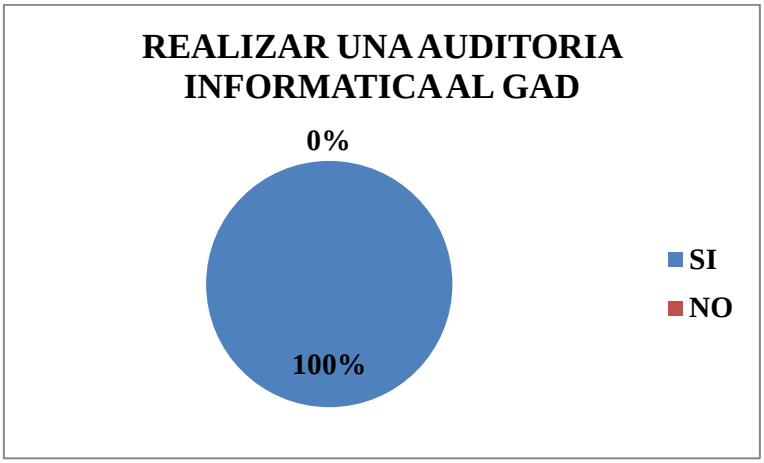
Análisis: El 95% del personal encuestado menciona que si se realizan copias de seguridad que permiten proteger los equipos informáticos mientras que el 5% no cuenta con copias de seguridad para poder salvaguardar su información. Se puede concluir que si se realizan copias de seguridad de la información diariamente en el Municipio.

10.- ¿Considera usted necesario realizar una auditoría Informática en el Gobierno Descentralizado del Cantón Guaranda para el uso adecuado de la información y de los equipos informáticos?

Tabla 10. ***Realizar una Auditoría Informática al GAD Municipal***

Realización de una auditoría informática	Frecuencia	%
SI	101	100,00
NO	0	0,00
TOTAL	101	100,00

Gráfico 10. ***Realizar una Auditoría Informática al GAD Municipal***



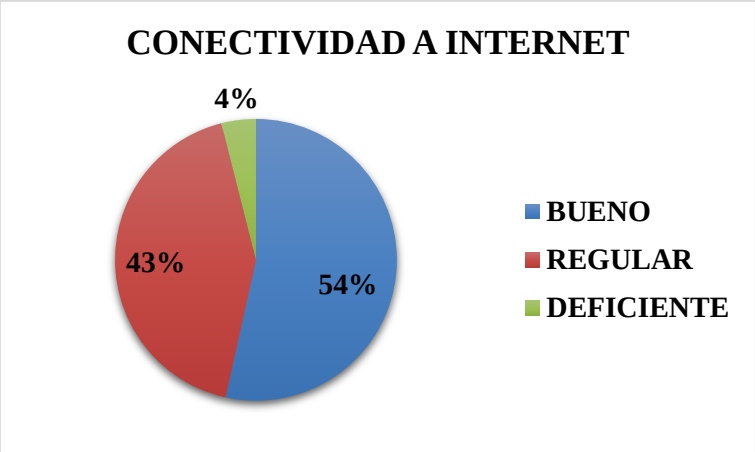
Análisis: Al aplicar las encuestas un 100% afirmo que si es necesario realizar una auditoría Informática dentro del GAD Municipal de Guaranda para tener un uso adecuado de la información y de los equipos informáticos y se puedo concluir que si es necesario realizar una auditoría Informática para poder determinar futuras falencias.

11. ¿La conectividad a internet en su área de trabajo:

Tabla 11. ***Conectividad a internet***

Conectividad de internet	Frecuencia	%
BUENO	54	53,47
REGULAR	43	42,57
DEFICIENTE	4	3,96
TOTAL	101	100,00

Gráfico 11. ***Conectividad a internet***



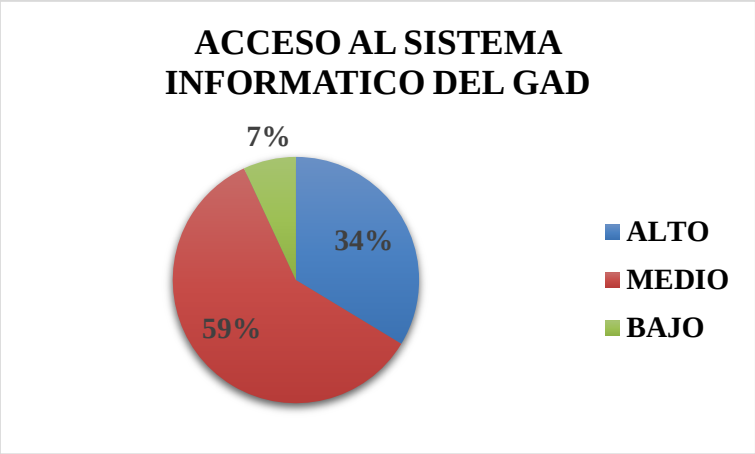
Análisis: Según los resultados de las encuestas realizadas a los funcionarios públicos el 54 % considera que la conectividad de internet es buena, el 43% menciona que es regular y el 4% que es deficiente al acceso a internet, lo cual se puede concluir que la mayor parte de los funcionarios tiene acceso a internet.

12. ¿La seguridad del acceso de los sistemas informáticos de la institución es?

Tabla 12. ***Acceso al sistema informático del GAD***

Seguridad a los sistemas informáticos	Frecuencia	%
ALTO	34	33,66
MEDIO	60	59,41
BAJO	7	6,93
TOTAL	101	100,00

Gráfico 12. ***Acceso al sistema informático del GAD***



Análisis: Del total de encuestados un 34% menciona que es alto el acceso a los sistemas informáticos del GAD Municipal de Guaranda un 60% manifiesta que es medio el acceso y el 7% menciona que es bajo el acceso a los sistemas informáticos. Se puede concluir que la seguridad de acceso a los sistemas informáticos es regular por lo cual es necesario tener una mayor seguridad al momento de entrar al sistema informático.

CAPITULO V PROPUESTA

2.17. PROPUESTA

2.18. Titulo

Auditoría Informática a los sistemas de información aplicados por el Gobierno Autónomo Descentralizado del Cantón Guaranda, Provincia Bolívar,2021.

2.18.1. Motivo

El Gobierno Autónomo Descentralizado de Cantón Guaranda está considerado como una entidad gubernamental para administrar el cantón de Guaranda de forma autónoma con la finalidad del bien común de la población Guarandeña y las necesidades del cantón como sus parroquias.

Esta institución está regida por dos poderes los cuales son: el nivel ejecutivo y el nivel legislativo cada uno de ellas representado por dignidades, este caso se podría decir representado por el señor alcalde del cantón y el legislativo por miembros del consejo cantón.

En el sitio web del GAD municipal, presenta un fallo de actualización en la información de algunos campos, adicionalmente cuenta con la consulta de servicios

en línea, ocasionando un malestar por que pide el portal un usuario y contraseña, que no ha sido debidamente entregado a la ciudadanía, por falta de información.

2.18.2. Alcance

En la presente investigación se utilizó como metodología al COBIT 4.0, Determinando la forma más efectiva de utilizar los sistemas de información y así alcanzar los objetivos del Gobierno Autónomo Descentralizado del Cantón Guaranda, realizando una evolución periódica de las (TI) para medir el grado de eficiencia y eficiencia, de acuerdo al COBIT hace referencia a sus dominios; planificar, organizar, adquirir e implementar, entregar y dar soporte, monitorear y Evaluar.

La metodología COBIT 4.0, permite la generación de recomendaciones que serán planteado en el informe final de auditoría para que más adelante se pueda tomar en cuenta.

2.18.3. Seguridad de los departamentos del GAD municipal de Guaranda

La seguridad en el GAD Municipal de Guaranda se considera en dos puntos la seguridad lógica y Física.

2.18.3.1. Seguridad Lógica

La seguridad lógica de GAD municipal de Guaranda, está a cargo de la unidad de informática de la institución, está a cargo de cuidar la integridad de los datos mediante procedimientos de respaldos de la información, como las copias de seguridad que se van almacenando estos procedimientos son ejecutados y controlados por la unidad de informática.

La unidad de informática este encargado del mantenimiento constante a los sistemas de informáticos, aplicaciones y software manejados en cada departamento de la institución, garantizando el óptimo funcionamiento de los mismos.

2.18.3.2. Seguridad Física

En el GAD municipal de Guaranda la seguridad Física es escasa, debido a que no existe un personal que se encargue de realizar el primer contacto con los usuarios brindando información y verificando el motivo de la visita y del porqué del ingreso a las instalaciones de la institución es libre permitiéndonos deambular independientemente por la institución.

En algunos departamentos el ingreso es controlado por la secretaria de los mismos, encargándose de preguntar el motivo de la visita y verificando la información.

En caso de necesitar documentación confidencial es importante tener un documento de aprobación escrita por el jefe del departamento o del señor alcalde.

2.19. Archivo Permanente

GAD MUNICIPAL DEL CANTÓN GUARANDA	
AUDITORÍA INFORMÁTICA	**A/P**
Archivo Permanente	**1/1**
Del 1 de enero al 31 de diciembre del 2021	

Razón Social	**GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA**
RUC	0260000250001
Provincia	Bolívar
Dirección	Convención de 1884 y García Moreno
Teléfono	(03)2551083- (03)2551088
Correo Electrónico	alcaldia@guaranda.gob.ec
Página Web	www.guaranda.gob.ec

	INICIALES	**FECHA**

ELABORADOR POR:	**JCH/FN**	**10-08-2022**
REVISADOS POR:	**M.A.M. V**	**10-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Índice del Archivo Permanente

Del 1 de enero al 31 de diciembre del 2021

I/AP

1/1

	INICIALES	FECHA
ELABORADOR POR:	**JCH/FN**	**10-08-2022**
REVISADOS POR:	**M.A.M.V**	**10-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

RESEÑA HISTORICA

Del 1 de enero al 31 de diciembre del 2021

R/H

1/1

RESEÑA HISTORICA

La existencia del palacio Municipal aproximadamente desde el año 1736, en que llego a la cuidad de Guaranda el 18 de Mayo Geodesica Francesa.

Esta casa fue propiedad en primera instancia del seño general jóse de Unda y Luna posteriormente paso a ser propiedad de Don Francisco Echeandia y es ahí donde nació uno de los Próceres guarandeños, Don Manuel de Echeandía.

Fue vivienda y oficina del Corregidor, en su torreón se observa un hermoso reloj que fue puesto en funcionamiento el 14 de Enero 1992, siendo Presidente del Consejo Municipal el Sr. José H Gonzáles Pozo.

En el palacio Municipal funciona el despecho del señor Alcalde, la oficina de los señores Concejales, algunas direcciones.

En el salon de la cuidad, ubicado en el segundo piso, tiene decoracion sobria y Elegante, que se realizan las sesiones semanales del concejo, las sesiones solemnes y demas actos de importancia para el Cantón, la cuidad y el cabildo.

	INICIALES	FECHA
ELABORADOR POR:	**JCH/FN**	**10-08-2022**
REVISADOS POR:	**M.A.M.V**	**10-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA **MV/I**

MISIÓN Y VISIÓN INSTITUCIONAL **1/1**

Del 1 de enero al 31 de diciembre del 2021

Misión

"El Gobierno Autónomo Descentralizado del Cantón Guaranda planifica, gestiona y administra el bienestar y desarrollo social, cultural, económico de su comunidad entregando con honestidad y eficiencia prestaciones y servicios colectivos de calidad de calidad con la firma compromiso de mantener una cuidad digna para vivir, trabajar e invertir."

Visión

"Ser reconocida como un Gobierno Autónomo Descentralizado modelo a nivel Nacional que ofrece servicios de consumo colectivo de calidad, que genera satisfacción y bienestar a la comunidad urbana y rural del Cantón Guaranda y otras partes interesadas que requieren servicios de calidad, así como a sus visitantes

nacionales y extranjeros, trabajando en sinergia con el pueblo para ser de Guaranda una cuidad de desarrollo económico, político y social, apta para invertir y vivir en armonía y seguridad”

Valores Institucionales del Gobierno Autónomo Descentralizado del Cantón Guaranda

El Gobierno Autónomo Descentralizado del Cantón Guaranda, como parte de su planificación Estratégica ha identificado los siguientes valores:

Liderazgos.

ES la capacidad de influir positivamente en fines de interés institucionales a través de un adecuado proceso de comunicación.

Mejoramiento Continuo.

Actividades recurrentes para aumentar la capacidad para cumplir con los requisitos.

Calidad del Servicio.

Es la capacidad de ofrecer los servicios institucionales superando las expectativas de las comunidad urbana y rural del Cantón Guaranda y otras partes interesadas.

Gestión por Resultados.

Es la capacidad de ejecutar las atribuciones y responsabilidades de la mejor manera para alcanzar los resultados deseados.

Compromiso.

Es la satisfacción de trabajar en equipo para llegar a un objetivo trazado y comprometernos como personas y como colaborarnos de nuestra institución que permite proyectar una mejor imagen institucional y brindar mejores obras y servicios a toda la ciudadanía.

Participación.

Es la capacidad de obtener la calidad total mediante el involucramiento entre el jefe y los colaboradores. Tomar en cuenta las ideas del resto para la toma de decisiones.

Trasparencia.

Ser claro en todas las acciones, participar de manera honesta en todos los actos de nuestras vidas, proporcionando así una imagen de integridad en la gestión del buen servicio a la colectividad.

Respeto.

Es la consideración que debe tener con todas las personas y la naturaleza que se encuentra en nuestro entorno.

Equidad.

Es la capacidad de distribuir, redistribuir y reorientar el recurso público para compensar las inequidades, garantizar la inclusión, la satisfacción de necesidades básicas, y el buen vivir (convivencia armónica entre seres humanos y el ambiente).

Objetivos Estratégicos Institucionales

Se establecen los siguientes objetivos estratégicos.

- Procurar el bienestar de la colectividad y contribuir al fomento y protección de los intereses locales.

- Planificar e impulsar el desarrollo del Cantón tanto en sus áreas urbanas como rurales enmarcadas en la competencia establecidas en la ley.

- Acrecentar el espíritu de integración de todos los actores sociales y económicos el civismo y la confraternidad de la población para lograr el creciente progreso del Cantón.

- Coordinar con otras entidades, el desarrollo y mejoramiento de la cultura, la asistencia social, turismo, medio ambiente y seguridad ciudadanía.

- Investigar, analizar y recomendar las soluciones más adecuadas a los problemas que enfrenta el Gobierno Autónomo Descentralizado, con arreglo a las condiciones cambiantes, en lo social, político, cultural y económico.

- Estudiar la normativa legal y recomendar la adopción de técnicas de gestión racionalizada y empresarial, con procedimientos de trabajo uniformes y flexibles tendientes a profesionalizar y especializar la gestión del gobierno local.

- Auspiciar y promover la realización de reuniones permanentes para discutir los problemas institucionales, mediante uso de mesa redondas, seminarios, talleres, conferencias, sinopsis, cursos y otras actividades de integración y trabajo.

- Capacitar al capital humano en el conocimiento de organización interna institucional, su normativa y funcionalidad, orientado al mejoramiento de los servicios y la atención ciudadana prevista en la gestión del Gobierno Autónomo Descentralizado.

- Mejorar y ampliar la cobertura de servicios de manera paralela al mejoramiento de la administración con el aporte de la comunidad.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**10-08-2022**
REVISADOS POR:	**M.A.M. V**	**10-08-2022**

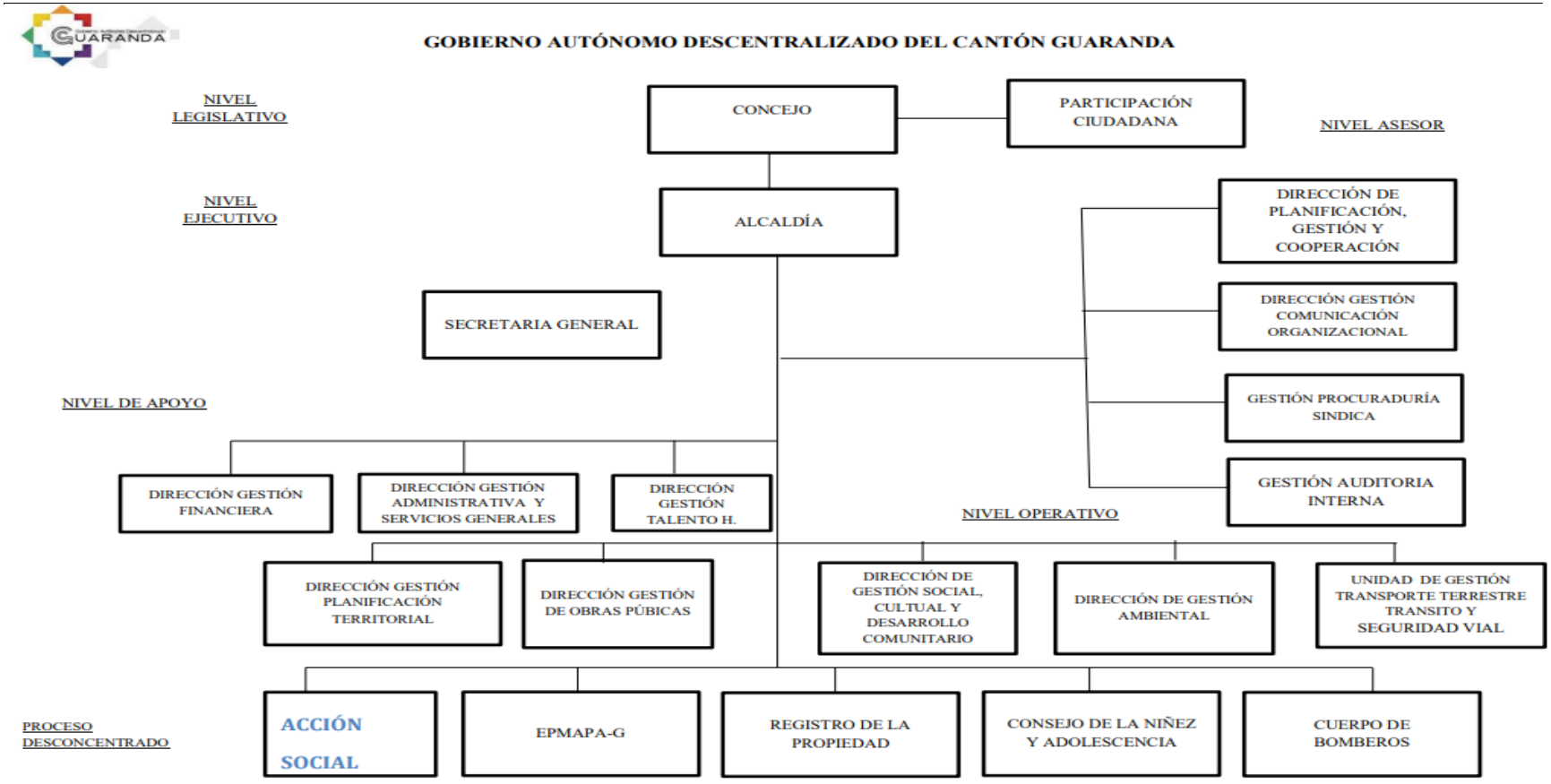
GOBIERNO DESENTRALIZADO MUNICIPAL DEL CANTÓN GUARANDA

Estructura Organizacional

Del 1 de enero al 31 de diciembre del 2021

E/O

1/1



GAD MUNICIPAL DEL CANTÓN GUARANDA

MARCAS DE AUDITORIA

Del 1 de enero al 31 de diciembre del 2021

M/A

1/1

MARCA	SIGNIFICADO
₡	Archivo Permanente
√	Revisado
H	Hallazgo
D	Debilidad
A-Z	Nota Explicativa
N/A	Procedimiento no aplicable
∑	Sumatoria (Vertical y Horizontal)
Ω	Sustenta con evidencia
A	Incumplimiento de normativa
¥	Confrontando con libros
µ	Corrección de libros
Ó	No reúne documentación
←	Pendiente de registro
ã	Conciliado
Æ	Circularizado
P/T	Papeles de trabajo
*	Evidencia

	INICIALES	FECHA

ELABORADOR POR:	**J.CH/F. N**	**10-08-2022**
REVISADOS POR:	**M.A.M. V**	**10-08-2022**

2.20. Archivo Corriente

ARCHIVO CORRIENTE

ALCALDÍA DE GUARANDA

Razón Social	**GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA**
RUC	0260000250001
Provincia	Bolívar
Dirección	Convención de 1884 y García Moreno
Teléfono	(03)2551083- (03)2551088
Correo Electrónico	alcaldia@guaranda.gob.ec
Página Web	www.guaranda.gob.ec

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**10-08-2022**
REVISADOS POR:	**M.A.M. V**	**10-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

ÍNDICE DEL ARCHIVO CORRIENTE

Del 1 de enero al 31 de diciembre del 2021

I/AC 1/1

ÍNDICE	REF.P/T
Archivo Corriente	**A/C 1/1**
Índice de Archivo Corriente	**I/AC 1/1**
Programa de Auditoria	**P/A 1/1**
FASE I: PLANIFICACIÓN DE LA AUDITORIA INFORMÁTICA	
• Planificación Preliminar	**PAI/PA 1/1**
FASE II: EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO	
• Control Interno • Cuestionarios	**ECI/PA 1/1**
FASE III: ANALISIS DE AREAS CRITICA	
• Análisis, Indicadores • Hallazgos	**AAC/PA**
FASE IV: REDACCIÓN DE INFORME Y COMUNICACIÓN DE RESULTADOS	
• Informe de auditoria	**RIC/PA**

		INICIALES	FECHA
	ELABORADOR POR:	J.CH/F. N	10-08-2022
	REVISADOS POR:	M.A.M. V	10-08-2022

GAD MUNICIPAL DEL CANTÓN GUARANDA
PROGRAMA DE AUDITORÍA
Del 1 de enero al 31 de diciembre del 2021

P/A
1/1

N°	PROCEDIMIENTO	Referencia	Elaborado por	Fecha
FASE I: PLANIFICACIÓN PREELIMINAR				
1	Elaboración del programa de Auditoría	**P/A 1/1**	**JC/FN**	10-08-2022
2	Visita de observación en las instalaciones del Municipio	**VO/I 1/1**	**JC/FN**	16-08-2022
3	Entrevista previa al alcalde del Municipio	**EPR/ALC 1/1**	**JC/FN**	18-08-2022
4	Recopilación de la información y documentación sobre la base legal de la entidad	**B/L 1/1**	**JC/FN**	19-08-2022
5	Realizar la notificación de inicio de Auditoria	**NI/A 1/1**	**JC/FN**	22-08-2022
6	Elaborar el memorándum de planificación	**M/P 1/1**	**JC/FN**	23-08-2022
FASE II: EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO				
7	Elaborar y aplicar cuestionarios sobre el control Interno basado en el COSO II	**C/CI**	**JC/FN**	24-08-2022
8	Elaborar la matriz de nivel de riesgo y confianza	**M/RC 1/2**	**JC/FN**	25-08-2022
9	Elaborar un informe sobre el control Interno	**HR/CCI 1/8**	**JC/FN**	26-08-2022
FASE III: ANALISIS DE AREAS CRITICAS				
10	Elaborar un inventario y un análisis sobre los indicadores de	**I/EE 1/4**	**JC/FN**	29-08-2022

	eficiencia y eficacia de la seguridad Informática			
	Desarrollar Hojas de hallazgos	**H/H 1/6**	**JC/FN**	30-08-2022
FASE IV: REDACCION DE INFORME Y COMUNICACIÓN DE RESULTADOS				
11	Carta de Presentación	**C/P 1/1**	**JC/FN**	1-09-2022
12	Elaborar el informe sobre la Auditoria Informática	**I/AI 1/2**	**JC/FN**	2-09-2022

	INICIALES	**FECHA**
ELABORADOR POR:	**J.CH/F. N**	**10-08-2022**

REVISADOS POR:	**M.A.M. V**	**10-08-2022**

2.20.1. Fase I: Planificación de la Auditoria Informática

GAD DEL CANTÓN GUARANDA **VISITA DE OBSERVACIÓN** **Del 1 de enero al 31 de diciembre del 2021**	**VO/I** **1/1**

Visita al Gobierno Autónomo Descentralizado del Cantón Guaranda

El Gobierno Autónomo Descentralizado del Cantón Guaranda se encuentra ubicado en las calles García Moreno y Convención 1884 frente al parque central de la cuidad de Guaranda.

Durante la vista a las instalaciones del municipio se puedo constatar que tiene bien estructurado sus departamentos y la distribución de sus empleados está acorde al organigrama institucional de la entidad.

Cada uno de los departamentos cuenta por lo menos con un computador para facilitar el trabajo de los funcionarios públicos, los cuales son responsables de los equipos informáticos y de la información almacenada dentro de los dispositivos.

Cuadro 6. Departamentos y equipos informáticos del GADl del Cantón Guaranda.

DEPARTAMENTO	**N° DE COMPUTADORAS**
Unidad de Sistemas	2
Servicios Municipales	2
Dirección Administrativa	3
Adquisiciones	2
Compras Publicas	2
Dirección Financiera	1
Presupuesto	1
Contabilidad	9
Tesorería	4
Recaudación	7
Dirección de Gestión de Talento Humano	8
Dirección de Comunicación	6
Procurador Sindico	4
Secretaria de Concejo	7
Alcaldía	2
Coordinador General	3
Total Σ	**63**

El sistema operativo que se utiliza en las computadoras de la entidad es el Windows 7, existe impresoras multifuncional para oficina dentro del municipio.

El alcalde y los empleados de la institución están dispuesto a cooperar para brindar la información necesario para emprender la auditoria Informática dentro la entidad. El Gobierno Autónomo Descentralizado del Cantón Guaranda mantiene un horario de atención a la ciudadanía de Lunes a Viernes, en la mañana de 8:00 am a 12:00pm y en la tarde de 14:00pm a 17:00 pm. Además, cuenta con todas las medidas de bioseguridad para la atención a la ciudadanía.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**16-08-2022**
REVISADOS POR:	**M.A.M. V**	**16-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Entrevista previa al señor alcalde

Del 1 de enero al 31 de diciembre del 2021

EPR/ALC

1/1

Nombre del entrevistador: Sr. Medardo Chimbo lema

Cargo: Alcalde del Municipio

Entrevistador: Fernanda Narváez

Dia Previsto: 18-08-2022 **HORA:** 10:30am

1. **¿Se ha realizado una Auditoria Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda hasta la actualidad?**

El Alcalde manifestó que no se ha realizado ninguna auditoria Informática dentro del Gobierno Autónomo Descentralizado.

2. **Existe un departamento destinado al manejo y control de la Informática**

El Alcalde menciona que si existe una unidad destinada al manejo de la información y del control informático.

3. **¿Usted usa firmas electrónicas para validar documentos que redacta y envía en representación Gobierno Autónomo Descentralizado del Cantón Guaranda?**

El Alcalde manifestó que si se usa firmas electrónicas para tramites en representación del Gobierno Autónomo Descentralizado del Cantón Guaranda.

4. **¿Considera usted que existe suficiente seguridad para proteger y salvaguardar la información almacenada dentro de los equipos informáticos?**

La seguridad en el municipio es muy baja para proteger y salvaguardar la información ya que puede haber hackeos dentro del sistemas de información.

5. **¿Según su criterio considera usted necesario realizar una auditoria Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda?**

El señor alcalde menciona que es necesario realizar una auditoria Informática para mejorar el manejo de la información y de los equipos informáticos para evitar riesgos y amenazas Informáticas.

6. **¿Cuenta el Gobierno Autónomo Descentralizado del Cantón Guaranda con sistema de control interno informático?**

La entidad no cuenta con sistema de control interno para la unidad Informática.

7. **¿Existe un plan de neutralización para contrarrestar los riesgos informáticos?**

El señor alcalde menciona que ha se ha implementado un plan de neutralización por lo cual existe la posibilidad que coexistan amenazas de riesgos informáticos.

8. **¿Existe partida presupuestaria suficiente para la adquirir equipos informáticos?**

El Gobierno Autónomo Descentralizado no cuenta una partida presupuestaria para ala adquisición de equipos informáticos**.**

9. **¿Se realiza capacitaciones al personal de la institución sobre le correcto uso de la información y de los equipos informáticos?**

La entidad no brinda capacitaciones al personal sobre el correcto uso de la información y de los equipos informáticos.

10. **¿Se realiza evaluaciones respecto a la eficiencia de los empleados de la unidad de Informática?**

Dentro de la entidad si se ha realizado evaluaciones constantes a la eficiencia y eficacia de la información que emite la unidad de Informática.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**18-08-2022**
REVISADOS POR:	**M.A.M. V**	**18-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Recopilación de la información y documentación sobre la Base Legal de la entidad **B/L 1/1**

Del 1 de enero al 31 de diciembre del 2021

- Constitución Política de la República del Ecuador
- Ley orgánica de la contraloría General del estado
- Ley de presupuesto del Sector Publico
- Ley orgánica de Régimen Municipal
- Ley Orgánica de Régimen Tributario Interno
- Ley Orgánica del Sistema Nacional de Contratación Publica
- Ley Orgánica de servicio Civil Y Carrera Administrativa y Unificación Homologación de Remuneraciones del sector publico
- Código Orgánico de Organización Territorial Autonomía y Descentralización (COOTAD)
- Código de Trabajo
- Código de Procedimiento Civil
- Código Orgánico Integral Penal, COIP
- Código Orgánico de la Función Judicial
- Codificación de la ley de Aguas
- Ley Orgánica de Participación Ciudadana
- Ley Orgánica de Defensa del Consumidor
- Ley de Arbitraje y Mediación

- Ley de la Jurisdicción Contencioso Administrativa
- Ley Orgánica del sistema Nacional de Contratación Pública (LOSNCP)
- Reglamento General a la LOSEP
- Reglamento de Talento Humano
- Reglamento General Sustitutivos de Bienes del Sector Publico
- Reglamento para el pago de Viáticos para la Movilización y Subsistencias en el Exterior para Servidores y Obreros Públicos

- Normativa de Contabilidad Gubernamental del Ministerio de Finanzas
- Estatuto Orgánico por proceso institucional
- Normas de Control interno de la Contraloría General de Estado

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**19-08-2022**
REVISADOS POR:	**M.A.M. V**	**19-08-2022**

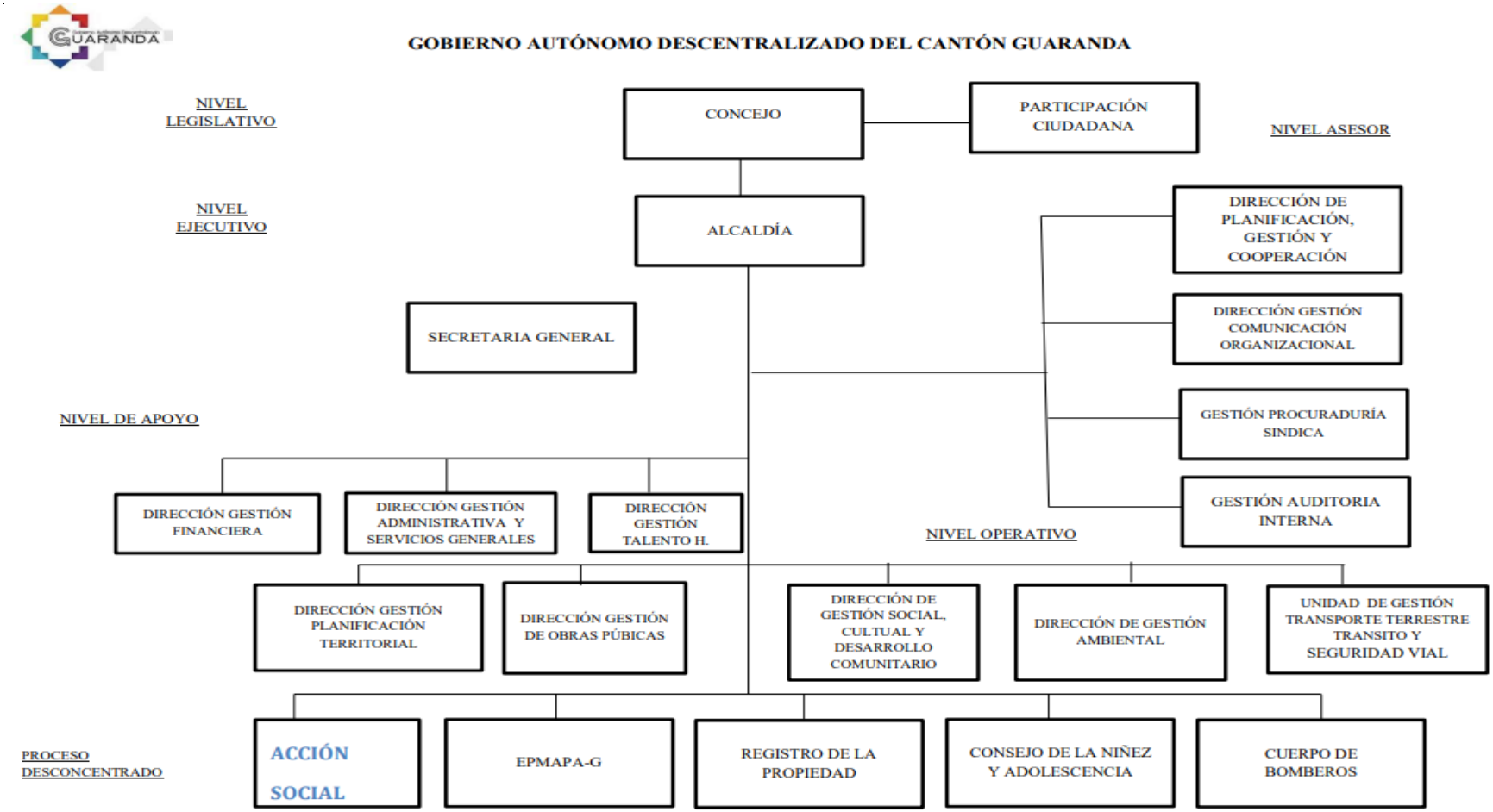
GOBIERNO DESENTRALIZADO MUNICIPAL DEL CANTÓN GUARANDA

Estructura Organizacional

Del 1 de enero al 31 de diciembre del 2021

E/O

1/1



GAD MUNICIPAL DEL CANTÓN GUARANDA	
NOTIFICACIÓN DE INICIO DE LA AUDITORIA	**N/AI**
INFORMÁTICA	**1/1**
Del 1 de enero al 31 de diciembre del 2021	

Guaranda, 22 de agosto del 2022

Sr. Medardo Chimbolema

ALCALDE DE GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA

Presente.

De mi consideración:

El motivo del presente es para notificar el inicio de la Auditoria Informatice que efectuara acuerdo a las Normas de Control Interno emitidas por la Contraloría General del Estado en lo referente a la Norma 410 sobre Tecnología de información y Comunicación, con el fin de obtener una opinión acerca de aspectos relacionados con la seguridad lógica, seguridad física, a aprovechamiento y utilización de las TIC´S y gestión de la información, el mismo que será llevado a cabo a través de la aplicación de encuestas, entrevistas, inspecciones físicas, y revisión de documentos con el fin de entregar un informa que contenga conclusiones y recomendaciones que será de utilidad para la toma de decisiones.

De manera más comedida solicito la colaboración y facilitación por parte de los servidores y servidoras públicas, para recabar información pertinente que contribuyan al desarrollo de la Auditoria Informática.

Atentamente,

Sr.Jhonathan Chimbo	Srta Fernanda Narváez
AUDITOR JUNIOR	**AUDITORA JUNIOR**

	INICIALES	**FECHA**

ELABORADOR POR:	**J.CH/F. N**	**22-08-2022**
REVISADOS POR:	**M.A.M. V**	**22-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

MEMORANDUM DE PLANIFICACIÓN

Del 1 de enero al 31 de diciembre del 2021

M/P

1/1

Guaranda, 23 de agosto del 2022

1. MOTIVO

La Auditoría Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar,2021 se realizará mediante la orden de trabajo N°1149 según el oficio del 25 de Julio del 2022.

2. Objetivo de la Auditoría

Objetivo General

Realizar una Auditoría Informática a los sistemas de información aplicados al Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar,2021 que permita determinar el grado de la eficiencia y eficacia en el desarrollo adecuando de los recursos de informáticos.

Objetivos Especificos

- Elaborar el marco teórico mediante la revisión de fuentes bibliográficas y científicas para que sirva de apoyo para emprender la Auditoría Informática.

- Establecer el marco metodológico respectivo con la determinación de los métodos técnicas e instrumentos de investigación que permita recabar información veraz, oportuna y confiable con la finalidad de realizar una apropiada Auditoría Informática.
- Presentar un informe de conclusiones y recomendaciones para mejorar los sistemas de información con el cumplimiento de los objetivos y metas institucionales.

3. ALCANCE

Esta investigación abarcara a la unidad de informática del Gobierno Autónomo Descentralizado del Cantón Guaranda, en el período comprendido entre el 01 de enero al 31 de diciembre del 2021.

4. PERSONAL ENCARGADO

Nombre	Cargo
Ing. Roy Olalla	Jefe de la Unidad Informática
Ing. Diana Alarcón	Asistente de la Unidad de informática
Ing. Jaime Gaibor	Asistente de la Unidad de informática

5. PRODUCTO DE LA AUDITORÍA

- Informe de Auditoría con Conclusiones y Recomendaciones

6. COLABORACIÓN

- Alcalde Sr. Medardo Chimbolema
- Ing. Roy Olalla jefe de la unidad informática
- Al personal del Municipio que tiene bajo su custodia los equipos informáticos e información almacenada dentro de los equipos.

7. Recursos Tecnológicos

Cantidad	Detalle
2	Computadoras portátiles
1	Escáner
1	Cámara digital
1	Celulares
1	Calculadora

8. Metodología a utilizarse

La metodología a emplearse de la Auditoria informática:

- Observación
- Entrevista
- Cuestionarios de control interno COSO II

FIRMA DE RESPONSABILIDAD

---------- ----------

Sr. Jhonathan Chimbo Srta. Fernanda Narváez

AUDITOR JUNIOR **AUDITORA JUNIOR**

Ing. Anabel Monar

SUPERVISORA

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**23-08-2022**
REVISADOS POR:	**M.A.M. V**	**23-08-2022**

2.20.2. Fase II: Evaluación del sistema de Control Interno

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

1/8

AMBIENTE INTERNO				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda. **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿El Municipio dispone de normas generales que supervisen la conducta del personal?	**x**		
2	¿Es necesario los valores éticos para incentivar una cultura organizacional dentro del Municipio?	**x**		
3	¿Existe un espacio de trabajo digno entre los empleados de la institución y sus supervisores?	**x**		
4	¿El personal del Municipio tiene capacitaciones sobre el manejo y la seguridad de los equipos informáticos?	**x**		
5	¿Se toma en cuenta las habilidades, la información y la experiencia a la hora de contratar al personal del Municipio?	**x**		

6	¿Tiene el personal del Municipio información esencial sobre la innovación de datos?	**x**		
7	¿Se encuentra definido el organigrama estructural del municipio?	**x**		
8	¿En el organigrama municipal se puede observar algún departamento asignado para el área de Informática?		**x**	
9	¿La Misión, Visión y Objetivos institucionales cubren los requerimientos tecnológicos del Municipio?		**x**	
10	¿El personal tiene presente la presencia de las Normas de Control Interno de la CGE?	**x**		
	TOTAL Σ	**8**	**2**	

TOTAL, DE RESPUESTAS	
POSITIVAS	**8**
NEGATIVAS	**2**
TOTAL	**10**

NIVEL DE CONFIANZA	$\frac{\textbf{Calificación Positiva}}{\textbf{Total Preguntas}} * \mathbf{100}$	
Nivel de Confianza	$\frac{8}{10} =$	**80%**
Nivel de riesgo	$100\% - 80\% =$	**20%**

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

Interpretación:

Los resultados alcanzados de la aplicados del Cuestionario de Control Interno al componente “Ambiente de Control” el Nivel de Confianza es 80% que representa un nivel alto, mientras que el nivel de riesgo es 20% lo que representa un nivel bajo, esto significa que los puntos analizados tienen un impacto parcial sobre las actividades que establezcan planes y estrategias que permita identificar y mitigar los riesgos.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

2/8

ESTABLECIMIENTO DE OBJETIVOS				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿Se determinan los objetivos institucionales del Municipio?	**x**		
2	¿Los objetivos institucionales contribuyen a la satisfacción del objetivo central y la visión del Municipio?	**x**		
3	¿Existen componentes establecidos para evaluar el riesgo en el caso de que no se cumplan los objetivos institucionales?		**x**	
4	¿Es consciente el personal de la presencia de los objetivos institucionales?	**x**		
5	¿Se actualizan a menudo los objetivos institucionales?	**x**		
	TOTAL Σ	**4**	**1**	

TOTAL, DE RESPUESTAS

POSITIVAS	**4**
NEGATIVAS	**1**
TOTAL	**5**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$	
Nivel de Confianza	$\frac{4}{5} =$	**80%**
Nivel de Riesgos	$100\% - 80\% =$	**20%**

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

Interpretación:

Los resultados alcanzados de la aplicados del Cuestionario de Control Interno al componente "Establecimiento de Objetivos" el Nivel de Confianza es de 80% que representa un nivel alto, mientras que el nivel de riesgo es de 20% lo que representa un nivel bajo, esto significa que los puntos analizados tienen un impacto por lo cual no existe componentes para evaluar los riesgos si en caso no se cumplen los objetivos institucionales.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

3/8

IDENTIFICACION DE EVENTOS				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿Los directivos están atentos a los cambios en la innovación?	**x**		
2	¿Existen sistemas para reconocer los riesgos informáticos?	**x**		
3	¿El personal del Municipio distingue los peligros potenciales que pueden influir en los recursos informáticos?	**x**		
4	¿La administración identifica los peligros externos que podrían influir en la fiabilidad	**x**		

	de los datos de los equipos informáticos del Municipio?			
	TOTAL Σ	**4**	**0**	

TOTAL, DE RESPUESTAS	
POSITIVAS	**4**
NEGATIVAS	**0**
TOTAL	**4**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$	
Nivel de Confianza	$\frac{4}{4} =$	**100%**
Nivel de Riesgo	$100\% - 100\% =$	**0%**

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

Interpretación

Los resultados alcanzados de la aplicados del Cuestionario de Control Interno al componente "Identificación de Eventos" el Nivel de Confianza es 100% que representa un nivel alto, mientras que el nivel de riesgo es 0% lo que representa un nivel bajo, esto significa que los puntos analizados tienen un impacto representativo sobre las actividades instituciones.

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

4/8

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

EVALAUCION DE RIESGO				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	

1	¿Existe un sistema de control interno Informático?	**x**		
2	¿Se ha evaluado el impacto del riesgo en los activos informáticos?		**x**	
3	¿Se reconocen los elementos que pueden provocar el riesgo informático?	**x**		
	TOTAL Σ	**2**	**1**	

TOTAL, DE RESPUESTAS	
POSITIVAS	**2**
NEGATIVAS	**1**
TOTAL	**3**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$	
Nivel de Confianza	$\frac{2}{3} =$	**66.67%**
Nivel de Riesgo	$100\% - 66.67\% =$	**33.33%**

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

Interpretación:

Los resultados alcanzados de la aplicados del Cuestionario de Control Interno al componente "Evaluación de Riesgo" el Nivel de Confianza es de un 66.67% que representa un nivel moderado, mientras que el nivel de riesgo es de 33.33% lo que representa un nivel moderado, esto significa que no se realizado una evaluación sobre el riesgo en los activos informáticos.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

5/8

RESPUESTA AL RIESGO
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda

Dirección: García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿Dispone la entidad un Plan de Contingencia para contrarrestar los riesgos informáticos?	**x**		
2	¿Se aplican sistemas, mecanismos o estrategias para disminuir el riesgo?	**x**		
3	¿Se toman acciones correctivas inmediatamente después de que se identifican los riesgos?	**x**		
	TOTAL Σ	**3**		

TOTAL, DE RESPUESTAS	
POSITIVAS	**3**
NEGATIVAS	**0**
TOTAL	**3**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$	
Nivel de Confianza	$\frac{3}{3} =$	**100%**
Nivel de Riesgo	$100\% - 100\% =$	**0%**

MATRIZ DE RIESGO Y CONFIANZA		
CONFIANZA		
BAJO	**MODERADO**	**ALTO**
15% - 50%	51% -75%	76%- 95%

RIESGO		
ALTO	**MODERADO**	**BAJO**
85 % - 50%	49% -25%	24% - 5%

Interpretación:

Los resultados alcanzados de la aplicados del Cuestionarios de Control Interno del COSO II sobre el componente “Respuesta del Riesgo” el Nivel de Confianza es de un 100% que representa un nivel alto, mientras que el nivel de riesgo es de un 0% lo que representa un nivel bajo, esto significa que los puntos analizados tienen un impacto representativo sobre las actividades instituciones.

	INICIALES	**FECHA**
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

6/8

ACTIVIDADES DE CONTROL				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿Se guardan respaldos de los datos de suma importancia que posee el Municipio?	**x**		
2	¿El personal se registra en el PC utilizando una contraseña?	**x**		
3	¿Se limita la utilización de páginas que no estén relacionadas con el trabajo propio del Municipio?	**x**		
4	¿Dispone el Municipio de protección para cubrir la pérdida o el robo de datos?	**x**		
5	¿Se actualiza periódicamente la programación de antivirus de los equipos informáticos para evitar la pérdida de datos?	**x**		
6	¿El personal que tiene acceso a los datos está limitado por una tarjeta de identificación?		**x**	
7	¿Se lleva a cabo un mantenimiento preventivo de los equipos informáticos?	**x**		
8	¿Existe un plan de gastos detallado para la adquisición de equipos informáticos?	**x**		
9	¿Se tienen en cuenta la marca, el modelo, el límite y las ventajas de ahorro en la obtención de equipos informáticos?	**x**		
	TOTAL **Σ**	**8**	**1**	

TOTAL, DE RESPUESTAS	
POSITIVAS	**8**
NEGATIVAS	**1**
TOTAL	**9**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$	
Nivel de Confianza	$\frac{8}{9} =$	**88.88%**
Nivel de Riesgo	$100\% - 88.88\% =$	**11.12%**

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

Interpretación

Los resultados alcanzados de la aplicados del Cuestionario de Control Interno al componente "Actividades de Control" el Nivel de Confianza es 88.88% que representa un nivel alto, mientras que el nivel de riesgo es 11.12% lo que representa un nivel bajo, esto significa que el personal del municipio tiene limitada la información de acuerdo a su tarjeta de identificación.

	INICIALES	**FECHA**
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**

REVISADOS POR:	**M.A.M. V**	**24-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

7/8

INFORMACIÓN Y COMUNICACIÓN				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿Existe comunicación entre la Administración y el personal del municipio?	**x**		
2	¿Se utilizan instrumentos, por ejemplo, la web, para transmitir datos importantes entre los departamentos del Municipio?		**x**	
3	¿La información relevante se comunica de manera oportuna al personal del Municipio?	**x**		
4	¿Se comunica a tiempo al personal cuando se ocasionan cambios imprevistos en el municipio?	**x**		
	TOTAL Σ	**3**	**1**	

TOTAL, DE RESPUESTAS	
POSITIVAS	**3**
NEGATIVAS	**1**
TOTAL	**4**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$	
Nivel de Confianza	$\frac{3}{4} =$	75%
Nivel de Riesgo	$100\% - 75\% =$	25%

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

Interpretación

Los resultados alcanzados de la aplicados del Cuestionarios de Control Interno al componente “Información y Comunicación” el Nivel de Confianza es de un 75% que representa un nivel alto, mientras que el nivel de riesgo es de un 25% lo que representa un nivel bajo, esto significa que la información de los departamentos es confidencial y segura.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Cuestionario de Control Interno COSO II

Del 1 de enero al 31 de diciembre del 2021

C/CI

8/8

MONITOREO				
Entidad: Gobierno Autónomo Descentralizado del Cantón Guaranda **Dirección:** García Moreno y Convención 1884 **Tipo de examen:** Auditoria **Unidad:** Informática				
N°	**PREGUNTA**	**Técnico**		**OBSERVACIONES**
		Si	**No**	
1	¿Se controla el uso de los equipos informáticos?	**x**		
2	¿Se inspecciona los equipos informáticos para garantizar que está en buen estado?	**x**		
3	¿Se inspecciona la entrada y la salida del personal en el Municipio?	**x**		
	TOTAL Σ	**3**		

TOTAL, DE RESPUESTAS	
POSITIVAS	**3**
NEGATIVAS	**0**
TOTAL	**3**

NIVEL DE CONFIANZA	$\frac{Calificación\ Positiva}{Total\ Preguntas} * 100$

Nivel de Confianza	$\frac{3}{3} =$	**100%**
Nivel de Riesgo	$100\% - 100\% =$	**0%**

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

Interpretación

Los resultados alcanzados de la aplicados del Cuestionarios de Control Interno al componente "Monitoreo" el Nivel de Confianza es de un 100% que representa un nivel alto, mientras que el nivel de riesgo es de un 0% lo que representa un nivel bajo, esto significa que los puntos analizados tienen un impacto representativo sobre las actividades instituciones.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**24-08-2022**
REVISADOS POR:	**M.A.M. V**	**24-08-2022**

CALCULO DE RIESGO Y CONFIZA

Fórmula para determinar el nivel de riesgo y confianza

Nivel de Confianza **Nivel de Riesgo**

$N = \frac{CP}{PT} * 100$ $NR = 100 - NC$

Dónde:

NC= Nivel de confianza

CP= Calificación Positiva

PT= Total de Preguntas

NR= Nivel de riesgo

MATRIZ DE PONDERACIÓN DE RIESGO Y CONFIANZA

La matriz de ponderación de riesgo y confianza sobre los cuestionarios de control interno aplicados al personal del Municipio.

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

	INICIALES	FECHA
ELABORADOR POR:	J.CH/F. N	25-08-2022

REVISADOS POR:	**M.A.M. V**	**25-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Matriz de Riesgo y Confianza

Del 1 de enero al 31 de diciembre del 2021

M/RC

2/2

RESUMEN DE EVALUACIÓN DE RIESGO Y CONFIANZA POR COMPONENTE								
N°	**COMPONENTES COSO II**	**N° PREGUNTAS**	**TECNICO**		**NIVEL DE CONFIANZA**		**NIVEL DE RIESGO**	
			SI	**NO**	**PONDERACIÓN**		**PONDERACION**	
1	**AMBIENTE INTERNO**	10	8	2	80%	Alto	20%	Bajo
2	**ESTABLACIMIENTO DE OBJETIVOS**	5	4	1	80%	Alto	20%	Bajo
3	**IDENTIFICACIÓN DE EVENTOS**	4	4	0	100%	Alto	0%	Bajo
4	**EVALUACIÓN DE RIESGOS**	3	2	1	66.67%	Moderado	33.33%	Moderado
5	**RESPUESTA AL RIESGO**	3	3	0	100%	Alto	0%	Bajo
6	**ACTIVIDADES DE CONTROL**	9	8	1	88.88%	Alto	11.12%	Bajo
7	**INFORMACION Y COMUNICACIÓN**	4	3	1	75%	Moderado	25%	Bajo
8	**MONITOREO**	3	3	0	100%	Alto	0%	Bajo
	TOTAL	41	35	6	690.55		109.45	
	PROMEDIO				85.37%	Alto	14.63%	Bajo

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**25-08-2022**
REVISADOS POR:	**M.A.M. V**	**25-08-2022**

Interpretación:

Como se puede observar en la matriz de resumen del nivel de riesgo y confianza se puede analizar en los resultados obtenido que el nivel de Confianza es Alto con un promedio del 85.37% y el nivel de riesgo es bajo con un 14.63%. Sin embargo, en la matriz se puede observar que en los componentes de “Evaluación de riesgo e Información de Comunicación” es un nivel de confianza moderado, esto se debe a que existe actividades que provocan un impacto medio y deben ser tomadas en cuenta por las autoridades pertinente.

	INICIALES	**FECHA**

ELABORADOR POR:	**J.CH/F. N**	**25-08-2022**
REVISADOS POR:	**M.A.M. V**	**25-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

Informe del Control Interno

Del 1 de enero al 31 de diciembre del 2021

I/EE 1/4

Guaranda, 26 de agosto del 2022

Sr. Medardo Chimbolema

ALCALDE DEL GOBIERNO AÚTONOMO DESCENTRALIZADO DEL CANTÓN GUARANDA

Presente. –

De mi consideración:

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

- **Falta de Capacitación Informática.**

  La entidad no capacita al personal sobre el manejo y seguridad de los activos informáticos. Las Normas de Control Interno de la CGE 410- 15 Capacitación Informática señala, las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que

utilizan los servicios de información, las cuales constaran en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. Estará orientado a los puestos de trabajo y a las necesidades de cada funcionario y además para la evaluación de desempeño institucional.

- **Inexistencia de un Departamento de Informática**

No existe un Departamento de Informática dentro del Organigrama estructura del municipio. Según las normas de control interno de la CGE 410-01 Organización Informática señala: La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permitirá efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además, debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

- **Inexistencia de mecanismo para identificar riesgos informáticos**

No existe mecanismos como controles, sistemas de aseguramiento para identificar los riesgos informáticos. Según las normas de control interno de la CGE 100-01 Control Interno señala: El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.

- **Inexistencia de un plan de contingencia**

La entidad no cuenta con un plan de contingencia para minimizar los riesgos. Según las normas de control interno de la CGE 410-11 plan de contingencia señala: El plan de contingencia será un documento de carácter confidencial que describe los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación de plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

- **Falta de personal de seguridad**

No se contratan vigilantes de seguridad para cuidar las instalaciones del municipio por las noches y fines de semana. Según las normas de control interno de la CGE 410-10 Seguridad de tecnología de información señala: los procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por las noches o en fin de semana.

- **Falta de supervisión en el manejo de los equipos informáticos**

No se supervisa el manejo de los equipos informáticos. Según las normas de control interno de la CGE 410-04 Políticas y procedimientos señala: Se implantará procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión den indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidas.

Después de aplicar los cuestionarios de control interno al personal del Municipio y realizar la matriz de nivel de riesgo y confianza de cada componente del COSO II, los resultados de fueron positivos, ya que tuvo un nivel de confianza **ALTO** del 85.37% y un riesgo bastante **BAJO** del 14.63%.

Particular que le comunicamos para fines pertinentes.

Atentamente,

Sr. Jhonathan Chimbo
AUDITOR JUNIOR

Srta. Fernanda Narváez
AUDITORA JUNIOR

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**26-08-2022**
REVISADOS POR:	**M.A.M. V**	**26-08-2022**

2.20.3. Fase III: Análisis de áreas criticas

GAD MUNICIPAL DEL CANTÓN GUARANDA

INVENTARIO DE COMPUTADORAS

Del 1 de enero al 31 de diciembre del 2021

I/EE

1/4

INVENTARIO DE COMPUTADORAS	
AREA	**N° DE COMPUTADORAS**
Unidad de Sistemas	2
Servicios Municipales	2
Dirección Administrativa	3
Adquisiciones	2
Compras Publicas	2
Dirección Financiera	1
Presupuesto	1
Contabilidad	9
Tesorería	4
Recaudación	7
Dirección de Gestión de Talento Humano	8
Dirección de Comunicación	6
Procurador Sindico	4
Secretaria de Concejo	7
Alcaldía	2
Coordinador General	3

Total Σ	**63**

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F.N**	**29-08-2022**
REVISADOS POR:	**M.A.M.V**	**29-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

INDICADORES DE EFICIENCIA Y EFICACIA

Del 1 de enero al 31 de diciembre del 2021

I/EE

2/4

Para la realización de los indicadores se tomó en cuenta la totalidad de 63 computadoras esto nos permitirá verificar la eficiencia y eficacia en el manejo adecuado de la información y de los equipos informáticos.

Los procesos realizados fueron las encuestas realizadas al jefe de la unidad de Informática.

EFICIENCIA

Presupuesto informático $= \frac{Presupuesto\ de\ quipos\ informaticos}{Presupuesto\ total} * 100 =$

$\frac{12.000}{6.872.868,39} = 0.2\%$

ANÁLISIS:

EL presupuesto asignado para el Municipio en el año 2021, es el 0,2% corresponde a los equipos informático y paquetes informáticos, un valor bajo referente a lo que necesita la entidad tanto en activos informáticos como los dispositivos para la seguridad.

EFICACIA

Sistema Operativo Actualizado=$\frac{\#\ Computadoras\ con\ Windows\ 10}{Total\ computadoras} * 100 = \frac{63}{63} =$ **100**%

ANALISIS:

Todas las computadoras del Municipio cuentan con un sistema operativo actualizado, el mismo que funciona de una manera muy rápida en la realización de cada una de las actividades que existe dentro de la entidad.

	INICIALES	FECHA
ELABORADOR POR:	J.CH/F. N	29-08-2022
REVISADOS POR:	M.A.M. V	29-08-2022

Acceso a Internet==$\frac{Computadoras\ con\ internet}{Total\ de\ computadoras} * 100 = \frac{63}{63} = 100\%$

ANÁLISIS:

Como nos refleja el indicador de eficiencia se concluye que el 100% de las computadoras cuentan con acceso a internet, haciendo que los usuarios de los equipos informáticos cumplan sus actividades de una manera eficiente y eficaz.

Mantenimiento preventivo=$\frac{Computadoras\ que\ se\ realiza\ mantenimiento\ preventivo}{Total\ de\ computadoras} *$

$100 = \frac{0}{63} = 0\%$

ANÁLISIS:

Se constató que ningún equipo de cómputo cuenta con un mantenimiento preventivo ya que son muchas computadoras a nivel del Municipio por lo que dificulta al técnico realizar esta actividad constantemente, por esta situación solo

actúa cuando existe un daño extremo en los sistemas de información en dicho equipo.

Actas de entrega/ recepción=

$$\frac{\boldsymbol{Computadoras\ entregadas\ con\ actas\ de\ entrega\ y\ recepcion}}{\boldsymbol{Total\ de\ computadoras}} * \mathbf{100} = \frac{\mathbf{63}}{\mathbf{63}} = \mathbf{100}\%$$

ANÁLISIS:

Las computadoras son entregadas en su totalidad con sus respectivas actas de entrega y recepción ya que de esta manera consta de manera documentada que el personal del Municipio recibió el equipo informático.

INDICADORES DE SEGURIDAD

Seguridad para ingresar al computador=$\frac{\boldsymbol{Computadores\ con\ contraseña}}{\boldsymbol{Total\ de\ computadoras}} * \mathbf{100} =$

$\frac{\mathbf{50}}{\mathbf{63}} = \mathbf{79,36}\%$

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F, N**	**29-08-2022**
REVISADOS POR:	**M.A.M. V**	**29-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA
INDICADORES DE EFICIENCIA Y EFICACIA
Del 1 de enero al 31 de diciembre del 2021

I/EE
4/4

ANÁLISIS:

Se observó que, de 63 computadoras examinadas, 50 de ellas cuentan con un usuario y contraseña para poder ingresar en el sistema operativo, las cuales representan el 79,36% de cumplimiento en el sistema de seguridad del Municipio.

Restricción de ingreso a redes sociales $= \frac{Restriccion\ de\ ingreso\ a\ redes\ sociales}{Total\ de\ computadoras} *$

$$\mathbf{100} = \frac{\mathbf{52}}{\mathbf{63}} = \mathbf{82,53}\%$$

De las 63 computadoras examinadas se pudo observar que 52 tienen restricción al uso de redes sociales ya que esto disminuiría el desempeño de los trabajadores en cada una de sus funciones, las mismas que corresponden 82,53% de seguridad.

ANÁLISIS:

Antivirus Actualizado$= \frac{Antivirus\ Actualizado}{Total\ de\ computadoras} * 100 = \frac{63}{63} = 100\%$

ANÁLISIS:

Las computadoras en su totalidad tienen instalado un antivirus el cual es actualizado cada año con su respectiva licencia dando un nivel de seguridad muy alto en los equipos informáticos que posee el Municipio.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**29-08-2022**
REVISADOS POR:	**M.A.M. V**	**29-08-2022**

GAD MUNICIPAL DEL CANTÓN GUARANDA

HOJAS DE HALLAZGOS

Del 1 de enero al 31 de diciembre del 2022

H/H

1/6

FALTA DE CAPACITACIÓN INFORMÁTICA
Condición El GAD Municipal de Guaranda no capacita de una manera adecuada al personal de sobre el uso y seguridad de los equipos informáticos.
Criterio Inobservancia de la Normas de Control Interno de la CGE **410-15 Capacitación Informática. -**señala: Se reconocerán las necesidades de preparación tanto para el personal de tecnología de información como para los usuarios que utilizan el sistema de información, que se recordarán para un plan de preparación Informática, elaborado mutuamente con la unidad de Talento Humano.
Causa No se da ninguna capacitación al personal del GAD Municipal de Guaranda ya que no cuenta con un presupuesto para este fin.

Efecto El personal del GAD Municipal de Guaranda no posee las habilidades ni la información adecuada para manejar la información de los ordenadores siendo ineficaces en la utilización de los sistemas informáticos
CONCLUSIÓN Dentro del GAD Municipal de Guaranda no presenta un plan de capacitación para el personal que utiliza los equipos informáticos, los mismos se capacitan de manera individual para desempeñar de una manera adecuada sus actividades.
RECOMENDACIÓN Se recomienda un Plan de capacitación en el personal sobre el uso de los sistemas informáticos de manera individual de acuerdo a las necesidades que cada trabajador para tener un mejor desempeño laboral ya que esto permitiría alcanzar el cumplimiento de los objetivos de la entidad.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/F. N**	**29-08-2021**
REVISADOS POR:	**M.A.M. V**	**29-08-2021**

INEXISTENCIA DE UN DEPARTAMENTO INFORMATICO
Condición No existe un Departamento de Informática dentro del Organigrama del GAD Municipal de Guaranda para verificar actividades y asesoría hacia los usuarios.
Criterio Inobservancia de la Normas de Control Interno de la CGE **410-01 Organización Informática** manifiesta: La unidad de tecnologías de la información se posicionará dentro de la estructura organizacional de la entidad para que pueda realizar actividades de asesoría y apoyo a la alta dirección y unidades usuarias, así como participar en la toma de decisiones organizacionales y generar cambios para la mejora tecnológica. Además, debe garantizar su independencia en el

dominio del usuario y hacer que el servicio llegue a todas las unidades de la entidad u organización.
Causa Falta de interés por parte de las máximas autoridades del GAD Municipal de Guaranda para la creación de un departamento informático, además que no hay un presupuesto para contratar personal capacitado en dicho departamento.
Efecto No existe una asesoría dentro del ámbito tecnológico tanto para los beneficiarios internos como externos del GAD Municipal de Guaranda impidiendo así un avance de la tecnología.
CONCLUSIÓN Dentro del organigrama institucional no existe un Departamento Informático que permita dar apoyo y un respaldo tecnológico a los usuarios tanto internos como externos de la institución.
RECOMENDACIÓN Realizar una restructuración en el Organigrama con la finalidad de crear un Departamento Informático según las necesidades de los sistemas que necesite la institución.

	INICIALES	**FECHA**
ELABORADOR POR:	**J.CH/F. N**	**29-08-2021**
REVISADOS POR:	**M.A.M. V**	**29-08-2021**

INEXISTENCIA DE MECANISMOS PARA IDENTIFICAR RIESGOS INFORMÁTICOS

Condición No cuentan con componentes tales como: controles, sistemas de protección para poder constatar los riesgos que pueden existir en los equipos informáticos.
Criterio Inobservancia de la Normas de Control Interno de la CGE **410-04 Políticas y procedimientos** nos indica: Se incorporarán controles sistemas de aseguramiento de la calidad y gestión de riesgos, al igual que directrices y estándares tecnológicos.
Causa Por la falta de interés de los Directivos del GAD Municipal de Guaranda no se ha elaborado políticas donde señalen mecanismos para poder identificar los riesgos informáticos.
Efecto No se puede constatar los riesgos más significativos que dañan la información dentro de los equipos informáticos, ya que se puede perder información de suma importancia por fallas en las computadoras de la entidad.
CONCLUSIÓN No existen políticas, procedimientos, controles o mecanismos que permita ayudar a verificar los riesgos informáticos imposibilitando contrarrestar daños futuros y perdidas de información en los equipos informáticos de la institución.
RECOMENDACIÓN Que se redacte políticas y procedimientos que se pueda identificar los riesgos dentro del sistema informático, los cuales deben ser documentados y expuestos con el personal del GAD Municipal de Guaranda.

	INICIALES	**FECHA**
ELABORADOR POR:	**J.CH/F. N**	**29-08-2021**
REVISADOS POR:	**M.A.M. V**	**29-08-2021**

INEXISTENCIA DE UN PLAN DE CONTINGENCIAS
Condición El GAD Municipal de Guaranda no presenta un Plan de Contingencias para evitar los riesgos informáticos.
Criterio Inobservancia de la Normas de Control Interno de la CGE **410-11 Plan de contingencia** menciona: El Plan de Contingencia será un documento confidencial que describa los procedimientos a seguir en caso de emergencia o falla Informática que provoque la interrupción del funcionamiento del sistema de información.
Causa La Administración no ha elaborado un Plan de contingencias que ayude a la protección de los equipos informáticos por varios factores como la falta de presupuesto, tiempo y personal.
Efecto El personal del GAD Municipal de Guaranda que maneja los equipos informáticos no cuenta con el conocimiento de cómo prevenir ante un fallo en los sistemas informáticos por consecuencia perdiendo tiempo, información que afectan a la entidad.
CONCLUSIÓN El GAD Municipal de Guaranda no cuenta con un Plan de Contingencias para que las máximas autoridades y el personal compensen los riesgos informáticos mediante medidas que ayuden a prevenir dichos problemas.

	INICIALES	FECHA
ELABORADOR POR:	**J.CH/ F. N**	**29-08-2021**
REVISADOS POR:	**M.A.M. V**	**29-08-2021**

FALTA DE PERSONAL DE SEGURIDAD
Condición No se emplean guardias de seguridad para cuidar las instalaciones del gobierno de la ciudad durante la noche y los fines de semana.
Criterio Inobservancia de la Normas de Control Interno de la CGE 410-10 Seguridad de tecnología de información señala: 8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.
Causa Contratar guardias de seguridad por la noche y los fines de semana está fuera del presupuesto.
Efecto En el caso de instalaciones municipales desprotegidas, puede existir el riesgo de robo de activos informáticos, lo que se traduce en una pérdida masiva de información y recursos económicos.
CONCLUSIÓN El Municipio emplea personal de seguridad de lunes a viernes, de 8:00 a. m. a 12:00 p. m. y de 12:00 a. m. a 6:00 p. m., pero no por la noche ni los fines de semana, lo que crea un riesgo de robo de activos informáticos internos Hora.
RECOMENDACIÓN Contratar guardias de seguridad las 24 horas del día, de lunes a domingo, para proteger las instalaciones del gobierno de la Ciudad y los recursos públicos que posee.

	INICIALES	**FECHA**
ELABORADOR POR:	**J.CH/F. N**	**29-08-2021**

REVISADOS POR:	**M.A.M. V**	**29-08-2021**

GAD MUNICIPAL DEL CANTÓN GUARANDA

HOJAS DE HALLAZGOS

Del 1 de enero al 31 de diciembre del 2021

H/H

6/6

FALTA DE SUPERVISIÓN EN EL MANEJO DE LOS EQUIPOS INFORMÁTICOS
Condición No se inspecciona el manejo que utiliza el personal en los equipos informáticos.
Criterio Inobservancia de la Normas de Control Interno de la **CGE 410-04 Políticas y procedimientos** señala: Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.
Causa Debido a la falta de recursos presupuestarios y económicos, no se contrató personal para supervisar la gestión de los equipos de cómputo, que se utilizaron para otros fines.
Efecto El personal puede hacer mal uso de los equipos de cómputo o incluso dañar estos equipos a través de una operación incorrecta del sistema operativo, lo que resulta en una pérdida de tiempo, información y recursos que le cuestan al GAD Municipal de Guaranda.
CONCLUSIÓN No existe una persona designada en esta ciudad para supervisar y supervisar el buen manejo de los equipos de cómputo, y el personal utiliza los equipos de acuerdo a sus conocimientos y experiencia.
RECOMENDACIÓN Contratar personal para supervisar la gestión de equipos de cómputo y funciones de tecnología de la información, y asistir en la evaluación de indicadores de desempeño.

	INICIALES	FECHA
ELABORADOR POR:	J.CH/F. N	29-08-2021
REVISADOS POR:	M.A.M. V	29-08-2021

2.20.4. Fase IV: Redacción de informe y comunicación de resultados

GAD MUNICIPAL DEL CANTÓN GUARANDA

CARTA DE PRESENTACIÓN

Del 1 de enero al 31 de diciembre del 2021

C/P 1/1

Guaranda, 02 de septiembre del 2022

Sr. Medardo Chimbolema

ALCALDE DE GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA

Presente.

De mi consideración:

Se ha realizado la **AUDITORÍA INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN APLICADOS POR EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA, PROVINCIA BOLÍVAR,2021,** el mismo que se realizó de acuerdo a las Normas de Auditoria Generalmente aceptadas, principios de control Interno, Normas de control de la Contraloría General del Estado y demás procedimientos técnicos considerando lo necesario para la auditoria.

Para la evaluación de Control Interno de se aplicó los componentes de COSO II, los mismo que facilitaron la evaluación y nos dieron a conocer áreas críticas que pueden afectar a las metas institucionales.

En la auditoria se obtuvo resultados en base a los análisis y de las encuestas aplicadas del Control Interno del COSO II, lo cual se obtuvo conclusiones y recomendaciones que será de gran ayuda la toma de decisiones dentro de la institución.

Atentamente,

---------- ----------

Sr. Jhonathan Chimbo Srta. Fernanda Narváez

AUDITOR JUNIOR **AUDITORA JUNIOR**

MOTIVO

La realización de la Auditoría Informática a los Sistemas de Información aplicados por el Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar, se llevó a cabo de conformidad a la Orden de Trabajo N° 1023- DTH-GADCG, emitida por los estudiantes Jhonathan Chimbo y Fernanda Narváez conforme al Proyecto de investigación aprobado por el Consejo Directivo de la Facultad de Ciencias Administrativas, Gestión Empresaria e Informática.

OBJETIVOS DEL EXAMEN

Objetivo General

- Realizar una Auditoría Informática a los sistemas de información aplicados al Gobierno Autónomo Descentralizado del Cantón Guaranda, provincia Bolívar,2021 que permita evaluar la eficiencia y eficacia del uso adecuando de los recursos de informáticos.

Objetivos Específicos

- Elaborar el marco teórico mediante la revisión de fuentes bibliográficas y científicas para que sirva de apoyo para emprender la Auditoría Informática.

- Establecer el marco metodológico respectivo con la determinación de los métodos técnicas e instrumentos de investigación que permita recabar información veraz, oportuna y confiable con la finalidad de realizar una apropiada Auditoría Informática.
- Presentar un informe de conclusiones y recomendaciones para mejorar los sistemas de información con el cumplimiento de los objetivos y metas institucionales.

ALCANCE

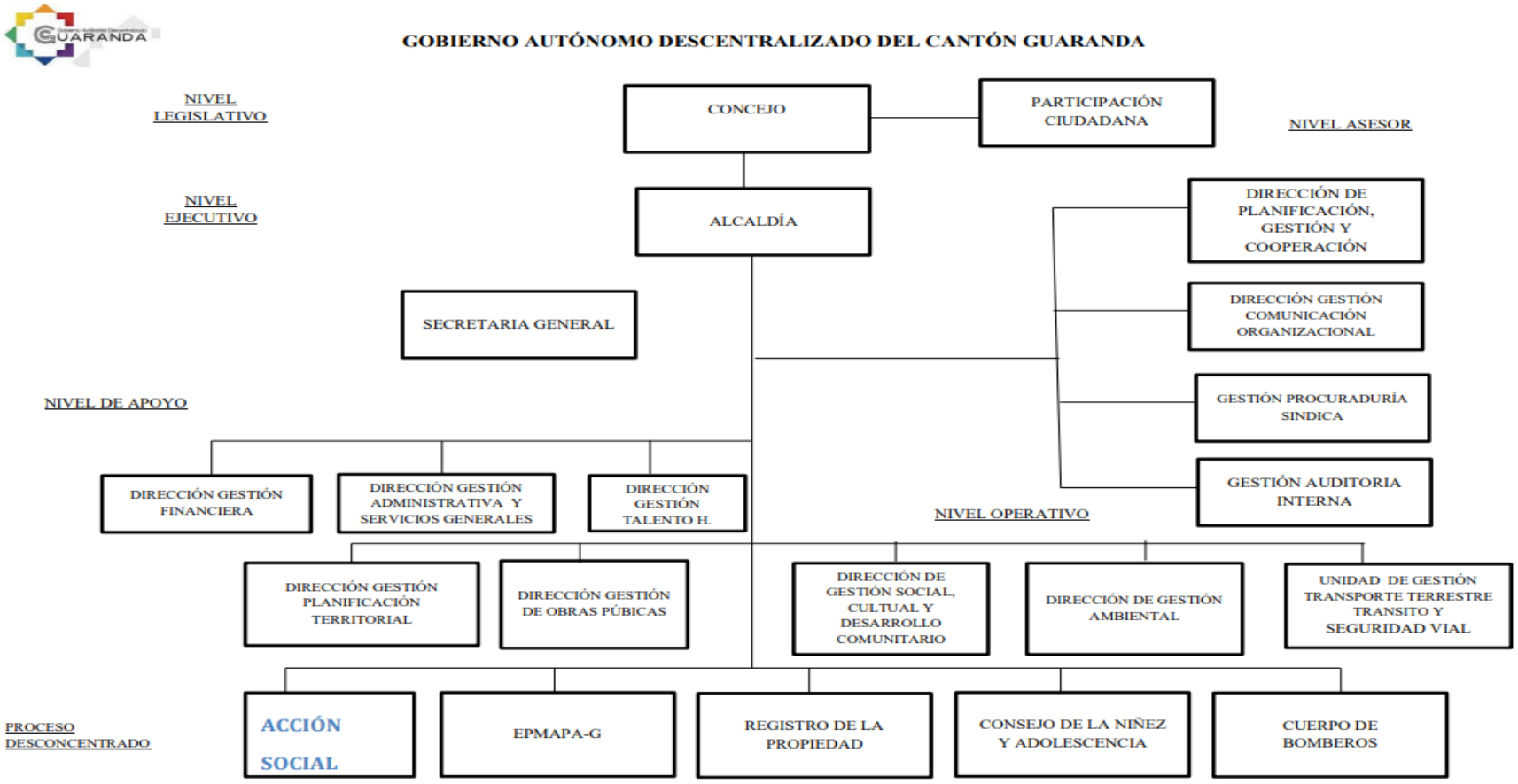
Esta investigación abarca la Auditoría Informática que se realizará al Gobierno Autónomo Descentralizado del Cantón Guaranda, Provincia Bolívar, en el período comprendido entre el 01 de enero al 31 de diciembre del 2021.

BASE LEGAL

- Constitución Política de la República del Ecuador
- Ley orgánica de la contraloría General del estado
- Ley de presupuesto del sector publico
- Ley orgánica de Régimen Municipal
- Ley Orgánica de Régimen Tributario Interno
- Ley Orgánica del Sistema Nacional de Contratación Publica
- Ley Orgánica de servicio Civil Y Carrera Administrativa y Unificación Homologación de Remuneraciones del sector publico
- Código Orgánico de Organización Territorial Autonomía y Descentralización (COOTAD)
- Código de Trabajo

- Código de Procedimiento Civil
- Código Orgánico Integral Penal, COIP
- Código Orgánico de la Función Judicial
- Codificación de la ley de Aguas
- Ley Orgánica de Participación Ciudadana
- Ley Orgánica de Defensa del Consumidor
- Ley de Arbitraje y Mediación
- Ley de la Jurisdicción Contencioso Administrativa
- Ley Orgánica del sistema Nacional de Contratación Pública (LOSNCP)
- Reglamento General a la LOSEP
- Reglamento de Talento Humano
- Reglamento General Sustitutivos de Bienes del Sector Publico
- Reglamento para el pago de Viáticos para la Movilización y Subsistencias en el Exterior para Servidores y Obreros Públicos
- Normativa de Contabilidad Gubernamental del Ministerio de Finanzas
- Estatuto Orgánico por proceso institucional
- Normas de Control interno de la Contraloría General de Estado

ESTRUCTURA ORGANIZACIONAL



2.21. RESULTADOS DE LA AUDITORÍA

2.21.1. Falta de Capacitación Informática

Según las Normas de Control Interno de la CGE 410- 15 Capacitación Informática señala, las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constaran en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. Estará orientado a los puestos de trabajo y a las necesidades de cada funcionario y además para la evaluación de desempeño e institucionales.

Conclusión

El municipio no cuenta con un plan de capacitación para el personal que utiliza los activos informáticos, los mismo que se capacitan de manera autónomo para desempeñar las funciones de sus labores.

Recomendación

Elaborar un plan de capacitación Informática de acuerdo a las necesidades de cada puesto de trabajo para ayudar al desarrollo laboral y el cumplimiento de los objetivos institucionales.

2.21.2. Inexistencia de un departamento de Informática

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

Conclusiones

No existe dentro del organigrama institucional un Departamento de Informática lo cual es algo necesario para poder brindar apoyo y asesoría técnica a los usuarios internos y externos.

Recomendaciones

Restructurar el organigrama institucional e incluir un presupuesto con el fin de incluir un departamento de Informática según las necesidades de la entidad.

2.21.3. Inexistencia de mecanismo para identificar riesgos

Según las normas de control interno de la CGE 100-01 Control Interno señala: El control interno es un proceso integral aplicado por la máxima autoridad, la

dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos.

Conclusión

No existe políticas, procedimientos, controles o mecanismos que ayudan a identificar los riesgos informáticos impidiendo minimizar posibles daños a los equipos informáticos y perdidas de información o hasta fugas de información.

Recomendación

Redactar políticas y procedimientos para identificar los riesgos informáticos los mismo que deberán ser documentados para la socialización en la entidad.

2.21.4. Inexistencia de un plan de contingencia

Según las normas de control interno de la CGE 410-11 plan de contingencia señala: El plan de contingencia será un documento de carácter confidencial que describe los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación de plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

Conclusiones

La entidad no cuenta con un plan de contingencia para que el personal pueda minimizar los riesgos informáticos los posibles riesgos informáticos pueden aparecer mediante medidas preventivas, detectivas y correctivas.

Recomendaciones

Diseñar un plan de contingencias con la finalidad de salvaguardar los activos informáticos cuando existan fallos en el sistema o emergencias.

2.21.5. Falta de personal de seguridad

Según las normas de control interno de la CGE 410-10 Seguridad de tecnología de información señala: los procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por las noches o en fin de semana.

Conclusiones

Dentro del municipio se cuenta con personal de lunes a viernes de 8:00 am – 12:00 am y de 12:00 am – 18:00pm no cuenta con personal para las noches y fines de semana.

Recomendación

Contratar vigilantes de seguridad de lunes a domingo, las 24 horas para cuidar las instalaciones del Municipio y lo recurso que posee la entidad.

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

Según las normas de control interno de la CGE 410-04 Políticas y procedimientos señala: Se implantará procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión den indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidas.

Conclusiones

Dentro del municipio no cuentan con una persona encarga que monitorea y supervisa el uso adecuado de los equipos informáticos, que el personal utiliza para sus actividades.

Recomendaciones

Designar a una persona que se encargue de revisar el manejo de los equipos informáticos y las funciones de tecnología de la información. Con ayuda de los indicadores de desempeño.

Cuadro 7. ***Indicadores***

NOMBRE DEL INDICADOR	FORMULA DE CALCULO	ANALISIS
Presupuesto informático	$=\frac{Presupuesto\ de\ quipos\ informaticos}{Presupuesto\ total} * 100 = \frac{12.000}{6.872.868,39} = 0.2\%$	EL presupuesto asignado para el Municipio en el año 2021, es el 0,2% corresponde a los equipos informático y paquetes informáticos, un valor bajo referente a lo que necesita la entidad tanto en activos informáticos como los dispositivos para la seguridad.
Sistema Operativo Actualizado	$\frac{\#\ Computadoras\ con\ Windows\ 10}{Total\ computadoras} * 100 = \frac{63}{63} = 100\%$	Todas las computadoras del Municipio cuentan con un sistema operativo actualizado, el mismo que funciona de una manera muy rápida en la realización de cada una de las actividades que existe dentro de la entidad.
Acceso a Internet	$\frac{Computadoras\ con\ internet}{Total\ de\ computadoras} * 100 = \frac{63}{63} = 100\%$	Como nos refleja el indicador de eficiencia se concluye que el 100% de las computadoras cuentan con acceso a internet, haciendo que los

		usuarios de los equipos informáticos cumplan sus actividades de una manera eficiente y eficaz.
Mantenimiento preventivo	$\frac{\textit{Computadoras que se realiza mantenimiento preventivo}}{\textit{Total de computadoras}} * \mathbf{100} = \frac{\mathbf{0}}{\mathbf{63}} = \mathbf{0}\%$	Se constató que ningún equipo de cómputo cuenta con un mantenimiento preventivo ya que son muchas computadoras a nivel del Municipio por lo que dificulta al técnico realizar esta actividad constantemente, por esta situación solo actúa cuando existe un daño extremo en los sistemas de información en dicho equipo
Actas de entrega/ recepción	$\frac{\textit{Computadoras entregadas con actas de entrega y recepcion}}{\textit{Total de computadoras}} * \mathbf{100} = \frac{\mathbf{63}}{\mathbf{63}} = \mathbf{100}\%$	Las computadoras son entregadas en su totalidad con sus respectivas actas de entrega y recepción ya que de esta manera consta de manera documentada que el personal del Municipio recibió el equipo informático.
Seguridad para ingresar al computador	$\frac{\textit{Computadores con contraseña}}{\textit{Total de computadoras}} * \mathbf{100} = \frac{\mathbf{50}}{\mathbf{63}} = \mathbf{79,36}\%$	Se observó que, de 63 computadoras examinadas, 50 de ellas cuentan con un usuario y contraseña para poder ingresar en el sistema operativo, las cuales representan el 79,36% de cumplimiento en el sistema de seguridad del Municipio.

Restricción de ingreso a redes sociales	$\frac{\boldsymbol{Restriccion\ de\ ingreso\ a\ redes\ sociales}}{\boldsymbol{Total\ de\ computadoras}} * \mathbf{100} = \frac{\mathbf{52}}{\mathbf{63}} = \mathbf{82,53}\%$	De las 63 computadoras examinadas se pudo observar que 52 tienen restricción al uso de redes sociales ya que esto disminuiría el desempeño de los trabajadores en cada una de sus funciones, las mismas que corresponden 82,53% de seguridad.
Antivirus Actualizado	$= \frac{\boldsymbol{Antivirus\ Actualizado}}{\boldsymbol{Total\ de\ computadoras}} * \mathbf{100} = \frac{\mathbf{63}}{\mathbf{63}} = \mathbf{100}\%$	Las computadoras en su totalidad tienen instalado un antivirus el cual es actualizado cada año con su respectiva licencia dando un nivel de seguridad muy alto en los equipos informáticos que posee el Municipio.

Sr. Jhonathan Chimbo

AUDITOR JUNIOR

Srta. Fernanda Narváez

AUDITORA JUNIOR

Ing. Anabel Monar

SUPERVISORA

2.22. CONCLUSIONES

El presente trabajo de investigación contempla las siguientes conclusiones:

- El Gobierno Descentralizado del Cantón Guaranda no es un centro de auditorías informáticas ya que no cuenta con herramientas de control para determinar la eficiencia y eficacia del uso adecuado de la información y de la seguridad en los equipos informáticos de la entidad.
- Se puede concluir que no se estaban cumpliendo con las normas de control interno de la CGE ya que no cuenta con un presupuesto para implementar manuales o capacitaciones a los funcionarios y que los mismos puedan tener el manejo correcto de los equipos informáticos.
- El gobierno municipal no cuenta con un departamento de informática que brinde un servicio técnico de manera responsable en la información obtenida en cada uno de los departamentos de la entidad.
- El Departamento de Talento Humano no tiene establecido un programa de capacitación para el uso y manejo de la información y de los recursos informáticos.
- Mediante el informe de auditoría que se elaboró con conclusiones y recomendaciones a las autoridades de la entidad se les permitirá conducir a una mejor toma de decisiones para así mejorar el manejo de la información en los equipos informáticos.

2.23. RECOMENDACIONES

- Se recomienda realizar auditorías informáticas al menos una vez al año a fin de contar con controles que midan la eficacia, eficiencia y seguridad del manejo de la información y de los equipos informáticos.
- Asesorar a directores y empleados sobre las normas de control interno de CGE para proteger los activos informáticos.
- Se propone establecer un Departamento de informática con el fin de controlar, supervisar y monitorear la confiabilidad y disponibilidad de los equipos de TI.
- Se recomienda que el Departamento de Talento Humano, en coordinación con Finanzas, asigne presupuesto al programa de capacitación del personal de la entidad para el manejo adecuado de la información en los equipos de informática de manera eficiente, eficaz y segura.
- Se recomienda que el alcalde y autoridades correspondientes se involucren más en el sector informático, dándole un lugar en la estructura organizacional, posicionándolo como un departamento para que pueda recibir los recursos suficientes para realizar proyectos que beneficien a la institución.

2.24. BIBLIOGRAFÍA

Bautista, E. (2009). *www.aeca.es.* Obtenido de https://www.aeca.es/old/buscador/infoaeca/articulosespecializados/pdf/auditoria/pdfauditoria/19.pdf

27001 Academy. (s.f.). Obtenido de 27001 Academy: https://advisera.com/27001academy/es/que-es-iso-27001/

Alcívar, B. (2021). *REPOSITORIO UNIVERSIDAD ESTATAL DE QUEVEDO* . Obtenido de https://repositorio.uteq.edu.ec/bitstream/43000/6261//1/t-uteq-156.pdf

Alvarez, F. (20 de 07 de 2007). *REDALYC.ORG.* Obtenido de https://www.redalyc.org/pdf/4259/425942331006.pdf

Arcenegui Rodrigo, J. I. (2003). Manual de Auditoria Financiera. En I. G. José Antonio Arcenegui Rodrigo, *Manual de Auditoria Financiera* (págs. 153-160). Desclee de Brouwer, S.A..

Arcentales, D., & Caycedo, X. (2017). *www.dialnet.unirioja.es.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Arens, A. (1996). Auditoria: Un enfoque integral.(6° edición). En A. Arens, *Auditoria: Un enfoque integral.(6° edición)* (págs. 15-34). Pearson Prentice Hall.

Arturo Ocampo Lopez, E. S. (2015). *Hadware y Software.* Universida Autónoma del Estado deHidalgo.

Becerra Efraín, S. G. (Enero de 2016). *Control Interno Coso II.* Obtenido de Control Interno Coso II: http://www.dspace.uce.edu.ec/bitstream/25000/21014/1/Control%20interno%20Coso%20II.pdf

Chiavenato, I. (1999). *Administracion de Recursos Humanos.* España: Editorial Mc Graw Hill.

CONEXIÓN EXAN. (02 de 2017). *www.esan.edu.pe*. Obtenido de https://www.esan.edu.pe/conexion-esan/la-auditoria-administrativa-una-accion-indispensable

Contraloria General del Estado. (16 de 12 de 2014). *NORMAS DE CONTROL INTERNO DE LA CONTRALORIA.* Obtenido de NORMAS DE CONTROL INTERNO DE LA CONTRALORIA: https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Costas Santos, J. (2015). *Segurida Informática.* Madrid: RA-MA.

De la Peña, A. (2011). AUDITORÍA. Un enfoque práctico.(1° EDICIÓN). En A. D. Gutierrez, *AUDITORÍA. Un enfoque práctico* (págs. 8-23). Madrid, ESPAÑA: Paraninfo.

Delgado, A. (2019). *www.smsauditores.com.ec*. Obtenido de https://smsecuador.ec/auditoria-de-estados-financieros/

Dextre, J. (2016). *www.revistas.pucp.edu.pe.* Obtenido de https://revistas.pucp.edu.pe/index.php/revistalidera/article/view/16896

Escrivá Gasco, G. (2013). Seguridad Informática. En G. Escrivá Gasco, *Seguridad Informática* (págs. 30-31). Madrid: Macmillan Iberia, S.A.

Espino García, M. (2015). Fundamentos de auditoria. En M. Espino García, *Fundamentos de auditoria* (pág. 23). Mexico D.F: Patria.

Estupiñan Gaitan, R. (2006). Control interno y Fraudes: analisis de informe coso I, II Y III con base en los ciclos trasaccionales (4.ed). En R. Estupiñan Gaitan, *Control interno y Fraudes* (págs. 41- 42). Bogota: Ecoe Ediciones.

Estupiñán Gaitán, R. (2014). Papeles de trabajo en la auditoria financiera: con base en las NAI- Normas de Aseguramiento de la información (3a.ed). En R. Estupiñán Gaitán, *Papeles de trabajo en la auditoria financiera: con base en las NAI- Normas de Aseguramiento de la información (3a.ed)* (pág. 54). Bogotá: Ecoe Ediciones.

EUROINNOVA. (2021). *www.euroinnova.ec.* Obtenido de https://www.euroinnova.ec/blog/que-es-auditoria-operacional

EXCELLENCE, I. (s.f.). *La norma ISO 27001. Aspectos claves de su diseño e implantación.* Obtenido de La norma ISO 27001. Aspectos claves de su diseño e implantación: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Fernández, N. G. (2006). *Cuardernos Didacticos.Ingenieria Informatica.N°48.* Oviedo,España: SERVITEC.

Gaitán, R. E. (2016). *Control interno y fraudes: analisis de informe COSO I, II Y III con base en los ciclo transaccionales.* Bogota: Ecoe Ediciones.

Gascó, G. E. (s.f.). *Seguridad Informatica.* Macmillan Iberia, S.A.

Gualsaqui, J. (2013). *REPOSITORIO UNIVERSIDAD CATÓLICA DEL ECUADOR* . Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/6078/T-PUCE-6320.pdf;sequence=1#:~:text=COBIT%205%20define%2017%20objetivos,%2C%20interna%2C%20aprendizaje%20y%20conocimiento.

Guitierrez, A. d. (2011). *Auditoría.Un enfoque práctico.(1° edición).* España: Paninfo.

Hernandez, E. H. (27 de Julio de 1993). *Auditoria de Informatica.(Un enfoque Metodologico).* Obtenido de Auditoria de Informatica.(Un enfoque Metodologico): http://eprints.uanl.mx/6977/1/1020073604.PDF

Hernandez, E. H. (2004). En *Auditoría Informática* (pág. 180). México: Compañia Editorial Continental.

Hernández, L., Gallego, L., Ordoñez, J., & Alvarez , G. (08 de 01 de 2021). *www.DIALNET.UNIRIOJA.ES.* Obtenido de https://dialnet.inirioja.es/servlet/articulo?codigo=8393213

IT GOVERNANCE INSTITUTE. (22 de Junio de 2009). Obtenido de http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03MarcoReferencial.pdf

Layedra, S. (2022). *REPOSITORIO UNIVERSIDAD TECNICA DE AMBATO.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/36112/1/T5536i.pdf

Lazaro, E. B. (2008). *Auditoría y Sistemas Informaticos.* Vedado,Habana,Cuba: Félix Varela.

Muñoz, C. (2002). *Audioría en sistemas computacionales.(1 edicion).* Mexico: Person Educación.

Nunñez, I. (2022). *REPOSITORIO DIGITAL ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/16760/1/82T01298.pdf

Nuño, P. (2017). *www.emprendepyme.net*. Obtenido de https://www.emprendepyme.net/auditoria-fiscal.html

Oz, E. (2008). *Administración de los sistemas de información.(Quinta edición).* Mexico: Cengage Learning Editores, S.A.

Piattini Mario & Del Peso Emilio. (2008). *Auditoria Informática: Un enfoque práctico(2a ed).* Mexico: Alfaomega.

Piattini Mario, D. p. (2015). Auditoria de Tecnologías y sistemas de Información. En E. d. Mario Piattini, *Auditoria de Tecnologías y sistemas de Información* (págs. 7-8). Madrid,España: RA-MA.

Piattini Velthuis, M. (2015). Auditoria de Tecnologia y sistemas de información . En M. Piattini Velthuis, *Auditoria de Tecnologia y sistemas de información* (págs. 382-383). Madrid: RA-MA.

Piattini Velthuis, Mario. (2015). Auditoria de tecnologia y sistemas de información. En M. Piattini Velthuis, *Auditoria de tecnologia y sistemas de información* (págs. 384-385). Madrid: RA-MA.

Piattini, M. G. (2003). *Auditoria Informática: Un Enfoque Práctico.* España: computec RAMA.

Placencia , E. (2019). *Repositorio de la Universidad Técnica de Machala* . Obtenido de http://repositorio.utmachala.edu.ec/bitstream/48000/14815/1/E-11326_PLACENCIA%20SALINAS%20EDGAR%20STALIN.pdf

Rivas, G. (200). *Auditoría Informática.* Madrid: Ediciones Diaz de Santos S.A.

Rodríguez, J., López, M., Fernández, K., & Organista, J. (2021). *WWW.SCIELO.COM.* Obtenido de https://www.scielo.br/j/tl/ah6bHTXxPMn9Gq8nfhGYWmwz/abstract/?lang=es

Sánchez, J. (02 de 2022). *www.economipedia.com*. Obtenido de https://economipedia.com/definiciones/auditoria-interna.html

Simon, C. (2006). Auditoría Informática. En C. Simon, *Auditoría Informática* (pág. 15). España.

Tabón, L. E. (16 de 09 de 2016). *Hallazgos de auditoría.* Obtenido de Hallazgos de auditoría: https://www.contraloriabga.gov.co/files/HALLAZGOS_LEMT.pdf

Tapia Carmen, G. E. (2016). *FUNDAMENTOS DE AUDITORIA. Aplicacion practicas de las Normas Internacionales de Auditoria.(1° edición).* Mexico: Instituto Mexicano de contadores Publicos.

Tapia, C., Mendoza , S., Castillo , S., & Guevara, D. (11 de 2019). *WWW.BOOKS.ES.* Obtenido de https://books.google.es/books

Universidad Católica San Pablo. (2021). *www.ucsp.edu.pe.* Obtenido de https://postgrado.ucsp.edu.pe/articulos/que-es-auditoria-externa/

Velásquez, F. (15 de Abril de 2015). *LA CONTRALORIA GENERAL DE LA REPUBLICA.* Obtenido de LA CONTRALORIA GENERAL DE LA REPUBLICA: https://doc.contraloria.gob.pe/documentos/(GU-SCPACU-02)00_Guia_Tecnicas_Auditoria.pdf

Weber, R. (1982). *Auditing: Conceptual Foundations and Practice.*

ANEXOS

Anexo 1. Cronograma tentativo (Gantt)

CRONOGRAMA TENTAIVO DE GANTT														
ACTIVIDADES	**MAYO**													
	2	**4**	**6**	**9**	**12**	**14**	**16**	**18**	**20**	**22**	**24**	**26**	**28**	**30**
Inducción sobre el proceso de la modalidad y análisis de la denuncia del tema														
Elaboración del anteproyecto														
Inscripción a la Unidad de Integración Curricular														
Entrega de Anteproyecto														
ACTIVIDADES	**JUNIO**													
	1	**2**	**3**	**6**	**8**	**10**	**14**	**16**	**18**	**20**	**22**	**24**	**27**	**30**
Corrección del Anteproyecto														
Revisión de la corrección del Anteproyecto														
Aprobación del anteproyecto a los pares académicos y revisión														
Observaciones de los pares académicos y certificación de cumplimiento														
Desarrollo del Trabajo de Integración Curricular														
Portada														
índice														
Cuerpo del Documento														
Datos Informativos														
Titulo														
Introducción														
ACTIVIDADES	**JULIO**													
	1	**4**	**6**	**8**	**12**	**14**	**18**	**20**	**22**	**25**	**27**	**28**	**29**	**30**

Antecedentes														
Problema														
Justificación														
Objetivo General														
Objetivos específicos														
Capitulo II - Marco teórico														
Certificado de cumplimiento														
Capitulo III- Metodología														
ACTIVIDADES	**AGOSTO**													
	1	**3**	**5**	**8**	**10**	**12**	**15**	**17**	**20**	**22**	**24**	**26**	**28**	**30**
Capitulo IV- Resultados														
Capitulo V- Propuesta														
Conclusiones														
Recomendaciones														
Bibliografía														
Anexos														
ACTIVIDADES	**SEPTIEMBRE**													
Entrega del Proyecto	**5**	**6**	**8**	**12**										

Anexo 2. Presupuesto

PRESUPUESTO						
N°	**MATERIAL**	**DETALLE**	**PARTICIPANTES**	**CANTIDAD**	**VALOR UNITARIO**	**COSTO**
1	Cuaderno	Para anotar la recolección de Datos	2	1	$ 1,75	$ 1,75
2	Internet	Uso de internet para el desarrollo de la investigación	2	1	$ 30,00	$ 30,00
3	Folders	Para entrega de diversos documentos	2	2	$ 1,00	$ 2,00
4	Impresiones	Impresiones del proyecto	2	630	$ 0,05	$ 31,50
5	Fotocopias	De oficios	2	10	$ 0,05	$ 0,50
6	Anillados	Anillados para entrega del Proyecto Final	2	3	$ 1,50	$ 4,50
7	CD	Para Grabar el proyecto Final	2	1	$ 2,50	$ 2,50
8	Alimentación	Alimentación	2	6	$ 2,50	$ 15,00
9	Transporte	Movilidad al Municipio de Guaranda	2	20	$ 0,30	$ 10,00
		Total				$ 97,75

Anexo 3. Carta de Aceptación del GAD del Cantón Guaranda

Guaranda
ALCALDÍA

DIRECCIÓN DE TALENTO HUMANO

Guaranda, 25 de julio del 2022
Oficio N° 1023- DTH-GADCG

Sr.
Jhonathan Chimbo

De mi consideración:

Saludos cordiales, en atención a requerimiento formulado mediante oficio S/N de fecha 05 de julio del 2022, que en lo principal versa sobre el cambio del tema del proyecto de titulación y solicita la respectiva autorización para continuar con el desarrollo del mismo, al respecto me permito informar que su requerimiento ha sido autorizado por lo que deberá coordinar actividades con el Ing. Alex Cordero, **DIRECTOR FINANCIERO.**

Puntualizando que con anterioridad se autorizó el desarrollo del proyecto mediante oficio N° 0748-DTH-GADCG de fecha 24 de Mayo del 2022.

Particular que remito para los fines consiguientes.

Atentamente,

Abg. Alexander Javier García Núñez
DIRECTOR DE TALENTO HUMANO

Por Guaranda yo me sumo

Dirección: Convención de 1884 y García Moreno
Teléfonos: (03) 2551083 - (03) 2551088 - (03) 2551089
E-mail: alcaldia@guaranda.gob.ec - www.guaranda.gob.ec

Anexo 4. Entrevista al señor Alcalde del GAD del Cantón Guaranda

ENTREVISTA AL SEÑOR ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA

1. **¿Se ha realizado una Auditoria Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda hasta la actualidad?**

   ----

2. **¿Existe un departamento destinado al manejo y control de la Informática?**

   ----

3. **¿Usted usa firmas electrónicas para validar documentos que redacta y envía en representación Gobierno Autónomo Descentralizado del Cantón Guaranda?**

   ----

4. **¿Considera usted que existe suficiente seguridad para proteger y salvaguardar la información almacenada dentro de los equipos informáticos?**

---

5. **¿Según su criterio considera usted necesario realizar una auditoria Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda?**

---

6. **¿Cuenta el Gobierno Autónomo Descentralizado del Cantón Guaranda con sistema de control interno informático?**

---

7. **¿Existe un plan de neutralización para contrarrestar los riesgos informáticos?**

---

8. **¿Existe partida presupuestaria suficiente para la adquirir equipos informáticos?**

---

9. **¿Se realiza capacitaciones al personal de la institución sobre le correcto uso de la información y de los equipos informáticos?**

   ---

10. **¿Se realiza evaluaciones respecto a la eficiencia de los empleados de la unidad de Informática?**

Anexo 5. Cuestionarios aplicados a los empleados del Municipio

ENCUESTAS A LOS EMPLEADOS DEL MUNICIPIO

1. **¿El Gobierno Autónomo Descentralizado del Cantón Guaranda cuenta con un departamento de Informático?**

   SI ☐

   NO ☐

2. **¿Se ha realizado alguna Auditoria Informática al Gobierno Autónomo Descentralizado del Cantón Guaranda?**

   SI ☐

   NO ☐

3. **¿Dentro del Municipio cuenta con un plan de contingencia para minimizar los riesgos informáticos?**

   SI ☐

   NO ☐

4. **¿Cree usted que el personal del Municipio maneja la información y los equipos informáticos de una manera adecuada?**

   SI ☐

   NO ☐

5. **¿El personal del Gobierno Autónomo Descentralizado del Cantón Guaranda cuenta con programas de capacitación relacionado al ingreso al sistema de la entidad?**

   SI ☐

   NO ☐

6. **¿Se utiliza firmas electrónicas para enviar o recibir información del Gobierno Autónomo Descentralizado del Cantón Guaranda?**

   SI ☐

   NO ☐

7. **¿Se restringe el uso de páginas web como redes sociales, entre otras páginas que no tienen relación con el trabajo del municipio?**

   SI ☐

   NO ☐

8. **¿Considera usted que el informe de una Auditoria Informática es un instrumento que permite a los directivos del Gobierno Autónomo Descentralizado del Cantón Guaranda tomar mejores decisiones?**

   SI ☐

   NO ☐

9. **¿Se realizan copias de seguridad de la información que tiene el Gobierno Autónomo Descentralizado del Cantón Guaranda con la finalidad de salvaguarda la información?**

   SI ☐

   NO ☐

10. **¿Considera usted necesario realizar una auditoria Informática en Gobierno Autónomo Descentralizado del Cantón Guaranda para el uso adecuado de la información y de los equipos informáticos?**

    SI ☐

    NO ☐

Anexo 6. Encuestas sobre el Control Interno COSO II

ENCUESTAS SOBRE LOS COMPONENTES DEL CONTROL INTERNO

AMBIENTE DE CONTROL

¿El Municipio dispone de normas generales que supervisen la conducta del personal?

SI ☐

NO ☐

Por qué…….

¿Es necesario los valores éticos para incentivar una cultura organizacional dentro del Municipio?

SI ☐

NO ☐

Por qué…….

¿Existe un espacio de trabajo digno entre los empleados de la institución y sus supervisores?

SI ☐

NO ☐

Por qué…….

¿El personal del Municipio tiene capacitaciones sobre el manejo y la seguridad de los equipos informáticos?

SI ☐

NO ☐

Por qué…….

¿Se toma en cuenta las habilidades, la información y la experiencia a la hora de contratar al personal del Municipio?

SI ☐

NO ☐

Por qué…….

¿Tiene el personal del Municipio información esencial sobre la innovación de datos?

SI ☐

NO ☐

Por qué…….

¿Se encuentra definido el organigrama estructural del municipio?

SI ☐

NO ☐

Por qué…….

¿En el organigrama municipal se puede observar algún departamento asignado para el área de Informática?

SI ☐

NO ☐

Por qué…….

¿la Misión, Visión y Objetivos institucionales cubren los requerimientos tecnológicos del Municipio?

SI ☐

NO ☐

Por qué…….

¿El personal tiene presente la presencia de las Normas de Control Interno de la CGE?

SI ☐

NO ☐

Por

qué…….

ESTABLECIMIENTO DE OBJETIVOS

¿Se determinan los objetivos institucionales del Municipio?

SI ☐

NO ☐

Por qué…….

¿Los objetivos institucionales contribuyen a la satisfacción del objetivo central y la visión del Municipio?

SI ☐

NO ☐

Por qué…….

¿Existen componentes establecidos para evaluar el riesgo en el caso de que no se cumplan los objetivos institucionales?

SI ☐

NO ☐

Por qué…….

¿Es consciente el personal de la presencia de los objetivos institucionales?

SI ☐

NO ☐

Por

qué…….

¿Se actualizan a menudo los objetivos institucionales?

SI ☐

NO ☐

Por

qué…….

IDENTIFICACIÓN DE EVENTOS

¿Los directivos están atentos a los cambios en la innovación?

SI ☐

NO ☐

Por qué…….

¿Existen sistemas para reconocer los riesgos informáticos?

SI ☐

NO ☐

Por qué…….

¿El personal del Municipio distingue los peligros potenciales que pueden influir en los recursos informáticos?

SI ☐

NO ☐

Por qué…….

¿La administración identifica los peligros externos que podrían influir en la fiabilidad de los datos de los equipos informáticos del Municipio?

SI ☐

NO ☐

Por

qué…….

EVALUACIÓN DE RIESGOS

¿Existe un sistema de control interno Informático?

SI ☐

NO ☐

Por qué…….

¿Se ha evaluado el impacto del riesgo en los activos informáticos?

SI ☐

NO ☐

Por qué…….

¿Se reconocen los elementos que pueden provocar el riesgo informático?

SI ☐

NO ☐

Por qué…….

RESPUESTA AL RIESGO

¿Dispone la entidad un Plan de Contingencia para contrarrestar los riesgos informáticos?

SI ☐

NO ☐

Por qué…….

¿Se aplican sistemas, mecanismos o estrategias para disminuir el riesgo?

SI ☐

NO ☐

Por qué…….

¿Se toman acciones correctivas inmediatamente después de que se identifican los riesgos?

SI ☐

NO ☐

Por qué…….

ACTIVIDADES DE CONTROL

¿Se guardan respaldos de los datos de suma importancia que posee el Municipio?

SI ☐

NO ☐

Por qué…….

¿El personal se registra en el PC utilizando una contraseña?

SI ☐

NO ☐

Por qué…….

¿Se limita la utilización de páginas que no estén relacionadas con el trabajo propio del Municipio?

SI ☐

NO ☐

Por qué…….

¿Dispone el Municipio de protección para cubrir la pérdida o el robo de datos?

SI ☐

NO ☐

Por qué…….

¿Se actualiza periódicamente la programación de antivirus de los equipos informáticos para evitar la pérdida de datos?

SI ☐

NO ☐

Por qué…….

¿El personal que tiene acceso a los datos está limitado por una tarjeta de identificación?

SI ☐

NO ☐

Por qué…….

¿Se lleva a cabo un mantenimiento preventivo de los equipos informáticos?

SI ☐

NO ☐

Por

qué…….

¿Existe un plan de gastos detallado para la adquisición de equipos informáticos?

SI ☐

NO ☐

Por

qué…….

¿Se tienen en cuenta la marca, el modelo, el límite y las ventajas de ahorro en la obtención de equipos informáticos?

SI ☐

NO ☐

Por

qué…….

INFORMACION Y COMUNICACIÓN

¿Existe comunicación entre la Administración y el personal del municipio?

SI ☐

NO ☐

Por qué…….

¿Se utilizan instrumentos, por ejemplo, la web, para transmitir datos importantes entre los departamentos del Municipio?

SI ☐

NO ☐

Por qué…….

¿La información relevante se comunica de manera oportuna al personal del Municipio?

SI ☐

NO ☐

Por qué…….

¿Se comunica a tiempo al personal cuando se ocasionan cambios imprevistos en el municipio?

SI ☐

NO ☐

Por

qué……

MONITOREO

¿Se controla el uso de los equipos informáticos?

SI ☐

NO ☐

Por qué…….

¿Se inspecciona los equipos informáticos para garantizar que está en buen estado?

SI ☐

NO ☐

Por qué…….

¿Se inspecciona la entrada y la salida del personal en el Municipio?

SI ☐

NO ☐

Por qué…….

Anexo 7. Entrevista al Alcalde

Anexo 8. Encuestas a los funcionarios del Municipio

Anexo 9. Encuesta del COSO II aplicada al jefe de la Unidad de Informática