TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO, EMPOOBANDO E.S.P y ALCALDÍA MUNICIPAL DE IPIALES

LUIS EDUARDO PANTOJA RODRIGUEZ
GERARDO ANTONIO RAMOS GOYES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2010

TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO, EMPOOBANDO E.S.P y ALCALDÍA MUNICIPAL DE IPIALES

LUIS EDUARDO PANTOJA RODRIGUEZ
GERARDO ANTONIO RAMOS GOYES

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

Director
ING. MANUEL BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2010

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado es Responsabilidad del autor.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Consejo Directivo de la Universidad de Nariño.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____
Jurado

_____
Jurado

San Juan de Pasto, 23 de Noviembre de 2010

AGRADECIMIENTOS

A Dios, por ser la fuerza incondicional que nos mantuvo firmes desde el inicio de nuestra carrera, hasta hoy que alcanzamos nuestros logros propuestos.

Al ingeniero Manuel Bolaños, por que sin su compromiso, orientación y colaboración no hubiera sido posible culminar con éxito este proceso que hoy celebramos.

A nuestras familias, que son la base fundamental de apoyo, para emprender cualquier proceso de alcanzar un logro que cambiara el rumbo de nuestras vidas.

A nuestros compañeros y amigos por el apoyo recibido durante todo el transcurso de la carrera.

DEDICATORIA

Dedicamos este trabajo a nuestros familiares por ser la base fundamental de nuestras vidas, por sus consejos y oportunidades para alcanzar nuevas metas, a nuestros profesores por su colaboración y entrega y a todos nuestros compañeros y amigos por servirnos de apoyo en todo el transcurso de la carrera.

RESUMEN

El proceso de auditoría es fundamental en cualquier entidad para verificar y fortalecer el desarrollo de sus procesos, además permite tener un mejor control de su funcionamiento. Las entidades públicas y privadas que manejan recursos del Estado Colombiano son controladas a través de auditorias desarrolladas por parte de entidades gubernamentales; una de esas entidades gubernamentales encargada de las actividades de control es la Contraloría Departamental de Nariño.

Este trabajo fue realizado para ejecutar una auditoria de sistemas encaminada a identificar las vulnerabilidades de seguridad tanto física como lógica que se presenta en el proceso de contratación de TI de la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P y la Alcaldía Municipal de Ipiales, además se evaluó el cumplimiento del decreto 1151 de 2008 relacionado con el Programa de Conectividad de Gobierno en Línea, proceso que es controlado por parte de la Contraloría Departamental de Nariño en las entidades del Departamento.

Este proceso se realizó dentro del marco de referencia “COBIT”- Objetivos de Control Para tecnologías de Información, del cual se seleccionaron diferentes procesos y objetivos de control clasificados en sus cuatro Dominios Generales; Planear y Organizar, Adquirir e Implementar, Entregar y Dar soporte y Monitorear y Evaluar.

Después del proceso de auditoría se prosiguió con la evaluación de la página web de las entidades; culminando este proceso con la formulación de recomendaciones para el mejoramiento del proceso de contratación de TI, y del cumplimiento del decreto 1151 de 2008 del Programa de Conectividad de Gobierno en Línea.

ABSTRACT

The audit process is fundamental to any entity to verify and strengthen the development of processes also allows for better control of its operation. Public and private entities that manage resources of the Colombian State are controlled through audits carried out by government entities, one of those government agencies responsible for monitoring activities is the Comptroller Department of Nariño.

This study was undertaken to perform an audit of systems designed to identify security vulnerabilities, both physically and logically presented in the recruitment of IT company Obras Sanitarias de la Province de Obando EMPOOBANDO E.S.P and the Municipality of Ipiales also evaluated the compliance of Decree 1151 of 2008 related to the Connectivity Agenda Government Online, a process that is controlled by the Comptroller Department of Nariño Department entities.

This process is conducted within the framework "COBIT" - Control Objectives for Information Technologies, which were selected different processes and control objectives categorized in four general domains; Plan and Organise, Acquire and Implement, Deliver and Support and Monitor and Evaluate.

After the audit process is continued with the evaluation of the website of the entities, this process culminated with the formulation of recommendations to improve the IT procurement process and the implementation of Decree 1151 of 2008 of the Government Program Connectivity Online.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Ambiente: Es el medio en que se desarrollo una programación específica.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Aplicación: Tipo de programa específicamente dedicado al proceso de una función concreta dentro de la entidad.

Auditor: Persona capacitada y experimentada que se designa por una autoridad competente, para revisar, examinar y evaluar los resultados de la gestión administrativa y financiera de una dependencia o entidad.

Auditoría: La auditoría puede definirse como 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 en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Bases de Datos: Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

COBIT Objetivos de Control para la información y Tecnologías relacionadas (COBIT, en inglés: Control Objectives for Information and Related Technology) es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

Confidencialidad: Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Contraloría Departamental de Nariño: Entidad que vigila la gestión fiscal de la administración pública y de los particulares o entidades que manejan fondos o bienes de la nación.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Criptografía: Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos.

Datos: Información antes de ser procesada.

Desastre: Cualquier evento que interrumpe las operaciones o servicios habituales de una entidad durante el tiempo suficiente como para verse afectada de manera significativa.

Disponibilidad: Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Factibilidad: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

Gestión de riesgos: Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Hardware: Es la parte física de un computador y más ampliamente de cualquier dispositivo electrónico, usualmente este término es utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología, así el hardware puede ser de un equipo electrónico, un equipo informático o un robot. En informática también se aplica a los periféricos de una computadora tales como el disco duro, CD-ROM, entre otros.

Impacto: El costo en términos cualitativos y cuantitativos que causo un problema en la entidad.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Internet: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

Metodología: Conjunto de métodos utilizados en la investigación científica

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

Password: Contraseña para equipo de cómputo o aplicación.

Política de seguridad: Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Procedimiento: Modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos, que permiten realizar una ocupación, trabajo, investigación, o estudio correctamente.

Procesamiento de datos: Conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipuleo y tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.

Proceso: Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Red: Servicio de comunicación de datos entre ordenadores.

Repositorio: Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros

Riesgo: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISO Guía 27005]: riesgo permanente que existe aun después de que se hayan tomado las medidas de seguridad necesarios.

SECOP: Sistema Electrónico para la Contratación Pública.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Servicios de tratamiento de información: Según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Servidor: Conjunto de hardware acompañado de sistema operativo especial para ser utilizado por múltiples usuarios, que ofrece una variedad de servicios a usuarios locales o foráneos que utilizan una o muchas aplicaciones.

SI: Sistema de Información.

SICE: Sistema de Información para la Contratación Estatal, que integra todos los datos relevantes de proceso de contratación estatal, permitiendo su autorregulación, control institucional y publicidad de las operaciones.

Sistema de Información: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

TI: Tecnologías de Información.

Técnica: La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCION

Actualmente los sistemas de información y las tecnologías de información han cambiado la forma en que operan las organizaciones. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y lo más importante su implantación logra ventajas operativas que se traducen en beneficios para las instituciones o empresas.

La seguridad de la información debe ser un proceso integrador. Esto quiere decir que con el uso de controles técnicos, administrativos y físicos, se debe lograr la confianza en los sistemas y garantizar que cumplan con los parámetros de: disponibilidad, integridad, confidencialidad, confiabilidad y desempeño.

Por otra parte, el gobierno propone ciertos lineamientos y normatividades que deben ser implementados a cabalidad por las entidades públicas, como es el caso del Portal Web que debe ser desarrollado por todas las entidades controladas y reguladas por el Estado, con dicho portal se busca aprovechar de mejor manera todos los recursos tecnológicos y de sistemas existentes con el objetivo de mejorar la comunicación y la prestación del servicio a la comunidad.

Desde el punto de vista de los sistemas de información se presenta un proyecto que nace del convenio interinstitucional que tiene la Universidad de Nariño con la Contraloría Departamental de Nariño firmado el tres (3) de Febrero de 2009, entre el señor rector Silvio Sánchez Fajardo y la contralora encargada Patricia Figueroa López, gracias a este convenio los estudiantes egresados de la Universidad tienen la facilidad de realizar sus pasantías y trabajos de grado en esta prestigiosa institución de control del Estado, esta clase de proyectos están encaminados a fortalecer la proyección social de nuestra Institución Educativa.

El proyecto planeado en conjunto con funcionarios de la Contraloría Departamental de Nariño involucra una auditoría de sistemas a diferentes entidades públicas del Departamento de Nariño, dentro de las cuales se seleccionaron a diez (10) teniendo en cuenta características establecidas por el ente de control. Este proyecto permite realizar cinco (5) trabajos de grado que incluye a diez (10) estudiantes egresados del programa de ingeniería de sistemas. El titulo del trabajo de grado, varía dependiendo de las dos entidades auditadas por cada bina de trabajo. Quedando este así: “TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO” cada trabajo de grado muestra los resultados encontrados en dos (2) entidades públicas del Departamento de Nariño, las cuales se organizaron de la siguiente manera:

Alcaldía municipal de Yacuanquer.
Alcaldía municipal de Tangua.
A cargo de Lennin Ibarra y Diego Meza.

Hospital universitario departamental de Nariño E.S.E.
Hospital civil de ipíales E.S.E.
A cargo de Luis Chávez y Ricardo Cabrera.

Empresa de obras sanitarias de la provincia de Obando EMPOOBANDO E.S.P.
Alcaldía municipal de ipíales.
A cargo de Luis Pantoja y Gerardo Ramos.

Alcaldía municipal de Chachagüí.
Alcaldía municipal de Buesaco.
A cargo de Liliana Caicedo y Claudia Ordoñez.

Gobernación de Nariño.
Instituto departamental de salud.
A cargo de Lucely Bravo y Adriana Cardona.

Cabe resaltar que para efectos de la realización del trabajo escrito, la unidad 1que hace referencia al marco teórico es común para los cinco trabajos presentados ante la Universidad de Nariño, la diferencia radica en la aplicación de las técnicas y dominios de CobiT, junto con los resultados encontrados en cada una de las entidades públicas del Departamento de Nariño que fueron objeto de estudio.

El proyecto se desarrolla para identificar por medio de un trabajo de auditoría de sistemas los diferentes hallazgos y vulnerabilidades de seguridad física y lógica, a las cuales se encuentra expuesta la información que manejan diariamente las entidades públicas del Departamento de Nariño, para desempeñar a cabalidad sus funciones y brindar un adecuado servicio a la comunidad.

El presente documento se organiza de la siguiente forma: en la primera parte se plantea el problema y su sistematización, se plantean los objetivos que se pretenden alcanzar luego se hablan de los antecedentes directamente relacionados con el proyecto, de la factibilidad y la metodología a seguir. En la última parte se especifican los recursos que se van a utilizar así como la distribución en tiempo de las tareas que están programadas para realizarse.

IDENTIFICACION DEL PROBLEMA

TITULO DEL PROYECTO

TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACIÓN Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO.

LINEA DE INVESTIGACION

Este proyecto corresponde a la línea de investigación Sistemas Computacionales.

DESCRIPCION DEL PROBLEMA

Planteamiento del problema La Contraloría Departamental de Nariño, es la encargada de realizar un seguimiento a las entidades públicas del Departamento, con el fin de garantizar el buen uso de los recursos asignados por el Gobierno, de igual forma es de vital importancia que la seguridad de la información que cada entidad pública maneja sea confiable e integra.

Hasta la fecha las entidades públicas no han sido sometidas a ningún tipo de proceso o estudio para identificar los posibles hallazgos y vulnerabilidades lógicas y físicas más relevantes que violen los lineamientos establecidos en el Decreto 1151 del 2008, que hace referencia al manual de implementación de la estrategia de gobierno en línea. Otro elemento importante es verificar como se lleva a cabo la contratación por cada una de las entidades públicas.

Actualmente la Contraloría Departamental Nariño no cuenta con un documento que permita corroborar el manejo correcto de los recursos por parte de las entidades públicas.

Formulación del problema ¿Cómo realizar la evaluación de los procesos que garantizan el buen uso de los recursos, la implementación del portal Web y la información que se maneja en las entidades públicas, para establecer los riesgos más relevantes a los que se encuentran expuestas y recomendar los ajustes pertinentes?.

Sistematización del problema

- ✓ ¿Cómo realizar la evaluación del sitio Web de las entidades públicas del Departamento de Nariño, para identificar el cumplimiento del Decreto 1151 del 2008 sobre Gobierno en Línea?

- ✓ ¿Cómo se encuentran las condiciones de seguridad lógica de la información del proceso de contratación en las entidades públicas del Departamento de Nariño?

- ✓ ¿Cómo están las condiciones de seguridad física de la información del proceso de contratación en las entidades públicas del Departamento de Nariño?

- ✓ ¿Cómo realizar la evaluación de los controles que garantizan la seguridad física y lógica de la información que maneja el proceso de contratación en las entidades públicas del Departamento de Nariño, para establecer los riesgos a los que se encuentra expuesta y recomendar controles para su protección?

OBJETIVOS

Objetivo general Aplicar técnicas de auditoría de sistemas a entidades públicas del Departamento de Nariño para evidenciar vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información manejada en el proceso de contratación, y el cumplimiento del Decreto 1151 sobre Gobierno en Línea.

Objetivos específicos

- ✓ Analizar diferentes técnicas de auditoría de sistemas para determinar cuáles deben ser utilizadas en cada una de las entidades tomadas como caso de estudio.

- ✓ Auditar el sitio Web de las entidades públicas del Departamento de Nariño tomadas como caso de estudio.

- ✓ Auditar el proceso de contratación de las entidades públicas del Departamento de Nariño tomadas como caso de estudio.

- ✓ Aportar información que permita a las entidades auditadas implementar las medidas necesarias, para garantizar que los trámites realizados por sus

usuarios tengan como materia prima información confiable, integra y confidencial, que asegure la trasparencia en los procesos.

JUSTIFICACION

"*La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de computo, su utilización, eficiencia y seguridad, de los elementos de una organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alterativos se logre una utilización más eficiente de la información que servirá para una eventual toma de decisiones*."[1]

La auditoria de sistemas es de gran importancia para el excelente desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un excelente nivel de seguridad.

Para ayudar a cumplir a cabalidad las funciones de la Contraloría Departamental Nariño, en el control que ejercen sobre las entidades públicas del Departamento de Nariño, es justificable la aplicación de medidas y estrategias para asegurar el adecuado y transparente manejo de los recursos asignados y la información que está a cargo de dichas entidades.

Por lo anterior, el proceso de auditoría de sistemas se convierte en elemento fundamental y de vital importancia, para determinar los hallazgos y vulnerabilidades más relevantes de seguridad física y lógica que actualmente se presentan en el sistema de contratación, además, poder determinar si el sitio web de las entidades cumplen con los lineamientos del Decreto 1151 de la estrategia de Gobierno en Línea.

Con la ejecución de la auditoria se beneficiarán los diferentes usuarios de estas entidades, ya que con base en los resultados presentados se podrán tomar las medidas necesarias, que permitan optimizar cada una de las tareas relacionadas con el procesamiento de la información.

ALCANCE Y DELIMITACION En el desarrollo de este proyecto se identificaron diferentes técnicas de auditoría de sistemas, y se utilizó la más adecuada en cada uno de los casos de estudio.

La aplicación de técnicas de auditoría de sistemas se realizó al proceso de contratación de TI de La Empresa de Obras Sanitarias de la Provincia de Obando

[1] ECHENIQE GARCIA José A., Auditoría en informática, segunda edición [2a] Ed., Mc Graw Hill D. F. 2005.

EMPOOBANDO E.S.P y La Alcaldía Municipal de Ipiales, con esto se identificó, comprobó y evaluó las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información que utilizan dichas entidades. Además, se auditó el sitio Web de las entidades y se verificó si cumplían con los lineamientos del Decreto 1151 del Programa de conectividad de Gobierno en Línea.

Los responsables se relacionaron así:

- Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P.
  Luis Eduardo Pantoja Rodríguez.

- Alcaldía Municipal de Ipiales.
  Gerardo Antonio Ramos Goyes.

Finalmente los resultados de este proceso se plasmaron en este informe que servirá para que estas entidades, tomen medidas preventivas y correctivas que subsanen los problemas detectados.

1. MARCO TEORICO

1.1. ANTECEDENTES

La auditoria de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia de que los datos que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de eficiencia.

Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información en uno solo, denominado sistema de información. En consecuencia por su naturaleza crítica, el enfoque de auditoría debe anotar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoria tradicional, o mediante la creación de unos nuevos.

A principios de los años 80's, se empiezan a utilizar técnicas de tratamiento de la información por medio de computadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia.

Con la introducción de nuevas tecnologías, pronto se detectaron las limitaciones de los métodos tradicionales para realizar la auditoria de sistemas. En su afán de maximizar la eficiencia de los procesos de auditorías, surgen nuevos modelos que se adecuan a las crecientes necesidades del sector de las tecnologías de la información, entre ellos se tienen:

Directrices gerenciales de COBIT, desarrollado por la *Information Systems Audit Control Associatio*n (ISACA):

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y controle los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

The Management of the Control of Data Information Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA):

Este modelo está basado en el concepto de errores que establece responsabilidades relacionadas con la seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA:

Este servicio pretende incrementar la confianza de alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si el sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de prueba determinado bajo un ambiente dado).

Modelo de Evaluación de Capacidades de software (CMM), desarrollado por el Instituto de Ingenieros de Software (SEI):

Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

ISO/IEC 27001(*Information Technology – Security Techniques – Information Security Management System – Requirements*)

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Según el conocido “Ciclo de Deming”: PDCA – acrónimo de plan, *Do Check, Act* (Planificar, Hace, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/17799 (Actual ISO ICE 27002) y tiene su origen en la revisión de la norma Británica *British Standard* BS 7799 – 2: 2002.

Si se revisan los antecedentes de proyectos relacionados con auditoría de sistemas en la universidad de Nariño se encuentran:
Proyecto: DEFINICION DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL CENTRO DE INFORMATICA DE LA UNIVERSIDAD DE NARIÑO.

Realizado por María Constanza Torres B. y Efraín Fajardo Guevara, el trabajo consistió en realizar los procesos de auditoría a la seguridad del centro de informática de la Universidad de Nariño.

1.2. ASPECTOS GENERALES SOBRE AUDITORIA

Inicialmente se puede definir a la auditoria, como el proceso sistemático mediante el cual se obtiene y evalúa una serie de evidencias emanadas de cualquier entidad y de sus actividades, sin importar de que tipo sean, esto con el fin de determinar el grado de correspondencia del contenido informativo con las evidencias recolectadas, debe ser un proceso objetivo y limpio desligado de cualquier interés, este proceso medidor y evaluador debe ayudar a determinar, con conocimiento y certeza razonable, la calidad de los procesos, el cumplimiento de normatividades, la eficiencia en la administración de los recursos, la eficacia con la que se logran los resultados de las estrategias planteadas, entre otros.

La auditoria es un proceso sistemático porque se construye con un conjunto de fases y/o actividades que se relacionan entre ellas, con el fin de lograr un objetivo especifico; esto con apego a las normas, objetivos y principios que regulan la auditoria.

En forma sencilla y clara escribe Holmes:

"... la auditoria es el examen de las demostraciones y registros administrativos. El auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos.".[2]

Se debe tener en claro que no se puede restringir a la auditoria a eventos solamente de carácter económico, ya que la labor de la auditoria es mucho mas amplia, por lo que se pueden abarcar aspectos administrativos, manejo de recursos humanos, técnicos y demás, esto hace que la auditoria sea la herramienta de control más completa y mas fundamentada.

Por lo tanto la auditoria se convierte en la herramienta más eficaz para aplicar una supervisión y un control, que contribuye a la creación de una cultura de disciplina en la organización, además permite descubrir a tiempo fallas en la estructura o puntos débiles existentes a nivel especifico o general.

[2] http://www.monografias.com/trabajos39/la-auditoria/la-auditoria.shtml.

La auditoria como función de control debe ser la herramienta a utilizar para ayudar a los funcionarios que tienen responsabilidad Administrativa, Técnica y Operacional a que no incurran en faltas. Y es por ello que aquí el Control debe ser creativo, inteligente, y constructivo de asesoramiento oportuno a todas las direcciones o gerencias a fin de que la toma de decisiones sea acertada, segura y se logren los objetivos, con la máxima eficiencia.

La responsabilidad de un procedimiento de auditoría debe ir más allá de la búsqueda de problemas y de responsables, la visión empresarial del siglo XXI le ha impuesto mucha más responsabilidad al proceso de auditoría, convirtiéndola en una herramienta de reingeniería capaz de retroalimentar procesos o crear unos nuevos, la auditoria se volvió capaz de identificar necesidades, problemas y soluciones a futuro, con estas facultades el proceso de auditoría se promueve como una función permanente y a largo plazo.

El proceso que se realiza en una empresa puede ser de dos tipos con sus respectivos enfoques:

Auditoría interna

Es una actividad independiente que realiza la empresa y que está encaminada a la revisión de operaciones contables además de la evaluación y medición de la eficacia de otros controles, con la finalidad de prestar un servicio a la dirección. Se aplica mejor en empresas medianas que tienden a aumentar en volumen, extensión geográfica y complejidad y se hace imposible el control directo de las operaciones por parte del director.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole un análisis objetivo, evaluaciones y recomendaciones pertinentes sobre las operaciones examinadas.

Otros objetivos que se busca concretar a través de la auditoría interna son: realizar investigaciones especiales solicitadas por la dirección, preparar informes de auditoría acerca de las irregularidades que pudiesen encontrarse como resultado de las investigaciones, expresando igualmente las recomendaciones que se juzguen adecuadas, vigilar el cumplimiento de la recomendaciones contenidas en los informes emitidos con anterioridad.

La auditoría interna posee varias ventajas: facilita una ayuda primordial a la dirección al evaluar de forma relativamente independiente los sistemas de organización y de administración, facilita una evaluación global y objetiva de los problemas de la empresa que generalmente suelen ser interpretados de una manera parcial por los departamentos afectados, pone a disposición de la

dirección un profundo conocimiento de las operaciones de la empresa, proporcionado por el trabajo de verificación de los datos contables y financieros, contribuye eficazmente a evitar las actividades rutinarias que generalmente se desarrollan en las grandes empresas, favorece la protección de los intereses y bienes de la empresa frente a terceros.

Auditoría externa

Se puede definir como los métodos empleados por una firma externa de profesionales para averiguar la exactitud del contenido de los estados financieros presentados por una empresa. Se trata de dar carácter público, mediante la revisión, a unos estados financieros que en principio eran privados.

Los objetivos de la auditoría externa son: proporcionar a la dirección y a los propietarios de la empresa unos estados financieros certificados por una autoridad independiente e imparcial, proporcionar asesoramiento a la gerencia y a los responsables de las distintas áreas de la empresa en materia de sistemas contables y financieros, procedimientos de organización y otras numerosas fases de la operatoria de una empresa, suministrar información objetiva que sirva de base a las entidades de información y clasificación crediticia, servir de punto de partida en las negociaciones para la compraventa de las acciones de una empresa, reducir y controlar riesgos accidentales, fraudes y otras actuaciones anormales, liberar implícitamente a la gerencia de sus responsabilidades de gestión.

Principios generales de la auditoría externa:

- **Exposición:** Los estados financieros deben recoger por completo y con claridad todas las transacciones de la empresa.
- **Uniformidad:** la base utilizada en la preparación de los estados financieros de un ejercicio no debe experimentar ninguna variación con respecto al ejercicio precedente.
- **Importancia o materialidad:** Este es el criterio que debe presidir el trabajo del auditor es la importancia económica o materialidad de las partidas.
- **Moderación:** De dos o más posibilidades igualmente validas se debe escoger siempre la que dé los resultados más desfavorables.

Normas generales de la auditoría externa.

Afectan a las condiciones que debe de reunir el auditor de y a su comportamiento en el desarrollo de la actividad de auditoría.

- Realización por una persona competente.
- Realización por una persona independiente.
- Cuidado profesional en la realización del trabajo y en la confección del informe.

Normas de trabajo de la auditoría externa.

Hacen referencia a la preparación y ejecución del trabajo a realizar por el auditor, regulan el conjunto de técnicas de investigación e inspección aplicables a los hechos relativos a los documentos contables sujetos a examen, mediante los cuales el auditor fundamenta su opinión responsable e independiente.

- Programación adecuada.
- Supervisión adecuada.
- Análisis del control interno para fijar el alcance de la pruebas.
- Opinión basada en un material y un trabajo razonablemente suficiente.

Normas del informe de la auditoría externa.

Regulan los principios que han de ser observados en la elaboración y presentación del informe de auditoría estableciendo la extensión y contenido de los diferentes tipos de informes, así como los criterios que fundamenten el modelo de informe a utilizar en cada caso.

- Expresión de si los estados financieros se ajustan a los principios de contabilidad generalmente aceptados.
- Expresión de si se han presentado los estados financieros de manera uniforme con respecto al periodo precedente.
- Exposiciones informativas razonablemente adecuadas a los estados financieros.
- El informe debe contener un dictamen sobre los estados financieros considerados en su conjunto.

Procedimientos de la auditoría externa.

Procedimientos de la auditoría externa son la serie de trabajos que hay que realizar para el adecuado cumplimiento de los principios y las normas, antes de presentar el informe definitivo. Se pueden señalar los siguientes procedimientos:

- Revisión de las actividades en las operaciones.
- Inspecciones físicas y recuentos.
- Obtención de pruebas de evidencia.
- Obtención de pruebas de exactitud.
- Preparación de reconciliaciones.

1.3. EL AUDITOR

El auditor se refiere a la persona que asume la responsabilidad de realizar un trabajo de este tipo, en todo caso el auditor debe poseer ciertas cualidades para afrontar un trabajo como este:

- El auditor debe dominar las técnicas y las metodologías que se utilizarán.
- Debe ser abierto en sus relaciones personales y debe saber dialogar.
- Debe poseer habilidades de carácter personal como independencia en el criterio, objetividad, diplomacia etc.
- El auditor debe mantener un cierto grado de independencia en los asuntos que se encuentra evaluando.
- El auditor tiene la obligación de realizar con esmero y cuidado el dictamen o informe para el que fue contratado.
- Debe poseer una actitud positiva frente a la entidad evaluada.
- Debe tener estabilidad emocional frente la entidad.
- Es su obligación la de respetar las ideas de los demás.
- Debe tener capacidad para la negociación.
- Sera discreto y respetuoso con la información de la empresa.
- Su comportamiento debe ceñirse a la ética profesional.

Dadas estas características el auditor responsablemente deberá cumplir con las siguientes funciones:

- Estudiar la normatividad, misión, objetivos, políticas, estrategias, planes y programas de trabajo.
- Desarrollar el programa de trabajo de una auditoria.
- Definir los objetivos, alcance y metodología para instrumentar una auditoria.
- Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones y sistemas utilizados.
- Recabar y revisar estadísticas sobre volúmenes y cargas de trabajo.
- Diagnosticar sobre los métodos de operación y los sistemas de información.
- Detectar los hallazgos y evidencias e incorporarlos a los papeles de trabajo.
- Respetar las normas de actuación dictadas por los grupos de filiación, corporativos, sectoriales e instancias normativas y, en su caso, globalizadoras.
- Proponer los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización.
- Analizar la estructura y funcionamiento de la organización en todos sus ámbitos y niveles.
- Revisar el flujo de datos y formas.

- Considerar las variables ambientales y económicas que inciden en el funcionamiento de la organización.
- Analizar la distribución del espacio y el empleo de equipos de oficina.
- Evaluar los registros contables e información financiera.
- Mantener el nivel de actuación a través de una interacción y revisión continua de avances.
- Proponer los elementos de tecnología de punta requeridos para impulsar el cambio organizacional.
- Diseñar y preparar los reportes de avance e informes de una auditoria.

1.4. TIPOS DE AUDITORIA

Existen algunos tipos de Auditoría entre los que la Auditoría de Sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática.

Entre los principales enfoques de Auditoría tenemos los siguientes:

1.4.1. Auditoría fiscal Es una comprobación científica y sistemática de los estados financieros, libros de cuentas, comprobantes y otros registros financieros y legales de una persona natural, firma o corporación realizado por un auditor con el fin de asegurar si los libros han sido llevados por los principios de contabilidad generalmente aceptados y así brindar confianza y credibilidad a las personas, ya sean naturales o jurídicas que puedan estar interesadas en los estados de la empresa. La persona quien realice la auditoría debe ser un ente ajeno a la empresa, de esta manera se evitan vínculos que puedan verse reflejados en una opinión positiva o parcialización a través de la empresa sin que la misma lo merezca. También es necesario mencionar que si la auditoría está hecha por una firma con una amplia y reconocida trayectoria esta otorgara una mayor credibilidad y confianza a las personas interesadas. En conclusión la auditoría fiscal se dedica a observar el cumplimiento de las leyes fiscales.

La auditoría fiscal tiene como principales objetivos:

- Determinar si sus sistemas contables son aceptables.
- Conocer si el catálogo de cuentas es aceptable.
- Verificar si se está al día en el cumplimiento de sus deberes formales.
- Detectar áreas de riesgo y saber exactamente que correctivos aplicar.

1.4.2. Auditoría financiera Es una revisión de los estados financieros similar a la auditoría externa. Su objetivo es expresar una opinión sobre si las cifras del balance y la cuenta de resultados presentan razonablemente la situación actual de la empresa de acuerdo con los principios de contabilidad generalmente aceptados.

En general la auditoría financiera busca comprobar la veracidad de los estados financieros de la empresa y preparar informes de acuerdo a principios contables.

1.4.3. Auditoria operacional Es una evaluación objetiva, constructiva, sistemática y profesional de las actividades relativas al proceso de gestión de una organización, con el fin de determinar el grado de eficiencia, eficacia, efectividad, economía, equidad, excelencia y valoración de costos ambientales, con que son manejados los recursos; la adecuación y fiabilidad de los sistemas de información y control, de manera que cumpla con las políticas establecidas para alcanzar sus objetivos.

Los informes emergentes de este tipo de auditoría son:

- Auditoría Operativa, relacionada básicamente con los objetivo de eficacia, eficiencia y economía.
- Evaluaciones del Sistema de Control Interno, cuyo propósito es evaluar el diseño y funcionamiento de los Sistemas establecidos.

La auditoría operativa implica:

- El período objeto de examen.
- Examen y verificación de la información relativa al desempeño institucional.
- Revisión y elaboración de informes sobre la administración de recursos.
- Análisis de actividades y procesos clave, evaluación de sistemas de información y control.
- Verificar la utilización de recursos públicos de conformidad a principios de eficiencia, efectividad, economía, eficacia, equidad y excelencia.
- Verificar el cumplimiento de metas y objetivos.
- Evaluar la gestión.

Este tipo de auditoría se aplica generalmente en el Sector Público, Sector Privado, Sector Social.

El objetivo primordial de la auditoria operacional es brindar a todo tipo de organización la información necesaria para utilizar esta poderosa herramienta en forma congruente con sus necesidades y capacidad instalada, a fin de evaluar su comportamiento y derivar las medidas requeridas para mejorar su desempeño.

Otras razones por las que se realiza esta auditoría son para establecer el grado en que la entidad y sus servidores han cumplido adecuadamente los deberes y atribuciones que les han sido asignados, determinar el grado en que el organismo y sus funcionarios controlan y evalúan la calidad tanto en los servicios que presta como en los bienes adquiridos y verificar que la entidad auditada cumpla con normas y demás disposiciones.

1.4.4. Auditoria administrativa Independientemente de ser ella misma parte integrante del sistema total de control superior, es la principal herramienta para la revisión y evaluación de los resultados logrados. Cumple con una doble misión: primero, como parte integrante del control superior; es decir, un medio para obtener y mantener el control; el segundo es; el medio principal para la medición y evaluación de resultados.

Por tanto la dirección superior, propietarios, accionistas, auditores financieros y otros interesados deben confiar en ésta, para la prevención de inconvenientes y para garantizar la adecuada marcha del sistema.

La auditoria administrativa, como función interna, puede verse desde el punto de vista de la organización como:

- Una extensión de la auditoría interna financiera.
- Función independiente de la administración financiera.
- Forma departamental con la auditoría interna.
- Órgano asesor del consejo de administración.

Las funciones de la auditoria administrativa deben quedar enmarcadas dentro de la organización de una empresa en una unidad, que por su situación jerárquica le permita la consecución de sus fines.

El nivel donde deberá quedar la unidad departamental de auditoría administrativa reunirá las siguientes características:

- Jerarquía suficiente para poder inmiscuirse en cualquier unidad administrativa de la empresa.
- Que el tipo de funciones de dicha unidad sea relacionado con la dirección, control y coordinación.
- Que tenga suficiente autoridad sobre los demás departamentos.

Funciones que se van a desarrollar en una auditoria administrativa:

- Investigación constante de planes y objetivos.
- Estudio de las políticas y sus prácticas.

- Revisión constante de la estructura orgánica.
- Estudio constante de las operaciones de la empresa.
- Analizar la eficiencia de la utilización de recursos humanos y materiales.
- Revisión del equilibrio de las cargas de trabajo.
- Revisión constante de los métodos de control.

1.4.5. Auditoria integral Es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la información financiera, al comportamiento económico y al manejo de una entidad con la finalidad de informar sobre el grado de correspondencia entre aquellos y los criterios o indicadores establecidos o los comportamientos generalizados.

El objetivo de la auditoria integral es evaluar los sistemas de control, implantados por la Gerencia General que le permitan medir el rendimiento económico y los recursos financieros de la empresa.

Además con la auditoria integral se pretende conocer la normativa que regula a la Auditoría Integral, analizar el ambiente de aplicación de la Auditoría Integral, verificar a través de la utilización de un conjunto estructurado de proceso tomando como objetivo la evaluación sistemática y permanente del ente económico para una aseveración verificable.

La Auditoría Integral implica la ejecución de un trabajo con un enfoque por analogía de las revisiones financieras, de cumplimiento, control interno y de gestión, sistema y medio ambiente con los siguientes objetivos:

- Determinar, si los Estados Financieros se presentan de acuerdo con los Principios de Contabilidad Generalmente Aceptados.
- Determinar, si el ente ha cumplido, en el desarrollo de sus operaciones con las disposiciones legales que le sean aplicables, sus reglamentos, los estatutos y las decisiones de los órganos de dirección y administración.
- Evaluar la estructura del control interno del ente con el alcance necesario para dictaminar sobre el mismo.
- Evaluar el grado de eficiencia en el logro de los objetivos previstos por el ente y el grado de eficiencia y eficacia con que se han manejado los recursos disponibles.
- Evaluar los mecanismos, operaciones, procedimientos, derechos a usuarios, responsabilidad, facultades y aplicaciones específicas de control relacionadas con operaciones en computadora.
- Evaluar el impacto medioambiental producido de manera directa o indirecta por empresas que presentan un perfil ambiental diferente, condicionado por los riesgos aparentes asociados con sus procesos y productos; la edad, historia y estado de una planta, el marco jurídico en el cual opera.

Los principios generales de auditoría integral son: independencia, objetividad, permanencia, certificación, integridad, planeamiento, supervisión, oportunidad, forma, cumplimiento de las Normas de Profesión.

Para que el ejercicio de la Auditoría Integral se desarrolle en un ambiente controlado, es importante conducirla dentro de un concepto de normas que provean una estructura, como la posibilidad de pronosticar los resultados.

La aplicación de normas ayudará a desarrollar una auditoría de alta calidad respondiendo a la necesidad de completar tareas difíciles en forma oportuna, evitando formar juicios prematuros basados en información incompleta por la falta de tiempo, asimismo, establecen orden y disciplina, produciendo auditorías efectivas, garantizando la veracidad de los hallazgos y el soporte adecuado para las recomendaciones, consecuentemente habrá una mayor aceptación por parte de la gerencia.

1.4.6. Auditoria de sistemas Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, 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.

Su finalidad es el examen y análisis de los procedimientos administrativos y de los sistemas de control interno de la compañía auditada. Al finalizar el trabajo realizado, los auditores exponen en su informe aquellos puntos débiles que hayan podido detectar, así como las recomendaciones sobre los cambios convenientes a introducir, en su opinión, en la organización de la entidad.

Normalmente, las empresas funcionan con políticas generales, pero hay procedimientos y métodos, que son términos más operativos. Los procedimientos son también sistemas; si están bien hechos, la empresa funcionará mejor. La auditoría de sistemas analiza todos los procedimientos y métodos de la empresa con la intención de mejorar su eficacia.

Existen varios campos de acción en los que la auditoria informática de sistemas puede operar, entre ellos se tienen las auditorias más destacadas del tipo:

- **Sistemas operativos** Engloba los Subsistemas de Teleprocesos, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir la posible incompatibilidad entre otros productos de Software Básicos adquiridos por la instalación y determinadas versiones de

aquellas. Deben revisarse los parámetros variables de las librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

- **Software básico** Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar que este no agreda ni condiciona al Sistema Igualmente, debe considerar el esfuerzo en términos de costes, por si hubiera alternativas más económicas. La auditoría, al igual que cualquier otra actividad, requiere de una buena planeación, que le permita desarrollarse eficientemente y oportunamente.

- **Auditoria web** La auditoría web está diseñada para identificar cuáles son los puntos débiles de la presencia online, para mejorarla y para que en los puntos fuertes se pueda sacar el máximo rendimiento a la internet.

  Con los diferentes tipos de auditoría web se podrá conocer:

  - ✓ Las limitaciones técnicas de la página
  - ✓ Que le falta a la página para estar optimizada
  - ✓ Quién y desde dónde vienen las visitas
  - ✓ Cómo se mueven los usuarios de la página
  - ✓ Qué productos o servicios visitan más los usuarios
  - ✓ Qué sitios enlazan la página
  - ✓ Con que palabras clave está mejor posicionada la pagina

1.5. AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

Desde hace varios años, motivados por el espectacular avance de los sistemas dentro de las organizaciones, surgió la necesidad de evaluar no solo los sistemas, sino también la información, sus componentes y todo lo relacionados con dichos sistemas informáticos, a lo que se le denominó auditoria de sistemas.

“La auditoria de sistemas es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y

regulaciones establecidas. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes".[3]

La auditoria de sistemas permite además verificar que la información desde su entrada, procedimientos, controles, almacenamientos y salidas, sea integra y verificable y por tanto permita el apoyo a la toma de decisiones dentro de una organización

Dentro de este procedimiento es necesario evaluar los mecanismos de control implantados en una organización, determinando así, si son adecuados y cumplen con los objetivos o estrategias, de esta manera, es posible proponer cambios que se deberían realizar para el mejoramiento de los mismos. Estos mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia. [4]

1.5.1. Alcance de la auditoria de sistemas Dentro del alcance de una auditoria de sistemas, es necesario determinar con precisión el entorno y los límites en que va a desarrollarse la auditoria de sistemas.

La indefinición de los alcances de la auditoria compromete el éxito o el fracaso de la misma. Así mismo, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar.

1.5.2. Objetivos de la auditoria de sistemas

- **Objetivo general de la auditoria de sistemas** El objetivo principal de la auditoria de sistemas es evaluar el uso adecuado de los sistemas para el correcto ingreso de datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la organización, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas de información dentro de la empresa.[5]

- **Objetivos específicos de la auditoria de sistemas**

[3] http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
[4] http://rie.cl/?a=31081
[5] http://www.monografias.com/trabajos5/audi/audi.shtml

- ✓ El control de la función informática.
- ✓ El análisis de la eficiencia de los Sistemas Informáticos.
- ✓ La verificación del cumplimiento de la Normativa en este ámbito.
- ✓ La revisión de la eficaz gestión de los recursos informáticos.

La auditoria de sistemas sirve para mejorar ciertas características en la empresa como:

- ✓ Eficiencia.
- ✓ Eficacia.
- ✓ Rentabilidad.
- ✓ Seguridad.

1.5.3. Principales pruebas y herramientas para efectuar una auditoria de sistemas

- **Pruebas sustantivas:** Estas pruebas permiten evaluar el grado de confiabilidad del sistema de información de la organización. Para esto se realiza una verificación por medio de observación, cálculos, muestreos, entrevistas, exámenes analíticos, revisiones y conciliaciones. evalúan de la misma manera la exactitud, integridad y validez de la información.

- **Pruebas de cumplimiento:** Estas pretenden evaluar y verifican el grado de cumplimiento de aquello extraído el análisis de la muestra. Permite evidenciar los controles existentes y que son aplicables efectiva y uniformemente.

Las principales herramientas de las que dispone un auditor informático son:

- ✓ Observación
- ✓ Realización de cuestionarios
- ✓ Entrevistas a auditados y no auditados
- ✓ Muestreo estadístico
- ✓ Flujogramas
- ✓ Listas de chequeo
- ✓ Mapas conceptuales

1.5.4. Perfiles profesionales de los auditores informáticos

Tabla 1. Actividades y conocimiento

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

www. http://www.monografias.com/trabajos5/audi/audi.shtml

1.5.5. Pasos a seguir para una auditoria de sistemas en una organización.

- **Estudio Preliminar** Para realizar dicho estudio se examinan las funciones y actividades generales del área o departamento de sistemas, con el fin de tener un contacto inicial con el personal de dicha área, y conocer a grandes rasgos la distribución del sistema, características de equipos, instalaciones y medidas de seguridad visibles.

Para su realización el auditor debe conocer lo siguiente:

- **Organización** Es de vital importancia conocer dentro del departamento o área de sistemas quien es el jefe, quien diseña y quien ejecuta, para lo cual es necesario conocer:

  - ✓ Organigrama: El organigrama permite conocer la estructura oficial dentro de la organización a auditar.
  - ✓ Departamentos: Es importante conocer los departamentos que hacen parte de la organización y las funciones que se deben llevar a cabo dentro de cada uno de ellos.
  - ✓ Relaciones Jerárquicas y funcionales entre órganos de la Organización: Es necesario verificar si dentro de la organización se cumplen las relaciones funcionales y jerárquicas que se evidencian dentro del organigrama. [3]

- **Corrientes de información** Los flujos de información entre los diferentes departamentos dentro de una organización son de vital importancia ya que evidencian una gestión eficiente, siempre y cuando estas corrientes no vayan en direcciones no contempladas dentro del organigrama.
  En muchas ocasiones es posible que se hayan creado canales de información alternativos, lo cual ocurre cuando existen pequeños o grandes fallos en la estructura de la organización.

  Además, la aparición de corrientes de información no planeados pueden obedecer a afinidades personales o desacato a las reglas establecidas. Los cuales pueden producir perturbaciones dentro de la organización.

- **Flujos de información** Dentro del proceso de auditoría es necesario verificar que los nombres de los cargos dentro de la organización correspondan a las funciones que realiza esa persona.

  Puede ocurrir que bajo nombres de cargos diferentes se realicen funciones idénticas, en este caso se estaría realizando tareas redundantes lo cual podría conllevar a deficiencias estructurales.

- **Entorno operacional** Es importante conocer por parte de los auditores de sistemas la referencia del entorno en el cual se va a trabajar, esto se logra determinando:

- ✓ Ubicación geográfica del o los centros de procesamiento de información de la empresa. Evaluando además el personal responsable de cada uno de ellos.
- ✓ Arquitectura y configuración de Hardware y Software: es fundamental la verificación de la compatibilidad e intercomunicación de los equipos ya que estas, están estrechamente ligadas a los grados de seguridad lógica de las organizaciones.
- ✓ Situación geográfica de los Sistemas: el equipo auditor debe estudiar la información que proporcione la organización sobre los elementos físicos y lógicos de las instalaciones.
- ✓ Comunicación y Redes de Comunicación: se debe disponer de un inventario, estado y características de las redes de comunicación.

➢ **Aplicaciones bases de datos** Finalmente para el equipo auditor es necesario tener una idea general de los procesos informáticos realizados dentro de la organización.

Para ello es necesario recolectar la siguiente información:

— Inventario de Hardware y Software.
— Volumen, antigüedad y complejidad de las Aplicaciones.

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones.

Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto:

- ✓ **Metodología del diseño:** La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.
  La documentación de programas disminuye gravemente el mantenimiento de los mismos.

- ✓ **Documentación:** El auditor recaudara información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.
  Estos datos proporcionan una visión aceptable de las características de la carga informática.

- **Determinación de recursos de la auditoría de sistemas** Por medio de los resultados del estudio preliminar es posible determinar los recursos humanos y físicos que son necesarios en el proceso de auditoría.

- **Elaboración del plan y de los programas de trabajo**

  El plan de trabajo se realiza de acuerdo a los siguientes criterios:

  - ✓ El proceso de auditoría se llevara a cabo en áreas generales o específicas.
  - ✓ La auditoria se hará de manera global o especifica.
  - ✓ De acuerdo a si se manejaran recursos genéricos o específicos se realizará un cronograma de trabajo.
  - ✓ El Plan establece disponibilidad futura de los recursos durante la revisión.
  - ✓ El Plan estructura las tareas a realizar por cada integrante del grupo auditoria.
  - ✓ En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

  Una vez elaborado el Plan, se procede a la Programación de actividades, esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

- **Actividades de la auditoría de sistemas** La auditoría de sistemas general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

  Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

  - ✓ Técnicas de Trabajo:

    - — Análisis de la información recabada del auditado
    - — Análisis de la información propia
    - — Cruzamiento de las informaciones anteriores
    - — Entrevistas
    - — Simulación
    - — Muestreos

  - ✓ Herramientas:

    - — Cuestionario general inicial
    - — Cuestionario Checklist
    - — Estándares
    - — Monitores
    - — Simuladores (Generadores de datos)

- Paquetes de auditoría (Generadores de Programas)
- Matrices de riesgo

✓ Informe Final

El informe final de la auditoria de sistemas se realiza por escrito, el cual contempla la siguiente estructura:

- Definición de objetivos y alcance de la auditoría
- Enumeración de temas objeto de la auditoria
- Cuerpo de la auditoria: para lo cual se mostrara los siguiente para cada tema:

    - Situación actual
    - Tendencias futuras
    - Puntos débiles y amenazas
    - Recomendaciones y planes de acción
    - Redacción posterior de la Carta de Introducción o Presentación

1.6 METODOLOGÍAS DE AUDITORIA DE SISTEMAS

La auditoria de sistemas en el ámbito empresarial, ha sido de gran importancia, puesto que con ella se pretende gestionar la información y sirve como apoyo a la toma de decisiones. Además se busca disponer de un sistema de información que sea eficiente y eficaz para obtener la mayor productividad y calidad posibles, debido a que la información se ha convertido en el activo más importante de las empresas.

En la actualidad, gran parte de las organizaciones consideran que la información y la tecnología representan activos importantes para la misma, sin dejar de lado otros activos indispensables, como los requerimientos de calidad, controles, seguridad e información. Por tal razón los directivos deben establecer un adecuado sistema de control interno, para proporcionar seguridad razonable, respecto a si están lográndose los objetivos como: promover la efectividad y eficiencia de las operaciones, proteger y conservar todos los recursos de la organización, cumplir las leyes y reglamentos internos y externos relacionados con la empresa.

Para esto, se hace necesario aplicar una auditoria de sistemas llevando a cabo una metodología adecuada, que permita evaluar de manera objetiva las vulnerabilidades o falta de controles existentes en la empresa.

Las metodologías desarrolladas y utilizadas en la auditoría y el control informático, se dividen en dos grupos:

- Cuantitativas
- Cualitativas

Las metodologías cuantitativas están basadas en un modelo matemático, diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Y las metodologías cualitativas están basadas en el criterio humano capaz de definir un proceso de trabajo. Así mismo, esta metodología establece métodos estadísticos y lógica borrosa, que requiere menos recursos humanos y menos tiempo que las metodologías cuantitativas.

Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo tiene la desventaja de depender mucho de la experiencia, habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica. [6]

En la auditoria de sistemas existen varias metodologías como: COBIT (ISACA), COSO, SAC, AICPA (SAS), IFAC (NIA), MARGERIT y EDP[7]. Sin embargo, las metodologías más utilizadas son: COBIT y COSO.

Estas últimas hacen parte de los modelos a seguir dentro del control interno y son necesarias para desarrollar cualquier proyecto de manera ordenada y eficaz, por lo que cada una cumple un papel importante y al optar por una de ellas, el auditor debe cumplirlas a cabalidad.

1.6.1. COBIT (Control Objectives for Information and related Technology) La Organización ISACA (Information Systems Audit and Control Association), se formo como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI) y el campo de control. A través de su Fundación, publicó en 1995 el COBIT, como resultado de cuatro años de intensa investigación [8].

El COBIT es una metodología utilizada en las empresas para auditar los sistemas de información, donde se evalúa la gestión y el control, enfocado a los administradores de las TI, los usuarios y los auditores encargados del proceso.

COBIT se aplica a los sistemas de información de toda la 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.

La estructura del modelo COBIT evalúa los criterios de información, como la seguridad y calidad, así como también se verifican los recursos que comprenden la tecnología de información, como el recurso humano, instalaciones, sistemas,

---

[6] PIATTINI, Mario y Emilio del Peso. Auditoría Informática. Un enfoque práctico. Editorial RA-MA.

[7] Tesis, Auditoria al modulo de historia clínica. Jenny Burgos y Carolina Domínguez. Año 2007. Pág. 59-60 y 87-94.

[8] http://www.degerencia.com/articulos/los_cinco_componentes_del_control_interno.

entre otros, y finalmente se realiza una evaluación sobre los procesos implicados en la organización.

Cuando se implementa el COBIT adecuadamente en una organización, se evalúa de manera ágil y consistente el cumplimiento de los objetivos de control, haciendo que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos de la empresa.

El modelo COBIT, clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios:

- **Dominio: Planificación y organización (PO)** Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

  Procesos:

  - **PO1 Definición de un plan estratégico**

    - ✓ PO1.1 Administración del Valor de TI
    - ✓ PO1.2 Alineación de TI con el Negocio
    - ✓ PO1.3 Evaluación del Desempeño y la Capacidad Actual
    - ✓ PO1.4 Plan Estratégico de TI
    - ✓ PO1.5 Planes Tácticos de TI
    - ✓ PO1.6 Administración del Portafolio de TI

  Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

  Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

    — La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

— El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

— Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.

— Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos.

➢ **PO2 Definición de la arquitectura de información**

- ✓ PO2.1 Modelo de Arquitectura de Información Empresarial
- ✓ PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
- ✓ PO2.3 Esquema de Clasificación de Datos
- ✓ PO2.4 Administración de Integridad

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

— La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.

— El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.

— La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

➢ **PO3 Determinación de la dirección tecnológica**

- ✓ PO3.1 Planeación de la Dirección Tecnológica
- ✓ PO3.2 Plan de Infraestructura Tecnológica
- ✓ PO3.3 Monitoreo de Tendencias y Regulaciones Futuras
- ✓ PO3.4 Estándares Tecnológicos
- ✓ PO3.5 Consejo de Arquitectura de TI

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- — La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

- — El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

- — Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.

- — Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

- **PO4 Definición de la organización y de las relaciones de TI**

- ✓ PO4.1 Marco de Trabajo de Procesos de TI
- ✓ PO4.2 Comité Estratégico de TI
- ✓ PO4.3 Comité Directivo de TI
- ✓ PO4.4 Ubicación Organizacional de la Función de TI
- ✓ PO4.5 Estructura Organizacional
- ✓ PO4.6 Establecimiento de Roles y Responsabilidades
- ✓ PO4.7 Responsabilidad de Aseguramiento de Calidad de TI
- ✓ PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
- ✓ PO4.9 Propiedad de Datos y de Sistemas
- ✓ PO4.10 Supervisión
- ✓ PO4.11 Segregación de Funciones
- ✓ PO4.12 Personal de TI
- ✓ PO4.13 Personal Clave de TI

- ✓ PO4.14 Políticas y Procedimientos para Personal Contratado
- ✓ PO4.15 Relaciones

Objetivo: Prestación de servicios de TI. Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- — El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.

- — Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

- — Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente.

- — Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

- — Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.

- — La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

- — Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar una asignación de personal adecuada en el presente y en el futuro.

- — El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

- ➢ **PO5 Manejo de la inversión**

- ✓ PO5.1 Marco de Trabajo para la Administración Financiera
- ✓ PO5.2 Prioridades Dentro del Presupuesto de TI
- ✓ PO5.3 Proceso Presupuestal
- ✓ PO5.4 Administración de Costos de TI

- ✓ PO5.5 Administración de Beneficios

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

- — Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.

- — El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información.

- — La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

- ➢ **PO6 Comunicación de la dirección y aspiraciones de la gerencia**

  - ✓ PO6.1 Ambiente de Políticas y de Control
  - ✓ PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
  - ✓ PO6.3 Administración de Políticas para TI
  - ✓ PO6.4 Implantación de Políticas de TI
  - ✓ PO6.5 Comunicación de los Objetivos y la Dirección de TI

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- — Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.

- — Las directrices tecnológicas.

— El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.

— El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.

— Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

- **PO7 Administración de recursos humanos**

  - ✓ PO7.1 Reclutamiento y Retención del Personal
  - ✓ PO7.2 Competencias del Personal
  - ✓ PO7.3 Asignación de Roles
  - ✓ PO7.4 Entrenamiento del Personal de TI
  - ✓ PO7.5 Dependencia Sobre los Individuos
  - ✓ PO7.6 Procedimientos de Investigación del Personal
  - ✓ PO7.7 Evaluación del Desempeño del Empleado
  - ✓ PO7.8 Cambios y Terminación de Trabajo

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

— El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.

— Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.

— La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.

— La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

- **PO8 Asegurar el cumplimiento con los requerimientos externos**

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales.
Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

— Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.

— Leyes, regulaciones y contratos.

— Revisiones regulares en cuanto a cambios.

— Búsqueda de asistencia legal y modificaciones.

— Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

— Privacidad.

— Propiedad intelectual.

— Flujo de datos externos y criptografía.

- **PO9 Evaluación de riesgos**

- ✓ PO9.1 Marco de Trabajo de Administración de Riesgos
- ✓ PO9.2 Establecimiento del Contexto del Riesgo
- ✓ PO9.3 Identificación de Eventos
- ✓ PO9.4 Evaluación de Riesgos de TI
- ✓ PO9.5 Respuesta a los Riesgos
- ✓ PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI. Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.

- Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.

- Actualización de evaluación de riesgos.

- Metodología de evaluación de riesgos.

- Medición de riesgos cualitativos y/o cuantitativos.

- Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.

- Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

- **PO10 Administración de proyectos**

  - ✓ PO10.1 Marco de Trabajo para la Administración de Programas
  - ✓ PO10.2 Marco de Trabajo para la Administración de Proyectos
  - ✓ PO10.3 Enfoque de Administración de Proyectos
  - ✓ PO10.4 Compromiso de los Interesados
  - ✓ PO10.5 Declaración de Alcance del Proyecto
  - ✓ PO10.6 Inicio de las Fases del Proyecto
  - ✓ PO10.7 Plan Integrado del Proyecto
  - ✓ PO10.8 Recursos del Proyecto
  - ✓ PO10.9 Administración de Riesgos del Proyecto
  - ✓ PO10.10 Plan de Calidad del Proyecto
  - ✓ PO10.11 Control de Cambios del Proyecto
  - ✓ PO10.12 Planeación del Proyecto y Métodos de Aseguramiento

- ✓ PO10.13 Medición del Desempeño, Reporte y Monitoreo del Proyecto
- ✓ PO10.14 Cierre del Proyecto

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión. Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- — Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

- — El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.

- — Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.

- — Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.

- — Presupuestos de costos y horas hombre.

- — Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.

- — Plan de administración de riesgos para eliminar o minimizar los riesgos.

- — Planes de prueba, entrenamiento, revisión post-implementación.

- ➢ **PO11 Administración de calidad**

- ✓ PO8.1 Sistema de Administración de Calidad
- ✓ PO8.2 Estándares y Prácticas de Calidad
- ✓ PO8.3 Estándares de Desarrollo y de Adquisición
- ✓ PO8.4 Enfoque en el Cliente de TI

- ✓ PO8.5 Mejora Continua
- ✓ PO8.6 Medición, Monitoreo y Revisión de la Calidad

Objetivo: Satisfacer los requerimientos del cliente. Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

— Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

— Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.

— Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.

— Documentación de pruebas de sistemas y programas.

— Revisiones y reportes de aseguramiento de calidad.

- **Dominio: Adquisición e implementación** Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Procesos:

- **AI1 Identificación de soluciones automatizadas**
  - ✓ AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio
  - ✓ AI1.2 Reporte de Análisis de Riesgos
  - ✓ AI1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos
  - ✓ AI1.4 Requerimientos, Decisión de Factibilidad y Aprobación

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario. Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.

- Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.

- Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.

- Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.

- Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso).
- Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.

- Aceptación de instalaciones y tecnología a través del contrato con el proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

- **AI2 Adquisición y mantenimiento del software aplicativo**

  - ✓ AI2.1 Diseño de Alto Nivel
  - ✓ AI2.2 Diseño Detallado
  - ✓ AI2.3 Control y Posibilidad de Auditar las Aplicaciones
  - ✓ AI2.4 Seguridad y Disponibilidad de las Aplicaciones
  - ✓ AI2.5 Configuración e Implantación de Software Aplicativo Adquirido
  - ✓ AI2.6 Actualizaciones Importantes en Sistemas Existentes
  - ✓ AI2.7 Desarrollo de Software Aplicativo
  - ✓ AI2.8 Aseguramiento de la Calidad del Software
  - ✓ AI2.9 Administración de los Requerimientos de Aplicaciones
  - ✓ AI2.10 Mantenimiento de Software Aplicativo

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio. Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- Requerimientos de archivo, entrada, proceso y salida.
- Interface usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- Personalización de paquetes.
- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- Controles de aplicación y requerimientos funcionales.
- Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

- **AI3 Adquisición y mantenimiento de la infraestructura tecnológica**

  - ✓ AI3.1 Plan de Adquisición de Infraestructura Tecnológica
  - ✓ AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
  - ✓ AI3.3 Mantenimiento de la Infraestructura
  - ✓ AI3.4 Ambiente de Prueba de Factibilidad

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios. Para ello se realizará una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.

— Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.

— Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

- **AI4 Desarrollo y mantenimiento de procedimientos**

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas. Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

— Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.

— Manuales de Operaciones y controles, de manera que estén en permanente actualización.

— Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

- **AI5 Instalación y aceptación de los sistemas**

- ✓ AI7.1 Entrenamiento
- ✓ AI7.2 Plan de Prueba
- ✓ AI7.3 Plan de Implantación
- ✓ AI7.4 Ambiente de Prueba
- ✓ AI7.5 Conversión de Sistemas y Datos
- ✓ AI7.6 Pruebas de Cambios
- ✓ AI7.7 Prueba de Aceptación Final.
- ✓ AI7.8 Promoción a Producción
- ✓ AI7.9 Revisión Posterior a la Implantación

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

— Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.

— Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.

— Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.

— Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

— Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera más económica.

- **AI6 Administración de los cambios**

  - ✓ AI6.1 Estándares y Procedimientos para Cambios
  - ✓ AI6.2 Evaluación de Impacto, Priorización y Autorización
  - ✓ AI6.3 Cambios de Emergencia
  - ✓ AI6.4 Seguimiento y Reporte del Estatus de Cambio
  - ✓ AI6.5 Cierre y Documentación del Cambio

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

— Identificación de cambios tanto internos como por parte de proveedores.

— Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.

— Evaluación del impacto que provocaran los cambios.

— Autorización de cambios.

— Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

— Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

- **Dominio: Entregar y dar soporte** En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos

➢ **DS1 Definición de niveles de servicio**

- ✓ DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio
- ✓ DS1.2 Definición de Servicios
- ✓ DS1.3 Acuerdos de Niveles de Servicio
- ✓ DS1.4 Acuerdos de Niveles de Operación
- ✓ DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio
- ✓ DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos

Objetivo: Establecer una comprensión común del nivel de servicio requerido. Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

— Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

— Definición de las responsabilidades de los usuarios y de la función de servicios de información.

— Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre

todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

- Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

- Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.

- Garantías de integridad.

- Convenios de confidencialidad.

- Implementación de un programa de mejoramiento del servicio.

- **DS2 Administración de servicios prestados por terceros**

  - ✓ DS2.1 Identificación de Todas las Relaciones con Proveedores
  - ✓ DS2.2 Gestión de Relaciones con Proveedores
  - ✓ DS2.3 Administración de Riesgos del Proveedor
  - ✓ DS2.4 Monitoreo del Desempeño del Proveedor

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos. Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

- Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.

— Requerimientos legales regulatorios con el fin de asegurar que estos concuerden con los acuerdos de seguridad identificados, declarados y acordados.

— Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

- **DS3 Administración de desempeño y capacidad**

  - ✓ DS3.1 Planeación del Desempeño y la Capacidad
  - ✓ DS3.2 Capacidad y Desempeño Actual
  - ✓ DS3.3 Capacidad y Desempeño Futuros
  - ✓ DS3.4 Disponibilidad de Recursos de TI
  - ✓ DS3.5 Monitoreo y Reporte

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado. Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

— Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información.

— Monitoreo y reporte de los recursos de tecnología de información.

— Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.

— Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño.

— Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

- **DS4 Asegurar el servicio continuo**

- ✓ DS4.1 Marco de Trabajo de Continuidad de TI
- ✓ DS4.2 Planes de Continuidad de TI
- ✓ DS4.3 Recursos Críticos de TI
- ✓ DS4.4 Mantenimiento del Plan de Continuidad de TI
- ✓ DS4.5 Pruebas del Plan de Continuidad de TI
- ✓ DS4.6 Entrenamiento del Plan de Continuidad de TI
- ✓ DS4.7 Distribución del Plan de Continuidad de TI
- ✓ DS4.8 Recuperación y Reanudación de los Servicios de TI
- ✓ DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
- ✓ DS4.10 Revisión Post Reanudación

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones. Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- — Planificación de Severidad.
- — Plan Documentado.
- — Procedimientos Alternativos.
- — Respaldo y Recuperación.
- — Pruebas y entrenamiento sistemático y singular.

- ➢ **DS5 Garantizar la seguridad de sistemas**

- ✓ DS5.1 Administración de la Seguridad de TI
- ✓ DS5.2 Plan de Seguridad de TI
- ✓ DS5.3 Administración de Identidad
- ✓ DS5.4 Administración de Cuentas del Usuario
- ✓ DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
- ✓ DS5.6 Definición de Incidente de Seguridad
- ✓ DS5.7 Protección de la Tecnología de Seguridad
- ✓ DS5.8 Administración de Llaves Criptográficas
- ✓ DS5.9 Prevención, Detección y Corrección de Software Malicioso
- ✓ DS5.10 Seguridad de la Red
- ✓ DS5.11 Intercambio de Datos Sensitivos

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico

que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.

- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión y suspensión de cuentas de usuario.

- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas.

- Manejo, reporte y seguimiento de incidentes, implementando capacidad para la atención de los mismos.

- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.

- Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización.

➢ **DS6 Educación y entrenamiento de usuarios**

- ✓ DS6.1 Identificación de Necesidades de Entrenamiento y Educación
- ✓ DS6.2 Impartición de Entrenamiento y Educación
- ✓ DS6.3 Evaluación del Entrenamiento Recibido

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados. Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.

— Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.

— Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

- **DS7 Identificación y asignación de costos**

  - ✓ DS7.1 Definición de Servicios
  - ✓ DS7.2 Contabilización de TI
  - ✓ DS7.3 Modelación de Costos y Cargos
  - ✓ DS7.4 Mantenimiento del Modelo de Costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI. Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

— Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.

— Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades.

— Tarifas, definiendo e implementando procedimientos de costos de prestar servicios, para ser analizados, monitoreados y evaluados asegurando al mismo tiempo la economía.

- **DS8 Apoyo y asistencia a los clientes de TI**

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente. Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

— Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda.

— Monitoreo de consultas y despacho, estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas.

— Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

- **DS9 Administración de la configuración**

  - ✓ DS9.1 Repositorio y Línea Base de Configuración
  - ✓ DS9.2 Identificación y Mantenimiento de Elementos de Configuración
  - ✓ DS9.3 Revisión de Integridad de la Configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios. Para ello se realizan controles que identifiquen y registren todos los activos de TI, así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

— Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición.

— Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración.

— Chequeo de software no autorizado, revisando periódicamente las computadoras personales de la organización.

— Controles de almacenamiento de software, definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas.

- **DS10 Administración de problemas**

  - ✓ DS10.1 Identificación y Clasificación de Problemas
  - ✓ DS10.2 Rastreo y Resolución de Problemas
  - ✓ DS10.3 Cierre de Problemas
  - ✓ DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder. Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

- **DS11 Administración de datos**

  - ✓ DS11.1 Requerimientos del Negocio para Administración de Datos
  - ✓ DS11.2 Acuerdos de Almacenamiento y Conservación
  - ✓ DS11.3 Sistema de Administración de Librerías de Medios
  - ✓ DS11.4 Eliminación
  - ✓ DS11.5 Respaldo y Restauración
  - ✓ DS11.6 Requerimientos de Seguridad para la Administración de Datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

- **DS12 Administración de las instalaciones**

  - ✓ DS12.1 Selección y Diseño del Centro de Datos
  - ✓ DS12.2 Medidas de Seguridad Física

- ✓ DS12.3 Acceso Físico
- ✓ DS12.4 Protección Contra Factores Ambientales
- ✓ DS12.5 Administración de Instalaciones Físicas

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas, lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado, definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

- ➢ **DS13 Administración de la operación**

  - ✓ DS13.1 Procedimientos e Instrucciones de Operación
  - ✓ DS13.2 Programación de Tareas
  - ✓ DS13.3 Monitoreo de la Infraestructura de TI
  - ✓ DS13.4 Documentos Sensitivos y Dispositivos de Salida
  - ✓ DS13.5 Mantenimiento Preventivo del Hardware

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

- **Dominio: Monitorear y evaluar** 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. Este es, precisamente, el ámbito de este dominio.

Procesos

- ➢ **M1 Monitoreo del proceso**

  - ✓ ME1.1 Enfoque del Monitoreo
  - ✓ ME1.2 Definición y Recolección de Datos de Monitoreo
  - ✓ ME1.3 Método de Monitoreo
  - ✓ ME1.4 Evaluación del Desempeño
  - ✓ ME1.5 Reportes al Consejo Directivo y a Ejecutivos
  - ✓ ME1.6 Acciones Correctivas

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados, para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

- **M2 Evaluar lo adecuado del control interno**

  - ✓ ME2.1 Monitoreo del Marco de Trabajo de Control Interno
  - ✓ ME2.2 Revisiones de Auditoría
  - ✓ ME2.3 Excepciones de Control
  - ✓ ME2.4 Auto Evaluación del Control
  - ✓ ME2.5 Aseguramiento del Control Interno
  - ✓ ME2.6 Control Interno para Terceros
  - ✓ ME2.7 Acciones Correctivas

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI. Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias, evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

- **M3 Obtención de aseguramiento independiente**

  - ✓ ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
  - ✓ ME3.2 Optimizar la Respuesta a Requerimientos Externos
  - ✓ ME3.3 Evaluación del Cumplimiento con Requerimientos Externos
  - ✓ ME3.4 Aseguramiento Positivo del Cumplimiento
  - ✓ ME3.5 Reportes Integrados

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo. Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

- **M4 Proveer auditoría independiente**

  - ✓ ME4.1 Establecimiento de un Marco de Gobierno de TI
  - ✓ ME4.2 Alineamiento Estratégico
  - ✓ ME4.3 Entrega de Valor
  - ✓ ME4.4 Administración de Recursos
  - ✓ ME4.5 Administración de Riesgos
  - ✓ ME4.6 Medición del Desempeño
  - ✓ ME4.7 Aseguramiento Independiente

  Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa.

Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoria, período de cobertura, naturaleza y trabajo de auditoría realizado, como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo.

Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

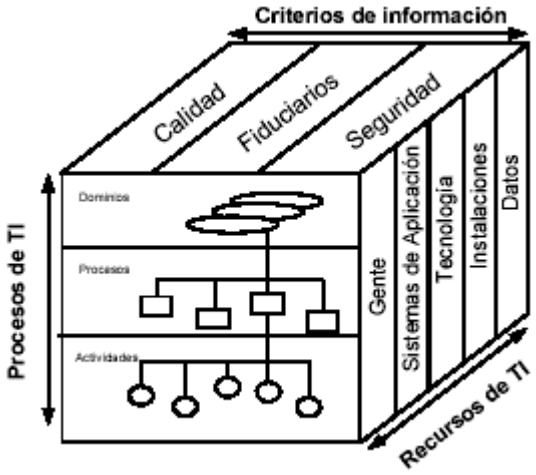
Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzarán y que los eventos no deseados se preverán o se detectaran, y corregirán"

Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

1. Los recursos de las TI
2. Los criterios empresariales que deben satisfacer la información
3. Los procesos de TI

Figura 1. Las tres dimensiones conceptuales de CobiT



Cobit 4.1

Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Además, se toma en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Toda organización, necesita desarrollar una tecnología que le permita rediseñar actividades y procesos para lograr un mejor desempeño en las mismas, es así como el COBIT es fundamental en toda empresa, pues esta metodología reduce posibles vulnerabilidades y riesgos de los recursos de las tecnologías de información y así mismo evalúa el resultado de los objetivos de la empresa.

1.7. TÉCNICAS DE AUDITORIA DE SISTEMAS

1.7.1. Selección de áreas de auditoría Dada la magnitud del universo por auditar, la revisión debe hacerse de manera selectiva, esta técnica es adecuada para empresas con múltiples localizaciones o sucursales, con el fin de dar prioridad a los procesos, se aplican evaluaciones estadísticas a estos en forma periódica, para poder clasificar cuales de estos procesos son claves para el proceso de auditoría.

El uso del computador es indispensable en esta técnica ya que se manejan grandes volúmenes de información y los tamaños de muestra son muy grandes, además esta herramienta mejora la efectividad y eficiencia de los procesos de auditoría, también proporciona pruebas de control efectivas.

Una desventaja de esta técnica es que la construcción de estos modelos es costosa y consume demasiado tiempo, además se deben tener conocimientos avanzados y especializados en materia de diseño y construcción.

- **Simulación- modelaje:** Esta técnica consiste en la creación de modelos conceptuales o físicos bajo ciertas condiciones para simular el comportamiento del sistema computacional, de un programa, o evaluar el sistema financiero en forma periódica (evaluar el incremento o decremento de las cuentas contables o áreas financieras en términos de ingresos, egresos y gastos, para determinar el crecimiento organizacional), estos modelos brindan la posibilidad de realizar pruebas controladas o realizar comparaciones entre valores proyectados y valores reales en materia financiera, con los resultados obtenidos en la simulación el auditor puede dar una opinión acerca del rendimiento del sistema y también proponer medidas de contingencia al respecto.

- **Sistema de puntajes (Scoring):** A diferencia de las anteriores técnicas la evaluación a los procesos y aplicaciones computarizadas se realiza de forma manual, con el fin de priorizar procesos con base en el análisis de riesgos, con la asignación de valores numéricos a las características claves, el auditor asignara la ponderación que este considere para cada factor, teniendo en cuenta el análisis de riesgo realizado con anterioridad que permita obtener un alto grado de confiabilidad , para llevar a cabo esta técnica se deberá diligenciar un formato de puntajes el que dará por resultado la clasificación para la auditoria.

1.7.2. Técnicas para operacionalizar la función de auditoría

- **Software de auditoría multisitio:** Es una técnica aplicable a grandes empresas que tengan diferentes centros electrónicos de datos (PED, Procesamiento electrónico de datos). Desarrollando un programa o grupo de programas e instalándolos en las regionales para que sean utilizados por los auditores. Se requiere que se guarde uniformidad en el software utilizado en los PED para facilitar el proceso de auditaje, esta técnica es aplicada en ambientes de procesamiento distribuido.

- **Centros de competencia:** Esta técnica funciona a la inversa que la técnica de multisitio, ya que centra toda la información de las regionales en un centro de competencia y después de su análisis, evaluación e informes son enviados a las sucursales para tomar las respectivas decisiones.

1.7.3. Técnicas para probar controles de sistemas en funcionamiento

- **Métodos de datos de prueba:** Las técnicas de datos de prueba se usan durante una auditoría alimentando datos en el sistema de computadora de una entidad y comparando los resultados obtenidos con resultados predeterminados. Un elemento de gran importancia en esta técnica es el diseño de los datos de prueba, lo que en últimas determinará la efectividad de esta técnica. Es recomendable seleccionar datos normales, ilógicos, imposibles, con valores extremos, etc. Un auditor podría usar esta técnica para:

  - ✓ Poner a prueba los controles específicos en los programas de cómputo, como son la clave de acceso en línea y los controles para el acceso a datos.

  - ✓ Colocar a prueba transacciones de prueba seleccionadas a partir de transacciones anteriores o creadas por el auditor para verificar las características específicas de procesamiento del sistema de cómputo de una dependencia. En general, estas transacciones se procesan fuera del procesamiento normal que utilice la dependencia.

  - ✓ Poner a prueba transacciones usadas en un mecanismo integrado de pruebas donde se establece una unidad modelo (por ejemplo, un departamento o empleado ficticio), a la cual se le registran las transacciones durante el ciclo de procesamiento normal.

- ✓ Realizar pruebas de cumplimiento de los controles generales, por ejemplo, el uso de datos de prueba para verificar los procedimientos de acceso a las bibliotecas del programa.

- ✓ Pruebas de cumplimiento de los controles de aplicación, por ejemplo, el uso de los datos de prueba para verificar el funcionamiento de un procedimiento programado.

Cuando se procesan los datos de prueba con el procesamiento normal de la entidad, el auditor se asegura de que las transacciones de prueba sean eliminadas posteriormente de los registros contables de la entidad.

Se debe tener en cuenta que si se trata de una entidad pequeña y se procesan volúmenes menores de datos, los métodos manuales pueden ser de costo más efectivo.

En los procedimientos de auditoría para controlar las aplicaciones de datos de prueba se deben realizar las siguientes acciones:

- ✓ Controlar la secuencia de presentación de datos de prueba cuando se extienda a varios ciclos de procesamiento.

- ✓ Realizar corridas de prueba que contengan pequeñas cantidades de datos de prueba antes de presentar los datos de prueba principales de la auditoría.

- ✓ Predecir los resultados de los datos de prueba y compararlos con la salida real de datos de pruebas, para las transacciones individuales.
- ✓ Confirmar que se usó la versión actual de los programas para procesar los datos de prueba.

- ✓ Poner a prueba si los programas usados para procesar los datos de prueba fueron utilizados por la entidad durante el periodo aplicable de auditoría.

En síntesis se puede emplear esta técnica para: evaluación de controles específicos, verificación de validaciones, prueba de perfiles de acceso, prueba a transacciones seleccionadas con las siguientes ventajas y desventajas:

Ventajas

- ✓ Se empieza por el inicio, tratando de verificar que el aplicativo este en capacidad de validar cualquier tipo de dato introducido en el sistema,

dejando por supuesto que se ingresen los datos validos y advirtiendo del intento de ingreso de datos incorrectos.[9]

- ✓ En la mayoría de los casos la información resultado estará protegida y libre de errores cuando el aplicativo permita validar los tipos de datos ingresados al sistema.

Desventajas

- ✓ Para obtener resultados preestablecidos posiblemente no se los pueda obtener de forma manual puesto que algunos procedimientos de auditoría dependen de un procesamiento mucho más complejo que otros (por ejemplo, análisis estadístico avanzado) o implica cantidades de datos que sobrepasarían cualquier procedimiento manual, implicaría la creación de módulos secuenciales de prueba para obtener dichos resultados.

- ✓ Al utilizarlas en sistemas que están en la etapa de producción generan costos por los retrasos ocasionados al hacer las respectivas pruebas.

- **Evaluación del sistema en caso base (BCSE)** Cuando la técnica de datos de prueba se mantiene en el tiempo, para ser consistente y cotidianamente aplicada al sistema en producción, toma el nombre de EVALUACION DEL SISTEMA DEL CASO BASE (ESCB), en tal caso, la prueba es más completa y requiere de un alto grado de cooperación entres usuarios, auditores y personal de sistemas.

  Esta técnica se utiliza en auditorias que hacen uso de controles preventivos y detectivos a los sistemas, los cuales manejan aplicativos para sistemas contables, sistema de nomina, sistemas estadísticos, etc., y en fin sistemas que deban validar los campos de datos que se ingresarán al aplicativo, y de forma paralela evaluar los procedimientos internos del sistema.

  Ventajas

  - ✓ Alta seguridad en los resultados que se van a obtener, puesto que para crear los datos de prueba se hacen participes los auditores, usuarios y el personal de sistemas que prepararán un material mucho más eficiente para ser objeto de la auditoria.

9, http://fccea.unicauca.edu.co/old/taac.htm

- ✓ Al no abandonarse la prueba en el sistema caso base, se puede perfeccionar el sistema ya que cuando se deje de encontrar errores adicionales de lógica o procesamiento se podría decir que se ha creado una versión mejorada de dicha aplicación, para poder desarrollar de mejor manera los cálculos a los datos introducidos a la aplicación y retornar información más confiable.

Desventajas

- ✓ Se necesitará preparar resultados pre calculados de forma manual para compararlos con los arrojados por el aplicativo.

- ✓ El uso de mayor tiempo y de personal.

- **Operación Paralela:** También conocida como pruebas de cumplimiento, se realiza una copia del sistema.

  Su uso radica en auditorias donde se haga uso de controles correctivos a los sistemas de información que cuentan con un mecanismo de procesamiento, en donde de antemano se sabe que posee algún tipo de error ya sea en su lógica de procesamiento al momento de realizar transacciones o en cálculos matemáticos.

Ventajas

- ✓ El hecho de llevar de la mano el sistema actual con el nuevo se convierte en una ventaja ya que se va a garantizar que el sistema nuevo funcione de la mejor manera posible, a fin de evitar futuras modificaciones en su lógica o procesamiento.

- ✓ Convertir un sistema ya sea manual o computarizado el cual presente algunas falencias, en un sistema considerablemente más eficiente y con mayor probabilidad de generar cálculos e información mucho más veraz y rápida.

Desventajas

- ✓ Si el sistema actual falla por lógica de procedimiento o por cálculos, el sistema nuevo también va a fallar puesto que van de la mano.

- **Facilidad de prueba integrada (Integrated Test Facility):** Su objetivo y uso es similar al método de datos de prueba, pero su diferencia principal radica en que su implementación se realiza sin detener el funcionamiento normal de la instalación, mezclando los datos de prueba con los datos reales, en la misma aplicación.

  En esta técnica se realiza un procesamiento simultáneo de datos de prueba que representan operaciones ficticias en un conjunto con datos de operaciones reales, durante un procesamiento real. Esto permite al auditor comparar los resultados de procesamiento de datos de prueba con los resultados previamente determinados. Si los resultados del procesamiento de los datos de prueba resultan conforme a lo esperado, es razonable suponer que el programa de computación procesa los datos reales tal como corresponde.

  Esta técnica no se propone revisar la validez de los datos de entrada sino que prueba la validez de los programas de computación que procesan los datos de entrada, a efectos de determinar si operan de conformidad con su diseño previamente aprobado.

  Esta técnica se utiliza en auditorias donde exista disposición de los datos reales de la entidad. Es optima cuando se utilizan para auditar los controles defectivos en los sistemas, se utiliza en auditorías externas de sistemas que manejen gran cantidad de tipos de datos en una única transacción, como son sistemas contables, sistema de nomina, sistemas estadísticos, etc., puesto que sus resultados arrojaran un informe intachable.

Ventajas

- ✓ No requiere una considerable pericia técnica por parte del auditor, sino más bien conocimiento y comprensión sobre el sistema.[10]

- ✓ Se utilizan datos reales y por ende se auditará cualquier tipo de transacción de las posibles que soporte el sistema.

- ✓ No es necesario solicitar la colaboración del equipo, puesto que las transacciones de prueba se procesan simultáneamente con las reales de la entidad. [10]

- ✓ Los resultados e informes obtenidos a través de la entidad ficticia permitirán de forma segura e inmediata analizar la eficiencia del sistema auditado.

Desventajas

- ✓ Existe la posibilidad de afectar la integridad de la información real. [10]

- ✓ Se requiere de un método efectivo que permita eliminar los informes producidos por la entidad ficticia, puesto que se podría borrar información real del sistema.

- **Simulación en paralelo:** Programas independientes creados por la auditoría para procesar datos reales y simular proceso real.

  Esta es una técnica en la que el auditor elabora, a través de lenguajes de programación o programas utilitarios avanzados, una aplicación similar a la que va a ser auditada, con el objetivo de ingresar simultáneamente la misma información en ambas aplicaciones para verificar la exactitud del procesamiento de datos de la aplicación en producción.

  También denominadas pruebas sustantivas, evaluación de la comparación entre los resultados de dos sistemas diferentes que han recibido los mismos datos de entrada. Simulación total o parcial de componentes del sistema.
  Esta técnica se utiliza en auditorias donde se tiene disposición de los datos reales de la entidad, por otra parte se utiliza para verificar controles detectivos en sistemas que manejan aplicativos software como son sistema contable, sistema de nomina, sistemas estadísticos, etc., con el fin de realizar control a la lógica de la aplicación y la precisión de los respectivos cálculos.

  Ventajas

  - ✓ Posee mayor disponibilidad de información, puesto que lo que hace es trabajar con los datos reales con los que cuenta la entidad auditada para sus procesos internos. De esta forma no se quedará sin ser evaluada ningún tipo de transacción de las que realiza el aplicativo de forma normal.

  - ✓ Al trabajar con datos reales se hace más confiables los informes resultado que se esperan obtener.

  Desventajas

  - ✓ Se hace necesario preparar módulos computarizados que simulen la aplicación real para poder obtener los resultados con los cuales se comparará los resultados obtenidos en la aplicación real.

1.7.4. Técnicas para seleccionar y monitorear transacciones Los procedimientos de auditoría son distintos de acuerdo con la filosofía y técnica de cada organización, entidad o de cada departamento. De ahí que se desprendan auditorias de todo tipo entre las que se encuentran las de informática que a su vez se dividen en categorías como las de métodos manuales y las de métodos asistidos por computadoras.

Por lo tanto cuando una auditoria se conduce en un entorno de CIS ("Auditoria en un entorno de sistemas de información por computadora") sus objetivos y su alcance no cambian a través del proceso, pero al aplicar los procedimientos de auditoría, se puede requerir técnicas que usen la computadora como una herramienta para dicha auditoria. A los usos diversos que se le pueden dar a la computadora se los conoce como Técnicas de Auditoria con Ayuda de Computadora (TAACs).

Estas técnicas son relativamente nuevas y son usadas generalmente por altas organizaciones que necesitan analizar información en grandes volúmenes, con las llamadas TAACs la auditoria se centra en el análisis de datos y no en la recolección de los mismos, además inmersas en las TAACs podremos encontrar modelos de auditoría como los siguientes:

- ✓ Selección de transacciones de entrada.
- ✓ Archivo de revisión de auditoría como control del sistema (SCARF).
- ✓ Archivo de revisión de auditoría por muestreo (SARF).
- ✓ Registros extendidos.

A partir de este análisis se pueden inferir algunos usos de las TAACs en general y cuándo se las debe aplicar; un ejemplo claro es cuando la escases de documentos de entrada o la nula visibilidad del proceso de auditoría puede requerir el uso de las TAACs en la aplicación de procedimientos de cumplimiento, además estos procesos se pueden mejorar en eficiencia y efectividad mediante el uso de esas TAACs.

La necesidad de controlar el procesamiento electrónico de datos en cualquier entidad, con el objetivo de garantizar el control permanente de las transacciones y de sus derivados, hacen de las siguientes técnicas de auditoría fundamentales en cualquier entidad, por lo tanto los escenarios de uso de estas técnicas de auditoría son innumerables en áreas que necesiten controlar anomalías que se susciten en sus procesos.

- **Selección de transacciones de entrada:** Esta técnica es ejecutada por un software de auditoría el cual es independiente a todos los sistemas, consiste en seleccionar y separar datos de entrada que son parte de las aplicaciones. Y se las hace en base al criterio del auditor.

  Entre las ventajas más significativas de este método es la seguridad del método, ya que no cabe espacio para el fraude o el error, además que el riesgo de alteración de los datos del sistema es evidentemente bajo.

  Se utiliza en auditorias para verificar los controles detectivos, utilizados en sistemas de información computarizados que hayan sido modificados, con el fin de verificar el buen funcionamiento de la lógica y los cálculos matemáticos.

  Ventajas

  - ✓ Esta técnica es relativamente fácil de aplicar.
  - ✓ No necesita modificar el código fuente de la aplicación.
  - ✓ No se presentan riesgos de alteración de la información generada por el sistema.

  Desventajas

  - ✓ Se requiere de un aplicativo que permita seleccionar los datos de entrada y las transacciones dependiendo de los parámetros que crea pertinente el auditor.

- **Archivo de revisión de auditoría como control del sistema (SCARF):** Este tipo de técnica consiste en incorporar aplicaciones de auditoría dentro del sistema para que ejecute rutinas de supervisión y monitoreo en forma permanente. La aplicación de este tipo de software se conoce como subrutina, a partir de esta subrutina se seleccionarán muestreos previamente definidos.

  Esta técnica se utiliza en sistemas que manejan aplicativos software; como son sistema contable, sistema de nomina, sistemas estadísticos, etc., los cuales manejan una gran numero de diversos tipos de transacciones con el fin de realizar control a la lógica de la aplicación y la precisión de los respectivos cálculos.

Ventajas

- ✓ Con esta técnica no solo se obtiene resultados para ser comparados sino que permite, supervisar, obtener muestreos y reportes de excepciones al momento de desarrollarse una transacción en el aplicativo. [11]

- ✓ Este tipo de técnica permiten auditar de forma más continua las transacciones producidas por un aplicativo, puesto que se incrustan módulos que permiten controlar de forma permanente el desarrollo de las transacciones.

- ✓ Permite abrir una ventana en la caja negra, para observar y controlar el proceso de la transacción.

Desventajas

- ✓ Trabaja con un gran número de transacciones, dependiendo del peso de trabajo que tenga el aplicativo de la entidad.

- ✓ Se hace necesario preparar e implantar las rutinas de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costos.

- ✓ Se requiere pericia técnica por parte del auditor.

- ✓ Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.[10]

- **Archivo de revisión de auditoría por muestreo (SARF):** Esta técnica es muy parecida a SCARF, la diferencia radica en que la selección de las transacciones ya no se hacen en forma automática predefiniéndolas sino que por el contrario se realizan al azar, esto con el fin de capturar archivos representativos para analizarlos con el apoyo de la estadística. Se requiere un analista de sistema o programador para que preparen los módulos a decisión del auditor.

  Esta técnica se utiliza para auditar sistemas que tengan gran carga de trabajo en cuanto a variedad de transacciones se refiere, como son sistemas que manejan aplicativos contable en bancos, aerolíneas, etc.

11, Auditoria de Sistemas en Funcionamiento (José Dagoberto Pinilla Guerrero)

Ventajas

- ✓ Posibilita el monitoreo permanente de la ejecución de una transacción particular del sistema.

- ✓ Permite abrir una ventana en la caja negra, para observar y controlar el proceso de la transacción reduciendo la posibilidad de fraude de la información.

- ✓ No trabaja con un gran número de transacciones, puesto que las selecciona al azar ya que se apoya en muestreos estadísticos.

Desventajas

- ✓ Se hace necesario preparar e implantar los módulos de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costos.

- ✓ Se requiere pericia técnica por parte del auditor.

- ✓ Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación. [10]

- **Registros extendidos:** Con la aplicación de pequeñas rutinas se recogen datos que han afectado el funcionamiento del sistema, todo este tipo de rutina se conocen como pistas de auditoría, los cuales dejan un historial de todas las actividades secuencias y/o fallos del sistema.

  Esta técnica se utiliza en auditorias para verificar los controles detectivos y correctivos en sistemas que manejan aplicativos software; como son sistema contable de bancos, sistema de nomina, sistemas estadísticos, etc. con el fin de obtener una pista de toda la información clave de las diferentes transacciones.

  Ventajas

  - ✓ Se incluye en algún tipo de registro de información significativa sobre las transacciones o el sistema, que luego pude ser consultada por el auditor.[12]

[12], http://elrincondeperolo.blogspot.com/2009/07/trabajo-de-auditoria.html

- ✓ Al igual que en SCARF este tipo de registros permiten auditar de forma más continua las transacciones producidas por los aplicativos software.

- ✓ Al guardar en un solo registro cualquier tipo de modificación que se hagan a las transacciones, será más fácil encontrar la causa de que se produzca algún tipo de información errónea o no valida.

Desventajas

- ✓ Se hace necesario preparar e implantar las rutinas de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costo de desarrollo.

- ✓ Se requiere pericia técnica por parte del auditor.

- ✓ Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.[10]

1.7.5. Técnicas para la auditoria de información almacenada El fin de un proceso auditor es asistir a la gerencia o al departamento auditado para brindar apoyo en la identificación de los diversos hallazgos y posibles riesgos, y formular soluciones que sirvan para el control que eviten estos errores y minimicen los riesgos, generalmente algunas tareas del proceso auditor toman demasiado tiempo como por ejemplo el planteamiento, desarrollo y documentación; la automatización de algunas tareas puede resultar muy productivo para el equipo auditor, especialmente en el caso de auditoría de sistemas donde algunos procesos se prestan para ser automatizados.

Estos procesos toman cada vez más fuerza a nivel mundial después de lo acontecido con los desfalcos que llevaron a la quiebra a grandes empresas como Parmalat (italiana) y Enron (norteamericana) los cual replantea el proceso de auditoría tanto interna, como externa y la utilización de herramientas informáticas tanto de nivel general como herramientas especializadas.

La automatización como se menciona anteriormente, se facilita para algunos procesos en la auditoria de sistemas, lo cual brinda algunos beneficios como la clara reducción en el tiempo y posiblemente de recursos en el desarrollo del proceso automatizado, la estandarización en los procesos y a su vez una mayor flexibilidad ante los cambios lo cual se puede ver reflejado en una mejora en la calidad, provee mecanismos de monitoreo y retroalimentación, además la posibilidad de realizar análisis con diversos criterios, tales como recalculo de operaciones, búsqueda avanzada de información, seguimiento de transacciones,

etc., convirtiéndose así en un poderoso aliado del equipo auditor permitiéndoles enfocarse en otros campos y obtener así un mejor y más profundo resultado.

El avance tecnológico que se ha vivido en los últimos años en el mundo ha generado la importancia para las personas y empresas de mantenerse actualizado e informado, pero esta información debe cumplir con ciertas características importantes como la veracidad, confiabilidad y oportunidad de la misma. Con el fin de obtener y gestionar esta información han surgido las NTIC (Nuevas Tecnologías de la Información y la comunicación); gracias a esto la información que se ha convertido en uno de los más valiosos recursos en las empresas, puede ser obtenida, tratada y almacenada para una mejor toma de decisiones.

Al introducir una herramienta tan poderosa como el computador en el proceso de auditoría esto conlleva a la utilización de herramientas informáticas para analizar la información que en su gran mayoría se encuentra en medios de almacenamiento magnético (discos duros, cd, dvd), con esto se busca evaluar la consistencia que presentan los sistemas de información, análisis de datos de una muestra de transacciones para verificar la integridad, consistencia y confiabilidad de la información presentada a través de los sistemas de información, el auditor debe desarrollar procedimientos en el que se consideren la herramientas informáticas como apoyo para la realización de la auditoria.

- **Aplicaciones estandarizadas para grandes volúmenes de información:** Es indispensable que las empresas realicen auditorias rigurosas frecuentemente, especialmente a las áreas más sensibles del negocio, realizar un manual del comportamiento de la empresa con las normas y procedimientos internos.

Ventajas

- ✓ Controlar el riesgo de fraudes en las empresas, para que se disminuyan las constantes quiebras empresariales que causaron fuertes impactos económicos negativos a nivel mundial, las cuales manejaban grandes volúmenes de información y que necesitaban de un ajuste en sus auditorías internas y externas.

- ✓ Las herramientas utilizadas en esta técnica son superiores a las técnicas manuales puesto que evalúan gran cantidad de información en menor tiempo y reducen costos.

- ✓ Amplían el alcance de la investigación y permiten realizar pruebas que no pueden efectuarse manualmente, en algunos casos los paquetes permiten la lectura de varios archivos simultáneamente.

- ✓ “Esta técnica utiliza herramientas que pueden ser usadas para seleccionar una muestra, analizar las características de una archivo, identificar tendencias en los datos y evaluar la integridad de los mismos”.[13]

- ✓ Estas herramientas de auditoría generalizadas pueden analizar los datos procesados por muchas aplicaciones, además de elevar la calidad y fiabilidad de las verificaciones realizadas, categorizar y muestrear datos de grandes volúmenes de información para realizar un análisis y ayudar a la toma de decisiones.

Desventajas

- ✓ Para tener en cuenta uno de los retos a afrontar por las aplicaciones estandarizadas para grandes volúmenes de información se da debido a la gran diversidad de ambientes de procesamiento de información ya que las características de los sistemas varían debido a los diferentes entornos de software y hardware, diferentes estructuras de datos, formatos de registros y funciones de procesamiento, poseen limitantes a la hora de verificar la lógica de procesamiento, para este tipo de aplicaciones es todavía complicado adaptarse a los cambios en los objetivos de la aplicación y otro inconveniente es capacitar a los auditores en el uso del software.

- ✓ En caso donde el volumen de información no sea muy amplio los métodos manuales son más efectivos y menos costosos, además algunos tipos de aplicaciones son costosas de desarrollar, implementar y operar.

- **Programas utilitarios y usos generales:** El auditor emplea esta técnica cuando en el proceso de auditoría requiere utilizar diferentes programas los cuales servirán para proteger y salvaguardar la información existente en la empresa.

Ventajas

- ✓ Es de gran ventaja utilizar esta técnica cuando se trata de manipular una gran cantidad de información y la empresa no cuenta con software especializado para dichas tareas.

- ✓ Los programas utilitarios son un aliado efectivo del software operacional, para posibilitar la optimización general de los recursos de informática.

- ✓ El auditor dispone de gran variedad de software general para la realización de tareas básicas de la auditoria tales como la documentación, creación de actas o presentación de informes o resultados. Estas herramientas no proveen una aplicación especializada en el proceso de la auditoría, aún así, considerando el proceso total de auditoría, estas herramientas son igualmente útiles. Entre muchas herramientas se encuentran paquetes de ofimática como Microsoft Office, hojas de cálculo como Excel, lotus 1-2-3, diseñadores de gráficos como Visio, Smart Draw o administradores de correo electrónico como Outlook; con estas herramientas se facilita la creación y administración de documentos, cálculos matemáticos y financieros, creación de diagramas de proceso, organigramas, presentación de gráficos estadísticos etc.

Desventajas

- ✓ Implica mucha complejidad técnica, puesto que el auditor requiere de mucho conocimiento para poder realizar una evaluación interna de la aplicación.

- ✓ Los programas utilitarios podrían fácilmente dañar el sistema, por lo tanto el auditor debe tomar ciertas medidas para evitar pérdida accidental de información y daño en los programas utilizados en la organización.

- ✓ Las herramientas utilizadas en esta técnica son muy limitadas en su funcionamiento y alcance con respecto al software hecho a la medida y el software especializado.

- **Software hecho a la medida:** Motivados por alcanzar los estándares de calidad internacional las empresas realizan auditorías internas con el fin de cumplir con los requerimientos exigidos, pero la contratación de un asesor o grupo de asesores conlleva a destinar grande presupuestos para cumplir con las auditorias en las empresas, por tal motivo se han visto en la tareas de realizar software especializados, específicos, hechos a la mediada o software de auditoría con sistemas expertos, permitiendo evaluar la gestión inicial en el tema de calidad, lo cual se refleja en la preparación que presentan a la hora de la realización de la auditoria.

  Permite examinar a las empresas en áreas sistematizadas, en donde se pueden crear o desarrollar programas especiales para la empresa, en este caso el auditor haría las veces de usuario y el área de sistemas la respuesta y la solución a los requerimientos del usuario.

Existen herramientas de mucha productividad para la auditoria, una de ellas es Groupware “una herramienta especializada que permite a equipos de negocios trabajar más rápido, compartir más información, comunicarse mas efectivamente, y hacer un mejor trabajo de completamiento de tareas.

Groupware es una forma natural de automatizar el proceso de auditoría. Que usa características de base de datos y procesamiento de flujo de trabajo que pueden ser usados para almacenar e integrar información recolectada y empleada en el proceso de auditoría.

Así como también toman un rol muy importante dentro de la auditoria las herramientas asistidas por computadora CAATs “usadas para evaluar la integridad de una aplicación, determinar la conformidad con procedimientos y monitorear los resultados de procesamientos.

Ventajas

- ✓ Actualmente existen diversas técnicas de auditoría, algunas de las cuales permiten un seguimiento y rastreo continuo de las aplicaciones mediante las llamadas rutinas embebidas. Su nombre se debe a que estas son rutinas que se incluyen en el desarrollo de las aplicaciones con el fin de realizar durante el funcionamiento de la aplicación auditada un monitoreo de las diversas transacciones y también se suele incluir un módulo anexo para obtener estadísticas e informes de dichas transacciones. Dado la naturaleza de estas técnicas la información se provee de primera mano, lo cual es una clara ventaja a la hora de realizar los análisis de las transacciones de la aplicación.

- ✓ Garantiza el cumplimiento de las normas legislativas y de la organización y en cualquier momento es posible ingresar, modificar, eliminar criterios de evaluación de las diferentes modalidades de auditoría existentes, ubicando errores y posibles fraudes, disminuyendo considerablemente el riesgo de no-detección de los problemas.

- ✓ Leer y comparar los datos de la empresa permitiendo que estos permanezcan intactos para preservar la calidad e integridad, ubicar errores y posibles fraudes, limpiar y normalizar los datos para garantizar la coherencia y los resultados.
- ✓ Restringe el acceso a la información de la auditoria ya que define usuarios con permisos de ejecución, consulta según su cargo para acceder al sistema.

- ✓ Satisfacen requerimientos específicos de la auditoria como por ejemplo una rutina de muestreo para la selección de transacciones.

- ✓ Ayudan a la administración de la empresa en forma permanente al crear rutinas que realicen tareas de actualización de datos, manejo de base de datos de grandes volúmenes de información.

- ✓ No presenta limitaciones relacionales con el lenguaje de consulta que emplea, diseño de procedimientos específicos al sistema informático empleado para el registro de operaciones.

- ✓ Permite la verificación de controles de aplicación, tales como: secuencia, integridad, rango, validez fecha.

- ✓ Permite organizar datos, consolidarlos y totalizarlos en función de los objetivos perseguidos por el auditor.

- ✓ Se puede simular en paralelo los procedimientos a partir de los mismos datos de entrada, para comparar los resultados obtenidos con los ficheros de salida de la aplicación auditada, en la práctica esta herramientas son de gran importancia a la hora de mejorar la evaluación de las áreas examinadas ya que estas permiten realizar pruebas de cumplimiento y pruebas sustantivas, poseen herramientas y gráficos estadísticos, retroalimentan sus bases de conocimiento y presentan informes flexibles y dinámicos.

Desventajas

- ✓ Conocimiento amplio en lenguajes de programación.

- ✓ El desarrollo de rutinas embebidas implica mayor tiempo y costos en el desarrollo de las aplicaciones.

- ✓ El hecho de ser software a la medida este no se puede aplicar a otros sistemas ni a otras empresas.

- ✓ Dependen en gran medida del sistema actual en uso en la entidad auditada y además necesitan un mantenimiento continuo del sistema para lograr una adaptación a las posibles actualizaciones y cambios del mismo.
- ✓ Estos programas y su documentación, deben ser antes revisados por el auditor, para pasar por un proceso de prueba y ensayo en donde se determinara si el software cumple con todas las normas y requerimientos de la empresa.

- **Backup o vaciado de archivos:** La técnica Backup o vaciado de archivos le permite al auditor examinar el contenido de los archivos que se encuentran en el computador, esto se hará mediante una copia o vaciado de archivos en un medio de almacenamiento cualquiera.

Ventajas

- ✓ Al hacer una Backup de los archivos, el auditor observará detalladamente cada uno de estos, realizando a su vez transacciones, que más adelante se comparan con los archivos originales, permitiendo así, obtener un resultado veraz y efectivo de los datos evaluados.

- ✓ Esta técnica es de muy útil para hacer copias de los archivos y como soporte de los centros de PED (Procesamiento electrónico de los datos), evitando una posible destrucción parcial o total de los mismos.

Desventaja

- ✓ No sería ventajoso emplear esta técnica cuando exista demasiada información, pues aumentaría tiempo y por lo tanto habría retraso en la evaluación.

1.7.6. Técnicas para examinar programas aplicativos

- **Snapshot: Auditoría operativa y de sistemas de información, herramientas de diagnostico en tiempo record. (Imagen Instantánea):** Es una técnica que permite tomar una copia o una fotografía de la memoria de un proceso para llegar a la toma de decisiones en el momento de su actividad. Esta técnica tiene en cuenta los datos de entrada.

Ventajas

- ✓ Manejar grandes volúmenes de información al permitir tomar una copia de la memoria de un proceso.

- ✓ Maneja instrucciones para reconocer y registrar el flujo de transacciones.

- ✓ Se sigue todo un proceso entre el auditor y los analistas o desarrolladores para llegar al producto final en el cual el auditor recibe toda la

documentación de los procesos para finalmente realizar el análisis de los objetivos predefinidos en la auditoria.

- ✓ Manejo de una clave especial para el manejo de la información (datos de entrada).
- ✓ Los snapshots son mucho más rápidos que los backups anteriores ya que solo necesitan trabajar con porciones de datos alteradas.
- ✓ Se pueden crear varios snapshots ya que el tamaño en disco es menor a la base de datos original.
- ✓ Es más fácil trabajar con snapshots y mucho más rápido para realizar copias de seguridad y restauraciones al sistema.
- ✓ Se pueden recuperar datos, eliminados por la snapshot para reparar la base de datos principal.
- ✓ Tiene la capacidad de restaurar la base de datos utilizando esta herramienta.
- ✓ Facilita al auditor comprender los pasos de procesamiento, verificando el flujo lógico del programa.

Desventaja

- ✓ La indexación de texto completo no se admite en la Snapshot
- ✓ Si los datos de la snapshot cambian en periodos cortos no se lograra una diferencia con los backups tradicionales.
- ✓ No se puede deshabilitar la base de datos primaria ya que los snapshot están atados a esta.
- ✓ Requiere bastante conocimiento de PED y de programación de computador, consume bastante tiempo.

- **Mapping:** Es una técnica que utiliza una herramienta la cual permite evaluar cada una de las instrucciones de un programa, presentando reportes, tanto del número de veces que es ejecutada una instrucción como el tiempo que duró el procesador en ejecutarlas.

Ventajas

- ✓ Permite deshabilitar instrucciones ilegales.
- ✓ Identifica instrucciones que no son utilizadas, pues es una técnica segura que sirve como soporte al control de calidad de sistemas para medir eficiencia.
- ✓ Ejecuta procedimiento de depuración de software.

Desventajas

- ✓ La desventaja es que se requiere de conocimientos avanzados en programación para su desarrollo, consume demasiado tiempo y es costosa.

- **Tracing y flujograma de control:** El Tracing es una técnica muy importante en cuanto a los lenguajes de programación, puesto que identifica y muestra las instrucciones que fueron ejecutadas y en que secuencia aparecen.

  El flujograma de control es una técnica muy valiosa puesto que permite evaluar los sistemas de una forma integral, tanto en el aspecto funcional como en el de control.

Ventajas

- ✓ Periódicamente deben ser evaluados ciertos factores o elementos que de una u otra manera brinden confiabilidad al sistema informático, ya que los equipos pueden fallar y producir accidentes informáticos, los errores humanos y los actos intencionales siendo estos los más perjudiciales e importantes.
- ✓ Se puede verificar quienes han ingresado al sistema a qué tipo de información han tenido acceso, que tipo de modificaciones realizaron (fecha, hora, si elimino o modifico información), una gran ventaja a la hora de auditar las entradas al sistema por parte de los usuarios.
- ✓ Tracing obtiene un listado de las transacciones utilizadas, permitiéndole al auditor identificar fácilmente el cumplimiento de los objetivos.
- ✓ Los flujogramas Facilitan la tarea de comparar el funcionamiento manual con el sistema total, verificando que esté funcionando de la forma en cómo están en la documentación.

- ✓ Además los flujogramas de control son excelentes para el entrenamiento de nuevos auditores.

- ✓ El flujograma de control, detecta las deficiencias en materia de control y en el tipo operacional.

- **Comparación de código y control de cambio:** La técnica de comparación de códigos se la utiliza para comparar códigos de una misma versión con el fin de comprobar que estos estén funcionando de una manera correcta.

  Esta técnica debe ser aplicada cuando ya existe un control de cambio, de otra forma se debe buscar alternativas que permitan la búsqueda de la evidencia.

  La técnica de control de cambio es la que verifica el número de bytes de los programas.

  Estas dos técnicas básicamente Impiden que personas infructuosas se sometan a la alteración o cambio de programas, afectando de esta manera a la empresa.

  Ventajas

  - ✓ En el control de cambio, evita el aumento de instrucciones perjudiciales para la empresa. Además esta técnica es muy confiable en cuanto a integridad de los programas y respaldando así el contenido de archivos.

  - ✓ Una ventaja en cuanto a comparación de código es la de ofrecer mayor seguridad en el cambio de programas y librerías de programas.

  - ✓ Se puede obtener una clara identificación del origen de un hallazgo en el código fuente, en qué versión se originó, inclusive, quién estuvo a cargo de dicho cambio.

  Desventajas

  - ✓ La técnica de comparación de código no proporciona evidencia sobre confiabilidad de los archivos de datos ni sobre eficiencia de los programas.

  - ✓ La desventaja de la técnica de control de cambio es que exige un riguroso sistema de control interno.

- ✓ No es recomendable aplicarla en empresas pequeñas o desarrollos simples, por lo que puede dificultar notablemente la aplicación de dicha técnica, el esfuerzo y recursos necesarios pueden ser excesivos para al final no obtener resultados significativos.

- ✓ Debe existir un historial de versiones. De otra forma no es posible aplicar esta herramienta, ya sea que se lleve control sobre las versiones o comparación de código.

- **Análisis de la lógica del programa:** Esta técnica consiste en evaluar la lógica del programa y el contenido de su documentación de forma descriptiva.

Ventajas

- ✓ Es la técnica que mejor controla todas las particularidades de un programa.

- ✓ Describe detalladamente un programa.

Desventajas

- ✓ Seguridad de que la información es una representación exacta de los programas utilizados. Que la documentación no esté desactualizada.

- ✓ El auditor debe tener el conocimiento del lenguaje de programación utilizado, para cumplir rápidamente con los objetivos de la auditoria. Que los auditores y revisores fiscales tengan el conocimiento básico en lenguajes de programación para que tengan una buena comunicación con el ingeniero de sistemas o con el experto en el tema.

- ✓ El auditor debe conocer ampliamente todos los sistemas a evaluar para estar al tanto de la forma de la relación entre módulos y programas para tener una mejor comprensión del sistema total.

- ✓ Utilizado únicamente para la evaluación de módulos, porque resulta dificultoso en programas extensos y sofisticados.

2. METODOLOGIA

La metodología utilizada para realizar la auditoria de sistemas al proceso de contratación de TI y el Portal Web de la Empresa de Obras Sanitarias de la provincia de Obando EMPOOBANDO E.S.P. y de la Alcaldía Municipal de Ipiales, se encaminó por las necesidades emanadas por la Contraloría Departamental de Nariño, que a su vez se fundamenta en las facultades otorgadas por la resolución 444 de 2005 “Metodología del Proceso Auditor de la Constitución Política”.

Este tipo de metodología encaja en el tipo de investigación cuantitativa, ya que los resultados finales se obtienen de un proceso de análisis y calificación de tipo numérica de acuerdo a la importancia de distintas variables.

Es responsabilidad de la administración, el contenido de la información suministrada por la entidad y analizada por la Contraloría Departamental de Nariño y el equipo auditor conformado por los estudiantes Luis Eduardo Pantoja Rodríguez y Gerardo Antonio Ramos Goyes.

La responsabilidad del organismo de control consiste en producir un informe integral, que contenga el concepto sobre la gestión adelantada por la administración de la entidad, donde también se incluyen pronunciamientos sobre el acatamiento a las disposiciones legales, a la calidad y a la eficiencia del Sistema de Control Interno.

De conformidad con lo anterior, se planeó y ejecutó el trabajo de manera que el análisis y el resultado de las pruebas, proporcionarán una base razonable para fundamentar la opinión y los conceptos expresados en el Informe.

Por las características propias de los procesos de auditoría, la metodología que se siguió para cumplir los objetivos propuestos, es de tipo empírico, puesto que se realiza recolección y análisis de información, además se toma como fuente primaria de información la observación directa por parte del equipo auditor, también se estudian y aplican conceptos y esquemas teóricos, cabe mencionar que esta metodología se clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas de forma directa e inmediata.

La auditoría realizada por el equipo auditor en compañía del funcionario Delegado por la Contraloría Departamental de Nariño fue dividida en varias etapas así:

Etapa I. Familiarización con el entorno. En esta etapa se realiza el estudio previo perteneciente al inicio de la Auditoria, con el propósito de conocer en detalle la conformación como tal de la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y la Alcandía Municipal de Ipiales, específicamente en el proceso de contratación de TI que se lleva a cabo en estas dos entidades, junto con la implementación que se ha venido realizando del Portal Web como requerimiento tecnológico para el cumplimiento del decreto 1151 de 2008 del Programa de Conectividad de Gobierno en Línea.

Los resultados de la exploración permiten hacer la selección de las técnicas y metodologías de auditoría que se van a utilizar para su desarrollo.

El equipo auditor se rigió por los lineamientos y normas de auditoría de la Contraloría Departamental de Nariño, se realizaron visitas a las entidades, de las cuales se sacó el mayor provecho con la realización de observación directa, además de la aplicación de entrevistas y charlas de carácter formal e informal con los funcionarios de las dos entidades.

Etapa II. Planeación de la auditoría de sistemas. En esta etapa se realiza la planificación de todo el proceso que se requiere para la realización de la auditoría.

Las actividades que se realizaron dentro de esta etapa fueron:

1. Identificar el alcance y los objetivos de la Auditoría a realizar.

2. Realizar el estudio inicial en la Empresa de obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y en la Alcaldía Municipal de Ipiales, para recolectar datos sobre la actividad del proceso de contratación de TI y el cumplimiento del decreto 1151 de 2008 del Programa de Conectividad de Gobierno en Línea.

3. Determinar los recursos necesarios para realizar la auditoría.

4. Elaboración del plan de trabajo.

Etapa III. Realización de las actividades de la auditoría. En esta etapa se hacen efectivas todas las actividades descritas en la etapa anterior, con la aplicación de las técnicas y metodologías que garanticen el cumplimiento de los objetivos planeados.

Las actividades que se realizaron dentro de esta etapa fueron:

1. Elaboración del plan de auditoría, para identificar dentro de los dominios del COBIT, los procesos y los objetivos de control que se van a evaluar.

2. Elaboración de los cuadros de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría, para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.

3. Realización de pruebas sobre los procesos seleccionados.

4. Elaboración de los cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.

5. Identificación de hallazgos dentro de los procesos evaluados.

6. Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.

7. Análisis del cumplimiento del decreto 1151 de 2008 del Programa de conectividad de Gobierno en Línea.

Etapa IV. Presentación del informe final. En esta etapa se realiza el informe final, en donde se describen los hallazgos encontrados y se hacen las recomendaciones pertinentes para subsanar dichas falencias, también se relacionan que partes del proceso de contratación de TI se encuentran funcionando sin ningún problema, para que las entidades identifiquen donde deben realizar las correcciones oportunas, además se produjo el informe donde se indica cómo se debe elaborar El Portal Web para que cumpla con los lineamientos establecidos en el decreto 1151 de 2008 del Programa de Conectividad de Gobierno en Línea.

Una vez elaborados los informes se dan a conocer a la Contraloría Departamental de Nariño para que esta a su vez los haga llegar a la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y a la Alcaldía Municipal de Ipiales respectivamente, para que se realicen las actividades de corrección necesarias.

4. DESARROLLO DEL TRABAJO

4.1. ARCHIVO PERMANENTE

El archivo permanente es la colección de documentos cuya información es válida en el tiempo y no es exclusiva de un periodo específico en el tiempo.

4.1.1 Leyes y decretos comunes. En este apartado se citaran las leyes y decretos que regularon el proceso de auditoría en las dos entidades.

EMPOOBANDO E.S.P., al ser una empresa dedicada a la prestación de servicios públicos domiciliarios ha sido encaminada a cumplir con ciertas leyes y normatividades que permitan el buen desarrollo de sus actividades, como son; la prestación eficiente y efectiva del servicio de agua potable a la comunidad de Ipiales y todos sus alrededores; cumplir con la rendición de cuentas por ser administración que utiliza recursos presupuestales del Estado; informar de manera oportuna y transparente tanto a la comunidad de Ipiales como a las entidades de control del estado. De esta manera EMPOOBANDO E.S.P podrá cumplir a cabalidad con sus objetivos establecidos a partir de su constitución como tal, de una forma clara y transparente ante los organismos de control.

EMPOOBANDO E.S.P., está sujeto a cumplir con la **ley 142 de 1994** de servicios públicos y algunas modificaciones de sus artículos. La ley 142 contempla 189 artículos divididos en diez (10) títulos, dentro de los cuales se estipula como debe manejarse la comunicación con las entidades de control, que para su objeto social es la Superintendencia de Servicios Públicos; la intervención del estado; las tarifas que se deben ajustar a los suscriptores del servicio, entre otros.

Dentro de la ley 142 se dispone del **título II** Regímenes de actos y contratos y Contratos Especiales para la gestión de los servicios públicos, el cual consta de 10 artículos en donde se establece la parte contractual de las empresas de servicios públicos.

El artículo 31. Régimen contractual define:
“Los contratos que celebren las entidades estatales que prestan los servicios públicos a los que se refiere esta ley no estarán sujetos a las disposiciones del Estatuto General de Contratación de la Administración Pública, salvo en lo que la presente ley disponga otra cosa.

Las Comisiones de Regulación podrán hacer obligatoria la inclusión, en ciertos tipos de contratos de cualquier empresa de servicios públicos, de cláusulas exorbitantes y podrán facultar, previa consulta expresa por parte de las empresas de servicios públicos domiciliarios, que se incluyan en los demás. Cuando la inclusión sea forzosa, todo lo relativo a tales cláusulas se regirá, en cuanto sea pertinente, por lo dispuesto en la Ley 80 de 1993, y los actos y contratos en los que se utilicen esas cláusulas y/o se ejerciten esas facultades estarán sujetos al control de la jurisdicción contencioso administrativa.

Las Comisiones de Regulación contarán con quince (15) días para responder las solicitudes elevadas por las empresas de servicios públicos domiciliarios sobre la inclusión de las cláusulas excepcionales en los respectivos contratos, transcurrido este término operará el silencio administrativo positivo."

Este articulo fue modificado a través del artículo 3 de la ley 689 del 2001 publicada en el diario oficial Nro. 44.537, de agosto del 2001.

Articulo 39. Contratos especiales. Define:

"Para los efectos de la gestión de los servicios públicos se autoriza la celebración, entre otros, de los siguientes contratos especiales:
39.1.- Contratos de concesión para el uso de recursos naturales o del medio ambiente. El contrato de concesión de aguas, es un contrato limitado en el tiempo, que celebran las entidades a las que corresponde la responsabilidad de administrar aquellas, para facilitar su explotación o disfrute. En estos contratos se pueden establecer las condiciones en las que el concesionario devolverá el agua después de haberla usado.

El acceso al espectro electromagnético para el servicio público de telecomunicaciones puede otorgarse por medio de un contrato de concesión, de acuerdo con la Ley 80 de 1993 y las leyes especiales pertinentes, pero sin que se aplique el artículo 19 de la Ley 80 de 1993 a bienes distintos de los estatales.
La remuneración que se pacte por una concesión o licencia ingresará al presupuesto de la entidad pública que celebre el contrato o expida el acto.
Cuando las autoridades competentes consideren que es preciso realizar un proyecto de interés nacional para aprovechamiento de aguas, o para proyectos de saneamiento, podrán tomar la iniciativa de invitar públicamente a las empresas de servicios públicos para adjudicar la concesión respectiva.
Las concesiones de agua caducarán a los tres años de otorgadas, si en ese lapso no se hubieren hecho inversiones capaces de permitir su aprovechamiento económico dentro del año siguiente, o del período que determine de modo general, según el tipo de proyecto, la comisión reguladora.
Los contratos de concesión a los que se refiere este numeral se regirán por las normas especiales sobre las materias respectivas.

39.2.- Contratos de administración profesional de acciones. Son aquellos celebrados por las entidades públicas que participan en el capital de empresas de servicios públicos, para la administración o disposición de sus acciones, aportes o inversiones en ellas, con sociedades fiduciarias, corporaciones financieras, organismos cooperativos de grado superior de carácter financiero, o sociedades creadas con el objeto exclusivo de administrar empresas de servicios públicos. Las tarifas serán las que se determinen en un proceso de competencia para obtener el contrato.
En estos contratos puede encargarse también al fiduciario o mandatario de vender las acciones de las entidades públicas en las condiciones y por los procedimientos que el contrato indique.
A los representantes legales y a los miembros de juntas directivas de las entidades que actúen como fiduciarios o mandatarios para administrar acciones de empresas de servicios públicos se aplicará el régimen de incompatibilidades e inhabilidades de los funcionarios que hayan celebrado con ellos el contrato respectivo, en relación con tales empresas.

39.3.- Contratos de las entidades oficiales para transferir la propiedad o el uso y goce de los bienes que destina especialmente a prestar los servicios públicos; o concesiones o similares; o para encomendar a terceros cualquiera de las actividades que ellas hayan realizado para prestar los servicios públicos; o para permitir que uno o más usuarios realicen las obras necesarias para recibir un servicio que las entidades públicas estén prestando; o para recibir de uno o más usuarios el valor de las obras necesarias para prestar un servicio que las entidades oficiales estén prestando; o para pagar con acciones de empresas los bienes o servicios que reciban.

39.4.- Contratos en virtud de los cuales dos o más entidades prestadoras de servicios públicos o éstas con grandes proveedores o usuarios, regulan el acceso compartido o de interconexión de bienes indispensables para la prestación de servicios públicos, mediante el pago de remuneración o peaje razonable.
Este contrato puede celebrarse también entre una empresa de servicios públicos y cualquiera de sus grandes proveedores o usuarios.
Si las partes no se convienen, en virtud de esta Ley la comisión de regulación podrá imponer una servidumbre de acceso o de interconexión a quien tenga el uso del bien.

39.5.- Contratos para la extensión de la prestación de un servicio que, en principio, sólo beneficia a una persona, en virtud del cual ésta asume el costo de las obras respectivas y se obliga a pagar a la empresa el valor definido por ella, o se obliga a ejecutar independientemente las obras requeridas conforme al proyecto aprobado por la empresa.

PARÁGRAFO. Salvo los contratos de que trata el numeral 39.1., todos aquéllos a los que se refiere este artículo se regirán por el derecho privado.

Los que contemplan los numerales 39.1., 39.2. y 39.3., no podrán ser cedidos a ningún título, ni podrán darse como garantía, ni ser objeto de ningún otro contrato, sin previa y expresa aprobación de la otra parte."

De acuerdo con lo anterior todos los demás tipos de contratos que adquiera una empresa prestadora de servicios públicos se harán con lo que rige el artículo 32 de la **ley 80 de 1993** el cual define:

"Son contratos estatales todos los actos jurídicos generadores de obligaciones que celebren las entidades a que se refiere el presente estatuto, previstos en el derecho privado o en disposiciones especiales, o derivados del ejercicio de la autonomía de la voluntad, así como los que, a título enunciativo, se definen a continuación:

1o. Contrato de obra.
Son contratos de obra los que celebren las entidades estatales para la construcción, mantenimiento, instalación y, en general, para la realización de cualquier otro trabajo material sobre bienes inmuebles, cualquiera que sea la modalidad de ejecución y pago. En los contratos de obra que hayan sido celebrados como resultado de un proceso de licitación o concurso públicos, la interventoría deberá ser contratada con una persona independiente de la entidad contratante y del contratista, quien responderá por los hechos y omisiones que le fueren imputables en los términos previstos en el artículo 53 del presente estatuto.

2o. Contrato de consultoría
Son contratos de consultoría los que celebren las entidades estatales referidos a los estudios necesarios para la ejecución de proyectos de inversión, estudios de diagnóstico, pre factibilidad o factibilidad para programas o proyectos específicos, así como a las asesorías técnicas de coordinación, control y supervisión.
Son también contratos de consultoría los que tienen por objeto la interventoría, asesoría, gerencia de obra o de proyectos, dirección, programación y la ejecución de diseños, planos, anteproyectos y proyectos. Ninguna orden del interventor de una obra podrá darse verbalmente. Es obligatorio para el interventor entregar por escrito sus órdenes o sugerencias y ellas deben enmarcarse dentro de los términos del respectivo contrato.

3o. Contrato de prestación de servicios
Son contratos de prestación de servicios los que celebren las entidades estatales para desarrollar actividades relacionadas con la administración o funcionamiento de la entidad. Estos contratos sólo podrán celebrarse con personas naturales cuando dichas actividades no puedan realizarse con personal de planta o requieran conocimientos especializados.
En ningún caso estos contratos generan relación laboral ni prestaciones sociales y se celebrarán por el término estrictamente indispensable.

4o. Contrato de concesión
Son contratos de concesión los que celebran las entidades estatales con el objeto de otorgar a una persona llamada concesionario la prestación, operación, explotación, organización o gestión, total o parcial, de un servicio público, o la construcción, explotación o conservación total o parcial, de una obra o bien destinados al servicio o uso público, así como todas aquellas actividades necesarias para la adecuada prestación o funcionamiento de la obra o servicio por cuenta y riesgo del concesionario y bajo la vigilancia y control de la entidad concedente, a cambio de una remuneración que puede consistir en derechos, tarifas, tasas, valorización, o en la participación que se le otorgue en la explotación del bien, o en una suma periódica, única o porcentual y, en general, en cualquier otra modalidad de contraprestación que las partes acuerden."

En concordancia con la ley 80 de 1993 se dispone la ley **1150 del 2007** por medio de la cual se introducen medidas para la eficiencia y la transparencia en la ley 80 y se dictan otras disposiciones generales sobre la contratación con recursos públicos.

Fundamentalmente se establecen con el título I **DE LA EFICIENCIA Y DE LA TRANSPARENCIA**

ARTÍCULO 2. DE LAS MODALIDADES DE SELECCIÓN. "La escogencia del contratista se Efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos y contratación directa, con base en las reglas estipuladas dentro de la ley en mención."

ARTÍCULO 3. DE LA CONTRATACIÓN PÚBLICA ELECTRONICA. "De conformidad con lo dispuesto en la Ley 527 de 1999, la sustanciación de las actuaciones, la expedición de los actos administrativos, los documentos, contratos y en general los actos derivados de la actividad precontractual y contractual, podrán tener lugar por medios electrónicos. Para el trámite, notificación y publicación de tales actos, podrán utilizarse soportes, medios y aplicaciones electrónicas. Los mecanismos e instrumentos por medio de los cuales las entidades cumplirán con las obligaciones de publicidad del proceso contractual serán señalados por el Gobierno Nacional.

Lo anterior, sin perjuicio de las publicaciones previstas en el numeral 3 del artículo 30 de la Ley 80 de 1993. Con el fin de materializar los objetivos a que se refiere el inciso anterior, el Gobierno Nacional desarrollará el Sistema Electrónico para la Contratación Pública, SECOP, el cual:

a) Dispondrá de las funcionalidades tecnológicas para realizar procesos de contratación electrónicos bajo los métodos de selección señalados en el artículo 2° de la presente ley según lo defina el reglamento;

b) Servirá de punto único de ingreso de información y de generación de reportes para las entidades estatales y la ciudadanía;

c) Contará con la información oficial de la contratación realizada con dineros públicos, para lo cual establecerá los patrones a que haya lugar y se encargará de su difusión a través de canales electrónicos e;

d) Integrará el Registro Único Empresarial de las Cámaras de Comercio, el Diario Único de Contratación Estatal y los demás sistemas que involucren la gestión contractual pública. Así mismo, se articulará con el Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, creado por la **Ley 598 de 2000**, sin que este pierda su autonomía para el ejercicio del control fiscal a la contratación pública."

Con respecto a la contratación y a lo establecido en la ley 1150 del 2007 de la eficiencia y la transparencia también entra a regir a las empresas de servicios públicos que manejan dineros del estado lo estipulado en la ley 598 del 2000 por la cual se crean el Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, el Catálogo Único de Bienes y Servicios, CUBS, y el Registro Único de Precios de Referencia, RUPR, de los bienes y servicios de uso común en la Administración Pública y se dictan otras disposiciones.
Para tal efecto se debe conocer los ingresos presupuestales que percibe la empresa de obras sanitarias de la provincia de Obando EMPOOBANDO E.S.P. y la Alcaldía Municipal de Ipiales, para poder establecer los contratos de mayor y menor cuantía, que son los contratos que se tendrán en cuenta para ser publicados a través del sistema de información de la contratación estatal SICE y el SECOP.

Según lo estipulado en el artículo 2., numeral 2. SELECCIÓN ABREVIADA numeral b) "La contratación de menor cuantía. Se entenderá por menor cuantía los valores que a continuación se relacionan, determinados en función de los presupuestos anuales de las entidades públicas expresados en salarios mínimos legales mensuales.

Para las entidades que tengan un presupuesto anual superior o igual a 1.200.000 salarios mínimos legales mensuales, la menor cuantía será hasta 1.000 salarios mínimos legales mensuales.

Las que tengan un presupuesto anual superior o igual a 850.000 salarios mínimos legales mensuales e inferiores a 1.200.000 salarios mínimos legales mensuales, la menor cuantía será hasta 850 salarios mínimos legales mensuales.

Las que tengan un presupuesto anual superior o igual a 400.000 salarios mínimos legales mensuales e inferior a 850.000 salarios mínimos legales mensuales, la menor cuantía será hasta 650 salarios mínimos legales mensuales.

Las que tengan un presupuesto anual superior o igual a 120.000 salarios mínimos legales mensuales e inferior a 400.000 salarios mínimos legales mensuales, la menor cuantía será hasta 450 salarios mínimos legales mensuales.

Las que tengan un presupuesto anual inferior a 120.000 salarios mínimos legales mensuales, la menor cuantía será hasta 280 salarios mínimos legales mensuales;"[13]

Leyes

Las leyes que rigen la contratación son los siguientes.

- Ley 142 de 1994
- Ley 80 de 1993
- Ley 1150 del 2007
- Ley 598 del 2000

Decretos

El decreto que rige los estatutos de implementación del Portal Web es el siguiente.

- Decreto 1151 del 2008 del Programa de Conectividad de Gobierno en Línea.

4.1.2. Empresa de obras sanitarias de la provincia de Obando EMPOOBANDO E.S.E

- **Antecedentes. EMPOOBANDO E.S.P.,** es una empresa de Servicios Públicos Domiciliarios de toda la comunidad de Ipiales y sus alrededores, que se dedica a la producción integral de agua, manejo de redes de acueducto y

[13], http://www2.igac.gov.co/igac_web/UserFiles/File/web%202008%20/ley%2080-93.pdf

alcantarillado y conservación del medio ambiente, satisfaciendo así las necesidades de todos los usuarios y contribuyendo al mejoramiento en la calidad de vida de la comunidad.
Ejecutando proyectos que abarcan obras como la reposición de redes en sectores donde se impulsa los proyectos de pavimentación y que necesariamente requieren de los acabados para garantizar la movilidad vehicular y peatonal, construcción de redes para ampliar la cobertura de servicio y garantizar el desarrollo urbanístico de predios destinados a vivienda principalmente de interés social.

De igual manera EMPOOBANDO E.S.P., se encarga de la administración y mantenimiento de las redes de acueducto y alcantarillado, para tal fin se cuenta con una cuadrilla permanente que atiende y soluciona oportunamente los daños y coordina diariamente el mantenimiento de las mismas, el mantenimiento permanente de las unidades de sumideros en el centro de la ciudad y participación en planes de contingencia para eventos masivos como las festividades de Ipiales y Corregimiento de las Lajas.

La empresa ha estado comprometida con garantizar un servicio de óptima calidad y este objetivo se puede corroborar en los análisis que se realizan en el Laboratorio de Control de Calidad de Agua Potable de EMPOOBANDO E.S.P; laboratorio que se encuentra autorizado por el Ministerio de Protección Social, es así que desde el año 2008 hasta la fecha los resultados se han clasificado dentro del nivel de Sin Riesgo según lo indica la resolución 2115 de 2007, de esta forma están trabajando para llevar a los ipialeños agua apta para el consumo humano.

- **Misión:** "**EMPOOBANDO E.S.P.,** es una empresa de Servicios Públicos Domiciliarios de todos, que se dedica a la producción integral de agua, manejo de redes de acueducto y alcantarillado y conservación del ambiente, satisfaciendo así las necesidades de nuestros usuarios y contribuyendo al mejoramiento en la calidad de vida de la comunidad".

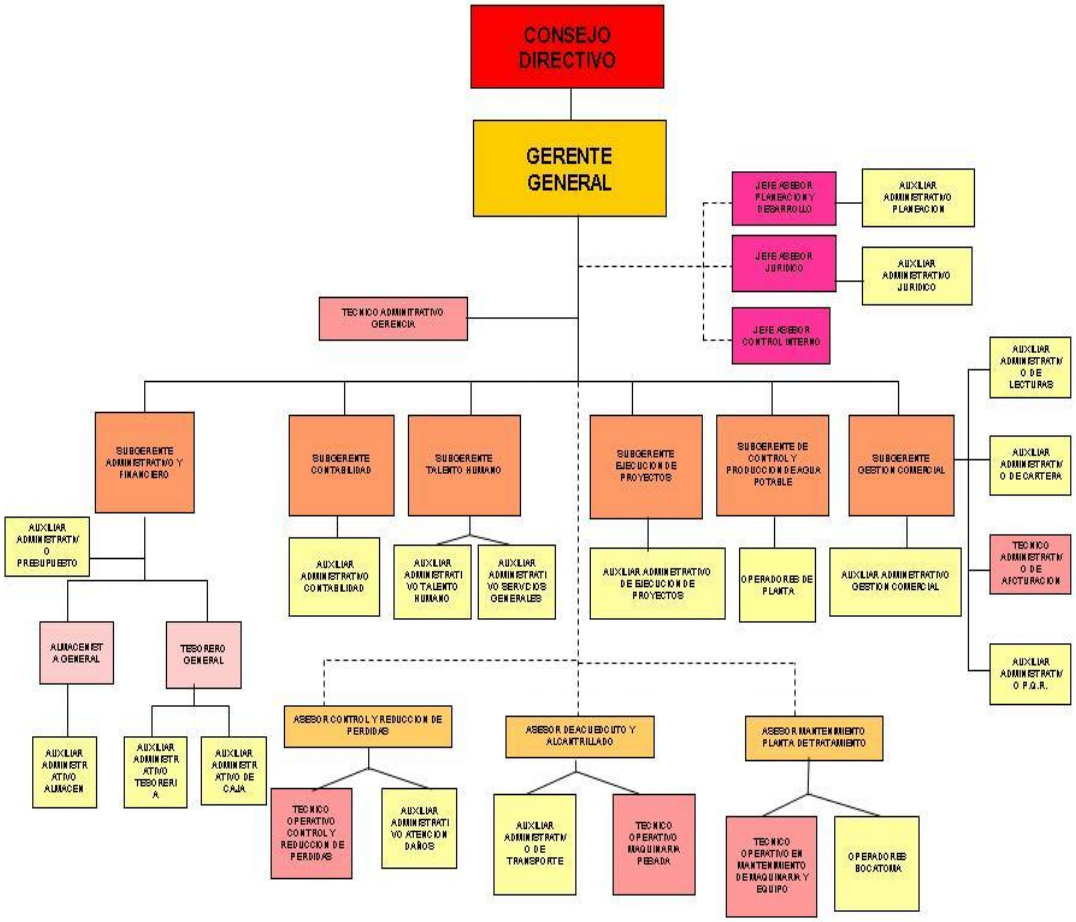
- **Visión:** "En el año 2011 seremos una empresa certificada en normas de calidad, con una política ambiental enfocada hacia el manejo integral del recurso hídrico, con Talento Humano capacitado y comprometido con la cultura del servicio generando satisfacción social".

- **Objetivos de calidad:** Para poder alcanzar la visión que tiene EMPOOBANDO se compromete a lo siguiente:

- ✓ “Mejorar la calidad, cobertura y continuidad en la prestación del servicio de acueducto y alcantarillado con eficiencia enfocada a satisfacer los requisitos legales, corporativos y de todos los usuarios.
- ✓ Garantizar un trato amable y cordial a todos los usuarios, además brindar información veraz y oportuna.
- ✓ Sensibilizar al usuario mediante campañas educativas sobre el uso racional del agua y los procesos internos de la Empresa.
- ✓ Contar con un talento humano competente y comprometido con la comunidad para brindar un servicio oportuno.
- ✓ Mejorar continuamente la eficiencia, eficacia y efectividad de los procesos a través del Sistema Integrado de Gestión (SIG) y de la Gestión Integral del Recurso Hídrico (GIRH).
- ✓ Garantizar la sostenibilidad financiera que permita la cobertura, calidad y continuidad del servicio.
- ✓ Actualización permanente de nuestros funcionarios para el mejoramiento continúo en la prestación del servicio.
- ✓ Garantizar que las actividades de la empresa se lleven en forma segura.
- ✓ Formular e implementar los planes ambientales para la Gestión Integral del Recurso Hídrico PSMV y PUEAA.
- ✓ Nos comprometemos a resolver en forma oportuna las peticiones, quejas y reclamos generados por el servicio”.

- **Organigrama de la empresa de obras sanitarias de la provincia de Obando EMPOOBANDO E.S.P.**

Figura 2. Organigrama EMPOOBANDO.



4.1.3. Alcaldía municipal de ipíales.

- **Misión:** "El Municipio de Ipiales es una entidad territorial fundamental de la división político administrativa del Estado, con autonomía política, fiscal y administrativa dentro de los límites que lo señalen la Constitución y la ley y cuya finalidad es el bienestar general y el mejoramiento de la calidad de vida de la población en su respectivo territorio", contando con el talento humano competente, en el marco de los principios de eficacia, eficiencia, publicidad, transparencia, moralidad, responsabilidad e imparcialidad.

- **Visión:** En el 2011 Ipiales será un municipio moderno, equitativo, agradable, ordenado y seguro, donde se generen las oportunidades de desarrollo, con capacidad territorial y competitividad humana, que mejoren y sustenten su calidad de vida en el marco de la globalización; sustentadas en la participación constructiva, alianza-público-privado, respeto, transparencia y gobernabilidad. Se destacará como un proveedor importante de alimentos en los mercados externos.

- **Políticas de calidad:** Con el fin de generar confianza al ciudadano, nuestros procesos están orientados a satisfacer las necesidades de nuestros usuarios y beneficiarios. Para su logro en la Administración Central del Municipio de Ipiales, estamos comprometidos a:

  - ✓ Garantizar la prestación de servicios con eficacia y eficiencia, en los términos de la constitución y la Ley.
  - ✓ Fomentar y propiciar los espacios de participación social en la toma de decisiones que los afecten.
  - ✓ Generar una cultura de servicio en la entidad, basada en la mejora continua de los procesos, la adecuada gestión de los recursos, autocontrol y compromiso con los principios éticos.

- **Objetivos de Calidad**

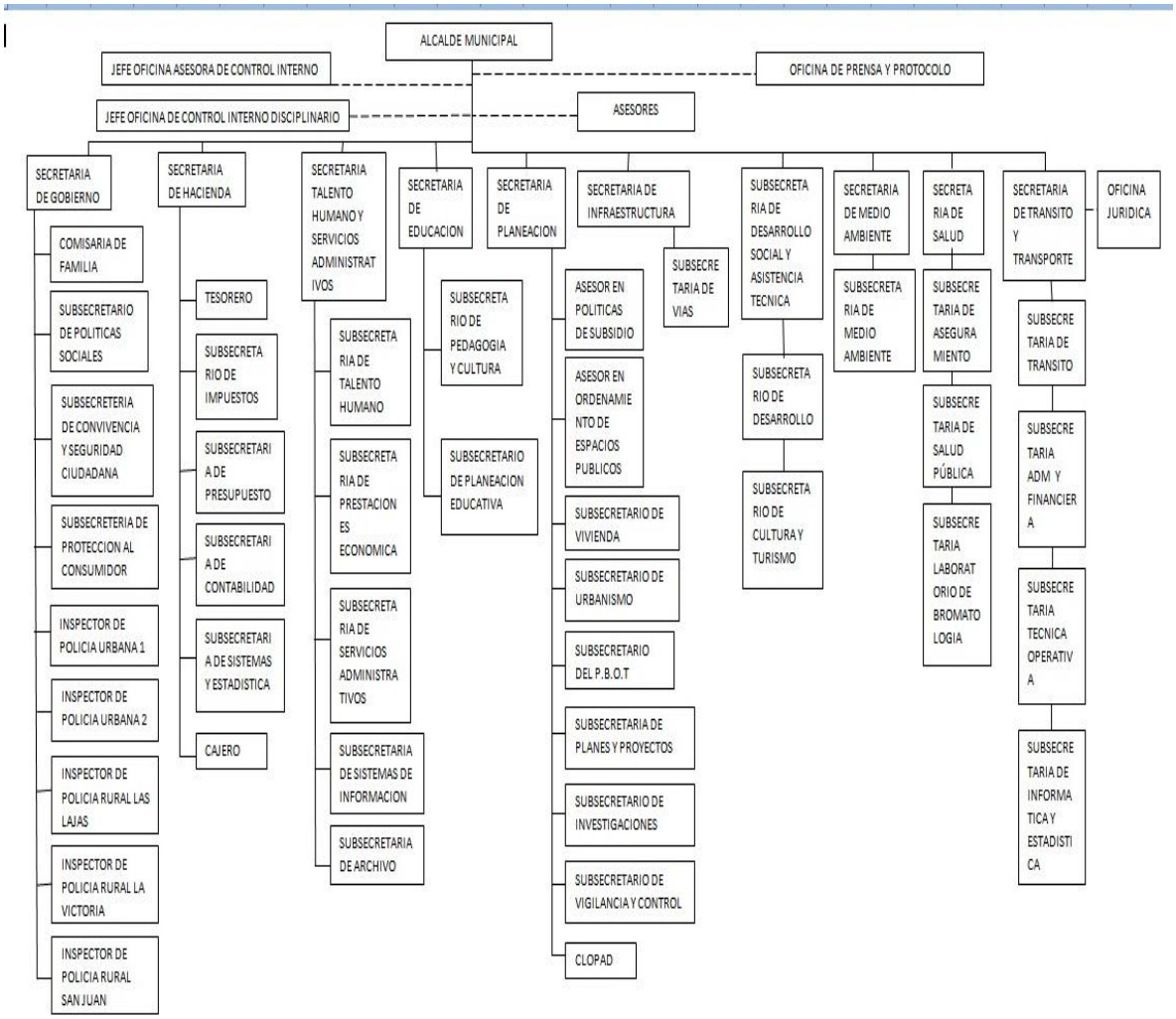
  - ✓ Incrementar el nivel de competencia y liderazgo en los servicios públicos de la Administración Central Municipal.

  - ✓ Fomentar y propiciar los espacios de participación social en la toma de decisiones que los afecten.

- ✓ Aumentar el grado de satisfacción de la atención y servicios prestados a las personas, familias y comunidades del Municipio de Ipiales.

- **Organigrama Alcaldía municipal de Ipiales.**

Figura 3. Organigrama Alcaldía de Ipiales



- **Manual de funciones de alcaldía municipal de ipíales (Comité de contratación):** Se transcribió el manual de funciones del comité de contratación extraído del manual de funciones general de la Alcaldía Municipal de Ipiales.

I. IDENTIFICACION

Nivel:	Asesor
Denominación del Empleo:	Jefe de Oficina Jurídica
Código:	115
Grado:	01
Número de Cargos:	Uno (1)
Dependencia:	Oficina Asesora Jurídica
Cargo del Jefe Inmediato:	Alcalde Municipal

II. PROPÓSITO PRINCIPAL

Brindar asesoría jurídica a la entidad, conceptuar y adelantar los procesos jurídicos internos y externos requeridos con el fin de que la administración cumpla con sus funciones dentro del marco exigido por la constitución nacional y las normas vigentes y la adecuada defensa de los intereses del estado.

III. DESCRIPCION DE FUNCIONES ESENCIALES

1. Interpretar y aplicar textos legales, jurisprudencia y doctrinas con el fin dar fundamento jurídico a las decisiones emitidas por el despacho del señor Alcalde y/o dependencias del nivel central que lo requieran.
2. Revisar el contenido jurídico de documentos relacionados con trámites administrativos a fin de garantizar su validez.
3. Emitir conceptos y absolver consultas sobre diversas situaciones de derecho originadas en los actos oficiales del municipio y aclarar situaciones jurídicas relacionadas con la interpretación y aplicación de la ley.
4. Asesora al despacho del Alcalde y demás dependencias en el trámite y solución de los asuntos jurídicos relacionados con la administración.
5. Asesorar en los asuntos que le sean encomendados con el propósito de fijar la posición jurídica de la Entidad.
6. Proyectar y revisar los actos administrativos y los documentos contractuales que se le encarguen de acuerdo con la normatividad vigente.
7. Apoyar el desarrollo de procesos de contratación y asistir a las diligencias que se le encarguen de forma que se cumplan los términos y condiciones previstas en la ley y se respeten los principios de la contratación pública.
8. Representar jurídicamente al municipio, en los procesos en que sea parte, cuando así lo disponga el Alcalde, e informar sobre el desarrollo de los mismos.
9. Elaborar y revisar los proyectos de decreto, resoluciones, acuerdos y demás actos administrativos que expida la administración municipal y verificar que se encuentren conforme a la ley.
10. Elaborar y revisar los contratos que sean necesarios para el normal funcionamiento de la administración cumpliendo los requisitos en las

normas de contratación estatal y aquellas de régimen especiales que deban aplicarse.

11. Asistir y asesorar a la administración Central en los asuntos de su competencia.
12. Mantenerse actualizado en cuanto a la legislación, la jurisprudencia y la doctrina para que sus actuaciones, documentos y conceptos den seguridad jurídica para la toma de decisiones.
13. Recopilar y mantener actualizadas las normas legales relacionadas con la administración municipal y velar por su adecuada difusión.
14. Presentar los informes en el ámbito administrativo que sean requeridos por las diferentes aéreas de la entidad y por las entidades externas que lo requieran.
15. Cumplir los indicadores de gestión, estándares de desempeño, mecanismos de evaluación y control a los procesos que desarrolle en el cumplimiento de las funciones propias del cargo.
16. Desempeñar las demás funciones que le sean asignadas por sus superiores para el cumplimiento de la misión de la Entidad, de acuerdo con la naturaleza, propósito principal y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. Intervención oportuna y eficaz en los procesos judiciales y extrajudiciales en los que sea parte el Municipio.
2. Conceptos fundamentados legal, doctrinal y jurisprudencialmente.
3. Conceptos jurídicos oportunos, pertinentes, claros y precisos acorde con la normatividad y la jurisprudencia vigentes.
4. Actos administrativos y documentos contractuales que respetan las normas vigentes emitidas de forma oportuna.
5. Actuaciones administrativas y procesos de contratación llevados de forma coherente, organizada, completa y dentro del marco de legalidad establecido en las normas vigentes.
6. Los documentos de las actuaciones administrativas y los procesos contractuales se organizan, custodian, y conservan para garantizar información completa y actual.
7. Informes consolidados sobre asuntos a su cargo presentados con oportunidad y claridad que influyan análisis y recomendaciones para el mejoramiento de la actividad en la Entidad.
8. Las actuaciones y los documentos judiciales elaborados con base en la normatividad vigente y la jurisprudencia procuran la defensa integral del estado.
9. Los documentos proyectados reflejan el análisis juicioso de cada caso a la luz de las normas legales, la jurisprudencia y la doctrina y dan seguridad en las actuaciones que adelante el municipio.
10. Distribución equitativa de los asuntos entre el personal de la oficina.

11. Control de calidad y de rendimiento de los trabajos realizados por los subalternos.
12. Actualización normativa.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Constitución Nacional.
2. Derecho Administrativo, civil, laboral, tributario.
3. Ley 80 de 1.993- Estatuto de Contratación Administrativa y las demás normas que lo modifican, completan o adicionan.
4. Ley 189 – 1.898 Legislación Indígena.
5. Régimen legal de la Administración Municipal.
6. Doctrina y Jurisprudencia Colombiana.
7. Acuerdos, Decretos y Resoluciones Municipales.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Título Profesional en Derecho y Tarjeta Profesional.	Un (1) año de experiencia profesional o relacionada con el cargo.

I. IDENTIFICACION

Nivel: Directivo
Denominación del Empleo: Subsecretario del Sistema de Información
Código: 45
Grado: 05
Número de Cargos: Uno (1)
Dependencia: Secretaria de Talento Humano y Servicios Administrativos.
Cargo del Jefe Inmediato: Secretario de Despacho (Talento Humano y Servicios Administrativos)

II. PROPOSITO PRINCIPAL

Dirigir y realizar las actualizaciones necesarias para la implementación y consolidación de los sistemas de información que sirvan de herramienta para el adecuado control de los procesos y actividades administrativas del municipio, en especial en lo que tiene que ver con el sistema de información para la vigilancia de la contratación estatal SICE y apoyar al Secretario de Talento Humano y Servicios Administrativos en la formulación, coordinación y seguimiento de las políticas, planes y programas relativos a las gestiones encomendadas al despacho a su cargo.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES:

1. Dirigir y coordinar las acciones para la implementación y consolidación de los sistemas de información mediante la obtención, ajuste y codificación de la información para que estos funcionen de manera adecuada.
2. Establecer y adoptar las medidas para codificar y ajustar el Plan de Compras de manera que cumpla con los requerimientos necesarios para su envió al SICE.
3. Definir los planes de mantenimiento y soporte, adoptarlos y aplicarlos con el fin que las aplicaciones, y en especial el SICE funcionen correctamente.
4. Realizar los ajustes que se requieran para que las aplicaciones sean eficientes y estén actualizadas y para tal efecto, crear, modificar y eliminar usuarios con sus respectivos roles según se quiera en la administración del sistema.
5. Publicar en cartera e internet las convocatorias para contratación que de acuerdo con las necesidades de la Alcaldía Municipal se presenten.
6. Recibir las publicaciones de ofertas y consultar los precios indicativos pre adjudicación de la propuesta para los contratos del Nivel Central.
7. Hacer las verificaciones que se estime necesarias, mediante la consulta en el portal del SICE para la gestión a su cargo se realice conforme las normas vigentes y asesorar sobre los ajustes o cambios que se deban tener en cuenta.

8. Presentar los informes en el ámbito administrativo que sean requeridos por las diferentes áreas de la Entidad y por las entidades externas que lo requieran.
9. Cumplir los indicadores de gestión, estándares de desempeño, mecanismos de evaluación y control a los procesos que desarrolle en el cumplimiento de las funciones propias del cargo.
10. Desempeñar las demás funciones que le sean asignadas por sus superiores para el cumplimiento de la misión de la Entidad, de acuerdo con la naturaleza, propósito principal y área de desempeño del cargo.
11. Administración de la información requerida por los entes de control de la contratación pública (informes Contraloría).
12. Apoyo administrativo en cuanto a normatividad requerida por las diferentes Subsecretarias.

IV. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. Las acciones de implementación y consolidación de los sistemas de información permite contar con herramientas actualizadas y eficientes para el manejo de las actividades.
2. La información del plan de compras esta adecuada los requerimientos técnicos necesarios y esta adecuadamente realizado para que sea útil para el SICE.
3. Los planes de mantenimiento se cumplen y las actividades de soporte permiten que los sistemas funcionen adecuadamente.
4. Los sistemas cuenten con los ajustes y modificaciones para hacerlos eficientes.
5. Las verificaciones se hacen de manera constante y permiten tener la información actualizada sobre el funcionamiento del sistema, los cambios, ajustes y novedades.
6. Los informes presentados son claros, completos y oportunos.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Ley 598 de julio 18/2.000: Creación del SICE.
2. Ley 80 de octubre 28/1.993: Contratación de la Administración Pública.
3. Decreto 3512 de diciembre 05/2.003: Reglamenta la organización y funciones para la operación del SICE.
4. Decreto 2170 de septiembre 30/2.002 regulación de la contratación de la Administración Pública.
5. Acuerdos y circulares emitidas por la Gerencia del SICE.
6. Ley 80 del 93.
7. Fundamentos de Administración Pública.
8. Sistemas de Información.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Título Profesional o Tecnólogo en Ingeniería de Sistemas.	Un (1) año de experiencia profesional o relacionada con el cargo.

I. IDENTIFICACION

Nivel: Directivo
Denominación del Empleo: Subsecretario de Sistemas y Estadísticas
Código: 45
Grado: 04
Número de Cargos: Uno (1)
Dependencia: Secretaria de Hacienda
Cargo del Jefe Inmediato: Secretario de Despacho (Hacienda)

II. PROPÓSITO PRINCIPAL

Dirigir y aplicar los procesos de sistematización de la información y estadística del nivel central y descentralizado del municipio, con el fin de agilizar y mantener actualizada la información contable, presupuestal y de bienes.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Diseñar, actualizar y optimizar los programas necesarios para el manejo de la información contable, presupuestal y de bienes.
2. Transferir electrónicamente las nóminas del personal de la Alcaldía Municipal y todas sus dependencias. Implementar programas de estadísticas para el análisis y manejo de toda la información de la Secretaria de Hacienda.
3. Disponer y ejecutar las actividades y medidas para mantener actualizadas las bases de datos del impuesto predial, del de industria y comercio y de los diferentes impuestos y tasas que se recaudan por Tesorería.
4. Disponer y ejecutar las actividades y medidas para mantener actualizada la información sistematizada del estado contable, financiero y presupuestal del Municipio.
5. Generar los reportes diarios y detallados de los recaudos por impuesto predial urbano y rural con información necesaria para adelantar el proceso de cobro.
6. Diseñar y preparar la información que se le quiera con el detalle suficiente para verificar el estado mensual de ingresos, gastos de funcionamiento, servicio de la deuda e inversión para contabilidad, tesorería y presupuesto.
7. Prepara y presentar los informes sobre las actividades desarrolladas con la oportunidad y periodicidad requeridas.
8. Cumplir los indicadores de gestión, estándares de desempeño, mecanismos de evaluación y control a los procesos que desarrolle en el cumplimiento de las funciones propias del cargo.
9. Desempeñar las demás funciones que le sean asignadas por su superior para el cumplimiento de la misión de la Entidad, de acuerdo con la naturaleza, propósito principal y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

Los programas para el manejo de la información contable, presupuestal y de bienes permite es una herramienta ágil y eficiente. La adecuación del sistema de información facilita el pago de los impuestos Municipales.

1. Las estadísticas, informes y reportes elaborados cumplen con los datos necesarios para cumplir su objetivo y contienen información clara y actual.
2. Las bases de datos y la información sistematizada se mantiene actualizadas.
3. El trabajo de campo prepara el funcionamiento de la red a nivel de las dependencias de la Alcaldía Municipal.
4. La adaptación del sistema programa el servicio de pago de los impuestos Municipales.
5. La reutilización de la red soluciona los requerimientos técnicos en sistemas.

V. CONOCIMIENTOS BÁSICOS O ESENCIALES

1. Conocimientos generales de temas presupuestales, tributarios, contables y de manejo de bienes.
2. Manejo de programas y bases de datos.
3. Conocimiento sobre el manejo de la información del Estado.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Título Profesional o Tecnólogo en Ingeniería de Sistemas.	Un (1) año de experiencia profesional o relacionada con el cargo.

4.2. ARCHIVO CORRIENTE

Este archivo está conformado por una colección de documentos y papeles de trabajo relacionados directamente con el proceso de auditoría.

4.2.1. Programa de auditoría. Para la realización del proceso de auditoría al proceso de contratación de TI de la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y la Alcaldía Municipal de Ipiales, se utilizará la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), se evaluarán algunos objetivos de control que se encuentran dentro de los dominios del COBIT así:

- **DOMINIO - PLANEAR Y ORGANIZAR (PO):** Este dominio hace referencia a la identificación de las ventajas y de cómo las tecnologías de información pueden contribuir de la mejor manera al logro de los objetivos de negocio. Los procesos que se realizarán y los objetivos de control que se evaluarán son los siguientes:

  - ✓ **Definir un plan estratégico de tecnologías de información (PO1).** Busca encaminar de la mejor manera las tecnologías de información, de tal forma que se logren alcanzar las metas propuestas con dichas tecnologías dentro del portafolio de servicios de la entidad, los objetivos de control que se evaluaran son:

    - — **Evaluación del desempeño y la capacidad Actual:** Se deberá establecer una evaluación a las actuales tecnologías de información que se manejan dentro de las entidades auditadas, con el objetivo de analizar si estas tecnologías satisfacen los requerimientos para los cuales fueron implementadas.

    - — **Plan Estratégico de TI:** Se deberá crear en EMPOOBANDO un equipo de trabajo dedicado al estudio de las nuevas tecnologías de información, con el objetivo de estar a la vanguardia dentro de las tecnologías y cumpliendo con las normatividades relacionadas con las tecnologías de información emitidas por el Estado.

  - ✓ **Determinar la dirección tecnológica (PO3).** Busca establecer si existen dentro de la Entidad estudios o planes que permitan la implementación de

nuevas tecnologías de información para satisfacer los requerimientos necesarios para alcanzar los objetivos del negocio, los objetivos de control que se evaluaran son:

- **Planeación de la dirección tecnológica:** El personal encargado de las tecnologías de información deberá realizar un estudio acerca de las tecnologías de información, con el objetivo de seleccionar la que mejor satisfaga los requerimientos de la empresa teniendo en cuenta el costo/beneficio.

✓ **Definición de la organización y de las relaciones de TI (PO4).** Busca asegurar la correcta prestación de los servicios de TI, los objetivos de control que se evaluarán son:

- **Funciones y responsabilidades:** La Oficina de Talento Humano deberá asegurar que todo el personal que maneje equipos de cómputo conozca sus funciones y responsabilidades en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad con respecto a la seguridad y al control interno.

- **Responsabilidad de la seguridad lógica y física:** La Oficina Talento Humano deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información, a los usuarios de equipos de cómputo.

- **Supervisión:** La Oficina de Talento Humano deberá implementar prácticas de supervisión adecuadas en EMPOOBANDO para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente, y para evaluar todo lo referente al personal que interactúa con las tecnologías de información.

- **Segregación de funciones:** La Oficina de Talento Humano deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico, además deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos.

- **Descripción de cargos para el personal que operan las tecnologías de información:** La Oficina de Talento Humano deberá asegurar que las descripciones en los cargos para el personal que opera las tecnologías de información sean establecidos y actualizados

regularmente. Estas descripciones de puestos deberán delinear claramente tanto la responsabilidad como la autoridad, incluir las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

- **Personal clave de TI:** La Oficina de Talento Humano deberá definir e identificar al personal clave de las tecnologías de información.

✓ **Administrar la inversión en tecnologías de información (PO5).** Busca establecer un marco de trabajo en donde se administre programas de inversión en las tecnologías de información, teniendo en cuenta el costo / beneficio, con el fin de garantizar los intereses de la empresa, los objetivos de control que se evaluaran son:

- **Evaluación de la oficina de sistemas:** La Gerencia de las entidades auditadas deberá analizar la posibilidad de implementar la oficina de Sistemas, a través de la cual se buscará administrar todo lo relacionado con el uso de las tecnologías de la información.

- **Marco de trabajo para la administración financiera:** Se debe organizar un grupo de trabajo que se encargue de administrar las inversiones de dinero en las tecnologías de información dentro de las entidades auditadas.

- **Administración de costos de tecnologías de información:** Dentro del marco de trabajo se debe hacer énfasis en la variación de los costos que existen al momento de implementar las tecnologías de información, comparando los costos reales con los presupuestados, con el fin de favorecer los intereses económicos de las entidades auditadas.

- **Administración de beneficios:** Cuando las tecnologías de información se encuentren implementadas y prestando sus servicios a los procesos internos de las entidades auditadas, se deben realizar monitoreos regulares con el objetivo de verificar que los beneficios prestados por dichas tecnologías están contribuyendo a la satisfacción de los requerimientos para los cuales fueron implementadas.

✓ **Administrar los recursos humanos (PO7).** Busca establecer procedimientos que permitan el buen reclutamiento, la correcta capacitación y la pertinente evaluación del desempeño laboral, al personal encargado de

manejar las tecnologías de información, los objetivos de control que se van a evaluar son:

- **Reclutamiento y retención de personal:** La contratación de personal para el manejo de las tecnologías de información se debe realizar con transparencia, analizando y verificando que los requisitos establecidos en el manual de funciones para dichos cargos, estén presentes en el perfil de la persona postulada para el empleo.

- **Entrenamiento del personal de TI:** Se debe capacitar adecuadamente al nuevo personal encargado del manejo y la administración de las tecnologías de información, con el objetivo de brindar, mantener y fortalecer sus conocimientos en las actividades y roles que les fueron asignadas.

- **Evaluación del desempeño del empleado:** Se debe realizar periódicamente evaluaciones a cada uno de los empleados que manejan y administran las tecnologías de información, verificando que su desempeño y compromiso con sus labores dentro de de las entidades auditadas los convierte en las personas idóneas para continuar con su labor al frente de dichas tecnologías.

✓ **Evaluación de riesgos (PO9).** Busca asegurar el logro de los objetivos de las tecnologías de información y responder a las amenazas hacia la provisión de servicios de TI, los objetivos de control que se evaluarán son:

- **Evaluación del riesgo del negocio:** Dentro de las entidades auditadas se deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos, utilizando los resultados de auditorías, inspecciones e incidentes identificados.

- **Enfoque de evaluación de riesgos:** Dentro de las entidades auditadas se deberá establecer un enfoque general para la evaluación de riesgos, que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar

asegurada por un método estructurado y por asesores expertos en riesgos.

- **Identificación de riesgos:** La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.
- **Medición de riesgos:** El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos, genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta la tecnología de información. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

- **Plan de acción contra riesgos:** El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos, para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

- **Aceptación de riesgos:** El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

- **DOMINIO - ADQUIRIR E IMPLEMENTAR (AI):** Para llevar a cabo la estrategia de tecnologías de información, las soluciones de tecnologías de información deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro de los procesos de la Entidad. Además, este dominio cubre los cambios y el mantenimiento realizados a las tecnologías de información. Los procesos que se realizarán y los objetivos de control que se evaluarán son los siguientes:

  - ✓ **Adquirir y mantener la infraestructura tecnológica (AI3).** Busca que las organizaciones implementen las plataformas adecuadas para soportar las aplicaciones de las tecnologías de información, los objetivos de control que se evaluarán son:

    - **Plan de adquisición de infraestructura tecnológica:** Las entidades auditadas deben contar con un grupo especializado en tecnologías de información, con el objetivo de realizar un estudio que le permita seleccionar las tecnologías de información adecuadas para satisfacer los requerimientos del negocio, haciendo uso de la visión que se tiene

con estas a futuro evitando modificaciones o cambios de las mismas a corto plazo.

- **Mantenimiento de la infraestructura:** Las tecnologías que se manejan actualmente en las entidades auditadas deben ser revisadas periódicamente, con el objetivo de analizar si están ajustadas a las necesidades de los procesos para los cuales fueron implementadas, o si por el contrario deben ser tenidas en cuenta para mantenimiento y actualizaciones debido al cambio en los procesos que manejan.

- **Mantenimiento preventivo para hardware:** El personal encargado del mantenimiento preventivo de los equipos de cómputo deberá calendarizar el mantenimiento rutinario y periódico del hardware, con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

- **Mantenimiento del software del sistema:** Deberán implementarse procedimientos para asegurar que el software utilizado en las tecnologías de información, sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

✓ **Adquirir recursos de TI (AI5).** Busca que las tecnologías de información se implementen y cumplan con sus funciones a cabalidad dentro de la entidad, a través del uso de recursos óptimos e idóneos tanto de hardware, software y servicios prestados por los humanos, los objetivos de control que se evaluarán son:

- **Administración de contratos con proveedores:** Dentro de las entidades auditadas se deben formular procedimientos para establecer contratos con proveedores de tecnologías de información, teniendo en cuenta las normatividades que rigen a EMPOOBANDO al desempeñarse como una empresa de servicios públicos y a la Alcaldía Municipal de Ipiales por su razón de ser, por otra parte los proveedores deben ser reconocidos a través del Sistema de información para la contratación estatal SICE, con el objetivo de que los contratos establecidos, modificados y concluidos por las entidades auditadas sean transparentes ante los entes de control del Estado.

- **Selección de proveedores:** Los proveedores de tecnologías de información deben ser seleccionados de manera justa y formal, para garantizar que la implementación de dichas tecnologías sea la que mejor les garanticen a las entidades auditadas alcanzar la satisfacción de esos requerimientos, teniendo en cuenta el costo/beneficio.

- **Adquisición de recursos de TI:** Para la contratación de tecnologías de información y de todos los recursos necesarios para su correcto funcionamiento, se debe especificar dentro de las respectivas clausulas las responsabilidades y obligaciones legales, financieras, organizacionales y documentales entre las partes. Se deben hacer cumplir los derechos y obligaciones, a fin de proteger los intereses de la entidad cuando dichos contratos no se están desarrollando a cabalidad en los términos y plazos pactados.

✓ **Administración de cambios (AI6).** Busca minimizar la probabilidad de riesgo y de interrupciones, alteraciones no autorizadas y errores en la infraestructura de las tecnologías de información, los objetivos de control que se evaluarán son:

- **Estándares y procedimientos para cambios:** Dentro de las entidades auditadas se deberán asegurar que todas las requisiciones de cambios tanto internos como por parte de proveedores, estén estandarizados y sujetos a procedimientos formales de administración de cambios.

- **Evaluación de impacto, priorización y autorización:** Todas las solicitudes deberán categorizarse, priorizarse y establecerse dentro de procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estado de su solicitud.

- **Cierre y documentación de cambio:** El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

- **DOMINIO - ENTREGAR Y DAR SOPORTE (DS):** En este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Los procesos que se realizarán y los objetivos de control que se evaluarán son los siguientes:

- ✓ **Asegurar el servicio continuo (DS4).** Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

  Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio. Los objetivos de control a evaluar serán:

  - **Recursos críticos de TI:** Las entidades mencionadas deberán poseer un plan de continuidad que identifique que programas, servicios, sistemas operativos, personal, bases de datos, archivos y demás son críticos para el mencionado proceso, así como los tiempos que se necesitarían para recuperar todos estos elementos en caso de una falla amplia.

  - **Almacenamiento de respaldos fuera de las instalaciones:** Las entidades mencionadas deberán proveer un respaldo externo diferente al de las instalaciones donde se realiza el proceso mencionado, todo con el fin de lograr una recuperación rápida en caso de falla mayor. El contenido de dichos respaldos deben determinarse por el grupo de personas involucradas en el proceso mencionado, ya que ellos son los responsables de dicho proceso. Las instalaciones deben apegarse a todas las políticas que las entidades mencionadas requieran y tengan dentro de sus estatutos. Además el respaldo debe ser verificado y actualizado periódicamente.

- ✓ **Garantizar la seguridad de sistemas (DS5).** Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

  Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios no autorizados. Los objetivos de control que se evaluarán son:

  - **Administración de la seguridad de TI:** La administración de seguridad por parte de las entidades mencionadas, debe ser llevada a cabo por la administración que será la encargada de que esta seguridad este en línea con los requerimientos del negocio.

    Lo que incluye:

    - Identificar los riesgos
    - Implementar planes de seguridad
    - Actualizar los planes de seguridad

- Monitoreo permanente del plan de seguridad
- Alinear los procedimientos de seguridad (Identificación, Autenticación, Acceso).

— **Plan de seguridad de TI:** Las entidades auditadas deberán poseer un plan de seguridad completo, teniendo en cuenta todos los factores que puedan afectar la seguridad, tales factores como infraestructura, cultura de seguridad al interior de las entidades, personal, software y hardware, esto con el fin de que el plan se cumpla a cabalidad junto con sus procedimientos y políticas.

— **Administración de la identidad con cuentas de usuarios:** Se deberá establecer por parte del personal encargado de administrar las tecnologías de información, todos los procedimientos necesarios para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión y suspensión o cambio de cuentas de usuario y contraseñas para el manejo de los equipos de cómputo. Deberá incluirse un procedimiento de aprobación formal que indique al propietario de los datos o del sistema los privilegios de acceso que se le han otorgado.

— **Revisión gerencial de cuentas de usuarios:** El personal encargado de administrar las tecnologías de información, deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso**.**

— **Pruebas, vigilancia y monitoreo de la seguridad:** El constante monitoreo de la seguridad tanto física como lógica por parte de los administradores y en si por parte de quienes están involucrados en el proceso mencionado, permitirá a las entidades auditadas garantizar la seguridad; por lo tanto el proceso de pruebas, vigilancia y monitoreo deberá ser implementado y mantenido en las entidades en cuestión.

— **Administración centralizada de identificación y derechos de acceso:** Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

— **Reportes de actividad de violación y seguridad:** El personal encargado de administrar las tecnologías de Información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en

forma regular para identificar y resolver incidentes que involucren actividades no autorizadas.

- **Prevención, detección y corrección de software malicioso:** Con respecto al software malicioso, tal como los virus computacionales gusanos y Caballos de Troya, las entidades auditadas deberán establecer un marco de referencia de adecuadas medidas de control de prevención, de detección y corrección de virus, con el objetivo de mantener la información integra, discreta y disponible.

- **Seguridad de la red:** Si existe conexión con Internet u otras redes públicas en la organización, se deberá contar con sistemas Firewall, dispositivos de seguridad o segmentaciones de red adecuados para proteger la información de cualquier acceso no autorizado a los recursos internos, además se deberá controlar en ambos sentidos cualquier flujo de información entre los equipos de cómputo que conforman la infraestructura tecnológica de red.

✓ **Administración de la configuración (DS9):** Busca tener en cuenta un repositorio de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base de conocimiento para el sano manejo de cambios, los objetivos de control que se evaluarán son:

- **Registro de la configuración:** Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario al momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo). El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

- **Repositorio y línea base de configuración:** Se deberá asegurar que los registros de configuración reflejen el estado real de todos los elementos de la configuración incluyendo la historia de los cambios.

- **Control de la configuración:** Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de la función de servicios de información sean revisadas periódicamente.

- **Revisión de integridad de la configuración:** El encargado del área de sistemas deberá revisar periódicamente la existencia de software no autorizado en los equipos de cómputo de la entidad.

✓ **Administración de datos (DS11):** Busca asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, los objetivos de control que se evaluarán son:

- **Acuerdos de almacenamiento y conservación:** El personal encargado de la administración de las tecnologías de información deberá establecer políticas y procedimientos donde se describan los medios y lugares donde se almacenaran, archivaran y retendrán la información tales como documentos escritos (contratos, actas, reportes, etc.), archivos digitales (datos, claves, programas, etc.).

- **Protección de información crítica a ser desechada:** El personal encargado de la administración de las tecnologías de información deberá definir e implementar políticas y procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos deberán garantizar que ninguna información marcada como "borrada" o "desechada", pueda ser accedida por personas internas o externas a la organización.

- **Administración de almacenamiento:** Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren información de recuperación, de la economía y las políticas de seguridad.

- **Períodos de retención y términos de almacenamiento:** Deberán definirse los períodos de retención y los términos de almacenamiento para documentos (contratos, actas, reportes, etc.), datos, programas, y mensajes (de entrada y de salida).

- **Respaldo y restauración:** Se deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación de la información. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

- **Funciones de respaldo:** Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

- **Almacenamiento de respaldos:** Los procedimientos de respaldo para los medios relacionados con las tecnologías de información, deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

✓ **Administración de instalaciones (DS12):** Busca proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas, los objetivos de control que se evaluarán son:

- **Selección y diseño del centro de datos:** Dentro de EMPOOBANDO se debe implementar una oficina de sistemas o centro de computo, el cual deberá considerar las leyes y regulaciones correspondientes para tal dependencia, además se deberá tener en cuenta el riesgo asociado a los desastres naturales, ambientales y a los causados por el hombre, con el objetivo de administrar de la mejor manera todo lo relacionado con las tecnologías de información de la Entidad.

- **Seguridad física:** Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse desde la entrada principal de la entidad hasta las oficinas donde se encuentran los equipos de computo que contienen información importante, incluso a las personas que laboran en la entidad pero que no hayan sido autorizadas a dicho acceso.

- **Discreción de las instalaciones de tecnología de información:** Se deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones donde se encuentran los equipos de computó que almacena la información importante, no sea fácil de localizar.

- **Escolta de visitantes:** Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del

grupo de operaciones de la función de servicios de información, sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes. Además deberían existir instalaciones de cámaras de seguridad que permitan el monitoreo permanente de las instalaciones tanto internas (pasillos y oficinas de área restringida) como externas de las entidades auditadas.

— **Protección contra factores ambientales:** Se deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección de los equipos de cómputo y de la información contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipos y dispositivos especializados para monitorear y controlar el ambiente.

- **DOMINIO - MONITOREAR Y EVALUAR (ME):** Todos los procesos que se manejan a través de las tecnologías de información dentro de las entidades auditadas necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio, los procesos y los objetivos de control que se evaluarán, son:

  ✓ **Monitorear y evaluar el control interno (M2):** Busca asegurar el logro de los objetivos de control interno establecidos para los procesos de tecnologías de información, proporcionando seguridad a las operaciones eficientes y cumplimiento de las leyes y regulaciones aplicables, los objetivos de control que se evaluarán son:

  — **Monitoreo del marco de trabajo de control interno:** Dentro de las entidades auditadas se deberán monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

  — **Operación oportuna de controles internos:** La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a las Gerencia de las entidades auditadas.

- **Reporte sobre el nivel de control interno:** El personal encargado de evaluar y monitorear el control interno deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas, con el objetivo de asegurar la efectividad continua de su sistema de control interno.

- **Aseguramiento de control interno:** El aseguramiento de control interno deberá ser establecido a través de una "auto-auditoría" o de una auditoría externa independiente, para evaluar el estado de seguridad en el que funcionan las actuales tecnologías de información y verificar que los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de las Gerencias de las entidades auditadas deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

✓ **Garantizar el cumplimiento con requerimiento externos (ME3).** Busca garantizar el cumplimiento de leyes, regulaciones y requerimientos contractuales en todos los procesos relacionados con las tecnologías de información, con el objetivo de mantener la transparencia, la integración y los reportes de cumplimiento en las tecnologías de información contratadas por las entidades auditadas, los objetivos de control que se evaluarán son:

- **Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales:** Dentro de las entidades auditadas se debe establecer políticas y procedimientos que les permitan la contratación con proveedores de tecnologías de información, teniendo en cuenta las normatividades y leyes Estatales que rigen a EMPOOBANDO por ser una empresa prestadora de servicios públicos y la Alcaldía Municipal de Ipiales por su razón social.

- **Optimizar la respuesta a requerimientos externos:** Se deben ajustar las políticas y procedimientos de las tecnologías de información, para garantizar que los requisitos legales y contractuales en la rendición de cuentas por parte de las entidades auditadas, se cumplan con trasparencia ante los sistemas y entes de regulación y control asignados por el Estado, como son el Sistema de información para la contratación Estatal (SICE), La Superintendencia de Servicios Públicos para EMPOOBANDO y La contraloría Departamental de Nariño respectivamente.

- **Aseguramiento positivo de cumplimiento:** Las entidades auditadas deberá garantizar que todo contrato celebrado con proveedores de

tecnologías de información se cumpla a cabalidad dentro de los plazos y términos acordados en el mismo, de lo contrario deberá tomar las medidas legales necesarias ante los organismos de regulación, con el objetivo de confirmar cualquier inconsistencia en el desarrollo del contrato en busca de una corrección oportuna.

4.2.2. Diseño de los elementos de auditoría. Para la realización de la auditoria a la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y la Alcaldía Municipal de Ipiales, se utilizaron distintos instrumentos de recolección de información los cuales se describen a continuación:

- **Observación directa:** La Contraloría Departamental de Nariño ha tomado la observación directa como el elemento de auditoría más importante en los procesos que adelanta en todo el Departamento de Nariño. Mediante visitas sorpresa se trata de recaudar el mayor volumen de información para su posterior análisis, es así como en la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y en la Alcaldía Municipal de Ipiales se realizaron visitas sorpresa en cada entidad.

- **Entrevistas:** Las entrevistas en las entidades fueron documentadas en apuntes realizadas por el funcionario de la Contraloría Departamental de Nariño con el apoyo del equipo auditor, cabe aclarar que estas entrevistas se realizaron en el transcurso de la primera inspección, en donde no existía previo aviso de dicha visita, por lo tanto la extracción de información de estas entrevistas se hace con el completo consentimiento de la Contraloría Departamental que ejerce el control sobre las entidades auditadas.

- **Cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría**: Con esta herramienta se identifica cual es la información que se necesita para evaluar un determinado proceso dentro de los dominios del COBIT, también se especifica en él, cuales son las pruebas de análisis y de ejecución que se deben realizar.

Los ítems relacionados a continuación son los que describirán el elemento de auditoría.

REF: Se refiere al ID del elemento.

ENTIDAD AUDITADA: En este espacio se indica el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, que para este caso será Contratación TI.

RESPONSABLES: En este espacio se indica los nombres del equipo auditor que están llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para este caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en especifico que se está auditando dentro de los dominios del COBIT.

FUENTES DE CONOCIMIENTO: En este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoría lo que servirá como respaldo del proceso.

REPOSITORIO DE PRUEBAS: Se divide en dos tipos de pruebas:

DE ANÁLISIS: Este espacio está destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Este espacio está destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Figura 4. Cuadro de definición de fuente de conocimiento, prueba de análisis de auditoria

CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS DE AUDITORIA	REF	EMPOOBANDO E.S.P

ENTIDAD AUDITADA	Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P.	**PAGINA**		
		1	DE	1
PROCESO AUDITADO	Proceso de Contratación TI			
RESPONSABLES	Luis Eduardo Pantoja Rodríguez			
	Gerardo Antonio Ramos Goyes			
MATERIAL DE SOPORTE	COBIT			
DOMINIO				
PROCESO				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	**DE EJECUCION**

AUDITORES RESPONSABLES:
LUIS EDUARDO PANTOJA RODRIGUEZ GERARDO ANTONIO RAMOS GOYES

- **Cuestionario cuantitativo:** El cuestionario cuantitativo mediante una calificación numérica ayuda a identificar la vulnerabilidad de los procesos.

Los ítems relacionados a continuación son los que describirán el elemento de auditoría.

REF: Se refiere al ID del elemento.

ENTIDAD AUDITADA: En este espacio se indica el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para este caso será Contratación TI.

RESPONSABLES: En este espacio se indica los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: En este espacio se indica el nombre del material que soporta el proceso, para este caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en especifico que se está auditando dentro de los dominios del COBIT.

PREGUNTA: Espacio donde se indica la descripción de la consulta de la cual se indagará.

SI – NO – NA: Posibilidades de respuesta, cumple, no cumple, o no aplica para la entidad.

PORCENTAJE DE RIESGO: Hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre más alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

El cálculo de este porcentaje se hace de la siguiente forma:

Porcentaje de riesgo parcial = (Total SI * 100) / Total

Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

Las equivalencias utilizadas para la puntuación serán de uno a cinco, siendo uno el valor mínimo considerado de poca importancia y cinco el máximo considerado de mucha importancia.

Figura 5. Cuestionario cuantitativo.

EMPOOBANDO E.S.P

CUESTIONARIO CUANTITATIVO

REF

ENTIDAD AUDITADA	Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO	PAGINA		
		1	DE	1
PROCESO AUDITADO	CONTRATACION TI			
RESPONSABLES	Luis Eduardo Pantoja Rodríguez – Gerardo Antonio Ramos Goyes			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		PROCESO		

PREGUNTA	SI	NO	NA	FUENTE
1.				
2.				

TOTALES	0	0	0
TOTAL CUESTIONARIO			

AUDITORES RESPONSABLES
LUIS EDUARDO PANTOJA RODRIGUEZ
GERARDO ANTONIO RAMOS GOYES

- **Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso:** Esta matriz fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

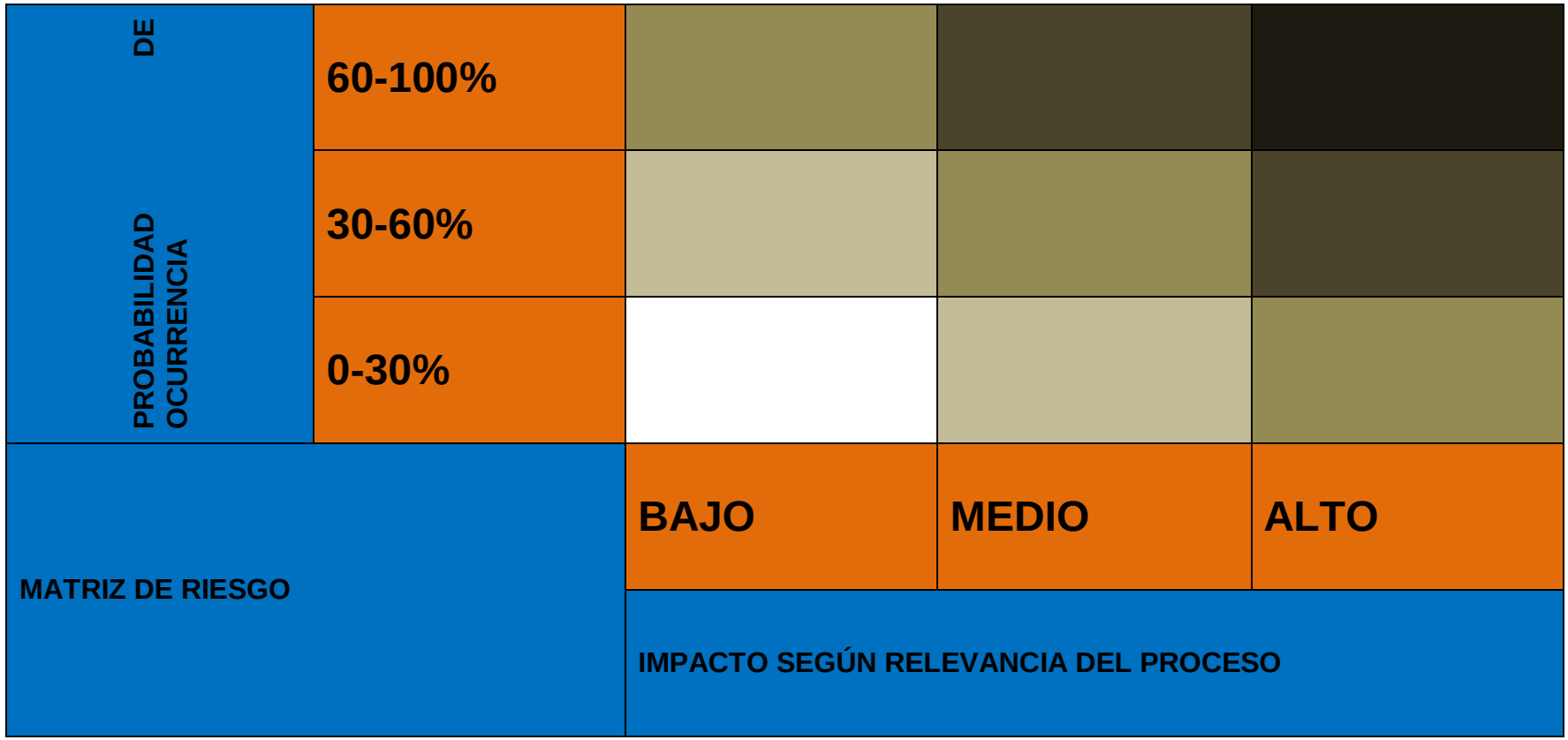
  En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

  Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

  Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

MATRIZ DE PROBABILIDAD DE OCURRENCIA E IMPACTO SEGÚN RELEVANCIA DEL PROCESO

Figura 6. Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso.



4.2.3. Hallazgos

A continuación se describirán los hallazgos encontrados en la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y en la Alcaldía Municipal de Ipiales.

DOMINIOS Y PROCESOS AUDITADOS

Los hallazgos encontrados en las entidades se presentarán en el orden de los dominios y procesos auditados los cuales fueron:

1) DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

- ✓ Definir un plan estratégico de tecnologías de información (PO1).
- ✓ Determinar la dirección tecnológica (PO3).
- ✓ Definición de la organización y de las relaciones de TI (PO4).
- ✓ Administrar la inversión en tecnologías de información (PO5).
- ✓ Administrar los recursos humanos (PO7).
- ✓ Evaluación de riesgos (PO9).

2) DOMINIO - ADQUISICION E IMPLEMENTACION (AI)

- ✓ Adquirir y mantener software aplicativo (AI2).
- ✓ Adquirir y mantener infraestructura tecnológica (AI3).
- ✓ Adquirir recursos de tecnologías de información (AI5).
- ✓ Administración de cambios (AI6).

3) DOMINIO - ENTREGAR Y DAR SOPORTE (DS)

- ✓ Garantizar la seguridad de los sistemas (DS5).
- ✓ Educar y entrenar a los usuarios (DS7).
- ✓ Administración de la configuración (DS9).
- ✓ Administración de datos (DS11).
- ✓ Administración de las instalaciones (DS12).

4) DOMINIO - MONITOREAR Y EVALUAR (ME)

- ✓ Monitorear y evaluar el control interno (ME2).
- ✓ Garantizar el cumplimiento con requerimientos externos (ME3).

4.2.4. Informe de auditoría

- **Objetivos:** Realizar Auditoria de Sistemas a las entidades públicas Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. y la Alcaldía Municipal de Ipiales, para evidenciar vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información manejada en el proceso de contratación de TI.

- **Objetivos específicos**

  - ✓ Analizar y evaluar políticas de control de riesgos dentro de las entidades.

  - ✓ Analizar las políticas existentes en las entidades que garantizan la seguridad física y lógica de la información.

  - ✓ Establecer el estado de las políticas que garantizan la continuidad en el proceso de contratación de las entidades.

  - ✓ Analizar el proceso de contratación de las entidades así como las vulnerabilidades a las que este se encuentra expuesto.

  - ✓ Aportar información que permita a las entidades auditadas implementar las medidas necesarias, para garantizar que los trámites realizados por sus usuarios tengan como materia prima información confiable, integra y confidencial, que asegure la trasparencia en los procesos.

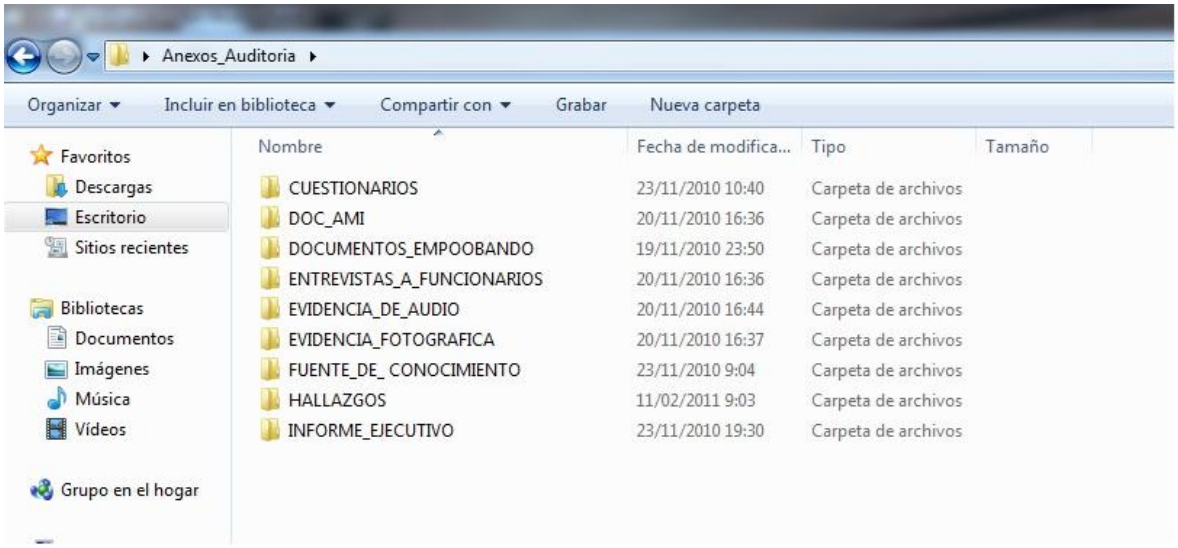
  - ✓ Analizar las instalaciones físicas que las entidades poseen, para garantizar la seguridad de la información.

- **Limitaciones:** La auditoria se realizó con normalidad, exceptuando la recolección de información de la Empresa de Obras Sanitarias de la Provincia de Obando, además cabe resaltar que en ningún momento se tuvo acceso a códigos fuentes, servidores en funcionamiento, ni módulos de aplicaciones puesto que estos no hacían parte de los lineamientos objeto de auditoría, de la entidad Contraloría Departamental Nariño.

- **Resultados de la auditoría:** Teniendo en cuenta que la auditoria se fundamenta en cuestionarios cuantitativos sugeridos dentro del CobiT, papelería de trabajo y evidencias tanto fotográficas como de audio de las dos entidades auditadas, los cuales se encuentran anexos en el CD-ROM adjunto. Es recomendable introducir el CD-ROM en la unidad del computador, esperar a

que se reproduzca automáticamente el CD y dar Clíck en “Abrir la carpeta para ver todos los archivos”, de no hacerse la reproducción automática ir a Mi PC y dar doble Clíck sobre la Unidad de CD-ROM; todo esto para mantener abierta la carpeta de los Anexos de la Auditoria, la cual debe contener en orden las siguientes carpetas (CUESTIONARIOS, DOC_AMI, DOCUMENTOS_EMPOOBANDO, ENTREVISTAS_A_FUNCIONARIOS, EVIDENCIA_DE_AUDIO, EVIDENCIA_FOTOGRAFICA, FUENTE_DE_CONOCIMIENTO, HALLAZGOS E INFORME_EJECUTIVO) (Figura 7).

Figura 7. Contenido de los anexos de auditoría.



Para mayor información acerca de lo que contiene cada uno de los anexos dirigirse a la página 186 sección ANEXOS, todo esto con el objetivo de hacer más efectiva, rápida y clara la búsqueda, tanto de pruebas como de la referenciación de los hallazgos descritos a lo largo del informe general de Auditoría.

La referenciación se establece de la siguiente manera: la palabra REF indicará que es necesario ubicar algún archivo que servirá de soporte para algún hallazgo, dentro de paréntesis cuadrados se describe la dirección donde se encuentra el archivo así: la parte que se encuentra a la izquierda del símbolo “/” es el nombre de la carpeta que contiene el archivo ubicada en el CD-ROM; y la parte que está a la derecha del símbolo “/” y en negrita corresponde al nombre del archivo evidencia que soporta el hallazgo (Figura 8).

Figura 8. Modelo de la referenciación.

Para ver como es el funcionamiento obsérvese el siguiente ejemplo:

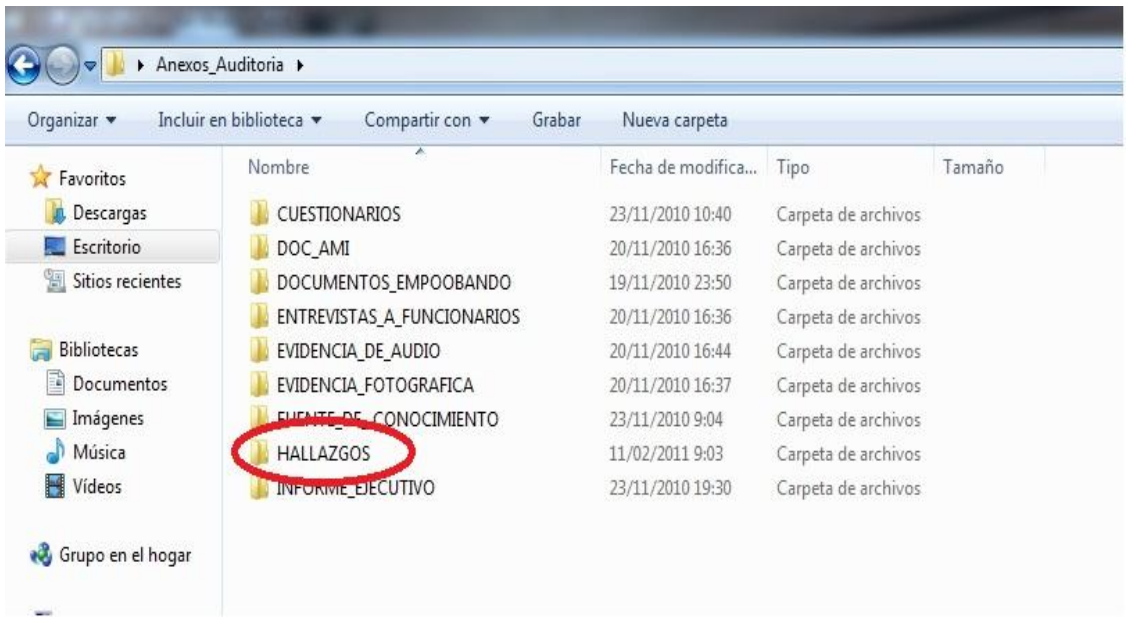
Hallazgo:

No se verifica que el proveedor de servicios de tecnologías de información se encuentre registrado en el SICE.

REF [HALLAZGOS**/HEMDO_08**]. Modelo de referenciación.

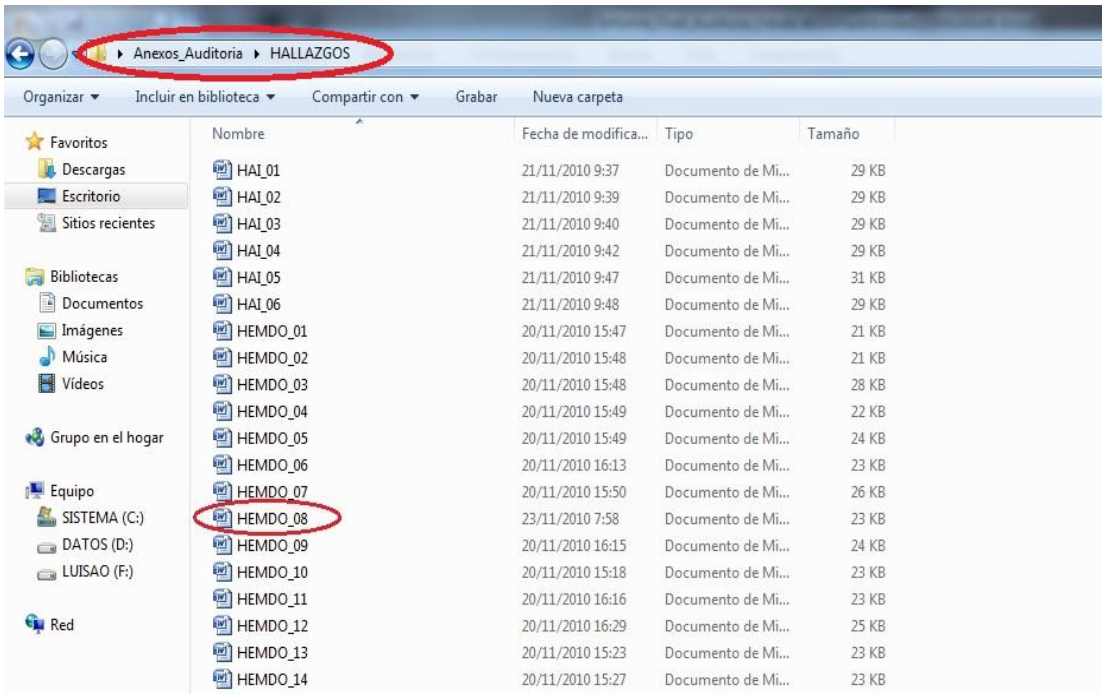
La palabra **REF** nos indica que debemos buscar un archivo que soporta nuestro hallazgo. Entonces nos vamos a la unidad de CD-ROM de nuestro computador, donde nos muestra el contenido de los Anexos de la auditoria y buscamos la carpeta HALLAZGOS (Figura 9),

Figura 9. Búsqueda de la carpeta hallazgos que contiene el archivo.



hacemos doble Clíck sobre la misma para entrar y ver su contenido. Posterior a esto buscamos el archivo **HEMDO_08** (Figura 10), el cual contiene la evidencia de nuestro hallazgo.

Figura 10. Búsqueda del archivo que contiene la evidencia.



Dentro del archivo HEMDO_08 se mostrará el nombre del archivo, la información de Auditoria, y la misma información descrita en los hallazgos del informe de auditoría (Figura 11);

Figura 11. Información de la tabla.

	HALLAZGO EMPOOBANDO E.S.P	REF
		HEMDO_08

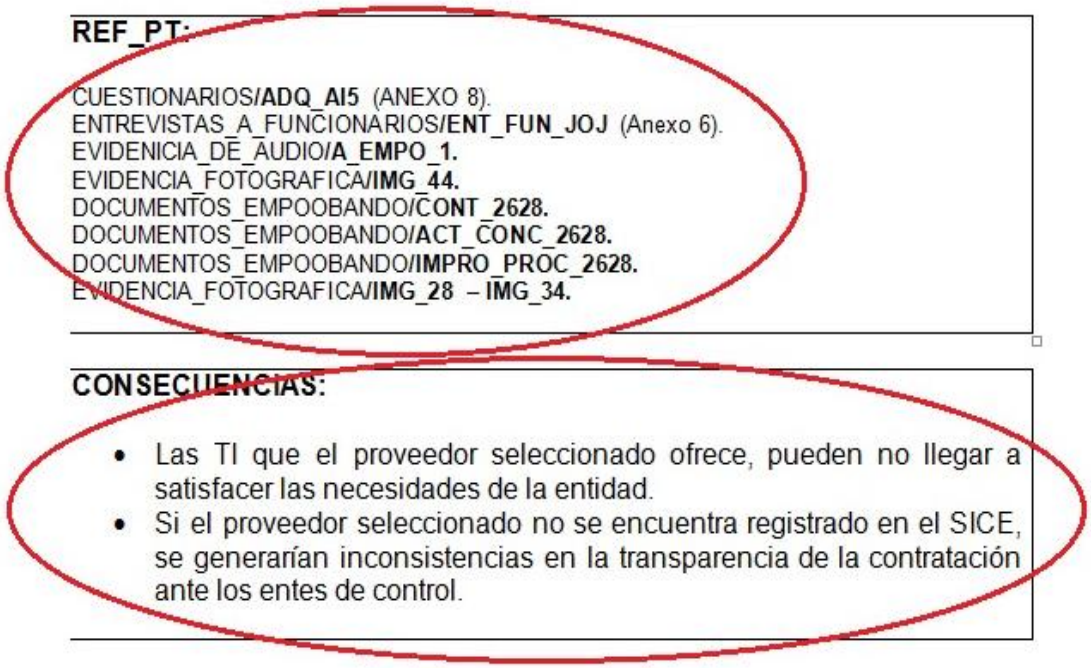
PROCESO AUDITADO	CONTRATACIÓN TI	**PÁGINA**	1 DE 2
RESPONSABLE	LUIS EDUARDO PANTOJA RODRIGUEZ GERARDO ANTONIO RAMOS GOYES		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Adquisición e implementación (AI)	**PROCESO**	Adquirir Recursos de TI (AI5).

DESCRIPCIÓN:

- Las políticas y procedimientos para la selección de los proveedores de las TI, no se aplican correctamente.
- No se verifica que el proveedor este registrado en el SICE.
- La selección del proveedor, en ocasiones no garantiza que la TI que éste ofrece satisfaga las necesidades de la entidad.
- La selección del proveedor, no se hace teniendo en cuenta el costo de la TI que éste ofrece y el beneficio que ésta otorgaría a la entidad.
- No se hacen cumplir las obligaciones que adquiere el proveedor con la entidad, cuando el contrato no se desarrolla a cabalidad en los términos y plazos pactados.

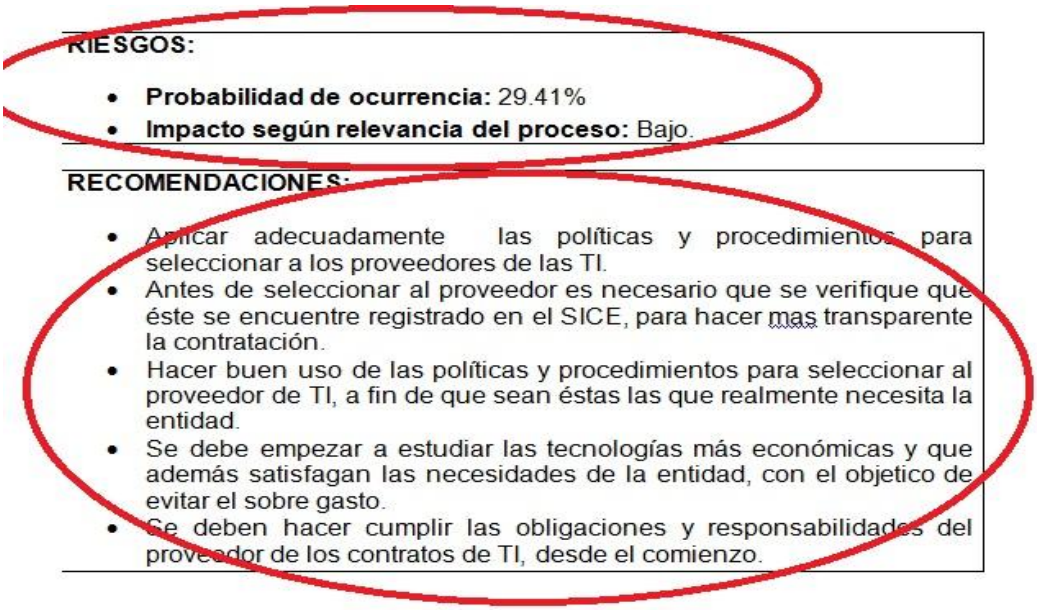
Además se muestra la referenciación hacia los papeles de trabajo que son la evidencia tanto fotográfica, entrevistas, documentos de las entidades conseguidos a través de la primera fase de la auditoria, etc.; también se muestra las consecuencias que traen para cada entidad los respectivos hallazgos (Figura 12);

Figura 12. Referenciación a papeles de trabajo y consecuencias que traen los respectivos hallazgos.



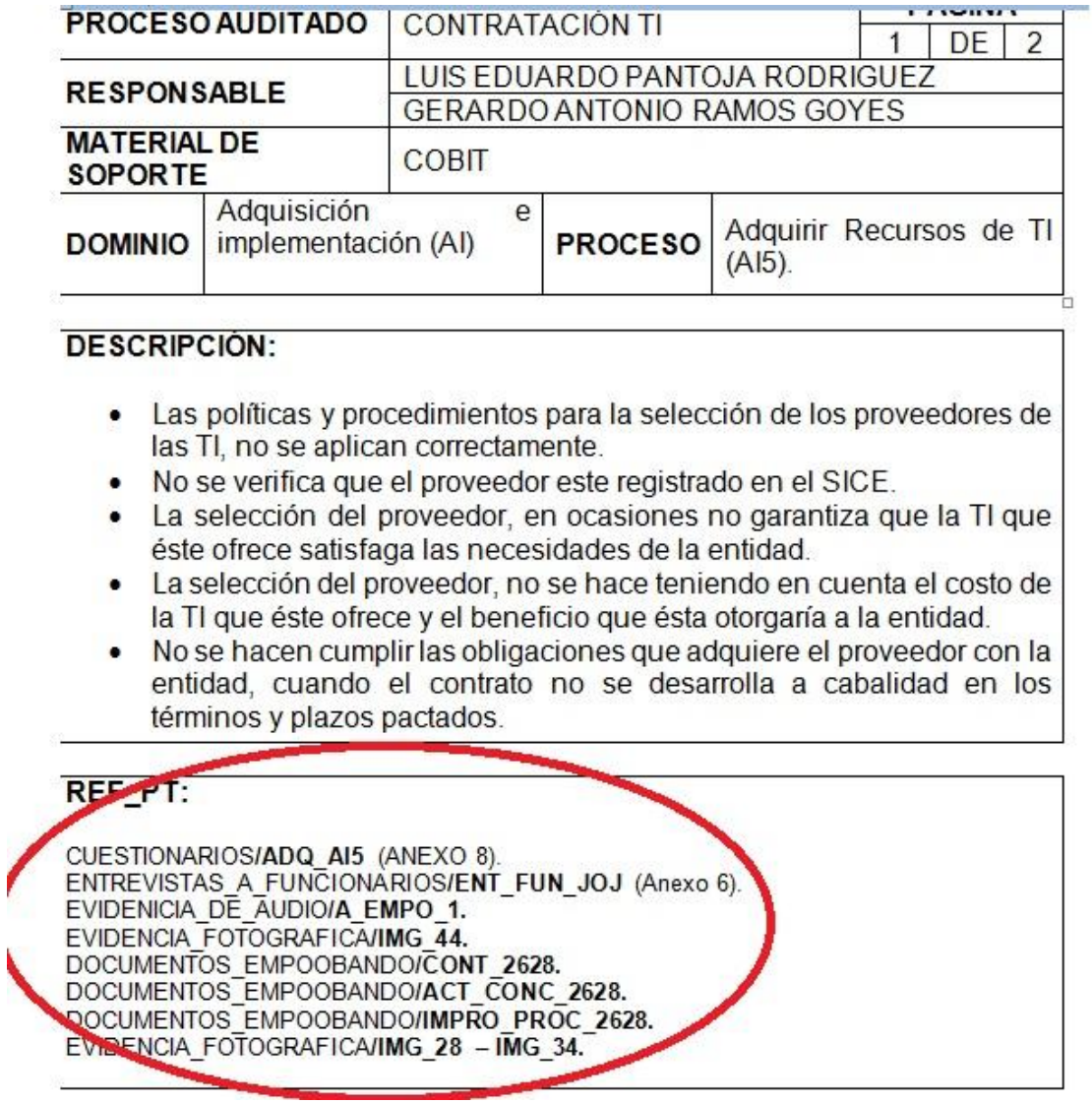
También se muestra el riesgo establecido a través de la probabilidad de ocurrencia y el impacto; por último se muestran las recomendaciones a seguir para mitigar los hallazgos. (Figura 13)

Figura 13. Probabilidad de ocurrencia y recomendación de hallazgos



Para llegar a las evidencias llamadas papeles de trabajo y a todas las evidencias descritas en toda referenciación a lo largo del trabajo, se deberá realizar los mismos pasos establecidos en el ejercicio anterior, puesto que manejan el mismo formato. (Figura 14, Figura 15).

Figura 14. Referencia papeles de trabajo en la tabla de hallazgos.



PROCESO AUDITADO	CONTRATACIÓN TI			PÁGINA 1 DE 2	
RESPONSABLE	LUIS EDUARDO PANTOJA RODRIGUEZ GERARDO ANTONIO RAMOS GOYES				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación (AI)	**PROCESO**	Adquirir Recursos de TI (AI5).		

DESCRIPCIÓN:

- Las políticas y procedimientos para la selección de los proveedores de las TI, no se aplican correctamente.
- No se verifica que el proveedor este registrado en el SICE.
- La selección del proveedor, en ocasiones no garantiza que la TI que éste ofrece satisfaga las necesidades de la entidad.
- La selección del proveedor, no se hace teniendo en cuenta el costo de la TI que éste ofrece y el beneficio que ésta otorgaría a la entidad.
- No se hacen cumplir las obligaciones que adquiere el proveedor con la entidad, cuando el contrato no se desarrolla a cabalidad en los términos y plazos pactados.

REF_PT:

CUESTIONARIOS/**ADQ_AI5** (ANEXO 8).
ENTREVISTAS_A_FUNCIONARIOS/**ENT_FUN_JOJ** (Anexo 6).
EVIDENICIA_DE_AUDIO/**A_EMPO_1.**
EVIDENCIA_FOTOGRAFICA/**IMG_44.**
DOCUMENTOS_EMPOOBANDO/**CONT_2628.**
DOCUMENTOS_EMPOOBANDO/**ACT_CONC_2628.**
DOCUMENTOS_EMPOOBANDO/**IMPRO_PROC_2628.**
EVIDENCIA_FOTOGRAFICA/**IMG_28 – IMG_34.**

Figura 15. Referencia papeles de trabajo en cuestionarios cuantitativos.

RESPONSABLES	Luis Eduardo Pantoja Rodríguez – Gerardo Antonio Ramos Goyes		
MATERIAL DE SOPORTE		COBIT	
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**	Administración de la Configuración (DS

	PREGUNTA	SI	NO	NA	REF
1.	¿Existe un inventario de la configuración de todos los equipos de cómputo que hace parte de las TI implementadas en EMPOOBANDO E.S.P.?	**5**			DOCUMENTOS_ EMPOOBANDO/ **INVENTARIO**
2.	¿Dentro de este inventario se tiene en cuenta lo siguiente: • ¿La configuración referente al Sistema Operativo, que soporta el funcionamiento de los equipos de cómputo de EMPOOBANDO?	**5**			ENTREVISTAS_A_ FUNCIONARIOS/ **ENT_FUN_ESM** (Anexo 1)
	• ¿La configuración del software instalado en los diferentes equipos de cómputo?	**5**			EVIDENCIA_DE_ AUDIO/**A_EMPO _1**
	• ¿Toda la información referente a licencias de los diferentes programas instalados?	**5**			
	• ¿La configuración referente al hardware instalado?	**5**			
3.	¿Existen políticas o procedimientos relacionados con la utilización de software (software permitido, software no permitido) en los equipos de cómputo?		**5**		
4.	¿Existen políticas o procedimientos relacionados con la utilización de hardware (hardware permitido, hardware prohibido) en los equipos de cómputo?		**5**		HALLAZGOS/ **HEMDO_10**
5.	¿Las políticas y procedimientos referentes a la utilización y configuración del software y del hardware estas		**5**		ENTREVISTAS_A_ FUNCIONARIOS/

I. Empresa de obras sanitarias de la provincia de Obando EMPOOBANDO E.S.P.

A continuación se presentan los resultados de la auditoría aplicada al proceso de Contratación de TI de la Empresa de Obras Sanitarias de la Provincia de Obando, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditados.

DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

Proceso COBIT PO1: Definir un plan estratégico de TI

Hallazgos

No existe un grupo encargado de administrar y evaluar el funcionamiento de las Tecnologías de Información que están implementadas actualmente en la entidad.

REF [HALLAZGOS**/HEMDO_01**].

Recomendaciones

- ✓ Delegar a una persona idónea la labor de administrar y evaluar el funcionamiento de las tecnologías de Información implementadas en la entidad.
- ✓ Realizar reuniones periódicas con los operarios de los Sistemas de Información, con el fin de encontrar algún tipo de anomalías en el desempeño de los servicios que estas Tecnologías prestan a los procesos de la entidad para los cuales fueron implementados.

Proceso COBIT PO3: Determinar la dirección tecnológica.

Hallazgos

- ✓ Se hacen estudios de las nuevas tecnologías de punta, pero no se tiene un grupo especializado experto en el tema.
- ✓ Los estudios que se hacen no se documentan de la mejor manera para dejarlos como base para una futura implementación.

REF [HALLAZGOS**/HEMDO_02**].

Recomendaciones

- ✓ Delegar a una o varias personas idóneas y conocedoras de las nuevas TI para que realicen estudios de factibilidad para implementarlas en la entidad.
- ✓ Documentar adecuadamente estos estudios de las nuevas TI, para dejarlos como base para futuras implementaciones o confrontaciones con nuevas TI que aparezcan.

Proceso COBIT PO4: Definición de la organización y de las relaciones de TI

Hallazgos

- ✓ No existe un manual de funciones actualizado para los trabajadores de EMPOOBANDO E.S.P.
- ✓ No existe un manual de funciones para el personal encargado del mantenimiento preventivo y correctivo de hardware y software.
- ✓ No existe manual de funciones para los trabajadores encargados de registrar la contratación en SICE y SECOP.
- ✓ No existen planes de contingencia para reemplazar a funcionarios en caso de ausencia.
- ✓ No existen políticas adecuadas para la contratación de personal que se involucre con tecnologías de la información.
- ✓ No se aplican los principios de meritocracia para seleccionar personal.
- ✓ No todas las personas que cumplan los requisitos pueden ser candidatas al cargo.

REF [HALLAZGOS**/HEMDO_03**].

Recomendaciones

- ✓ Se recomienda actualizar el manual de funciones para los trabajadores de EMPOOBANDO E.S.P.
- ✓ Se recomienda crear un manual de funciones específico para los trabajadores que realizan el mantenimiento de hardware y software de la entidad.
- ✓ Se recomienda crear un manual de funciones específico para los funcionarios encargados de registrar en los sistemas SICE y SECOP.
- ✓ Se debe eliminar la dependencia hacia los funcionarios, con el objetivo de que los procesos críticos y su información este soportado por al menos dos funcionarios del mismo nivel.
- ✓ Se debe crear una política completamente clara acerca del proceso que permite la contratación de TI, esto debe hacerse desde el personal que hace la solicitud para la contratación de TI, hasta el personal encargado de evaluar y aprobar dicha solicitud. Esto permitirá que la entidad

contrate TI mucho más acorde a las necesidades que se tienen sin perder de vista el costo de su implementación.

- ✓ Se debe hacer uso del principio de meritocracia para seleccionar el personal nuevo para las TI, con el objetivo de que se desarrollen a cabalidad las funciones para dichos cargos.

Proceso COBIT PO5: Administrar la inversión de TI

Hallazgos

- ✓ No existe un grupo idóneo para administrar los costos reales con los presupuestados para la implementación de las TI.
- ✓ No existen unas políticas bien establecidas para la administración de los costos reales con los presupuestados para la adquisición de las TI.
- ✓ Los costos no se monitorean para detectar cuando existen desviaciones.

REF [HALLAZGOS**/HEMDO_04**].

Recomendaciones

- ✓ Delegar el proceso de administración de costos reales con los presupuestados, a personal idóneo y conocedor de la importancia de las TI para la entidad.
- ✓ Establecer unas políticas claras, que permitan llevar a cabo y de forma optima el proceso de administrar los presupuestos encaminados a la implementación de las TI.
- ✓ Monitorear el estudio de los costos de implementación de TI, para poder tomar los correctivos necesarios en caso de existir desviaciones en el tiempo.

Proceso COBIT PO7: Administración de recursos humanos de TI

Hallazgos

- ✓ No existen políticas y/o procedimientos claros, ni personal idóneo para realizar el proceso de contratación de personal para TI.
- ✓ No se toma en cuenta especificaciones mínimas para asignar un cargo.
- ✓ No se aplican procesos de selección transparentes ante la sociedad.
- ✓ No se dan a conocer de forma clara cuales son las funciones, responsabilidades y políticas de seguridad de la información a los empleados nuevos para las TI.
- ✓ No se evalúa periódicamente el rendimiento del personal encargado de las TI.

- ✓ No existen planes de contingencia para evitar el cese de actividades en caso de ausencia de un trabajador indispensable en lo referente a las TI.

REF [HALLAZGOS**/HEMDO_05**].

Recomendaciones

- ✓ Crear políticas y procedimientos claros para la contratación de personal de TI, con el objetivo de hacer que esta actividad sea optima, ajustada a las necesidades y que sobre todo garantice los intereses de la entidad.
- ✓ Delegar para la solicitud, estudio y aprobación de la contratación de TI a personal idóneo y conocedor de estas tecnologías.
- ✓ Se debe tener en cuenta algunas especificaciones mínimas como el perfil (técnico - profesional), tiempo de experiencia, etc. para los cargos de las Tecnologías de Información.
- ✓ Al momento de seleccionar al personal para los cargos relacionado con las TI, hacer uso del principio de meritocracia para contratar personal idóneo y calificado para realizar las funciones en dichos cargos.
- ✓ Implementar un manual de funciones para los cargos relacionados con las tecnologías de información. Con el objetivo de darla a conocer a los empleados nuevos y antiguos.
- ✓ Implementar y dar a conocer a los funcionarios de la entidad, las políticas y procedimientos para la seguridad de la información de las TI.
- ✓ Evaluar periódicamente a los funcionarios relacionados con las tecnologías de información, para verificar la calidad de su trabajo y desempeño.
- ✓ Si no se puede eliminar la dependencia de los funcionarios para ciertas actividades criticas relacionadas con las TI, sería recomendable crear un plan de contingencia para que algún funcionario en el mismo nivel pueda reemplazar al trabajador que se encuentra ausente.

Proceso COBIT PO9: Evaluación y análisis de riesgos

Hallazgos

- ✓ No se evalúa periódicamente la probabilidad e impacto de los riesgos identificados, que inciden en la pérdida de la información que manejan las TI.
- ✓ No se encuentra muy bien documentado el plan de contingencia para la recuperación de la información en caso de pérdida o alteración de la misma.
- ✓ No existen políticas o procedimientos guía, para la adquisición de pólizas de seguro ante el riesgo residual.

REF [HALLAZGOS**/HEMDO_06**].

Recomendaciones

- ✓ Se recomienda evaluar periódicamente la probabilidad de ocurrencia e impacto de los riesgos en contra de la información de las TI, a fin de disminuirlos gradualmente para mitigar su efecto.
- ✓ Documentar adecuadamente el plan de contingencia para la recuperación de la información de las TI, con el objetivo de que esta tarea sea fácil, automática y se lleve a cabo en su totalidad.

DOMINIO - ADQUIRIR E IMPLEMENTAR (AI)

Proceso COBIT AI3: Adquisición y mantenimiento de la Infraestructura tecnológica.

Hallazgos

- ✓ Las políticas y procedimientos para la adquisición de sistemas de información no se encuentran bien fundamentadas.
- ✓ No se tiene en cuenta los riesgos tecnológicos que se pueden adquirir cuando se implementa cualquier tecnología de información.
- ✓ No se hacen evaluaciones de factibilidad a las TI implementadas en la entidad.
- ✓ El manual de funciones y/o procedimientos para el mantenimiento preventivo de los equipos de la entidad no es completo.
- ✓ El manual de funciones y/o procedimientos para la reparación de equipos defectuosos de la entidad no son los más óptimos.
- ✓ Dentro de las políticas y procedimientos para la adquisición de hardware, no se encuentra bien fundamentada ni documentada la adquisición de hardware en grandes cantidades.
- ✓ Dentro de las políticas y procedimientos para la adquisición de software, no se encuentra bien fundamentada ni documentada la adquisición de software a gran escala.

REF [HALLAZGOS**/HEMDO_07**].

Recomendaciones

- ✓ Se debe documentar adecuadamente las políticas para la adquisición de los Sistemas de Información.
- ✓ Dentro de las políticas para adquirir los SI, se deben tener en cuenta los riegos tecnológicos que pueden haber con su implementación.
- ✓ Se debe revisar y evaluar el servicio que están prestando las TI implementadas en la entidad actualmente.

- ✓ Se debe completar las políticas para el mantenimiento de hardware (limpiar físicamente, desfragmentar disco, borrar archivos temporales, etc.), con el objetivo de evitar daños en un futuro.
- ✓ Se deben implementar algunos procedimientos documentables (entrega del equipo a mantenimiento, recepción del equipo por parte de mantenimiento, entrega del equipo ya reparado al funcionario responsable del equipo, recibido a satisfacción) de rutina, dentro de las políticas de reparación de hardware, con el fin de que el proceso de intercambiar los equipos con el personal de mantenimiento sea más transparente.
- ✓ Se debe modificar las políticas y procedimientos para que se permita la adquisición de hardware especializado.
- ✓ Se debe modificar las políticas y procedimientos para que se permita la adquisición de software a gran escala.

Proceso COBIT AI5: Adquirir recursos de TI

Hallazgos

- ✓ Las políticas y procedimientos para la selección de los proveedores de las TI, no se aplican correctamente.
- ✓ No se verifica que el proveedor este registrado en el SICE.
- ✓ La selección del proveedor, en ocasiones no garantiza que la TI que éste ofrece satisfaga las necesidades de la entidad.
- ✓ La selección del proveedor, no se hace teniendo en cuenta el costo de la TI que éste ofrece y el beneficio que ésta otorgaría a la entidad.
- ✓ No se hacen cumplir las obligaciones que adquiere el proveedor con la entidad, cuando el contrato no se desarrolla a cabalidad en los términos y plazos pactados.

REF [HALLAZGOS**/HEMDO_08**].

Recomendaciones

- ✓ Aplicar adecuadamente las políticas y procedimientos para seleccionar a los proveedores de las TI.
- ✓ Antes de seleccionar al proveedor es necesario que se verifique que éste se encuentre registrado en el SICE, para hacer más transparente la contratación.
- ✓ Hacer buen uso de las políticas y procedimientos para seleccionar al proveedor de TI, a fin de que sean éstas las que realmente necesita la entidad.

- ✓ Se debe empezar a estudiar desde las tecnologías más económicas que satisfagan las necesidades de la entidad, con el objetivo de evitar el sobre gasto.
- ✓ Se deben hacer cumplir las obligaciones y responsabilidades del proveedor de los contratos de TI, desde el comienzo.

DOMINIO - ENTREGAR Y DAR SOPORTE (DS)

Proceso COBIT DS5: Garantizar la seguridad de sistemas

Hallazgos

- ✓ No existe un plan de seguridad para que los funcionarios de la entidad sean identificados de manera única.
- ✓ El acceso a los equipos de cómputo que contienen información critica, no se restringe con cuenta de usuario y contraseña.
- ✓ No existen políticas ni procedimientos para la escogencia de contraseñas.
- ✓ No existe un documento que permita entrenar a los empleados nuevos sobre la seguridad en las TI dentro de la entidad.
- ✓ No existe personal ni procedimientos para detectar y eliminar software dañino.
- ✓ Los programas antivirus instalados en los equipos de cómputo, no se actualizan en cortos periodos de tiempo.

REF [HALLAZGOS**/HEMDO_09**].

Recomendaciones

- ✓ Se debe crear y poner en marcha un plan que permita identificar de manera única a los funcionarios de la entidad.
- ✓ Se debe hacer uso de las cuentas de usuario y contraseña en los equipos de cómputo, para garantizar la seguridad de la información.
- ✓ Se deben crear y poner en práctica las políticas y procedimientos, para realizar el proceso de creación, escogencia, almacenamiento y cambio de contraseñas de forma segura, para restringir el acceso a la información de los equipos de cómputo.
- ✓ Se debe crear los documentos que permitan instruir a los nuevos funcionarios sobre la seguridad de las TI de la entidad.
- ✓ Se debe contar con una persona experta en la detección y eliminación de software dañino (virus), para evitar posibles daños y pérdidas de los equipos de cómputo y la información de las TI, respectivamente.
- ✓ Actualizar en cortos periodos de tiempo el software que defiende los equipos de cómputo de la entidad.

Proceso COBIT DS9: Administración de la configuración

Hallazgos

- ✓ No existen políticas y procedimientos respecto al software que la entidad permite instalar en los equipos de cómputo.
- ✓ No existen políticas y procedimientos respecto al hardware permitido por la entidad.
- ✓ No existe ningún tipo de control para evitar que los funcionarios utilicen software y hardware desconocido o ajeno a la entidad.

REF [HALLAZGOS**/HEMDO_10**].

Recomendaciones

- ✓ Crear y poner en marcha políticas y procedimientos claros, que permitan dar a conocer a los funcionarios que hardware y software pueden instalar en los equipos de cómputo de la entidad.
- ✓ Realizar controles periódicos a los equipos de cada uno de los funcionarios, con el objetivo de verificar que el hardware y software instalado en estos, es el permitido por la entidad.

Proceso COBIT DS11: Administración de datos

Hallazgos

- ✓ No existen políticas y procedimientos documentados para establecer cómo, cuándo y dónde se hacen las copias de seguridad de la información que maneja la entidad.
- ✓ No existen procedimientos definidos para la eliminación de la información de los equipos de cómputo.
- ✓ No existen procedimientos definidos para los periodos de retención de las copias de seguridad de la información.
- ✓ La información de contratación de TI y demás, es almacenada en el archivo central de la entidad, junto con las copias de seguridad que descansan solo en ese lugar, lo que ocasionaría pérdidas ante posibles desastres o daños en los medios que la contienen.

REF [HALLAZGOS**/HEMDO_11**].

Recomendaciones

- ✓ Crear la documentación de las políticas y procedimientos para las copias de seguridad de la información de la entidad.

- ✓ Crear procedimientos para la eliminación de información de los equipos de cómputo.
- ✓ Crear un plan dentro de las políticas y procedimientos, para almacenar las copias de seguridad en un lugar exterior a la entidad.
- ✓ Crear políticas y procedimientos que permitan establecer los periodos de tiempo que permanecerán vigentes las copias de seguridad, según el tiempo de creación y relevancia para la entidad.

Proceso COBIT DS12: Administración del las instalaciones

Hallazgos

- ✓ No existen políticas de seguridad para el ingreso a las instalaciones de la entidad, incluyendo las áreas restringidas.
- ✓ No existen políticas y procedimientos documentados, para asegurar las instalaciones ante cualquier eventualidad de desastre causada por el ambiente o por personas inescrupulosas.
- ✓ No existen políticas para la adquisición de pólizas de seguro para daños en las instalaciones y los equipos de cómputo.
- ✓ La entidad no cuenta con un centro de cómputo adecuado, y no posee la seguridad necesaria para el ingreso al personal no autorizado.
- ✓ Las instalaciones no cuentan con dispositivos detectores de humo, calor, supresores de humo, etc.
- ✓ Las instalaciones no cuentan con un servicio de cámaras de seguridad ni personal de seguridad dentro de ellas.

REF [HALLAZGOS**/HEMDO_12**].

Recomendaciones

- ✓ Se recomienda establecer políticas de seguridad para el ingreso a las instalaciones de la entidad.
- ✓ Se recomienda desarrollar, plasmar e implementar políticas para proteger las instalaciones ante cualquier eventualidad de desastre causada por el ambiente o por personas inescrupulosas.
- ✓ Se recomienda establecer políticas para adquirir pólizas de seguro, para las instalaciones y equipos de cómputo de la entidad.
- ✓ Se recomienda crear un centro de cómputo con las condiciones necesarias para asegurar las condiciones de trabajo de las TI.
- ✓ Se recomienda la instalación de dispositivos (detectores de humo, calor, etc.) que permitan la detección de fuego.
- ✓ Se recomienda que las instalaciones estén monitoreadas por el servicio de cámaras de seguridad, además que los vigilantes hagan presencia dentro de las instalaciones.

DOMINIO - MONITOREAR Y EVALUAR (ME)

Proceso COBIT M2: Evaluar lo adecuado del control interno

Hallazgos

- ✓ No existen políticas y procedimientos encaminados al monitoreo de las actividades que garantizan la seguridad física y lógica de la información de las TI.

REF [HALLAZGOS**/HEMDO_13**].

Recomendaciones

- ✓ Crear las políticas de monitoreo, que permitan brindar mayor seguridad física y lógica a los activos de las tecnología de la información y del proceso de Contratación de TI.

Proceso COBIT M3: Garantizar el cumplimiento con requerimientos externos

Hallazgos

- ✓ No se verifica que el proveedor de TI, se encuentre registrado en el Sistema de Información para la Contratación Estatal, antes de celebrar algún contrato de esta naturaleza.
- ✓ No se comparan los costos de las ofertas de contratos de TI con los estipulados en el RUPR (Registro Único de Precios de Referencia).
- ✓ Los contratos de TI, no son registrados en los tiempos estipulados por la norma, y muchos de ellos ni siquiera se registran en el SICE.

REF [HALLAZGOS**/HEMDO_14**].

Recomendaciones

- ✓ Verificar los lineamientos establecidos en la ley 598 del 2000, en donde se describen los requisitos a tener en cuenta para contratar TI con los proveedores.
- ✓ Comparar los costos de las ofertas de contratos del TI, con los establecidos por el RUPR.
- ✓ Realizar el registro de la Contratación de TI, como lo dicta la norma.

II. **Alcaldía Municipal de Ipiales:** A continuación se presentan los resultados de la auditoría aplicada al proceso Contratación TI de la Alcaldía Municipal de

Ipiales, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditado.

DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

Proceso COBIT PO3: Definir un plan estratégico de TI.

Hallazgos

- ✓ No existe personal idóneo en el campo de búsqueda de nuevas tecnologías de información para la entidad.
- ✓ No existen políticas ni procedimientos relacionadas con el estudio y análisis de nuevas tecnologías de información para ser implementadas en la entidad.
- ✓ No se lleva un registro documentado de los estudios de nuevas tecnologías de información.

REF [HALLAZGOS**/HAI_01**].

Recomendaciones

- ✓ Asignar personal idóneo para que se encargue del estudio de búsquedas de nuevas TI, a fin que éstas se ajusten a las necesidades sin dejar de lado el presupuesto y evitar así el sobre gasto.
- ✓ Crear políticas que estén relacionadas con la búsqueda de nuevas tecnologías de información para implementarlas en la entidad.
- ✓ Documentar los estudios que se realicen de nuevas tecnologías de información para lograr implementarlas en el futuro.

Proceso COBIT PO4: Definición de la organización y las relaciones de TI.

Hallazgos

No existe un manejo eficiente en el proceso de registro contractual en el portal SICE, puesto que se presentan irregularidades en el registro de algunos contratos.

REF [HALLAZGOS**/HAI_02**].

Recomendaciones

Realizar un manejo eficiente del proceso de los registros contractuales en el portal SICE, a fin de mantener la transparencia en este proceso ante los entes de control estatal.

Proceso COBIT PO5: Administrar la inversión de TI.

Hallazgos

No se realiza un proceso de monitoreo para la administración de costos reales con los presupuestados y no existe reporte oportuno cuando se detectan desviaciones.

REF [HALLAZGOS**/HAI_03**].

Recomendaciones

Implementar el proceso de monitoreo para administrar los costos reales con los presupuestados con el fin de detectar a tiempo las desviaciones.

DOMINIO - ENTREGAR Y DAR SOPORTE (DS)

Proceso COBIT DS11: Administración de los datos

Hallazgos

Las políticas relacionadas con copias de seguridad no contemplan la realización diaria de las mismas, sabiendo que en dependencias como es la de Hacienda se maneja información crítica todo los días.

REF [HALLAZGOS**/HAI_04**].

Recomendaciones

Modificar las políticas relacionadas con copias de seguridad, para realizar diariamente algunas de ellas y así minimizar el riesgo de pérdida de información critica para la entidad.

Proceso COBIT DS12: Administración de las instalaciones

Hallazgos

- ✓ No existen política adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones.
- ✓ Dentro de las políticas de seguridad para el acceso a la instalación no se tiene en cuenta la identificación, autenticación y autorización de los individuos que ingresan a las instalaciones.
- ✓ No se controla el acceso de elementos que faciliten el robo como es el caso de los bolsos.

- ✓ No se tiene en cuenta dentro de las políticas de seguridad de la entidad el registro de equipos de cómputo como son portátiles que ingresan a las instalaciones.
- ✓ No se tiene en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes, para controlar sus acciones en las instalaciones.
- ✓ No existe la instalación de dispositivos en el lugar donde se ubican los servidores (detectores humo, supresores de fuego) que permitan detectar y prevenir incendios.
- ✓ No existe la instalación de cámaras que permitan monitorear el interior de las instalaciones de la entidad.

REF [HALLAZGOS**/HAI_05**].

Recomendaciones

- ✓ Crear políticas adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones para evitar robos o perdida de la información.
- ✓ Crear políticas adecuadas en el campo de seguridad referente a la identificación, autenticación y autorización, de los individuos que ingresan a las instalaciones, con el objetivo de impedir que se atente contra los intereses de la entidad.
- ✓ Controlar el acceso de elementos como son bolsos para evitar que estos faciliten robos.
- ✓ Tener en cuenta dentro de las políticas de seguridad de la entidad, el registro de equipos de cómputo como son portátiles para impedir robo de equipos y robo de información de la entidad.
- ✓ Tener en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes para impedir robos, sabotajes en contra de la entidad.
- ✓ Instalar dispositivos como son (detectores de humo, supresores de fuego) para evitar sufrir un fortuito.
- ✓ Instalar cámaras en el interior de la alcaldía para registrar las actividades sospechosas de los individuos que ingresan a las instalaciones.

DOMINIO - MONITOREAR Y EVALUAR (ME)

Proceso COBIT M3: Evaluar lo adecuado del control interno

Hallazgos

No existe un registro para los contratos adquiridos mediante proveedores en el portal SICE dentro de los términos y tiempos establecidos por la ley.

REF [HALLAZGOS**/HAI_06**].

Recomendaciones

Realizar un registro de los contratos adquiridos mediante proveedores en el portal SICE en los términos y tiempos establecidos por la ley y así contribuir a la transparencia en el proceso de contratación.

Evaluación de la usabilidad y del decreto 1151 de 2008 de Gobierno en Línea. Alcaldía municipal de Ipiales.

Tabla 2. Información portal web Alcaldía de Ipiales.

1. La Entidad cuenta con un sitio Web?	
Nombre de la entidad	Alcaldía Municipal de Ipiales.
Municipio	Ipiales
Nit.	8000990957
Dirección	Parque 20 de Julio Edf. CAM Ipiales (Nariño)
Teléfono	7734044
Correo Electrónico	contactenos@ipiales-nariño.gov.co
X	SI
	NO
	En desarrollo
2. Si cuenta con un sitio web, o está en desarrollo escriba la dirección.	
	http://ipiales-narino.gov.co
3. La entidad cuenta con un Comité de Gobierno en línea? Si la respuesta es positiva indicar el acto administrativo y fecha de expedición.	
	SI ACTO ADMINISTRATIVO _____
X	NO
4. Si la respuesta fue SI, relacione los cargos de los integrantes del Comité de Gobierno en Línea:	
	_____
	_____
	_____
	_____
	_____
5. Con que periodicidad se reúne el comité de Gobierno en línea	
	Mensualmente
	Bimensualmente
	Trimestralmente
	Semestralmente
	Otro CUAL?
6. El comité realiza un seguimiento sobre la implementación de Gobierno en línea en la entidad?	
	SI
	NO
7. El comité ha realizado algún informe sobre el avance de la implementación de la estrategia del Gobierno en línea.	
	SI

	NO

Las siguientes preguntas pertenecen a la primera Fase de la estrategia (Información en línea), y deberán responderse teniendo en cuenta la inclusión o existencia de la respectiva información, en el sitio Web de la Entidad.

Marcar **SI** cuando el sitio Web contenga la información indicada.
Marcar **NO** cuando el sitio Web no tenga la información indicada.
Marcar **EN DESARROLLO** cuando el ítem respectivo se encuentre en elaboración.

Tabla 3. Primera fase de desarrollo del portal web Alcaldía de Ipiales.

1. Acerca de la Entidad	SI	NO	EN DESARROLLO
a. Misión y visión	X		
b. Objetivos y funciones	X		
c. Organigrama		X	
d. Localización física (incluyendo todas las sedes o sucursales)	X		
e. Teléfonos y/o líneas gratuitas y fax	X		
f. Correo electrónico de contacto	X		
g. Horarios y días de atención al público	X		
h. Directorio de funcionarios principales	X		
i. Directorio de entidades	X		
j. Directorio de agremiaciones y asociaciones		X	

2. Leyes y normatividad vigentes	SI	NO	EN DESARROLLO
a. Leyes/ Ordenanzas /Acuerdos	X		
b. Decretos		X	
c. Resoluciones y/u otros actos administrativos de carácter general		X	
d. Proyectos de normatividad		X	

3. Presupuesto	SI	NO	EN DESARROLLO
a. Presupuesto aprobado en ejercicio de acuerdo con las normas vigentes	X		
b. Información histórica de presupuestos		X	

4. Políticas, planes, programas y proyectos institucionales	SI	NO	EN DESARROLLO

Tabla 3. Primera fase de desarrollo del portal web Alcaldía de Ipiales. (Continuación)

a. Políticas, planes y/o líneas estratégicas		X	
b. Programas y proyectos en ejecución	X		
c. Contacto con dependencia responsable		X	

5. Contratación	SI	NO	EN DESARROLLO
a. Información sobre Licitaciones, selecciones abreviadas, concurso de mérito y Contratación Directa		X	
b. Información sobre Contratos en Ejecución	X		

6. Control y rendición de cuentas	SI	NO	EN DESARROLLO
a. Entes de control que vigilan a la Entidad	X		
b. Informes de gestión	X		
c. Metas, indicadores de gestión y/o desempeño y resultados		X	
d. Plan de mejoramiento	X		

7. Servicios de información	SI	NO	EN DESARROLLO
a. Información para niños	X		
b. Preguntas y respuestas frecuentes		X	
c. Boletines y publicaciones			X
d. Noticias	X		
e. Calendario de actividades	X		
f. Glosario	X		
g. Política de privacidad y condiciones de uso		X	

8, Estándares de Presentación	SI	NO	EN DESARROLLO
a. Identidad visual (escudo de la República e identidad visual de la Entidad)	X		
b. Enlace al Portal del Estado Colombiano www.gobiernoenlinea.gov.co	X		
c. Fecha de la última actualización del sitio Web	X		
d. División de los contenidos (dividido)	X		
e. Uso de colores (pocos colores, sin caer en un diseño monótono)	X		
f. Manejo de vínculos (textos que indiquen claramente al usuario el contenido de la página Web)	X		

Tabla 3. Primera fase de desarrollo del portal web Alcaldía de Ipiales. (Continuación)

9. Estándares de Funcionalidad	SI	NO	EN DESARROLLO
a. Mapa del sitio	X		
b. Acceso a la página de inicio	X		
c. Acceso al menú principal	X		

10. Estándares Técnicos	SI	NO	EN DESARROLLO
a. Nombre del dominio con formato www.nombredelaentidad.gov.co, .edu.co ó .mil.com	X		
b. Tiempo de despliegue de una página en el navegador de usuario no mayor a 20 segundos	X		
c. Elementos como gráficos o archivos sonoros marcados y/o etiquetados con una descripción de su contenido	X		
d. Elementos gráficos que se muevan, parpadeen se desplacen o se actualicen automáticamente con la posibilidad de ser detenidos temporal o totalmente.	X		

Herramienta de verificación de cumplimiento de los lineamientos del decreto 1151 de 2008, proporcionado por la contraloría departamental de Nariño.

Usabilidad

Institución: ***Alcaldía Municipal de Ipiales***
Url: http://ipiales-narino.gov.co
Evaluador: ***Luis Eduardo Pantoja Rodríguez – Gerardo Antonio Ramos G.***
Fecha: ***19/06/2010***
Nota: ***7.13***

Tabla 4. Evaluación de usabilidad Alcaldía de Ipiales.

20%		1. Usabilidad	7,215	1,4431
	40%	1.1 Comprensibilidad Global del Sitio	8,208	3,2833
		1.1.1 Esquema de Organización Global	10	
		1.1.1.1 Mapa del Sitio	10	
		1.1.1.2 Índice Global (por Temas, etc.)	10	
		1.1.1.3 Tabla de Contenidos	10	
		1.1.2 Calidad en el Sistema de Etiquetado	5,5	
		1.1.2.1 Etiquetado Textual	9	
		1.1.2.2 Etiquetado con Iconos	2	
		1.1.3 Visita Guiada	N/A	
		1.1.3.1 Visita Convencional	N/A	
		1.1.3.2 Visita Virtual (con Tecnología VR)	N/A	
		1.1.4 Página Principal	9,333	
		1.1.4.1 Navegabilidad de la página principal	10	
		1.1.4.2 Impacto de la página principal	8,667	
		1.1.4.2.1 La página principal refleja la idea del sitio	10	
		1.1.4.2.2 La página principal deja claro que puedo hacer en el sitio	9	
		1.1.4.2.3 La página principal se ve bien al deshabilitar las imágenes	7	
		1.1.5 Consistencia de la navegación	8	
	10%	1.2 Mecanismos de Ayuda y Retroalimentación en línea	5	0,475
		1.2.1 Calidad de la Ayuda	5	
		1.2.1.1 Ayuda Explicatoria acerca del sitio	10	
		1.2.1.2 Ayuda de la Búsqueda	0	
		1.2.2 Indicador de Ultima Actualización	6	
		1.2.2.1 Global (de todo el sitio Web)	10	
		1.2.2.2 Restringido (subsitio o página)	0	
		1.2.2.3 Por noticias (Solo ultimas noticias)	8	
		1.2.3 Directorio de Enlaces	8	
		1.2.3.1 Enlaces a sitios de Interes	10	
		1.2.3.2 Enlaces a asociaciones de interes	6	
		1.2.4 Facilidad FAQ	0	
	10%	1.3 Aspectos de Interfaces y Estéticos	9,833	0,9833

Tabla 4. Evaluación de usabilidad Alcaldía de Ipiales (Continuación).

		1.3.1 Cohesividad al Agrupar los Objetos de Control Principales	**8**	
		1.3.2 Permanencia y Estabilidad en la Presentación de los Controles Principales	**10**	
		1.3.2.1 Permanencia de Controles Directos	10	
		1.3.2.2 Permanencia de Controles Indirectos	10	
		1.3.2.3 Estabilidad	10	
		1.3.3 Preferencia Estética	**9**	
		1.3.4 Uniformidad en el Estilo del sitio	**10**	
	10%	**1.4 Misceláneas**	**5**	
		1.4.1 Soporte a Lenguaje Extranjero	**0**	
		1.4.2 Descarga de contenidos	**N/A**	
		1.4.2.1 Descarga de contenidos a multidispositivo	N/A	
		1.4.2.2 Descarga de contenidos	N/A	
		1.4.3 Intrusión publicitaria	**10**	
	15%	**1.5 Usabilidad de los Textos**	**10**	**1,5**
		1.5.1 Textos adaptados para la Web	**10**	
		1.5.1.1 Textos breves	10	
		1.5.1.2 Textos escaneables	10	
		1.5.1.3 Estilo de escritura conciso	10	
	15%	**1.6 Clasificación de la información**	**5,5**	**0,825**
		1.6.1 Categorías	5,5	
		1.6.1.1 Claridad de las categorías	6	
		1.6.1.2 Cohesión de las categorías	5	
10%		**2. Accesibilidad**	**9,75**	**0,975**
	70%	**2.1 Accesibilidad para usuarios con discapacidades**	**9,5**	**6,65**
		2.1.1 Discapacidades visuales	**10**	
		2.1.1.1 Posibilidad de modificar el tamaño de las fuentes	10	
		2.1.1.2 Combinaciones de color (para usuarios con ceguera al color)	N/A	
		2.1.1.3 Markup claro para poder ser leído por un lector de pantalla	N/A	
		2.1.1.4 Etiquetas ALT en todas las imágenes	9	
		2.1.2 Discapacidades auditivas	**9**	
	10%	**2.2 Acceso a navegadores no gráficos**	**N/A**	
	10%	**2.3 Acceso Multidispositivo**	**10**	**1**
15%		**3. Funcionalidad**	**8,482**	**1,2723**
	50%	**3.1 Aspectos de Búsqueda**	**7**	**3,5**
		3.1.1 Mecanismo de Búsqueda en el Sitio	**4**	
		3.1.1.1 Búsqueda Restringida (por secciones)	0	

Tabla 4. Evaluación de usabilidad Alcaldía de Ipiales (Continuación).

		3.1.1.2 Búsqueda Global	8	
		3.1.2 Búsqueda siempre disponible	**10**	
	50%	**3.2 Aspectos de Navegación y Exploración**	**9,964**	**4,9821**
		3.2.1 Navegabilidad Local (de subsitio)	**9,75**	
		3.2.1.1 Nivel de Interconexión	9	
		3.2.1.2 Orientación	10	
		3.2.1.2.1 Indicador del Camino	10	
		3.2.1.2.2 Etiqueta de la Posición Actual	10	
		3.2.2 Navegabilidad Global	**10**	
		3.2.2.1 Acoplamiento entre Subsitios	10	
		3.2.3 Objetos de Control Navegacional	**10**	
		3.2.3.1 Permanencia y Estabilidad en la Presentación de los Controles Contextuales	**10**	
		3.2.3.1.1 Permanencia de los Controles Contextuales	10	
		3.2.3.1.2 Estabilidad	10	
		3.2.3.2 Nivel de Desplazamiento	**10**	
		3.2.3.2.1 Desplazamiento Vertical	10	
		3.2.3.2.2 Desplazamiento Horizontal	10	
		3.2.4 Predicción Navegacional	**10**	
		3.2.4.1 Enlace con Título (enlace con texto explicatorio)	10	
		3.2.4.2 Calidad de la Frase del Enlace	10	
		3.2.5 Funciones Misceláneas y Específicas del Dominio	**10**	

40%		**4 Contenidos**	**5,049**	**2,0194**
	30%	**4.1 Información Institucional**	**10**	**3**
		4.1.2 Plan de Accion	**10**	
		4.1.2.1 Planes de accion actual	10	
		4.1.1.2 Planes de accion futuros	10	
		4.1.3 Información sobre las Dependencias	**10**	
		4.1.3.1 Funciones de las dependencias	10	
		4.1.3.2 Horarios de atencion de las Dependencias	10	
		4.1.4 Valores Institucionales	**10**	
		4.1.4.1 Misión y Visión	10	
		4.1.4.3 Historia	10	
	18%	**4.2 Información sobre las directivas institucionales**	**1,5**	**0,27**
		4.2.1 Curriculum de los directivos	**3**	
		4.2.1.1 Intereses Institucionales	3	
		4.2.1.2 Hoja de vida	3	
		4.2.3 Información de contacto	**0**	
		4.2.3.3 Mail directivo	0	
	13%	**4.4 Información sobre las Dependencias**	**5**	**0,65**
		4.4.1 Objetivos	**3**	

Tabla 4. Evaluación de usabilidad Alcaldía de Ipiales (Continuación).

		4.4.2 Funciones	**7**	
	13%	**4.5 Información sobre Beneficios a Usuarios**	**0**	**0**
		4.5.1 Lista de beneficios	**0**	
		4.5.2 Descripción de las beneficios	**0**	
		4.5.3 Información adicional	**0**	
	13%	**4.6 Información de contacto de la Institución**	**3,792**	**0,4929**
		4.6.1 Ubicación	**5,333**	
		4.6.1.1 Como llegar (transportes, distancias, etc.)	8	
		4.6.1.2 Mapa geográfico	8	
		4.6.1.3 Mapa interno	0	
		4.6.2 Contacto con responsables / asesores	**2,25**	
		4.6.2.1 Nombre	3	
		4.6.2.2 Correo	0	
		4.6.2.3 Teléfono	3	
		4.6.2.4 Fax	3	
	13%	**4.8 Información para externos a la Institucion**	**10**	
		4.8.2 Claridad de Misión y Visión	**10**	
		4.8.3 Información geográfica	**10**	

7,5%		**5. Confiabilidad**	**9,556**	**0,7167**
	50%	**5.1 Ausencia de Deficiencias y Errores**	**8,667**	**4,3333**
		5.1.1 Errores de Enlaces	**6**	
		5.1.1.1 Enlaces Rotos	6	
		5.1.1.2 Enlaces Inválidos	6	
		5.1.1.3 Enlaces no Implementados	6	
		5.1.2 Errores o Deficiencias Varias	**10**	
		5.1.2.1 Deficiencias o cualidades ausentes debido a diferentes navegadores	10	
		5.1.2.2 Nodos Web Muertos (sin enlaces de retorno)	10	
		5.1.2.3 Nodos Destinos (inesperadamente) en Construcción	10	
		5.1.3 Enlaces externos a instituciones prestigiosas	**10**	
	25%	**5.2 Utilización de estándares del W3C**	**10**	**2,5**
		5.2.1 HTML	10	
		5.2.2 CSS	10	
	25%	**5.3 Actualizacion periódica de la información**	**10**	**2,5**

7,5%		**6. Eficiencia**	**9,333**	**0,7**
	60%	**6.1 Accesibilidad de Información**	**10**	**6**
		6.1.1 Soporte a Versión sólo Texto	**N/A**	
		6.1.2 Legibilidad al desactivar la Propiedad Imagen del Browser	**10**	
		6.1.2.1 Imagen con Título	10	

Tabla 4. Evaluación de usabilidad Alcaldía de Ipiales (Continuación).

		6.1.2.2 Legibilidad Global	10	
	20%	**6.2 Rendimiento**	**10**	**2**
	20%	**6.3 Tiempo de descarga**	**8**	**1,6**

Herramienta para la evaluacion de desempeño y calidad de software patenetada en la unidersidad de Salamanca.

A raiz de las evaluaciones descritas anteriormente el equipo auditor plasmo una serie de recomendaciones, junto con el soporte legal que fueron entregados a la Contraloria Departamental de Nariño y que se describen a continuacion.

4.3 INFORME TÉCNICO PRESENTADO A LA ENTIDAD CONTRALORÍA DEPARTAMENTAL DE NARIÑO

4.3.1. Informe empresa de obras sanitarias de la provincia de Obando EMPOOBANDO E.S.P. En el siguiente apartado se encuentra descrito el informe técnico presentado ante la entidad Contraloría Departamental de Nariño por parte del equipo auditor.

OFICINA DE SISTEMAS
HALLAZGOS ADMINISTRATIVOS
EMPRESA DE OBRAS SANITARIAS DE LA PROVINCIA DE OBANDO

DATOS GENERALES DE LA AUDITORIA

Modalidad de Auditoria	Auditoria de sistemas.
Periodo Evaluado	2008.
Líneas de Auditoria	Decreto 1151 del 14 de abril de 2008.
Contratación	
Seguridad informática	
Fecha de Iniciación	20/Octubre/2009.
Líder Equipo Auditor	Ing. Julián Yecít Melo Zambrano.

DATOS GENERALES DE LA ENTIDAD

Nombre o razón Social	Empresa de Obras Sanitarias de la Provincia de Obando Empoobando E.S.P.
NIT No.	800140132.
Naturaleza Jurídica	E.S.P.
Representante Legal	Juan Carlos Bustos Montenegro.
Cargo	Gerente.

Dirección. Carrera 7 calle 30 Esquina Barrio Puenes.

EVALUACION DEL DECRETO 1151 DEL 14 DE ABRIL DE 2008

Revisando y analizado el cumplimiento de los lineamientos del decreto 1151 de 2008 por medio de la confrontación del MANUAL PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA DE LA REPÚBLICA DE COLOMBIA con cada uno de los ítems de la página web y teniendo en cuenta que en el artículo 8 del presente decreto establece que se debe cumplir hasta la fase de información la cual tiene un plazo máximo de 1ro de noviembre de 2008, el grupo auditor logró establecer que la entidad no cumple con ninguno de los lineamientos, puesto que no cuenta con el Portal Web. Además argumentan desconocer el decreto y sus implicaciones:

CONCEPTO TECNICO

Revisando los lineamientos del decreto 1151 de 2008, se encontró que esta entidad no posee el portal Web, el cual lo solicita el Gobierno Nacional por medio del Ministerio de Comunicaciones, a través del Programa Agenda de Conectividad, con la responsabilidad de coordinar la implementación de la Estrategia de Gobierno en Línea requerido en el decreto 1151 del 14 de Abril del 2008, por tal razón la empresa no ha está dando cumplimiento con las fechas fijadas dentro del decreto en mención para la implementación del Portal Web.

Por otra parte se encontró que por presunta falta de preocupación y de información correcta por parte de los funcionarios de la empresa EMPOOBANDO, no se tiene el Portal Web requerido, sino que se tiene un Link en la Pagina de la Alcaldía de Ipiales **www.ipiales-narino.gov.co** pagina de Gobierno en línea que posee la Alcaldía de Ipiales. Dentro de este link se muestra únicamente la información general de la Empresa. [EVIDENCIA_FOTOGRAFICA**/IMG_60 - IMG_64**].

Para el cumplimiento de las fases y de los plazos establecidos por la estrategia de Gobierno en Línea el Procurador General, Alejandro Ordóñez Maldonado, expidió la circular No. 058, dirigida a todos los funcionarios que integran la Administración Pública, del orden nacional y territorial.

“De esta manera, en defensa del derecho a la información y en procura de garantizar el cumplimiento de disposiciones constitucionales y legales, la Procuraduría General de la Nación considera conveniente advertir la necesidad de dar cumplimiento a lo dispuesto en el Decreto 1151 de 2008 y el Manual para la implementación de la Estrategia de Gobierno en línea.”

Señala la circular 058, que el incumplimiento de lo dispuesto en el Decreto y el Manual implicará sanciones disciplinarias por parte de este organismo.

Por Otra parte se observa que no se maneja un Correo Electrónico Institucional que le permita darse a conocer como una entidad más autónoma e independiente. [EVIDENCIA_FOTOGRAFICA**/IMG_64**]. La dirección del correo electrónico que se maneja es **empoobando@hotmail.com.** Lo ideal y recomendado por el Ministerio de Comunicaciones es que se maneje un correo institucional para la empresa, en donde se pueda dar a conocer quien emite comunicados o a quien se le escribe en caso de algún proceso en donde se deba interactuar con la comunidad, un ejemplo podría ser: **gerencia@empoobando.com** el dominio de esta dirección ya da a conocer que se maneja un correo particular para la empresa EMPOOBANDO y de esta forma cada funcionario o dependencia puede crear su cuenta con ese dominio en particular.

La Estrategia de Gobierno En Línea contribuye con la construcción de un Estado más eficiente, más transparente, más participativo y que preste mejores servicios a los ciudadanos y a las empresas, mediante el aprovechamiento de las Tecnologías de la Información y las Comunicaciones. Esta estrategia se compone entonces de tres objetivos estratégicos:

- Mejorar la provisión de servicios a los ciudadanos y las empresas: considera el establecimiento de nuevas formas de relación gobierno-ciudadano que permitan al Estado brindar sus servicios en forma eficiente, eficaz, con calidad y con independencia de las variables de tiempo y espacio.

- Fortalecer la transparencia del Estado y la participación ciudadana: se concentra en el fomento y la creación de mecanismos que permitan al ciudadano jugar un rol activo en el quehacer del país, abriendo nuevos espacios y formas de participación ciudadana sustentado en gran parte por la publicidad de información.

- Mejorar la eficiencia del Estado: busca la concepción y el establecimiento de procesos al interior de las entidades del Estado que permitan la integración de los sistemas de los diferentes servicios, compartir recursos y mejorar la gestión interna en las instituciones públicas y por consiguiente la eficiencia del Estado.

ANALISIS DE CONFORMACION DE COMITÉ DE GOBIERNO EN LINEA:

Una vez realizada la visita a la entidad se determinó que no se ha conformado hasta la fecha un comité de gobierno en línea

ANALISIS DE LA FASE DE INFORMACION Al no cumplir con la implementación del Portal Web requerido a través del decreto 1151 de 2008 de la Estrategia de

Conectividad de Gobierno en Línea, se establece que no cumple con los siguientes ítems:

- Horarios y días de atención al público
- Directorio de entidades
- Directorio de agremiaciones y asociaciones
- Leyes/ ordenanzas /acuerdos, decretos, resoluciones y/u otros actos administrativos de carácter general.
- Proyectos de normatividad: Son normas que están en proceso de expedición, de temas relacionados con la competencia de la entidad, durante el período de su presentación hasta su sanción. En la página no se muestra ningún proyecto de normatividad
- Presupuesto aprobado en ejercicio de acuerdo con las normas vigentes.
- Información histórica de presupuestos.
- Políticas, planes y/o líneas estratégicas, programas y proyectos en ejecución, contacto con dependencia responsable.
- Información sobre licitaciones, selecciones abreviadas, concurso de mérito y contratación directa.
- Información sobre Contratos en Ejecución.
- Metas, indicadores de gestión y/o desempeño y resultados: Se debe publicar la información relacionada con metas, indicadores de gestión y/o desempeño y los resultados mensualizados frente a las metas. No existen publicados indicadores de gestión y/o desempeño con resultados mensualizados y confrontados con las metas.
- Información para niños, calendario de actividades, glosario, política de privacidad y condiciones de uso.
- Boletines y publicaciones.
- Noticias.
- Escudo de la república de Colombia, Enlace al Portal del Estado Colombiano www.gobiernoenlinea.gov.co, fecha de la última actualización del sitio Web.

OBSERVACIONES

El grupo auditor logró determinar que la entidad no cumple con los lineamientos establecidos en el manual para la implementación de la estrategia de gobierno en línea.

Por lo anterior se solicita:

- Cumplir con el decreto 1151 de gobierno en línea (Desde la primera fase).

EVALUACION DE LA PUBLICIDAD DEL PROCEMIENTO DE CONTRATACIÓN EN EL SECOP (SISTEMA ELECTRÓNICO PARA LA CONTRATACIÓN PÚBLICA)

Revisando y analizando el Sistema Electrónico Para la Contratación (SECOP) y teniendo en cuenta la normatividad vigente para el periodo evaluado, particularmente los decretos 066 de 2008 y 2474 de 2008, el grupo auditor realizó la correspondiente búsqueda de procesos para el periodo evaluado y teniendo en cuenta el nivel de contratación de la entidad se encontró que presuntamente viola estas normas debido que no se encuentra registrado en este portal.

CONCEPTO TECNICO

El grupo auditor, después de verificar la información suministrada en Sistema Electrónico para la contratación Pública logró determinar que la entidad no garantiza la publicidad de todos los procedimientos y actos asociados a los procesos de contratación establecidos en la normatividad.

“Ley 1150 de junio 16 de 2007, por medio de la cual se introducen medidas para la eficiencia y la transparencia en la ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos.

Artículo 3o. De la contratación pública electrónica. De conformidad con lo dispuesto en la Ley 527 de 1999, la sustanciación de las actuaciones, la expedición de los actos administrativos, los documentos, contratos y en general los actos derivados de la actividad precontractual y contractual, podrán tener lugar por medios electrónicos. Para el trámite, notificación y publicación de tales actos, podrán utilizarse soportes, medios y aplicaciones electrónicas. Los mecanismos e instrumentos por medio de los cuales las entidades cumplirán con las obligaciones de publicidad del proceso contractual serán señalados por el Gobierno Nacional.

Lo anterior, sin perjuicio de las publicaciones previstas en el numeral 3 del artículo 30 de la Ley 80 de 1993.

Con el fin de materializar los objetivos a que se refiere el inciso anterior, el Gobierno Nacional desarrollará el Sistema Electrónico para la Contratación Pública, SECOP, el cual:

a) Dispondrá de las funcionalidades tecnológicas para realizar procesos de contratación electrónicos bajo los métodos de selección señalados en el artículo 2° de la presente ley según lo defina el reglamento;

b) Servirá de punto único de ingreso de información y de generación de reportes para las entidades estatales y la ciudadanía;

c) Contará con la información oficial de la contratación realizada con dineros públicos, para lo cual establecerá los patrones a que haya lugar y se encargará de su difusión a través de canales electrónicos y;
d) Integrará el Registro Único Empresarial de las Cámaras de Comercio, el Diario Único de Contratación Estatal y los demás sistemas que involucren la gestión contractual pública. Así mismo, se articulará con el Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, creado por la Ley 598 de 2000, sin que este pierda su autonomía para el ejercicio del control fiscal a la contratación pública.

Decreto 2178 de junio 26 de 2006, por medio del cual se crea el Sistema Electrónico para la Contratación Pública.

Decreto 066 de enero 16 de 2008 y el Decreto 2474 de julio 7 de 2008, Por medio de los cuales se reglamenta parcialmente la ley 1150 de 2007 sobre las modalidades de selección, publicidad y selección objetiva, y se dictan otras disposiciones, artículo 8 establece:

La publicidad a que se refiere este artículo se hará en el Sistema Electrónico para la Contratación Pública (SECOP) a través del Portal Único de Contratación, cuyo sitio web será indicado por su administrador. Con base en lo anterior, se publicarán los siguientes documentos, según corresponda a cada modalidad de selección:

1. El aviso de la convocatoria pública

2. Los proyectos de pliegos de condiciones

3. Las observaciones y sugerencias a los proyectos a que se refiere el numeral anterior y el documento que contenga las apreciaciones de la entidad sobre las observaciones presentadas.

4. El acto que dispone la apertura del proceso de selección, para el cual no será necesaria ninguna otra publicación.

5. Los pliegos de condiciones definitivos.

6. El acta de la audiencia de aclaración de los pliegos de condiciones y en general las aclaraciones que se presenten durante el proceso de selección y las respuestas a las mismas.

7. Las adendas a los pliegos de condiciones.

8. El informe de evaluación a que se refiere el numeral 8 del artículo 30 de la Ley 80 de 1993, así como el de evaluación del concurso de meritos a que se refiere el artículo 68 del presente decreto.
9. El acto de adjudicación y el acta de la audiencia pública de adjudicación en los casos de licitación pública.

10. El acto de declaratoria de desierta de los procesos de selección.

11. El contrato, las adiciones, modificaciones o suspensiones y la información sobre las sanciones ejecutoriadas que se profieran en el curso de la ejecución contractual o con posterioridad a ésta.

12. El acta de liquidación de mutuo acuerdo, o el acto administrativo de liquidación unilateral."

OBSERVACIONES

Revisada y analizada la información obtenida del portal único de contratación del SECOP ***www.contratos.gov.co***, el grupo auditor logró determinar que la entidad no se encuentra registrada en el portal en mención puesto que no está obligada a cumplir a cabalidad con los lineamientos establecidos por la normatividad vigente, por el simple hecho de que para la contratación se rige por la Ley 142 de 1994, la cual les permite a todas las empresas prestadoras de servicios públicos establecer unas normas del derecho privado para este proceso. [DOCUMENTOS_EMPOOBANDO**/ACUER_004,** EVIDENCIA_FOTOGRAFICA**/IMG_65**].

EVALUACION AL SISTEMA DE INFORMACION PARA LA VIGILANCIA DE CONTRATACION ESTATAL SICE

Revisada y analizada la información obtenida del portal web del estado **www.sice-cgr.gov.co/** el grupo auditor logró determinar que existen 165 contratos registrados por parte de EMPOOBANDO en el año 2006, [EVIDENCIA_FOTOGRAFICA**/IMG_37, IMG_38**]. Estos contratos poseen ciertas alarmas que se originan por concepto de:

- ORDENADOR DE CONTRATO PRINCIPAL NO ACTIVO EN FECHA DE CIERRE, ADJUDICACION Y FIRMA DEL CONTRATO.
- EL PROVEEDOR NO ESTA REGISTRADO EN EL SICE.

[EVIDENCIA_FOTOGRAFICA**/IMG_44**].

Por otra parte el contrato Nro. 2628 firmado el 30 de Noviembre de 2006 que presenta irregularidades de cumplimiento por parte del contratista y hasta la fecha no ha sido entregado [DOCUMENTOS_EMPOOBANDO**/CONT_2628, ACT_CON_2628, IMPRO_PROC_2628**], también presenta irregularidades en su registro, que es pertinente para su control en el Sistema de Información para la Contratación Estatal SICE. [EVIDENCIA_FOTOGRAFICA**/IMG_45, IMG_42, IMG_41**].

Además para los años 2007 y 2008 no se encontró ningún registro de contratos efectuados por EMPOOBANDO E.S.P. [EVIDENCIA_FOTOGRAFICA**/IMG_39 - IMG_41**].

El grupo auditor después de analizar la información registrada por EMPOOBANDO E.S.P. en el sistema de SICE se permite manifestar que la entidad debe tener presente la Ley 598 del 2000, la cual permite la autorregulación, control institucional y publicidad de las operaciones contractuales.

CONCEPTO TECNICO

El grupo auditor, después de verificar la información suministrada en el portal web logró determinar que esta no cumple a cabalidad con lo estipulado en la Ley 598 del 2000 por la cual se crean el Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, el Catálogo Único de Bienes y Servicios, CUBS, y el Registro Único de Precios de Referencia, RUPR, de los bienes y servicios de uso común en la administración Pública.

El Sistema de Información para la Vigilancia de la Contratación Estatal es una herramienta de información, de ordenación y control, que aporta datos y cifras relevantes para el proceso de contratación, con la principal finalidad de darle transparencia y publicidad a la contratación pública, proteger los recursos públicos y adoptar mecanismos para evitar la corrupción.

Entre las bondades del SICE encontramos las siguientes:

- Permite la interacción de los contratantes, los contratistas, la comunidad y los órganos de control.
- Suministra elementos para facilitar la contratación en línea, garantiza la selección objetiva y contribuye a la transparencia de la contratación pues divulga los procesos contractuales.
- Facilita el control, pues permite que éste se ejerza posterior y selectivamente.
- Integra la tecnología para hacer más eficiente y segura la contratación.

Con el SICE se pretende además cumplir algunos fines como los siguientes:

- ✓ Reducir costos en la contratación de la administración, esto es, hacerla más económica.
- ✓ Garantizar los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad, publicidad, eficiencia, equidad, transparencia, responsabilidad y control social.
- ✓ Mejorar sustancialmente los procesos relacionados con la planeación, elaboración de planes de compras y presupuesto de las entidades.
- ✓ Optimizar los estudios de mercado en los procesos de contratación, usando la tecnología informática.
- ✓ Garantizar el acceso a la consulta de la información de los procesos de selección.
- ✓ Impulsar y promover un cambio institucional, social y cultural frente a la corrupción.

El portal en Internet del SICE, está constituido por una serie de recursos informáticos que permiten disponer de toda la información y servicios en tiempo real y en línea, para el cumplimiento de sus funciones.

Por otro lado, uno de los propósito del SICE es el de dotar a la Administración Pública y a la comunidad en general de un sistema de información que la provea de datos y cifras actualizadas, veraces y de fácil acceso, que sean necesarios para realizar un juicioso análisis del mercado, que sirva y colabore en la planificación, programación, control y ejecución del plan de compras.

En vista de lo anterior el grupo auditor se permite recordar la normatividad vigente que establece el sistema de información para la vigilancia de contratación estatal así:

- LEY 598 de julio 28 del 2000, por la cual se crean el Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, el Catálogo Único de Bienes y Servicios, CUBS, y el Registro Único de Precios de Referencia, RUPR, de los bienes y servicios de uso común en la Administración Pública y se dictan otras disposiciones.

- DECRETO NÚMERO 3512 DE 2005 DE DICIEMBRE DE 2003, Por el cual se reglamenta la organización, funcionamiento y operación del Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, creado mediante la ley 598 de 2000, y se dictan otras disposiciones.

OBSERVACIONES

Revisada y analizada la información obtenida del portal web del estado www.sice-cgr.gov.co/ el grupo auditor logró determinar que la entidad no cumple a cabalidad

con los lineamientos establecidos por la normatividad vigente para el periodo auditado.

Por lo anterior se solicita:

- Cumplir con el registro y publicación de la contratación.

EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

CONCEPTO TECNICO

La ley 527 de agosto 8 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, además se establecen las entidades de certificación y se dictan otras disposiciones. La entidad cumple con los artículos que le aplican. Aunque dado un análisis de la visita por parte del grupo auditor se pudo observar que las políticas de seguridad necesitan mayor control y soporte técnico, además se necesita establecer unos protocolos mucho más claros y de mayor confiabilidad para este fin.

OBSERVACIONES

Se revisó la seguridad informática en la visita realizada el día 20 de Octubre de 2009 y se constató que la entidad cumple con la mayoría de los lineamientos de la ley 527 de 1999, aunque no cuenta con un certificado de seguridad informática como se establece en el Capítulo III de la mencionada ley.

Por lo anterior se solicita:

- Los documentos correspondientes a las políticas de seguridad existente.

A las Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P., se dió a conocer el resultado de la Auditoria a través de un informe ejecutivo, el cual contempla las fortalezas y debilidades encontradas en el proceso de análisis con la herramienta COBIT y las normatividades emitidas por el Estado, encaminadas hacia un estado más transparente, además contiene las respectivas recomendaciones. [INFORME_EJECUTIVO**/IE_EMPO**].

4.3.2. Informe alcaldía municipal de Ipiales. En el siguiente apartado se encuentra descrito el informe técnico presentado ante la entidad Contraloría Departamental de Nariño por parte del equipo auditor.

OFICINA DE SISTEMAS
HALLAZGOS ADMINISTRATIVOS
ALCALDIA MUNICIPAL DE IPIALES

DATOS GENERALES DE LA AUDITORIA

Modalidad de Auditoria	Auditoria de sistemas.
Periodo Evaluado	2008.
Líneas de Auditoria	Decreto 1151 del 14 de abril de 2008.
Contratación	
Seguridad informática	
Fecha de Iniciación	20/Octubre/2009.
Líder Equipo Auditor	Ing. Julián Yecít Melo Zambrano.

DATOS GENERALES DE LA ENTIDAD

Nombre o razón Social.	Alcaldía Municipal de Ipiales.
NIT No.	8000990957.
Naturaleza Jurídica	Alcaldía.
Representante Legal	Gustavo Estupiñan.
Cargo	Alcalde
Dirección.	Ipiales (N).

EVALUACION DEL DECRETO 1151 DEL 14 DE ABRIL DE 2008

Análisis de comité de gobierno en línea:

Una vez revisada la información enviada por la entidad se determinó no se ha conformado hasta la fecha un comité de gobierno en línea.

Análisis de fase de información En la fase de información no cumplió con los siguientes ítems:

- Directorio de entidades.
- Directorio de agremiaciones y asociaciones.
- Presupuesto aprobado en ejercicio de acuerdo con las normas vigentes.
- Políticas, planes y/o líneas estratégicas, programas y proyectos en ejecución, contacto con dependencia responsable.

- Información sobre licitaciones, selecciones abreviadas, concurso de mérito y contratación directa.
- Metas, indicadores de gestión y/o desempeño y resultados: Se debe publicar la información relacionada con metas, indicadores de gestión y/o desempeño y los resultados mensualizados frente a las metas. No existen publicados indicadores de gestión y/o desempeño con resultados mensualizados y confrontados con las metas.
- Escudo de la república de Colombia, Enlace al Portal del Estado Colombiano www.gobiernoenlinea.gov.co, fecha de la última actualización del sitio Web.

OBSERVACIONES

Revisada y analizada la información obtenida del portal web de la Alcaldía Municipal de Ipiales **http://www.ipiales-nariño.gov.co/**, el grupo auditor logro determinar que la entidad no cumple muy a cabalidad con los lineamientos establecidos en el manual para la implementación de la estrategia de gobierno en línea

Por lo anterior se solicita:

- Plan de acción y crear un comité de gobierno en línea

EVALUACION DE LA PUBLICIDAD DEL PROCEMIENTO DE CONTRATACIÓN EN EL SECOP (SISTEMA ELECTRÓNICO PARA LA CONTRATACIÓN PÚBLICA)

Revisando y analizando el Sistema Electrónico Para la Contratación (SECOP) y teniendo en cuenta la normatividad vigente para el periodo evaluado, particularmente los decretos 066 de 2008 y 2474 de 2008, el grupo auditor no encontró ninguna anomalía en la información contractual que se encuentra registrada en el portal.

OBSERVACIONES

Revisada y analizada la información obtenida del portal único de contratación del **SECOP *www.contratos.gov.co***, el grupo auditor logro determinar que la entidad cumple a cabalidad con los lineamientos establecidos por la normatividad vigente para el periodo auditado.

EVALUACION AL SISTEMA DE INFORMACION PARA LA VIGILANCIA DE CONTRATACION ESTATAL SICE

Revisando, analizando y constatando la información del Sistema de Información para la Vigilancia de Contratación estatal con la información facilitada por la Alcaldía Municipal de Ipiales, el grupo auditor logró establecer que presuntamente no se cumple con el registro total de los contratos para su publicación en el Portal SICE. [DOCUMENTOS_AMI**/CONT_01,** EVIDENCIA_FOTOGRAFICA**/IMG_05 - IMG_23**].

OBSERVACIONES

Revisada y analizada la información obtenida del portal web del estado ***www.sice-cgr.gov.co/*** el grupo auditor logró determinar que la entidad no cumple a cabalidad con la funcionalidad del sistema de información para la vigilancia de contratación estatal el cual integra todos los datos relevantes de proceso de contratación, permitiendo su autorregulación, control institucional y publicidad de las operaciones.

EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

OBSERVACIONES

Se revisó la seguridad informática en la visita realizada el día 20 de Octubre de 2009 y se constató que la entidad cumple con la mayoría de los lineamientos de la ley 527 de 1999, aunque no cuenta con un certificado de seguridad informática como se establece en el Capítulo III de la mencionada ley. Además las condiciones en las que se encontraban los equipos suponen una falta de políticas claras de seguridad.

Por lo anterior se solicita:

- Los documentos correspondientes a las políticas de seguridad.

A la Alcaldía Municipal de Ipiales, se dio a conocer el resultado de la Auditoria a través de un informe ejecutivo, el cual contempla las fortalezas y debilidades encontradas en el proceso de análisis con la herramienta COBIT y las normatividades emitidas por el Estado encaminadas hacia un estado más transparente, además contiene las respectivas recomendaciones. [INFORME_EJECUTIVO**/IE_AMI**].

5. CONCLUSIONES

- Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos y suministran una plataforma de información necesaria para la toma de decisiones, por eso es de vital importancia para la consecución de los objetivos de las diferentes entidades, consolidar esfuerzos para garantizar la seguridad física y lógica de los elementos que los conforman.

- La auditoría de sistemas es la herramienta que a través de una serie de procedimientos metódicos de observación, análisis y ejecución, permite identificar las diferentes vulnerabilidades de seguridad física y lógica. Así mismo es el instrumento por medio del cual se realizan recomendaciones para corregir las deficiencias encontradas y fortalecer las medidas de seguridad encaminadas a garantizar la integridad, confidencialidad y confiabilidad de la información.

- Los funcionarios encargados de la administración y el manejo de los Sistemas y las Tecnologías de la información, enfocan sus esfuerzos para asegurar la operatividad de éstos, descuidando la implementación de controles que garanticen la seguridad física y lógica de la información.

- El buen uso de las TI y SI dependen de la administración y visión tecnológica que tenga cada uno de los responsables en la gerencia de las entidades, sin importar las normatividades emitidas por la Ley y las sugerencias y labor emprendida de los profesionales del área de sistemas.

- EMPOOBANDO E.S.P. a diferencia de la Alcaldía Municipal de Ipiales posee muchas deficiencias en cuanto al uso de las tecnologías de información. Mientras que la Alcaldía de Ipiales actúa mucho mas de acuerdo a lo que dictamina la Ley.

- El trabajo del ingeniero en la administración pública es más complejo que en la labor independiente, puesto que se nota por parte de muchos funcionarios el temor a los cambios que trae para su beneficio, la implementación de nuevas tecnologías de información.

6. RECOMENDACIONES

- Realizar un análisis juicioso y detallado del entorno organizacional de la Empresa de Obras Sanitarias de la Provincia de Obando EMPOOBANDO E.S.P. para identificar claramente sus metas y objetivos, con el fin de crear manual de funciones y manual de procedimientos claros y completos, para que los empleados cumplan a cabalidad sus labores dentro de la entidad, dando cumplimiento con todos los requerimientos que solicita la ley.

- Crear en EMPOOBANDO E.S.P. el área de sistemas, teniendo en cuenta que esté bien fundamentada con procedimientos y manual de funciones, que permitan a los trabajador encargados, contribuir de manera eficiente en el proceso de Contratación de TI, seguridad de la información y adelantar conforme lo dictamina la ley el portal web para el programa de Gobierno en Línea.

- Establecer planes de mejoramiento que conlleven a la certificación de calidad de los procesos, en especial el de la contratación de TI y seguridad de la información.

- Garantizar el buen funcionamiento de los Sistemas y las Tecnologías de la Información en cada una de las entidades, mediante la aplicación de procesos de auditoría de sistemas.

- Generar políticas que promuevan la realización periódica de auditorías de sistemas, que sirvan como instrumentos para el fortalecimiento tecnológico y sean herramientas que ayuden a lograr el cumplimiento de los objetivos de las entidades.

- Garantizar la existencia de planes de contingencia y planes de continuidad para los Sistemas de Información implementados en cada una de las entidades.

BIBLIOGRAFIA

- ECHENIQE GARCIA José A., Auditoría en informática, segunda edición 2a Ed., Mc Graw Hill D. F. 2005.

- PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

- JOSE DAGOBERTO PINILLA FORERO, "Auditoría informática. Un enfoque operacional" En Bogotá Colombia 1995. ed.: ECOE.

- Auditoria de Sistemas en Funcionamiento (José Dagoberto Pinilla Guerrero).

- COBIT 4.1 ®, Marco de Trabajo – Objetivos de Control – Directrices Generales – Modelos de Madurez.

    - PIATTINI, Mario y Emilio del Peso. Auditoría Informática. Un enfoque práctico. Editorial RA-MA.

- Tesis, Auditoria al modulo de historia clínica. Jenny Burgos y Carolina Domínguez. Año 2007. Pág. 59-60 y 87-94.

BIBLIOGRAFIA WEB

- http://www.monografias.com/trabajos39/la-auditoria/la-auditoria.shtml.
- http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
- http://rie.cl/?a=31081
- http://www.monografias.com/trabajos5/audi/audi.shtml
- http://www.degerencia.com/articulos/los_cinco_componentes_del_control_interno
- [10]http://www.google.com.co/search?hl=es&q=desventajas+de+utilizar+registros+extendidos%2Bauditoria&btnG=Buscar&aq=f&aqi=&a
- http://fccea.unicauca.edu.co/old/taac.htm
- http://elrincondeperolo.blogspot.com/2009/07/trabajo-de-auditoria.html
- http://www.oracle.com/global/lad/database/audit-vault.html
- http://www.sprydoc.com/document/www.isaca.org+cobiT4.1spanish.pdf
- http://www.galeon.com/anaranjo/tipos_audi.htm
- http://es.wikipedia.org/wiki/COBIT
- http://ciberconta.unizar.es/LECCION/seguro/100.HTM
- http://www.isaca.org
- http://www.eafit.edu.co/.../boletin54COBITMODELOPARAAUDITORIAYCONTROLDESIS
- http://www.monografias.com/trabajos27/papeles-auditoria/papeles-auditoria.shtml
- http://www.aciem.org/bancoconocimiento/l/ley6892001/Ley%20689%20de%202001.pdf

- http://www.eaav.gov.co/portal/images/documentos/ley_142_de_1994.pdf
- http://www.mineducacion.gov.co/1621/articles-85593_archivo_pdf4.pdf

- http://www.manizales.unal.edu.co/archivo/descargas/ley_594.pdf

- http://www.ccmagdalenamedio.org.co/arch/Decretos_leyesPP2009/LEY_1150_2007_REFORMA_LEY_80.pdf

- http://www2.unicolmayor.edu.co:8080/cmc/hermesoft/portal/home_3/rec/arc_2225.pdf

- Portal Web del Sistema de Información para la Contratación Estatal. http://www.sice-cgr.gov.co/entidad.html

- Portal Web del Sistema Electrónico de la Contratación Pública. http://www.contratos.gov.co/consultas/inicioConsulta.do

- Portal Web de la Alcaldía Municipal de Ipiales. http://ipiales-narino.gov.co/nuestraalcaldia.shtml?apc=a1f1--&m=d

ANEXOS

Los anexos relacionados a continuación se entregan en medio magnéticos y se adjuntan al presente informe.

FUENTE_DE_CONOCIMIENTO

ANEXO 1.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO1. Definir un Plan Estratégico de TI. – DFC_PO1.

ANEXO 2.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO3. Determinar la Dirección Tecnológica – DFC_PO3.

ANEXO 3.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO4. Definición de la Organización y de las Relaciones de TI – DFC_PO4.

ANEXO 4.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO5. Administrar la Inversión de TI – DFC_PO5.

ANEXO 5.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO7. Administrar los Recursos Humanos – DFC_PO7.

ANEXO 6.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO9. Evaluación y Análisis de Riesgo – DFC_PO9.

ANEXO 7.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – AI3. Adquisición y Mantenimiento de Infraestructura Tecnológica - DFC_AI3.

ANEXO 8.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – AI5. Adquirir Recursos de TI - DFC_AI5.

ANEXO 9.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS5. Garantizar la seguridad de sistemas – DFC_ DS5.

ANEXO 10.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS9. Administración de la configuración – DFC_DS9.

ANEXO 11.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS11. Administración de datos – DFC_DS11.

ANEXO 12.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS12. Administración de las instalaciones – DFC_ DS12.

ANEXO 13.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - M2. Evaluar lo adecuado del control interno – DFC_ M2.

ANEXO 14.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – M3. Garantizar el Cumplimiento con Requerimientos Externos – DFC_ M3.

ANEXO 15.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO1. Definir un Plan Estratégico de TI. – DFC_PO1.

ANEXO 16.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO3. Determinar la Dirección Tecnológica – DFC_PO3.

ANEXO 17.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO4. Definición de la Organización y de las Relaciones de TI – DFC_PO4.

ANEXO 18.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO5. Administrar la Inversión de TI – DFC_PO5.

ANEXO 19.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO7. Administrar los Recursos Humanos – DFC_PO7.

ANEXO 20.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – PO9. Evaluación y Análisis de Riesgo – DFC_PO9.

ANEXO 21.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – AI2. Adquirir y Mantener Software Aplicativo - DFC_AI2.

ANEXO 22.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – AI3. Adquisición y Mantenimiento de Infraestructura Tecnológica - DFC_AI3.

ANEXO 23.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – AI5. Adquirir Recursos de TI - DFC_AI5.

ANEXO 24.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – AI6. Administración de Cambios - DFC_AI6.

ANEXO 25.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – DS2. Administrar los Servicios de Terceros – DFC_ DS2.

ANEXO 26.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS5. Garantizar la seguridad de sistemas – DFC_ DS5.

ANEXO 27.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – DS7. Educar y Entrenar a los Usuarios – DFC_DS7.

ANEXO 28.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS9. Administración de la configuración – DFC_DS9.

ANEXO 29.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS11. Administración de datos – DFC_DS11.

ANEXO 30.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS12. Administración de las instalaciones – DFC_ DS12.

ANEXO 31.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - M2. Evaluar lo adecuado del control interno – DFC_ M2.

ANEXO 32.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría – M3. Garantizar el Cumplimiento con Requerimientos Externos – DFC_ M3.

CUESTIONARIOS

ANEXO 1.
Cuestionario Cuantitativo – PO1. Definir un Plan Estratégico de TI - PLAN_ PO1.

ANEXO 2.
Cuestionario Cuantitativo – PO3. Determinar la Dirección Tecnológica – PLAN_PO3.

ANEXO 3.
Cuestionario Cuantitativo – PO4. Definición de la Organización y de las Relaciones de TI – PLAN_PO4.

ANEXO 4.
Cuestionario Cuantitativo – PO5. Administrar la Inversión de TI – PLAN_PO5.

ANEXO 5.
Cuestionario Cuantitativo – PO7. Administrar los Recursos Humanos – PLAN_PO7.

ANEXO 6.
Cuestionario Cuantitativo - PO9. Evaluación y Análisis de Riesgo – PLAN_ PO9.

ANEXO 7.
Cuestionario Cuantitativo - AI3. Adquirir y Mantener la Infraestructura Tecnológica – ADQ_ AI3.

ANEXO 8.
Cuestionario Cuantitativo – AI5. Adquirir Recursos de TI – ADQ_ AI5.

ANEXO 9.
Cuestionario Cuantitativo - DS5. Garantizar la seguridad de sistemas – ESS_DS5.

ANEXO 10.
Cuestionario Cuantitativo - DS9. Administrar la configuración – ESS_DS9.

ANEXO 11.
Cuestionario Cuantitativo - DS11. Administración de datos – ESS_DS11.

ANEXO 12.
Cuestionario Cuantitativo - DS12. Administración de las instalaciones – ESS_DS12.

ANEXO 13.
Cuestionario Cuantitativo - ME2. Evaluar lo Adecuado del Control Interno – MON_ME2.

ANEXO 14.
Cuestionario Cuantitativo – ME3. Garantizar el Cumplimiento con Requerimientos Externos – MON_ME3.

ANEXO 15.
Cuestionario Cuantitativo – PO1. Definir un Plan Estratégico de TI - PLAN_ PO1.

ANEXO 16.
Cuestionario Cuantitativo – PO3. Determinar la Dirección Tecnológica – PLAN_PO3.

ANEXO 17.
Cuestionario Cuantitativo – PO4. Definición de la Organización y de las Relaciones de TI – PLAN_PO4.

ANEXO 18.
Cuestionario Cuantitativo – PO5. Administrar la Inversión de TI – PLAN_PO5.

ANEXO 19.
Cuestionario Cuantitativo – PO7. Administrar los Recursos Humanos – PLAN_PO7.

ANEXO 20.
Cuestionario Cuantitativo - PO9. Evaluación y Análisis de Riesgo – PLAN_ PO9.

ANEXO 21.
Cuestionario Cuantitativo – AI2. Adquirir y Mantener Software Aplicativo – ADQ_ AI2.

ANEXO 22.
Cuestionario Cuantitativo - AI3. Adquirir y Mantener la Infraestructura Tecnológica – ADQ_ AI3.

ANEXO 23.

Cuestionario Cuantitativo – AI5. Adquirir Recursos de TI – ADQ_ AI5.

ANEXO 24.
Cuestionario Cuantitativo – AI6. Administración de Cambios – ADQ_ AI6.

ANEXO 25.
Cuestionario Cuantitativo – DS2. Administrar los Servicios de Terceros – ESS_DS2.

ANEXO 26.
Cuestionario Cuantitativo - DS5. Garantizar la seguridad de sistemas – ESS_DS5.

ANEXO 27.
Cuestionario Cuantitativo – DS7. Educar y Entrenar a los Usuarios – ESS_DS7.

ANEXO 28.
Cuestionario Cuantitativo - DS9. Administrar la configuración – ESS_DS9.

ANEXO 29.
Cuestionario Cuantitativo - DS11. Administración de datos – ESS_DS11.

ANEXO 30.
Cuestionario Cuantitativo - DS12. Administración de las instalaciones – ESS_DS12.

ANEXO 31.
Cuestionario Cuantitativo - ME2. Evaluar lo Adecuado del Control Interno – MON_ME2.

ANEXO 32.
Cuestionario Cuantitativo – ME3. Garantizar el Cumplimiento con Requerimientos Externos – MON_ME3.

ENTREVISTAS_A_FUNCIONARIOS

ANEXO 1.
Formato Entrevista Responsable del Área de Sistemas (Mantenimiento) - ENT_FUN_ESM

ANEXO 2.
Formato Entrevista Responsable Del Área de Sistemas – ENT_FUN_ES.

ANEXO 3.
Formato Entrevista Subgerente de Producción y Control de Calidad – ENT_FUN_SPC.

ANEXO 4.
Formato Entrevista Auxiliar Administrativo de Planeación – ENT_FUN_AP.

ANEXO 5.
Formato Entrevista Jefe Asesor de Planeación – ENT_FUN_JAP.

ANEXO 6.
Formato Entrevista Jefe Oficina Jurídica– ENT_FUN_JOJ.

Anexo 7.
Entrevista al secretario de hacienda de la Alcaldía Municipal de Ipiales – ENT_FUN_SH.

Anexo 8.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

Anexo 9.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

Anexo 10.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

Anexo 11.
Entrevista al secretario de hacienda de la Alcaldía Municipal de Ipiales – ENT_FUN_SH.

Anexo 12.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

Anexo 13.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

Anexo 14.
Entrevista a la ingeniera de sistemas auxiliar encargada de la Alcaldía Municipal de Ipiales – ENT_FUN_ISA.

Anexo 15.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

Anexo 16.
Entrevista al jefe de sistemas de la Alcaldía Municipal de Ipiales – ENT_FUN_JS.

DOCUMENTO_EMPOOBANDO

Acta Conciliatoria entre EMPOOBANDO y T.A.O. referente al incumplimiento del contrato 2628 - ACT_CONC_2628.

Acuerdo 004, por medio de la cual EMPOOBANDO posee políticas internas de derecho privado para la contratación de TI - ACUER_004.

Características del Procedimiento de la Gestión Financiera - CARACT_FIN.

Características del Procedimiento de Mantenimiento de Equipos - CARACT_MANTE_EQUI.

Contrato 2628, que se incumplió por parte del contratista T.A.O. - CONT_2628.

Tabla encaminada al mantenimiento de equipos de computo - CRONO_MANTE.

Respuesta de Improbación Dictada por el Juzgado Séptimo Administrativo - IMPRO_PROC_2628.

Manual Obsoleto que se manejaba en EMPOOBANDO - MANU_FUN.

Mapa de Riesgo para la Implementación del Manual MECI - MAP_RIESG_EMPO.

Procedimiento de Contratación de EMPOOBANDO - PROCED_CONTRA.

Procedimientos de la Dependencia de Jurídica - PROCED_JURIDI.

Documento que describe el procedimiento de mantenimiento de equipos de cómputo de EMPOOBANDO - PROCED_SISTE_MANTE.

DOC_AMI:
Contrato que no aparece registrado en el portal SICE – CONT_01.

Contrato que sigue proceso de continuidad con el proveedor y verificación de pólizas – CONT_02.

Contrato que sigue proceso de continuidad con el proveedor – CONT_03.

Contrato que sigue proceso de continuidad con el proveedor – CONT_04.

Ficha de registro de los elementos Hardware y Software de Equipos – FICHA_01.

Ficha de registro de los elementos Hardware de Equipos – FICHA_02.

Manual de funciones para los empleados de la Alcaldía Municipal de Ipiales – MANU_F_A_M_I.

Manual de funciones para el Jefe de la oficina asesora jurídica – MANU_F_J_O_A_J.

Manual de funciones para el Jefe del área de sistemas – MANU_F_J_S.

Manual de funciones para el subsecretario de sistemas de información – MANU_F_S_S_I.

Manual de procedimientos de contratación para la modificación y liquidación de contratos – MOD_LIQ_CONTRA.

Manual de procedimientos de contratación para licitación – LICITACION.

Manual de procedimientos de contratación para el concurso de meritos – PROC_CONC_MERITOS.

Manual de procedimientos de contratación para la selección abreviada – PROC_SELCC_ABREVIADA.

Manual de procedimientos de contratación directa mínima – CONT_DIREC_MINIMA.

Manual de procedimientos de contratación directa menor – CONT_DIREC_MENOR.

Manual de procedimientos de contratación de interés público – CONT_INT_PUBLICO.
Inventario de los elementos de cómputo y de oficina de la Alcaldía Municipal de Ipiales – INVENTARIO.

EVIDENCIA_DE_AUDIO
Entrevista al funcionario Auxiliar Administrativo de Planeación de EMPOOBANDO – A_EMPO_1.

Entrevista al funcionario Auxiliar Administrativo de Planeación de EMPOOBANDO – A_EMPO_2.

Entrevista realizada al jefe del área de sistemas de la alcaldía municipal de Ipiales – A_AMI_01.

Entrevista realizada al jefe del área de sistemas de la alcaldía municipal de Ipiales – A_AMI_02.

Entrevista realizada a la ingeniera auxiliar encargada del área de sistemas de la Alcaldía Municipal de Ipiales – A_AMI_03.

Entrevista realizada al jefe de la oficina jurídica de la Alcaldía Municipal de Ipiales – A_AMI_04.

Entrevista realizada a la subsecretaria de talento humano de la Alcaldía Municipal de Ipiales – A_AMI_05.

Entrevista realizada al subsecretario de sistemas de información para contratación de la Alcaldía Municipal de Ipiales – A_AMI_06.

Entrevista realizada a la secretario de talento humano de la alcaldía municipal de Ipiales – A_AMI_07.

EVIDENCIA_FOTOGRAFICA
Contiene todas las evidencias fotográficas e Impresiones de pantalla que permiten fundamentar los hallazgos y los procesos que son bien llevados en EMPOOBANDO E.S.P. y en la Alcaldía Municipal de Ipiales, Se cuenta con 65 imágenes de las cuales de IMG_1 – IMG_27 pertenecen a evidencia de la Alcaldía Municipal de Ipiales y de la IMG_28 – IMG_65 pertenecen a la evidencia de EMPOOBANDO E.S.P.

HALLAZGOS

HEMDO_01.
Hallazgo en el proceso (Definir un plan estratégico de TI) PO1 – HEMDO_01.

HEMDO_02.
Hallazgo en el proceso (Determinar la Dirección Tecnológica) PO3. – HEMDO_02.

HEMDO_03.
Hallazgo en el proceso (Definición de la Organización y de las Relaciones de TI) PO4 – HEMDO_03.

HEMDO_04.
Hallazgo en el proceso (Administrar la Inversión de TI) PO3 – HEMDO_04.

HEMDO_05.

Hallazgo en el proceso (Administración de Recursos Humanos de TI) PO7 – HEMDO_05.

HEMDO_06.
Hallazgo en el proceso (Evaluación y Análisis de Riesgo) PO9 – HEMDO_06.

HEMDO_07.
Hallazgo en el proceso (Adquisición y mantenimiento de la Infraestructura Tecnológica) AI3 – HEMDO_07.

HEMDO_08.
Hallazgo en el proceso (Adquirir Recursos de TI) AI5 – HEMDO_08.

HEMDO_09.
Hallazgo en el proceso (Garantizar la Seguridad de Sistemas) DS5 – HEMDO_09.

HEMDO_10.
Hallazgo en el proceso (Administración de la Configuración) DS9 – HEMDO_10.

HEMDO_11.
Hallazgo en el proceso (Administración de Datos) DS11 – HEMDO_11.

HEMDO_12.
Hallazgo en el proceso (Administración de las Instalaciones) DS12 – HEMDO_12

HEMDO_13.
Hallazgo en el proceso (Evaluar lo Adecuado del Control Interno) ME2 – HEMDO_13.

HEMDO_14.
Hallazgo en el proceso (Garantizar el Cumplimiento con Requerimientos Externos) ME3 – HEMDO_14.

HAI_01.
Hallazgo en el proceso (Definir un plan estratégico de TI) PO3 – HAI_01.

HAI_02.
Hallazgo en el proceso (Definición de la Organización y de las Relaciones de TI) PO4 – HAI_02.

HAI_03.
Hallazgo en el proceso (Administrar la Inversión en TI) PO5 – HAI_03.

HAI_04.
Hallazgo en el proceso (Administrar los datos) DS11 – HAI_04.

HAI_05.
Hallazgo en el proceso (Administración de instalaciones) DS12 – HAI_05.

HAI_06.
Hallazgo para el proceso (Garantizar el cumplimiento con requerimientos externos) ME3 – HAI_O6.

INFORME_EJECUTIVO
IE_AMI.
Contiene el informe ejecutivo presentado a la Alcaldía Municipal de Ipiales como resultado del proceso de Auditoria – IE_AMI.

IE_EMPO
Contiene el informe ejecutivo presentado a la Empresa de Obras Sanitarias de la Provincia de Obando como resultado del proceso de Auditoria – IE_EMPO.