TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO, ALCALDÍA MUNICIPAL DE TANGUA Y ALCALDÍA MUNICIPAL DE YACUANQUER

LENNIN GEOVANNY IBARRA GONZALEZ
DIEGO MAURICIO MEZA GARCIA

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, ALCALDÍA MUNICIPAL DE TANGUA Y ALCALDÍA MUNICIPAL DE YACUANQUER

LENNIN GEOVANNY IBARRA GONZALEZ
DIEGO MAURICIO MEZA GARCIA

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

Director
ING. MANUEL BOLAÑOS GONZALEZ

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 son Responsabilidad de los autores.

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____
Jurado

_____
Jurado

San Juan de Pasto, 2010

AGRADECIMIENTOS

Al ingeniero Manuel Bolaños por su compromiso y entrega que fueron fundamentales en el proceso que hoy culminamos.

Al ingeniero Julián Melo por brindarnos su acompañamiento desde la Contraloría Departamental de Nariño y hacer posible nuestra investigación.

A los abogados asesores de la Contraloría y externos que nos apoyaron a lo largo de nuestro trabajo de grado.

A nuestras familias parte fundamental de nuestras vidas a quienes les debemos todos nuestros logros.

A nuestros amigos por el apoyo recibido.

DEDICATORIA

A nuestros padres, hermanos e hijos, a nuestros amigos, compañeros y profesores por ser parte de nuestra formación como Ingenieros.

RESUMEN

El objetivo de este trabajo es observar cómo la Contraloría Departamental de Nariño evalúa las diferentes entidades que manejan presupuesto público, qué actores se encargan de hacerlo, qué tipo de evaluación realiza, qué factores evalúa, cómo presenta sus resultados y qué impacto tienen los mismos en las instituciones.

Dicha evaluación se realizó en forma de una auditoría de TI, analizando si las entidades cumplen con sus objetivos y metas, los requerimientos contratación, sus procesos y procedimientos, y la seguridad de la información. Esta auditoría se realiza sobre los recursos TI que incluyen al menos cuatro dimensiones: aplicaciones, información, infraestructura y personas.

Dentro de las entidades auditadas es de vital importancia la auditoría de sistemas e informática para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y mantengan un buen nivel de seguridad permitiéndoles así cumplir a cabalidad sus objetivos y metas de negocio.

Para la realización de este documento se toma como casos de estudio la Alcaldía Municipal de Tangua y la Alcaldía Municipal de Yacuanquer, esta auditoría se la realizó con el fin de identificar las vulnerabilidades de seguridad de TI del proceso de contratación, tanto física como lógica; además se evaluó el cumplimiento del decreto 1151 del 14 de abril de 2008 concerniente a Gobierno en Línea utilizando como punto de partida para el análisis el manual para la implementación de la estrategia de gobierno en línea de la república de Colombia. Basándose en estas evaluaciones y análisis el grupo auditor entregará recomendaciones para mitigar los riesgos detectados y optimizar el uso de los recursos de TI.

La auditoría de seguridad informática que se realizo sobre el proceso de contratación teniendo en cuenta las buenas prácticas brindadas por los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) a través de un marco de trabajo de dominios y procesos, las cuales están enfocadas fuertemente en el control y menos en la ejecución. Para el caso de estudio se auditó los objetivos de control del proceso DS5 (Garantizar la seguridad de sistemas), que forma parte del dominio Dar y Entregar Soporte (DS), así como sus relaciones con los demás dominios y procesos.

ABSTRACT

The objective of this Project is to observe how the Contraloría Departamental de Nariño evaluates the different entities that manage the public Budget, which employees are the ones uncharged of doing so, what type of evaluation is made, what factors are evaluated, how are the results presented and what impact do these have on the institutions.

This evaluation was made in an IT audit form, analyzing if the entities fulfill their objectives and goals, the hiring requirements, its processes and procedures, and the security of information. This audit is made for the resources of IT that include at least four dimensions: applications, information, infrastructure and people.

The systems and IT audit is of vital importance inside the audited entities guarantee the good performance of the IT systems, since it provides the necessary controls so that the systems can be reliable and can maintain a good security level, allowing them to fulfill their business objectives and goals in a faultless manner.

For the realization of this document, cases of study from the Alcaldía Municipal de Tangua and the Alcaldía Municipal of Yacuanquer are taken into account. This audit was made with the goal of identifying the security vulnerabilities of IT and the physical as well as logical of the hiring process; The fulfilling of decree 111 of April 14 of 2008 that concerns the Gobierno en Linea was also evaluated using the manual of analysis for the implementation of government strategy of the Republic of Colombia as a starting point. Based on these evaluations and analysis, audit group will give the recommendations to mitigate the detected risks and optimize the use of IT resources.

The audit of IT security that was made regarding the hiring process, and taking into account the good practices given by the Control Objectives for Information and related Technology, through which a margin of work of domains and processes, which are strongly focused on the control and less on the execution. For the case study, the control objectives of process DS5, which is part of the give and deliver support domain, as well as their relationships with the other domains and processes were audited.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Para efectos del correcto entendimiento del presente trabajo de grado se aportan las siguientes definiciones tomando en cuenta, cuando sea necesario, la normatividad vigente para el periodo 2008:

BIENES Y SERVICIOS DE USO COMÚN. (Art. 8 Decreto 3512 de 2003). Son aquellos que usualmente adquirieren las entidades y particulares que manejan recursos públicos, para el normal ejercicio de sus funciones.

CADUCIDAD. (Art. 18 Ley 80 de 1993). La caducidad es la estipulación en virtud de la cual si se presenta alguno de los hechos constitutivos de incumplimiento de las obligaciones a cargo del contratista, que afecte de manera grave y directa la ejecución del contrato y evidencie que puede conducir a su paralización, la entidad por medio de acto administrativo debidamente motivado lo dará por terminado y ordenará su liquidación en el estado en que se encuentre.

CATÁLOGO ÚNICO DE BIENES Y SERVICIOS, CUBS. (Art. 8 Decreto 3512 de 2003). Es el conjunto de códigos, identificaciones y estandarizaciones de los bienes y servicios de uso común o de uso en contratos de obra que la administración pública y los particulares o entidades que manejan recursos públicos pueden adquirir, estandarizados en función de sus propiedades físicas, químicas y de uso, clasificados en códigos que permiten una identificación para cada uno de ellos.

CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL – CDP. Se expide con el objeto de que antes de iniciar cualquier proceso contractual que afecte las apropiaciones presupuestales se verifique y garantice la existencia de apropiación suficiente para atender el respectivo egreso, generando al ordenador del gasto seguridad en la ejecución y a los posibles oferentes certeza en la seriedad de la solicitud de propuestas.

COMODATO. (Art. 2200 Código Civil). El comodato o préstamo de uso es un contrato en que la una de las partes entrega a la otra gratuitamente una especie mueble o raíz, para que haga uso de ella, y con cargo de restituir la misma especie después de terminar el uso.

Este contrato no se perfecciona sino por la tradición de la cosa.

CONCURSO DE MÉRITOS. (Numeral 3, Art. 2 Ley 1150 de 2007). Corresponde a la modalidad prevista para la selección de consultores o proyectos, en la que se podrán utilizar sistemas de concurso abierto o de

precalificación. En este último caso, la conformación de la lista de precalificados se hará mediante convocatoria pública, permitiéndose establecer listas limitadas de oferentes utilizando para el efecto, entre otros, criterios de experiencia, capacidad intelectual y de organización de los proponentes, según sea el caso.

CONSORCIO. (Art. 7 Ley 80 de 1993). Cuando dos o más personas en forma conjunta presentan una misma propuesta para la adjudicación, celebración y ejecución de un contrato, respondiendo solidariamente de todas y cada una de las obligaciones derivadas de la propuesta y del contrato. En consecuencia, las actuaciones, hechos y omisiones que se presenten en desarrollo de la propuesta y del contrato, afectarán a todos los miembros que lo conforman.

CONTRALORÍA. (Art. 267 Constitución Política de 1991). Como tal, tiene la misión de procurar el buen uso de los recursos y bienes públicos y contribuir a la modernización del Estado, mediante acciones de mejoramiento continuo en las distintas entidades públicas.

CONTRATO. (Art. 864 Código de Comercio). El contrato es un acuerdo de dos o más partes para constituir, regular o extinguir entre ellas una relación jurídica patrimonial, y salvo estipulación en contrario, se entenderá celebrado en el lugar de residencia del proponente y en el momento en que éste reciba la aceptación de la propuesta.

CONTRATO ESTATAL. Se considera contrato estatal a todo acto jurídico generador de obligaciones que celebren las entidades a que se refiere el estatuto general de contratación de la administración pública, previstos en las normas civiles y comerciales o en disposiciones especiales, o derivados del ejercicio de la autonomía de la voluntad.

CONTRATO O CONVENCIÓN. (Art. 1495 Código Civil). Contrato o convención es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa. Cada parte puede ser de una o de muchas personas.

CONTENIDO DEL CONTRATO ESTATAL. (Art. 40 Ley 80 de 1993). Las estipulaciones de los contratos serán las que de acuerdo con las normas civiles, comerciales y las previstas en esta ley, correspondan a su esencia y naturaleza.

Las entidades podrán celebrar los contratos y acuerdos que permitan la autonomía de la voluntad y requieran el cumplimiento de los fines estatales.

En los contratos que celebren las entidades estatales podrán incluirse las modalidades, condiciones y, en general, las cláusulas o estipulaciones que las partes consideren necesarias y convenientes, siempre que no sean contrarias a la Constitución, la ley, el orden público y a los principios y finalidades de esta ley y a los de la buena administración.

En los contratos de empréstito o cualquier otra forma de financiación de organismos multilaterales, podrán incluirse las previsiones y particularidades contempladas en los reglamentos de tales entidades, que no sean contrarias a la Constitución o a la ley.

CONTRATO DE CONCESIÓN. (Numeral 4, Art. 32 Ley 80 de 1993). 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.

CONTRATO DE CONSULTORÍA. (Numeral 2, Art. 32 Ley 80 de 1993). 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.

CONTRATO DE OBRA. (Numeral 1, Art. 32 Ley 80 de 1993). 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.

CONTRATO DE PRESTACIÓN DE SERVICIOS. (Numeral 3, Art. 32 Ley 80 de 1993). 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.

ECUACIÓN CONTRACTUAL. (Art. 27 Ley 80 de 1993). En los contratos estatales se mantendrá la igualdad o equivalencia entre derechos y obligaciones surgidos al momento de proponer o de contratar, según el caso. Si dicha igualdad o equivalencia se rompe por causas no imputables a quien resulte afectado, las partes adoptarán en el menor tiempo posible las medidas necesarias para su restablecimiento.

ENTIDADES ESTATALES. (Numeral 1 Art. 2 Ley 80 de 1993). Se denominan entidades estatales:

a) La Nación, las regiones, los departamentos, las provincias, el distrito capital y los distritos especiales, las áreas metropolitanas, las asociaciones de municipios, los territorios indígenas y los municipios; los establecimientos públicos, las empresas industriales y comerciales del Estado, las sociedades de economía mixta en las que el Estado tenga participación superior al cincuenta por ciento (50%), así como las entidades descentralizadas indirectas y las demás personas jurídicas en las que exista dicha participación pública mayoritaria, cualquiera sea la denominación que ellas adopten, en todos los órdenes y niveles.

b) El Senado de la República, la Cámara de Representantes, el Consejo Superior de la Judicatura, la Fiscalía General de la Nación, la Contraloría General de la República, las contralorías departamentales, distritales y municipales, la Procuraduría General de la Nación, la Registraduría Nacional del Estado Civil, los ministerios, los departamentos administrativos, las superintendencias, las unidades administrativas especiales y, en general, los organismos o dependencias del Estado a los que la ley otorgue capacidad para celebrar contratos.

FORMA DEL CONTRATO ESTATAL. (Art. 39 Ley 80 de 1993). Los contratos que celebren las entidades estatales constarán por escrito y no requerirán ser elevados a escritura pública, con excepción de aquellos que impliquen mutación del dominio o imposición de gravámenes y servidumbres sobre bienes inmuebles y, en general, aquellos que conforme a las normas legales vigentes deban cumplir con dicha formalidad.

INTERPRETACIÓN UNILATERAL. (Art. 15 Ley 80 de 1993). Si durante la ejecución del contrato surgen discrepancias entre las partes sobre la interpretación de algunas de sus estipulaciones que puedan conducir a la paralización o a la afectación grave del servicio público que se pretende satisfacer con el objeto contratado, la entidad estatal, si no se logra acuerdo, interpretará en acto administrativo debidamente motivado, las estipulaciones o cláusulas objeto de la diferencia.

INTERVENTOR. Servidor público o persona designada por la entidad para velar por el cabal cumplimiento del contrato.

LICITACIÓN PÚBLICA. (Parágrafo Art. 30 Ley 80 de 1993). Procedimiento mediante el cual la entidad estatal formula públicamente una convocatoria para que, en igualdad de oportunidades, los interesados presenten sus ofertas y seleccione entre ellas la más favorable.

MODELO DE MADUREZ. (COBIT). El modelo de madurez describe dónde se encuentra la empresa respecto a un estándar basado en el cumplimiento de metas y objetivos del COBIT.

MODIFICACIÓN UNILATERAL. (Art. 16 Ley 80 de 1993). Si durante la ejecución del contrato y para evitar la paralización o la afectación grave del servicio público que se deba satisfacer con él, fuere necesario introducir variaciones en el contrato y previamente las partes no llegan al acuerdo respectivo, la entidad en acto administrativo debidamente motivado, lo modificará mediante la supresión o adición de obras, trabajos, suministros o servicios.

Si las modificaciones alteran el valor del contrato en un veinte por ciento (20%) o más del valor inicial, el contratista podrá renunciar a la continuación de la ejecución. En este evento, se ordenará la liquidación del contrato y la entidad adoptará de manera inmediata las medidas que fueren necesarias para garantizar la terminación del objeto del mismo.

OBJETIVO DE CONTROL. (COBIT). Los objetivos de control describen los diferentes objetivos que se deben hacer para cumplir con el objetivo del proceso.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT).
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.

PLIEGO DE CONDICIONES. Documento que detalla claramente los requerimientos para la presentación de las propuestas por parte de los oferentes.

PORTAL DEL SECOP. (Decreto 066 de 2008). El Portal Único de Contratación se constituye como la Fase Informativa del Sistema Electrónico para la Contratación Pública – SECOP.

PORTAL DEL SICE. (Art. 8 Decreto 3512 de 2003). Está constituido por una serie de recursos informáticos que le permiten a los usuarios disponer, a través de páginas web en Internet, de toda la información y servicios en tiempo real y en línea, para el cumplimiento de las funciones del SICE. Se accede vía Internet mediante la dirección: www.sice-cgr.gov.co El Portal tiene dos componentes: uno público para el acceso de la ciudadanía en general y otro que corresponde al software aplicativo SICE de uso de los usuarios con password de ingreso.

PRECIO DE COMPRA. (Art. 8 Decreto 3512 de 2003). Es el precio de un bien o servicio de uso común o de uso en contratos de obra pactado en el contrato, incluido el IVA y excluidos otros gravámenes.

PRECIO DE OFERTA. (Art. 8 Decreto 3512 de 2003). Es el valor monetario que los proveedores de bienes y servicios de uso común o de uso en contratos de obra señalan al momento de presentar en firme a una entidad su correspondiente propuesta. El precio de oferta incluirá IVA y excluirá otros gravámenes.

PRECIO DE REFERENCIA. (Art. 8 Decreto 3512 de 2003). Es el valor monetario que los proveedores interesados en vender bienes y servicios de uso común o de uso en contratos de obra a la administración pública y a los particulares o entidades que manejan recursos públicos, deben registrar en el RUPR, bajo las condiciones que se establecen en el Sistema. El precio de referencia incluirá IVA y excluirá otros gravámenes.

PRECIO INDICATIVO. (Art. 8 Decreto 3512 de 2003). Es el promedio de los precios de referencia de un bien o servicio de uso común o de uso en contratos de obra registrados por los proveedores en el SICE.

PROCESO. (COBIT). Un proceso es un conjunto de objetivos de control, entradas y salidas hacia otros procesos y la información respectiva a las metas y métricas.

PROCESO. (Entidad Pública). Un proceso lo constituyen un conjunto de procedimientos que describen detalladamente cómo se debe ejecutar una acción.

REGISTRO DE UN PROVEEDOR. (ART. 8 DECRETO 3512 DE 2003). Es la actividad realizada por un proveedor para ingresar al SICE, como condición para suministrar bienes y servicios de uso común o de uso en contratos de obra, a los organismos que conforman la administración pública y a los particulares o entidades que manejan recursos públicos.

SELECCIÓN ABREVIADA. (Numeral 2, Art. 2 Ley 1150 de 2007). La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.

SELECCIÓN OBJETIVA. (Art. 5 Ley 1150 de 2007). Es objetiva la selección en la cual la escogencia se haga al ofrecimiento más favorable a la entidad y a los fines que ella busca, sin tener en consideración factores de afecto o de interés y, en general, cualquier clase de motivación subjetiva.

SERVICIOS DE APOYO A LA GESTIÓN. Son aquellos en los que la persona contratada realiza labores predominantemente materiales y no calificadas, para la atención de necesidades de la entidad, sin que sea posible entender comprendida dentro de los mismos, la contratación de actividades que supongan la intermediación de la relación laboral, ni la contratación de empresas de servicios temporales.

SERVICIOS PROFESIONALES. Corresponden a aquellos de naturaleza intelectual diferentes a los de consultoría que se derivan del cumplimiento de las funciones de la entidad.

SERVIDORES PÚBLICOS. (Numeral 2 Art. 2 Ley 80 de 1993). Se denominan servidores públicos:

a) Las personas naturales que prestan sus servicios dependientes a los organismos y entidades de que trata este artículo, con excepción de las asociaciones y fundaciones de participación mixta en las cuales dicha denominación se predicará exclusivamente de sus representantes legales y de los funcionarios de los niveles directivo, asesor o ejecutivo o sus equivalentes en quienes se delegue la celebración de contratos en representación de aquéllas.

b) Los miembros de las corporaciones públicas que tengan capacidad para celebrar contratos en representación de éstas.

SERVICIOS PÚBLICOS. (Numeral 3 Art. 2 Ley 80 de 1993). Se denominan servicios públicos: Los que están destinados a satisfacer necesidades colectivas en forma general, permanente y continua, bajo la dirección, regulación y control del Estado, así como aquellos mediante los cuales el Estado busca preservar el orden y asegurar el cumplimiento de sus fines.

SISTEMA DE INFORMACIÓN PARA LA VIGILANCIA DE LA CONTRATACIÓN ESTATAL, SICE.
(Art. 3 Decreto 3512 de 2003). Es una herramienta de información, ordenación y control que incorpora las cifras relevantes del proceso de contratación estatal, con el fin de confrontarlas en línea y en tiempo real, con los precios de referencia incorporados en el Registro Único de Precios de Referencia, RUPR, de acuerdo con los parámetros de codificación del Catálogo Único de Bienes y Servicios, CUBS, garantizando una contratación sin detrimento de los recursos públicos.

El sistema permitirá la interacción de los contratantes, los contratistas, la comunidad y los órganos de control, suministrando instrumentos para facilitar la contratación en línea, garantizar la selección objetiva, divulgar los procesos contractuales y facilitar un control posterior y selectivo, todo lo anterior con tecnología, eficiencia y seguridad.

SISTEMA ELECTRÓNICO PARA LA CONTRATACIÓN PÚBLICA, SECOP. ES un sistema electrónico que permite la consulta de información sobre los procesos contractuales que gestionan, tanto las entidades del Estado sujetas al Régimen de Contratación establecido en el Estatuto General de Contratación, como las que voluntariamente coadyuvan a la difusión de la actividad contractual.

El principal objetivo del Portal es promover la transparencia, eficiencia y uso de tecnologías en la publicación por Internet de las adquisiciones públicas para el beneficio de empresarios, organismos públicos y de la ciudadanía en general, así como mejorar las formas de acceso a la información respecto de lo que compra y contrata el Estado, con el consiguiente impacto económico que ello genera en la pequeña, mediana y grande empresa, en los niveles locales e internacionales.

SUBASTA INVERSA. (Art. 14 Decreto 066 de 2004). Se entiende por subasta inversa para la presentación de la oferta, la puja dinámica efectuada electrónicamente, mediante la cual los oferentes, durante un tiempo determinado, ajustan su oferta respecto de aquellas variables susceptibles de ser mejoradas, con el fin de lograr el ofrecimiento que por tener el menor costo evaluado represente la mejor relación costo-beneficio para la entidad, de acuerdo con lo señalado en el pliego de condiciones.

UMBRAL DE PRECIOS. (Art. 8 Decreto 3512 de 2003). Es el intervalo de

variación razonable del precio de contratación de un bien o servicio de uso común o de uso en contratos de obra.

TERMINACIÓN UNILATERAL. (Art. 17 Ley 80 de 1993). La entidad en acto administrativo debidamente motivado dispondrá la terminación anticipada del contrato en los siguientes eventos:

1°. Cuando las exigencias del servicio público lo requieran o la situación de orden público lo imponga.

2°. Por muerte o incapacidad física permanente del contratista, si es persona natural, o por disolución de la persona jurídica del contratista.

3°. Por interdicción judicial o declaración de quiebra del contratista.

4°. Por cesación de pagos, concurso de acreedores o embargos judiciales del contratista que afecten de manera grave el cumplimiento del contrato.

Sin embargo, en los casos a que se refieren los numerales 2°. y 3°. de este artículo podrá continuarse la ejecución con el garante de la obligación.

TIPO DE CONTRATO. Corresponde a la clasificación o características de contrato, dentro de las cuales se encuentran, entre otros, los de obra pública, suministro, consultoría, concesión, compraventa, transporte, seguro, prestación de servicios, arrendamiento, convenio o comodato.

UNIÓN TEMPORAL. (Art. 7 Ley 80 de 1993). Cuando dos o más personas en forma conjunta presentan una misma propuesta para la adjudicación, celebración y ejecución de un contrato, respondiendo solidariamente por el cumplimiento total de la propuesta y del objeto contratado, pero las sanciones por el incumplimiento de las obligaciones derivadas de la propuesta y del contrato se impondrán de acuerdo con la participación en la ejecución de cada uno de los miembros de la unión temporal.

URGENCIA MANIFIESTA. (Art. 42 Ley 80 de 1993). Existe urgencia manifiesta cuando la continuidad del servicio exige el suministro de bienes, o la prestación de servicios, o la ejecución de obras en el inmediato futuro; cuando se presenten situaciones relacionadas con los estados de excepción; cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, en general, cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección públicos.

La urgencia manifiesta se declarará mediante acto administrativo motivado.

VEEDURÍA CIUDADANA. (Art. 1 Ley 850 de 2003). El mecanismo democrático de representación que le permite a los ciudadanos o a las diferentes organizaciones comunitarias, ejercer vigilancia sobre la gestión pública, respecto a las autoridades, administrativas, políticas, judiciales, electorales, legislativas y órganos de control, así como de las entidades públicas o privadas, organizaciones no gubernamentales de carácter nacional o internacional que operen en el país, encargadas de la ejecución de un programa, proyecto, contrato o de la prestación de un servicio público.

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 integrado. 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 a los cuales las entidades públicas deben acogerse, como es el caso de los portales Web, con dichos portales se busca utilizar los recursos de sistemas ya existentes con el objetivo de prestar un mejor servicio a la comunidad.

Desde el punto de vista de los sistemas de información se presenta un proyecto 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.

- Titulo del proyecto. El titulo del proyecto de grado es TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACIÓN Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO

- Línea de investigación. Este proyecto corresponde a la línea de investigación Sistemas Computacionales.

- 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. La sistematización del problema es la siguiente:

- ¿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 (TI) en las entidades públicas del Departamento de Nariño?

- ¿Cómo están las condiciones de seguridad física de la información del proceso de contratación (TI) 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 (TI) en las entidades públicas del Departamento de Nariño para establecer los riesgos a los que se encuentra expuesta y recomendar controles para su protección?

- 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 (TI), y el cumplimiento del Decreto 1151 sobre Gobierno en Línea.

- Objetivos Específicos. Los objetivos específicos son los siguientes:

- 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 (TI) 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.

- Justificación. 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.

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

  La aplicación de técnicas de auditoría de sistemas se realizo al proceso de contratación (TI) de la Alcaldía Municipal de Tangua y la Alcaldía Municipal de Yacuanquer, con esto se identifico, comprobó y evaluó las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información que utilizan dichas entidades. Además, se audito el sitio Web de las entidades y se verifico si cumplían con los lineamientos del Decreto 1151 de la estrategia de Gobierno en Línea.

Las entidades a auditar fueron:

- Alcaldía Municipal de Tangua

- Alcaldía Municipal de Yacuanquer

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, ósea 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 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 por que 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 que 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..

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 más 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.

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 falta. 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 herramienta de reingeniería capaz de retroalimentar procesos o crear 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:

1.2.1 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.

1.2.2 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 utilizaran.
- 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 a 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 el trabajo o 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 compañía.

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.

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.

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. 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.

Los objetivos específicos de la auditoria de sistemas son:

- 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 auditoría de sistemas. Las principales pruebas y herramientas para efectuar una auditoría de sistemas son las siguientes:

- 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. A continuación en la tabla 1 se resumen las profesiones y las actividades relacionadas con dichas profesiones.

Tabla 1: Actividades y conocimientos

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.

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.

- 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.

- 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:
    - o Situación actual
    - o Tendencias futuras
    - o Puntos débiles y amenazas
    - o Recomendaciones y planes de acción
    - o 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.

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.

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, 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. Los procesos que forman parte de este dominio son:

  - **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 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. Los procesos que se incluyen en este dominio son:

  - **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 realizara 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. Los procesos que pertenecen a este dominio son:

  - **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 de manera de asegurar que estos concuerde 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 singulares

- **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, suspensión 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 implementado 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 computo y aseguren el trato justo de los departamentos usuarios y sus necesidades

  - ✓ Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, 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 Monitoreo:** 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. Los procesos que forman parte de este dominio son:

  - **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 Auditoria 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.

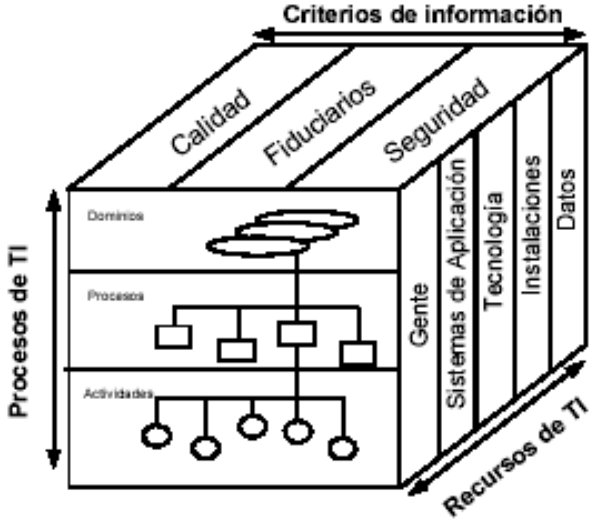
Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

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 alcanzaran 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:

- Los recursos de las TI
- Los criterios empresariales que deben satisfacer la información
- Los procesos de TI

Figura 1: Las tres dimensiones conceptuales de COBIT



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.

1.6.2 COSO (Sponsoring Organizations of the Treadway Commission).

COSO inicio en 1985 recomendando que las organizaciones patrocinadoras de la Comisión trabajen juntas para desarrollar sistemas integrados de orientación sobre el control interno.

El modelo COSO define el control interno como un conjunto de procesos, realizado por los directivos de una organización, y creado para garantizar el logro de los objetivos.

COSO consta de cinco elementos, estos elementos proporcionan un marco eficaz para describir y analizar el sistema de control interno, los cuales son:

- **Entorno de Control:** Sirve como base para los demás componentes del control interno, proporcionando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos, el estilo de funcionamiento de la administración, la delegación de los sistemas de autoridad, así como los procesos de gestión y desarrollo de las personas en la empresa.

- **Evaluación del riesgo:** Cada empresa se enfrenta a una variedad de riesgos de fuentes externas e internas que deben ser evaluados. Una condición previa para la evaluación de riesgos es el establecimiento de objetivos y por lo tanto la evaluación de riesgos es la caracterización y análisis de los riesgos relevantes para la consecución de los objetivos asignados. La evaluación de riesgos es un requisito previo para establecer cómo los riesgos deberían ser manejados.

- **Las actividades de control:** Las actividades de control son las políticas y procedimientos que ayudan a asegurar la gestión de las directivas se llevan a cabo. También garantizan la toma de medidas necesarias para hacer frente a los riesgos que pueden obstaculizar el logro de los objetivos de la entidad. Las actividades de control se originan en toda la organización, en todos los niveles y en todas las funciones. Estos incluyen una amplia gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de desempeño operativo, la seguridad de los activos y la separación de funciones.

- **Información y comunicación:** Los sistemas de información juegan un papel importante en los sistemas de control interno que producen los informes, incluidos los operativos, financieros y el cumplimiento de información relacionada, que permiten elaborar y controlar la entidad. De manera más amplia, la comunicación eficaz debe garantizar los flujos de información hacia abajo, y hasta a través de la organización.

- **Seguimiento:** Los sistemas de control interno deben ser supervisados, un proceso que evalúa la calidad del desempeño del sistema en el tiempo. Esto se logra a través de continuas actividades de supervisión o evaluaciones por separado. Las fallas de control interno detectadas a través de estas actividades deberían notificar las medidas de planificación y correctivas garantizando la mejora continua del sistema.

Algunas diferencias entre COSO y COBIT, que son los dos modelos más difundidos actualmente son:

- El modelo COSO está enfocado a toda la empresa, mientras que el COBIT se limita a las tecnologías de la información (TI).

- El COBIT establece como uno de sus objetivos la seguridad de la información, por el contrario COSO, no lo toma en cuenta en su evaluación.

El modelo de control interno que presenta el COSO no es muy completo, a diferencia de la metodología COBIT que contempla políticas, procedimientos y estructuras organizativas, además de procesos para definir el modelo de control interno.

1.7 TÉCNICAS DE AUDITORIA DE SISTEMAS EN FUNCIONAMIENTO

1.7.1 Técnicas administrativas. Las técnicas que ocupan este campo son:

- **Selección de Áreas de Auditoria.** 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 y 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 y 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. Las técnicas de auditoría que ocupan este campo son:

- **Software de auditoria 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. Estas técnicas están orientadas básicamente a verificar cálculos que sean realmente complejos, comprobar su exactitud en el procesamiento y verificar que cumplan con los controles preestablecidos en el correspondiente manual.

- **Métodos de datos de prueba.** También llamada "lotes de prueba" (test decks), consiste en realizar transacciones simuladas que incluye cualquier condición posible, conteniendo además de datos validos, datos y condiciones que el sistema no puede manejar por falta de controles propios, debe contener pruebas validas e invalidas y ser procesadas por el sistema, el auditor debe conocer de antemano cuales serian los resultados para poder compararlas con los resultados obtenidos en la prueba. Esta técnica es utilizada en la fase de prueba de los programas, antes de enviarlos a producción.

- **Evaluación del sistema en caso base (BCSE).** Este procedimiento está orientado en probar la lógica de los programas de aplicación, con la utilización de archivos de prueba desarrollados específicamente para verificar la exactitud del procesamiento, con la cooperación de los usuarios, auditores y personal de sistemas, a diferencia de el método de datos de prueba este no se abandona sino que se actualiza o mantiene permanentemente, evolucionando junto al sistema.

- **Operación paralela.** Cuando se sistematiza un proceso en el computador, se utiliza esta técnica llevando los dos sistemas el manual y el computarizado en paralelo hasta cuando los resultados de estos dos coincidan, a partir de este momento se da de baja el antiguo sistema. Esta técnica es muy utilizada para probar nuevos sistemas y poder así verificar su exactitud.

- **Facilidad de prueba integrada (integrated test facility).** Para esta técnica se crea un ambiente ficticio en el cual se desarrolla la auditoria, la efectividad de esta técnica está orientada en probar la lógica del procesamiento y es muy utilizada en sistemas ON-LINE. Se usa para comparar los resultados de los datos arrojados por la prueba con los resultados ya predeterminados.

- **Simulación en paralelo.** Se diferencia de las técnicas de Datos de prueba y de Facilidad de prueba integrada, ya que estas procesan datos simulados en proceso reales y por el contrario la técnica de simulación en paralelo procesa datos reales en programas simulados.

  Esta técnica utiliza datos de entrada de los programas de la aplicación los procesa y trata de producir los mismos resultados, comparándolos al final buscando si son iguales o existen discrepancias.

1.7.4 Técnicas para seleccionar y monitorear transacciones. Estas técnicas son las más relevantes dentro del proceso de evaluación de un sistema. Estas técnicas son las que definen la forma, manera, cantidad y calidad de capturar una muestra del sistema para ser evaluada.

Generalmente el auditor utiliza pruebas de rangos, técnicas de muestreo y condiciones de error. Esto lo hace en base a criterio y experiencia profesional.

- **Selección de transacciones de entrada.** Esta es una técnica muy segura ya que la información del sistema no corre ningún riesgo de alteración, en esta técnica el auditor selecciona y separa datos de entrada que bajo su criterio profesional y su experiencia son los idóneos para correrlos en un software de auditoría independiente de los programas aplicativos, estos datos seleccionados son sometidos a un examen detallado.

- **Archivo de revisión de auditoría como control del sistema (SCARF).** SCARF (System Control Audit File): esta técnica consiste en la inserción de módulos de auditoría dentro del programa de aplicación, para que ejecute una supervisión y monitoreo de forma permanente, una vez que el auditor precisa los requerimientos a los programadores en la fase de diseño, estas rutinas actúan como huéspedes dentro de las aplicaciones, esta técnica es utilizada en ambiente online para determinar que transacciones son sospechosas.

- **Archivo de revisión de auditoría por muestreo (SARF).** SARF (simple audit review file): esta técnica a diferencia de la anterior selecciona aleatoriamente las transacciones con el fin de obtener un archivo para la evaluación, esta técnica es utilizada por los auditores externos generando estadísticas de muestra y producción, una desventaja de esta técnica es su alto costo de desarrollo y producción.

- **Registros extendidos.** Esta técnica se basa en conservar un historial de las transacciones de todas las actividades, errores y/o fallos del sistema en un archivo durante varios periodos o años, para evitar la pérdida de las pistas de auditoría. Una desventaja de esta técnica es costo extra de almacenamiento de datos.

1.7.5 Técnicas para la auditoría de información almacenada. Para realizar un análisis en los archivos de la entidad auditada necesariamente se deben emplear aplicaciones que nos permitan realizar un análisis eficiente a un volumen información almacenada tanto en archivos producidos por el software del sistema, como en los datos almacenados en un SGBD. Con este fin se ha realizará una clasificación de aplicaciones para asistir al auditor en dicha tarea según el tamaño del sistema, propósito y tipo de aplicación.

- **Aplicaciones estandarizadas para grandes volúmenes de información.** Estos programas son generalmente paquetes de software robustos, los cuales manejan estándares pre establecidos para el procesamiento de información, realizan tareas como la clasificación, análisis estadísticos, comprobación de resultados, simulación de ambientes, etc.

  Estos programas suelen ser utilizados generalmente en el área contable de la empresa, con el fin de comprobar posibles errores en los cálculos, comparación de información de inventarios, etc.

  En la actualidad los paquetes de auditoría suelen ser más versátiles y automatizados, aunque así cómo los software de auditoría han avanzado, los sistemas a los que se aplican también y pero cada vez más se tienen en cuenta los estándares establecidos para el desarrollo de estos sistemas y esto facilita el desarrollo del software para auditarlos.

  Actualmente software como ACL el cual cuenta con un alta reputación, capaz de realizar un monitoreo continuo de transacciones, buscar errores y puntos débiles en los controles y pagos**,** y Auditor® el cual es capaz de importar archivos de más de 100 sistemas contables automáticamente.

- **Programas utilitarios y usos generales.** Este tipo de programas no son especializados o específicos para la labor de auditoría, sin embargo pueden ser utilizados como apoyo para obtener información acerca de archivos y bases de datos de las entidades.

  Estos programas son desarrollados a menudo por los fabricantes de sistemas operativos, grupos de seguridad y soporte, mantenimiento, fabricantes de computadoras o los proveedores de bases de datos. Sin embargo estas aplicaciones así como pueden proveer apoyo en las auditorías, podrían proveer apoyo a posibles fraudes debido a su gran capacidad para acceder a los archivos y bases de datos y modificarlos.

  Un ejemplo claro de este tipo de aplicaciones es Oracle Audit Vault, el cual es un programa ofrecido por el proveedor del SGBD Oracle. Aunque esta es una

aplicación no enfocada en algún sistema en particular (ej. Sistema contable, nomina, ventas), es un software con múltiples características y herramientas que pueden servir para el desarrollo de las auditorias en bases de datos de proveedores Oracle y Microsoft SQL Server.

- **Software hecho a medida**. Este tipo de software le ofrece al auditor una solución especializada para un tipo de tarea específica en una entidad, generalmente se desarrollan para tareas poco complejas y manejo de bajos volúmenes de información, debido a que el proceso de desarrollo de estos software requieren un costo en esfuerzo y tiempo que se elevaría a medida que se eleva la complejidad de las tareas. Por tales razones es bueno que en caso de que el sistema de la entidad deba ser actualizado el equipo auditor puede pedir que se incluyan características de auditoría en dichas actualizaciones.

  En cualquier caso, se debe seguir todo el proceso de ingeniería de software para obtener un mejor resultado, es decir, especificar unos requerimientos, realizar un análisis, diseñar una solución y realizar las respectivas pruebas.

- **BackUp o vaciado de archivos.** Esta técnica consiste en copiar los archivos de información y bases de datos en medios de almacenamiento externos o impresos, esto además de proveer un soporte de copias de seguridad a la entidad permite realizar seguimientos por parte del auditor y depurar las transacciones realizadas por el sistema auditado con el apoyo de pruebas de escritorio o el apoyo de algún software que sirva para depurar el proceso y los resultados.

1.7.6 Técnicas para examinar programas aplicativos. Los programas aplicativos son aquellos que la entidad utiliza en el desarrollo de sus procesos y están incluidos en los procedimientos para cumplir ciertas tareas u objetivos. Todas las aplicaciones que se vean inmersas en algún proceso de la entidad deben ser examinadas, para esto se pueden utilizar variadas técnicas, algunas de ellas se describen a continuación.

- **Snapshot.** El snapshot o imagen instantánea es una técnica muy sencilla que permite al auditor tomar instantáneas de las aplicaciones en ejecución y en momentos claves para realizar seguimiento a estas.

  En caso de las aplicaciones que manejan archivos de datos, se deben incluir rutinas que capturen las instantáneas del estado de la aplicación en ciertas ocasiones o entradas especiales. En caso de tratarse de bases de datos, se pueden incluir triggers que se disparen en cierto momento, acceso, entrada o modificación de la información.

- **Mapping.** Es una técnica avanzada de auditoría, sirve para realizar análisis de una aplicación en ejecución, verifica su rendimiento, identifica las funcionalidades utilizadas y las que no lo son, y las posibles ejecuciones de código no autorizado.

- **Tracing y Flujograma de control.** Esta técnica consiste en realizar un rastreo a modo de depuración de las transacciones utilizadas para realizar un proceso y poder compararlo con los procedimientos pre establecidos para dicho proceso.

  El resultado de este tipo de técnicas puede expresarse como un flujo de trabajo, de esta forma es fácil de interpretar y encontrar posibles defectos en el flujo de la información.

- **Comparación de código y control de cambio.** Esta técnica se utiliza para examinar los cambios entre versiones consecutivas con el fin de auditar los mantenimientos y actualizaciones propuestos. En la actualidad se suele usar CVS para gestionar y controlar estos cambios, además que provee un estándar entre desarrolladores, podría proveer también una forma estándar de auditar el control de versiones.

  Se puede utilizar además, comparación de bytes y resultados de la aplicación instalada y en funcionamiento, y un clon actualizado de dicha aplicación, esto con el fin de evitar la intrusión de código no autorizado y evitar de esta forma posibles fraudes.

- **Análisis de la lógica del programa.** Está técnica consiste en una revisión concienzuda de la documentación del proceso de desarrollo de la aplicación, realizar comparaciones con el código y los procedimientos, de esta forma verificar el correcto funcionamiento de la aplicación y que sigue los procedimientos establecidos por la entidad y los requerimientos de dicha aplicación. Además esta técnica permite al auditor emitir conceptos sobre la documentación del programa. Esta técnica implica un amplio conocimiento de lenguajes de programación, debido a que se debe poder entender el código de las aplicaciones auditadas.

  Estas técnicas son muy útiles para el auditor sin embargo realizar una auditoría completa a todos los elementos de las aplicaciones puede resultar costoso tanto en esfuerzo, tiempo y dinero, por tal razón es mejor que la auditoria se enfoque, en lo posible se audite el control interno y verificar los controles que se están aplicando son los adecuados.

1.8 VENTAJAS Y DESVENTAJAS DE LAS TÉCNICAS PARA PROBAR CONTROLES DE SISTEMAS EN FUNCIONAMIENTO

1.8.1 Técnicas para probar controles de sistemas en funcionamiento. Las técnicas de auditoría que ocupan este campo son:

- **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 determinara la efectividad de esta técnica. Es recomendable seleccionar datos normales, ilógicos, imposibles, con valores extremos, etc. Un auditor podría usar esta técnica para:

  a) 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.

  b) 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.

  c) 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.

  d) 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.

  e) 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.

  f) 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.

g) 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.

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

i) Controlar la secuencia de presentación de datos de prueba cuando se extienda a varios ciclos de procesamiento.

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

k) Predecir los resultados de los datos de prueba y compararlos con la salida real de datos de pruebas, para las transacciones individuales.

l) Confirmar que se usó la versión actual de los programas para procesar los datos de prueba.

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

n) 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 validos y advirtiendo del intento de ingreso de datos incorrectos.

  - ✓ 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.

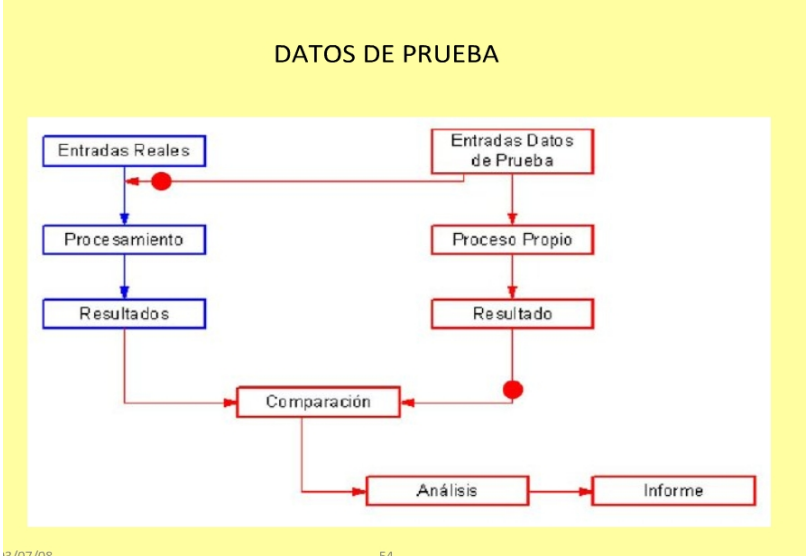
- **Desventajas**

  - ✓ 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 genera costos por los retazos ocasionados al hacer las respectivas pruebas.

Figura 2: Datos de prueba



http://www.slideshare.net/marcifus/auditora-taacs

- **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.

- ✓ 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**

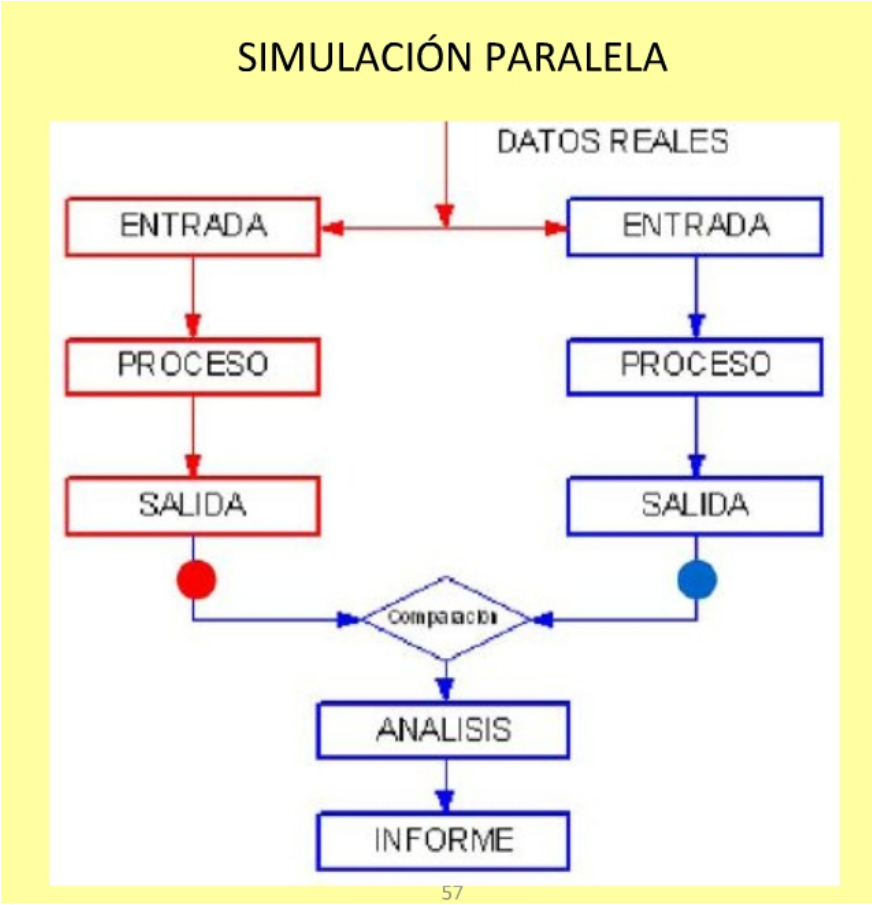
  - ✓ El hecho de llevar de la mano el sistema actual con el nuevo se convierte en una ventaja ya que se va a garantizar que el sistema nuevo funcione de la mejor manera posible, a fin de evitar futuras modificaciones en su lógica o procesamiento.

  - ✓ Convertir un sistema ya sea manual o computarizado el cual presente algunas falencias, en un sistema mucho 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.

Figura 3: Simulación Paralela



http://www.slideshare.net/marcifus/auditora-taacs

- **Facilidad de prueba integrada (Integrated Test Facility).** Su objetivo y uso es similar método de datos de prueba pero su gran 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.

  - ✓ 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.

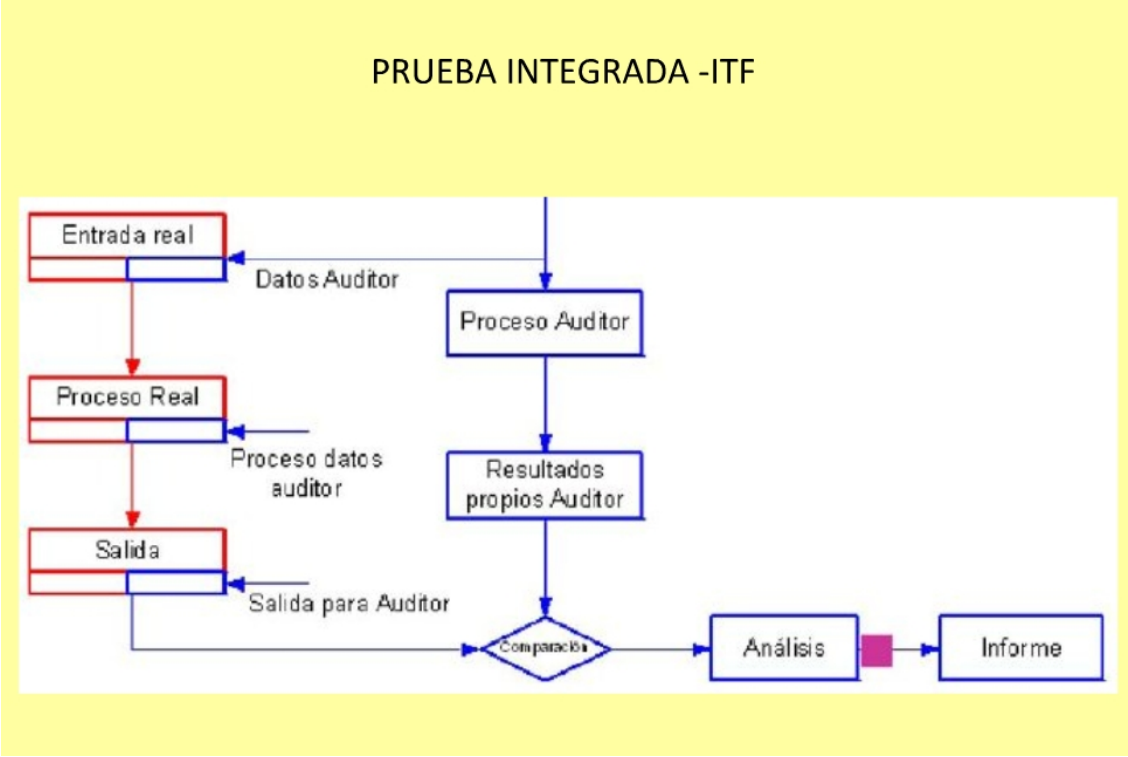
  - ✓ Los resultados e informes obtenidos a través de la entidad ficticia permitirán de forma segura e inmediata analizar la eficiencia del sistema auditado.

- **Desventajas**

  - ✓ Existe la posibilidad de afectar la integridad de la información real.

  - ✓ 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.

Figura 4: Pruega Integrada ITF



http://www.slideshare.net/marcifus/auditora-taacs

- **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 deposición 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 quedara 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.

1.8.2 Técnicas para seleccionar y monitorear transacciones. Los procedimientos de auditoría son distintos de acuerdo con la filosofía y técnica de cada organización o 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:

a) Selección de transacciones de entrada.

b) Archivo de revisión de auditoría como control del sistema (SCARF).

c) 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 cuando 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.

Figura 5: Registros extendidos

Fuente: http://www.slideshare.net/marcifus/auditora-taacs

- **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, ya 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 seleccionaran 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.

    - ✓ 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.

- **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.

  - **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.

- **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 información significativa sobre las transacciones o el sistema, que luego pude ser consultada por el auditor.

  - ✓ 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.

1.8.3 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.

Categorización de las herramientas de software:

a) Herramientas de productividad de auditoría.

b) Reducen el tiempo empleado en tareas administrativas.

c) Groupware es una forma que permite automatizar procesos de auditoría y realizar una mejor coordinación del equipo auditor, un ejemplo de groupware es Lotus notes, permite compartir información, comunicarse más efectivamente a los diferentes equipos de negocios y puede adaptarse fácilmente a la labor de auditoría; este producto proporciona varios servicios como accesos a bases de datos, plataformas de comunicación, procesamiento de flujo de trabajo, entre otros.

d) Herramientas de auditoría asistidas por computadora (CAATs)

Tabla 2: CAATs

BASICOS	INTERMEDIOS	COMPLEJOS
• Procesadores de texto (MS WORD) • Presentaciones (MS Power Point, Flash) • Plantillas de cálculo (MS Excel) • Programas estadísticos (SPSS) • Software de producción personal	• ACL (Auditor Control Language) • IDEA (Interactive Data Extraction and Analysis) • Productos Methodware: • Ranking Advisor • ProAudit Advisor • COBIT Advisor • Audit Builder	• ORACLE • SQL Server • Informix • MySQL • MS Access • TOAD

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.

La auditoria se encarga de evaluar y controlar la información procesada, efectuando seguimientos de todo el entorno humano, tecnológico y flujo grama de procesos y procesamiento de datos, que hace que la información llegue al destino final, con esto se busca evitar errores, deficiencias en procedimientos, riesgos de sabotaje, fraude o pérdidas económicas para la empresa.

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.

    - ✓ 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.

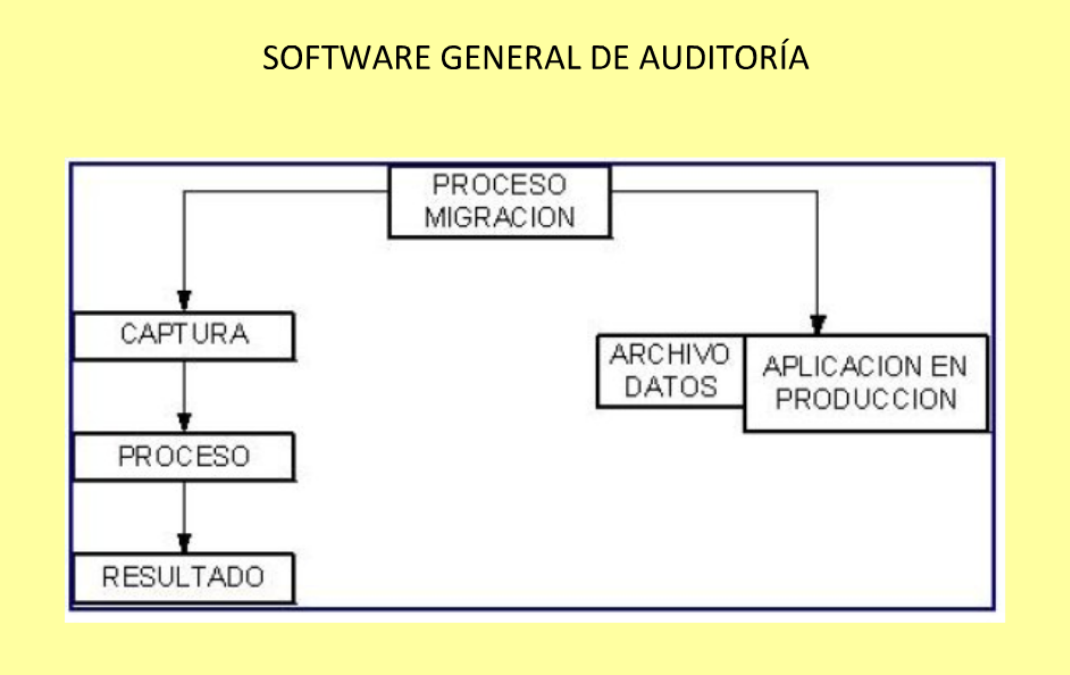
  - **Desventajas:**

    - ✓ 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.

Figura 6: Software general de auditoría



Fuente: http://www.slideshare.net/marcifus/auditora-taacs

- **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.

- **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.

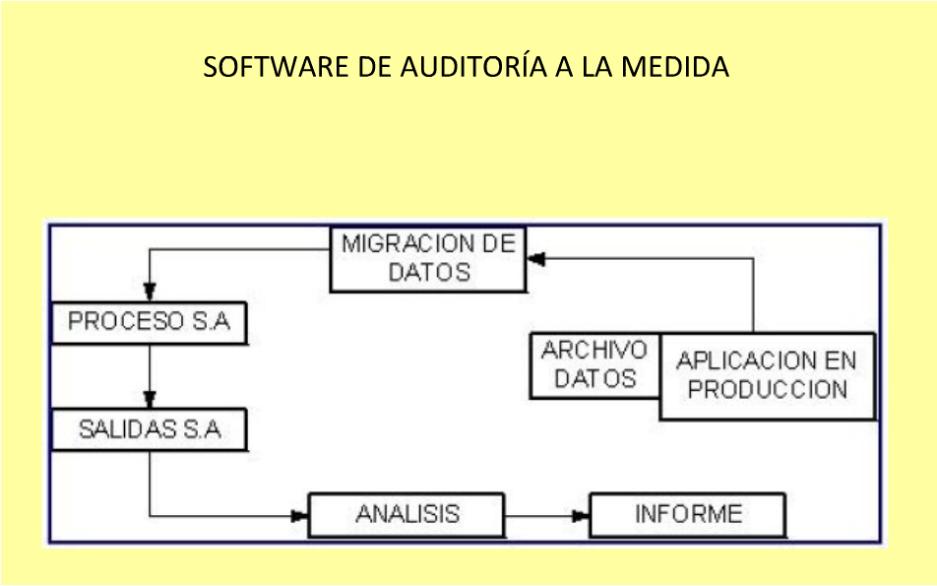
  - ✓ Estos programas y su documentación, deben ser antes revisados por el auditor, para pasar por un proceso de prueba y ensayo en donde se determinara si el software cumple con todas las normas y requerimientos de la empresa.

- **Aplicaciones.** 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 más 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 compuotadora CAATs usadas para evaluar la

integridad de una aplicación, determinar la conformidad con procedimientos y monitorear los resultados de procesamientos.

Figura 7: Software de auditoría a la medida



http://www.slideshare.net/marcifus/auditora-taacs

- **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.

1.8.4 Técnicas para examinar programas aplicativos. Las técnicas de auditoría que ocupan este campo son:

- **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.

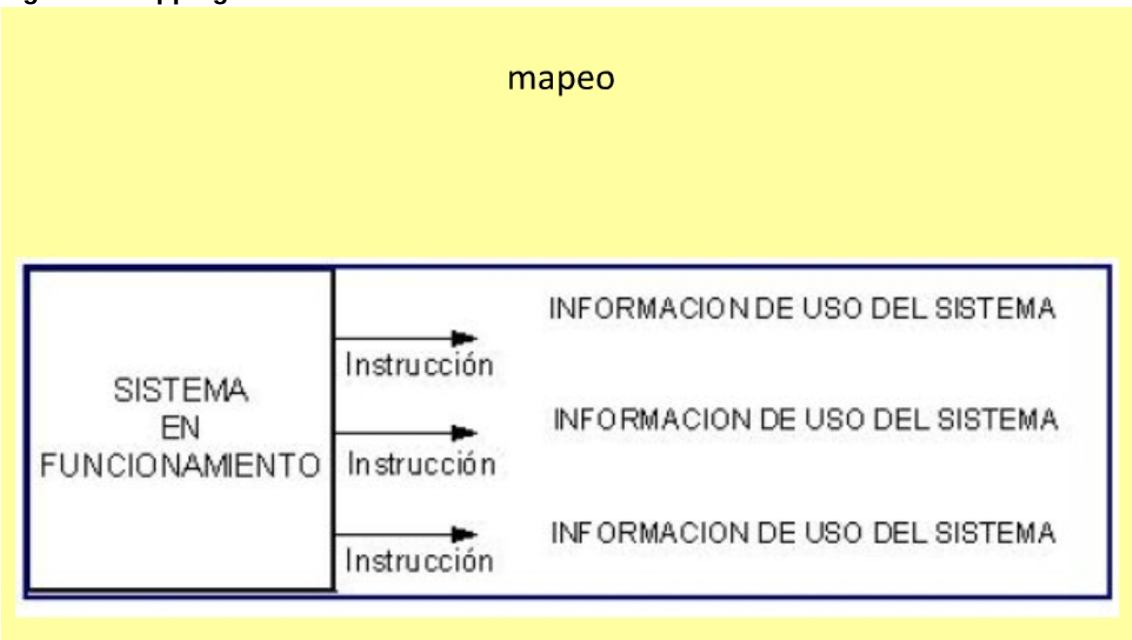
    - ✓ Identifica instrucciones que no son utilizadas. Pues es una técnica segura que sirve como soporte al control de calidad de sistemas para medir eficiencia.

    - ✓ 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.

Figura 8: Mapping



http://www.slideshare.net/marcifus/auditora-taacs

- **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:**

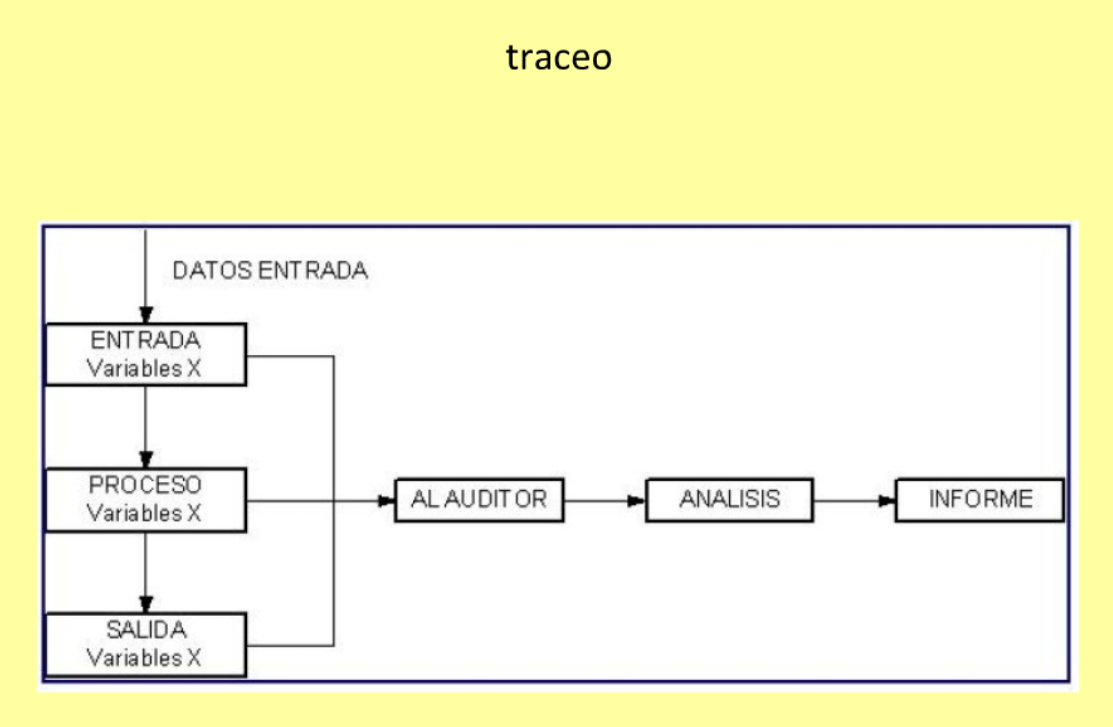
    ✓ Periódicamente deben ser evaluados ciertos factores o elementos que de una u otra manera brinden confiabilidad al sistema informático, ya que los equipos pueden fallar y producir accidentes informáticos, los errores humanos y los actos intencionales siendo estos los más perjudiciales e importantes.

    ✓ Con el fin de evitar en gran parte se presente este tipo de problemas el sistema debe contar con un componente de identificación de usuarios, asignado roles y permisos de acceso y atribuciones, aquí es donde tracing actúa, verificando a posteriori 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.

Figura 9: Tracing



http://www.slideshare.net/marcifus/auditora-taacs

- **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:**

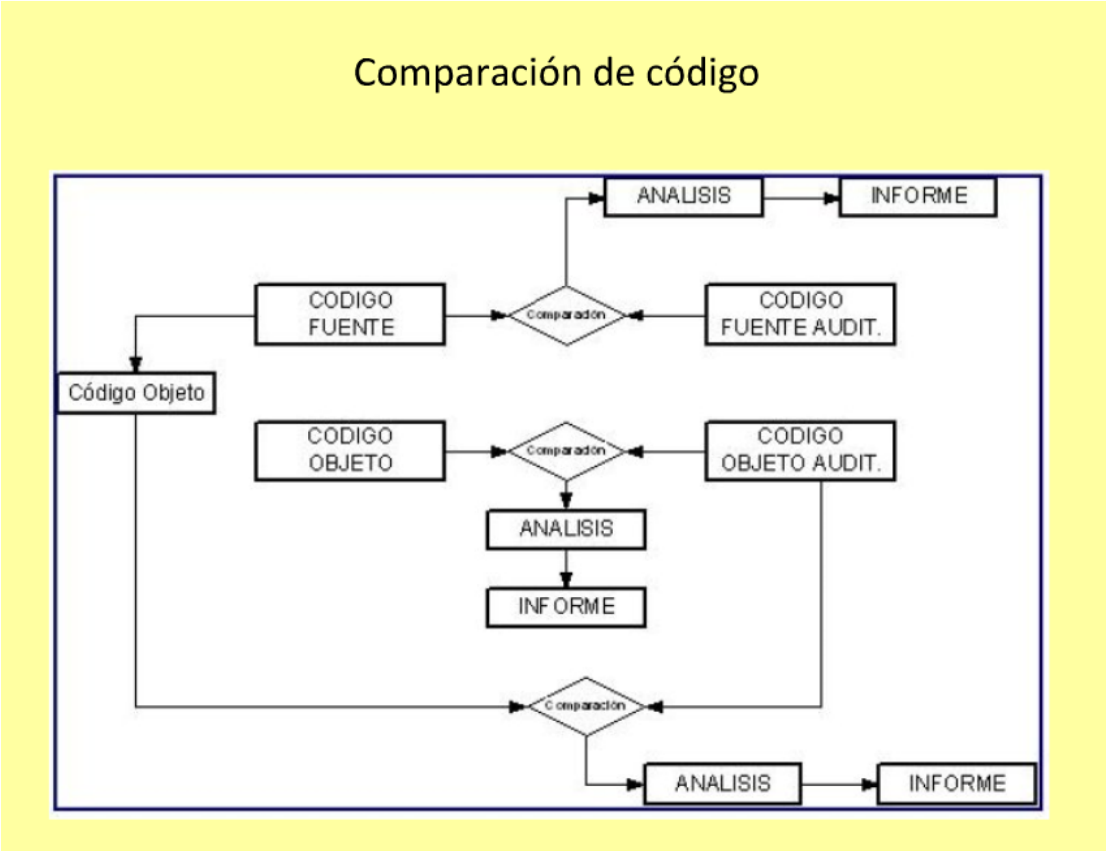
  - ✓ La técnica de comparación de código no proporciona evidencia sobre confiabilidad de los archivos de datos ni sobre eficiencia de los programas.

  - ✓ 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.

Figura 10: Comparación de código



http://www.slideshare.net/marcifus/auditora-taacs

- **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 y las páginas web de las entidades Alcaldía municipal de Tangua y Alcaldía municipal de Yacuanquer, se rigió 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 se enmarca 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 General de Nariño y el equipo auditor conformado por los estudiantes Lennin Geovanny Ibarra González y Diego Mauricio Meza García.

La responsabilidad del órgano de control consiste en producir un informe integral que contenga el concepto sobre la gestión adelantada por la administración de la entidad e incluye pronunciamientos sobre el acatamiento a las disposiciones legales y la calidad y eficiencia del Sistema de Control Interno.

De conformidad con lo anterior, se planeó y ejecutó el trabajo de manera que el examen y el resultado de las pruebas proporcionaran 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, porque se realiza recolección y análisis de datos, 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, también cabe mencionar que esta metodología 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 de la entidad Contraloría Departamental de Nariño fue dividida en varias etapas así:

- **Etapa I. Familiarización con el Entorno.** En esta etapa se realiza el estudio previo al inicio de la Auditoria con el propósito de conocer en detalle las

entidades Alcaldía municipal de Tangua y Alcaldía municipal de Yacuanquer y en si del proceso de contratación que se lleva a cabo en estas dos entidades, además del tratamiento que se le ha venido dando a la página web como herramienta para el cumplimiento del decreto 1151 de 2008 de Gobierno en Línea.

Los resultados de la exploración permiten, además, hacer la selección de las técnicas y metodologías de auditoría a utilizar.

El equipo auditor se rigió por las normas de auditoría de la entidad Contraloría Departamental de Nariño, se realizaron visitas a las entidades, de las cuales se saco 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 realizo 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:

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

  - Realizar el estudio inicial en las entidades Alcaldía municipal de Tangua y Alcaldía municipal de Yacuanquer, para recolectar datos sobre el funcionamiento del proceso de contratación y del cumplimiento del decreto 1151 de 2008 de Gobierno en Línea.

  - Determinar los recursos necesarios para realizar la auditoría.

  - Elaboración del plan de trabajo.

- **Etapa III. Realización de las Actividades de la Auditoría.** En esta etapa se hicieron efectivos todos los planteamientos de la etapa anterior, con la aplicación de las metodologías y técnicas escogidas que garantizaron el cumplimiento de los objetivos planeados.

  Las actividades que se realizaron dentro de esta etapa fueron:

  - 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.

- 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.

- Realización de pruebas sobre los procesos seleccionados.
- Elaboración de los Cuestionarios cualitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.

- Identificación de hallazgos dentro del proceso evaluado.

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

- Análisis del cumplimiento del decreto 1151 de 2008 de Gobierno en Línea

- **Etapa IV. Presentación del Informe Final.** En esta etapa se realizo el informe final, en donde se describieron los hallazgos encontrados y se hacen las recomendaciones pertinentes para subsanar dichos errores, también se relacionan que partes del proceso de contratación (TI) se encuentran sin problemas para que las entidades sepan donde realizar las correcciones del caso, también se produjo el informe donde se indican algunas apreciaciones de como elaborar la pagina web para que cumpla con los lineamientos del decreto 1151 de 2008 de Gobierno en Línea.

  Una vez elaborados los informes fueron enviados a la Contraloría Departamental de Nariño para que esta a su vez los haga llegar a las entidades auditadas con el fin de que se presenten las correcciones necesarias.

3. DESARROLLO DEL PROYECTO

3.1 ARCHIVO PERMANENTE

El archivo permanente es la colección de documentos e información que resulta útil para conocer la institución en sus aspectos generales, esta información refleja las características y el funcionamiento real de la institución, esta será válida para el periodo auditado 2008 ya que los diferentes documentos varían según el periodo de gobierno.

3.1.1 Archivo permanente común. En este apartado se citaran los elementos comunes a los archivos permanentes para ambas entidades.

- **Normatividad vigente para el periodo auditado (2008).** La normatividad vigente para el periodo auditado es:

  - Constitución Política de Colombia 1991Artículos 2, 29, 90, 209, 267, 270, 273, 355.

  - Ley 80 de 1993 por la cual se expide el Estatuto General de Contratación de la Administración Pública.

  - Ley 87 de 1993 por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

  - Ley 42 de 1993 sobre la organización del sistema de control fiscal financiero y los organismos que lo ejercen.

  - Ley 190 de 1995 por la cual se dictan normas tendientes a preservar la moralidad en la Administración Pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa.

  - Ley 489 de 1998 por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.

- Ley 598 de 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.

- Ley 599 de 2000 por el cual se expide el Código Penal.

- Ley 610 de 2000 por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.

- Ley 617 de 2000 Por la cual se reforma parcialmente la Ley 136 de 1994, el Decreto Extraordinario 1222 de 1986, se adiciona la ley orgánica de presupuesto, el Decreto 1421 de 1993, se dictan otras normas tendientes a fortalecer la descentralización, y se dictan norma para la racionalización del gasto público nacional.

- Ley 678 de 2001 Por medio de la cual se reglamenta la determinación de responsabilidad patrimonial de los agentes del Estado a través del ejercicio de la acción de repetición o de llamamiento en garantía con fines de repetición.

- Ley 734 de 2002 por la cual se expide el Código Disciplinario Único.

- Ley 789 de 2002 por la cual se dictan normas para apoyar el empleo y ampliar la protección social y se modifican algunos artículos del Código Sustantivo de Trabajo.

- Ley 819 de 2003 por la cual se dictan normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal y se dictan otras disposiciones".

- Ley 828 de 2003 por la cual se expiden normas para el Control a la Evasión del Sistema de Seguridad Social.

- Ley 1150 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.

- Decreto 777 de 1992 por el cual se reglamentan la celebración de los contratos a que refiere el inciso segundo del artículo 355 de la Constitución Política.

- Decreto 1403 de 1992 por el cual se modifica el Decreto 0777 de 1992.
- Decreto 1477 de 1995 por el cual se reglamenta la Ley 190 del 6 de junio de 1995 en materia de publicación de contratos en el Diario Único de Contratación Pública.

- Decreto 287 de 1996 (Artículos 3 y 4) por el cual se reglamentan los artículos 24, 25, 29 y 30 de la Ley 80 de 1993.

- Decreto 327 de 2002 por medio del cual se deroga el Decreto 2504 de 2001 y se reglamenta el parágrafo 3° del artículo 41 de la Ley 80 de 1993.

- Decreto 610 de 2002 por medio del cual se reglamenta la Ley 358 de 1997.

- Decreto 2170 de 2002 (Artículos 6, 9 y 24) por el cual se reglamenta la ley 80 de 1993, se modifica el decreto 855 de 1994 y se dictan otras disposiciones en aplicación de la Ley 527 de 1999.

- Decreto 2800 de 2003 “Por el cual se reglamenta parcialmente el literal b) del artículo 13 del Decreto-ley 1295 de 1994”.

- Decreto 3512 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.

- Decreto 1145 de 2004 “Por el cual se dictan disposiciones relacionadas con el desarrollo del Sistema General de Información Administrativa del Sector Público, SUIP.

- Decreto 4660 de 2007 por medio del cual se reglamenta el artículo 58 de la Ley 863 de 2003.

- Decreto 2474 de 2008 por el cual se reglamenta parcialmente la ley 80 de 1993 y la ley 1150 de 2007 sobre las modalidades de selección, publicidad, selección objetiva, y se dictan otras disposiciones.

- Decreto 4828 de 2008 por el cual se expide el régimen de garantías en la contratación de la Administración Pública.

- Decreto 4444 de 2008 por el cual se reglamenta parcialmente el literal e) del numeral 2° del artículo 2° de la Ley 1150 de 2007. Regula la enajenación de bienes del Estado.

- Decreto 4881 de 2008 por el cual se reglamenta parcialmente la Ley 1150 de 2007 en relación con la verificación de las condiciones de los proponentes y su acreditación para el Registro Único de Proponentes a cargo de las Cámaras de Comercio y se dictan otras disposiciones.

- **Algoritmos para la contratación estatal.** En la tarea de investigación y consulta de la norma el grupo auditor encontró que podría ser difícil el trabajo de diagnóstico y análisis de las pruebas si no se cuenta con los papeles de trabajo que soporten adecuadamente la auditoria y un claro entendimiento de la norma. Es por esto que el grupo auditor decidió agregar a los papeles de trabajo del archivo permanente de las entidades los algoritmos de contratación estatal para los mecanismos de selección más comunes para la mayor cuantía y la menor cuantía dispuestos por la ley 80 de 1993 y sus modificaciones hasta el periodo auditado, construyendo así un punto de partida para entender mejor la norma para nosotros como ingenieros (figura 11 y figura 12).

Figura 11: Licitación pública

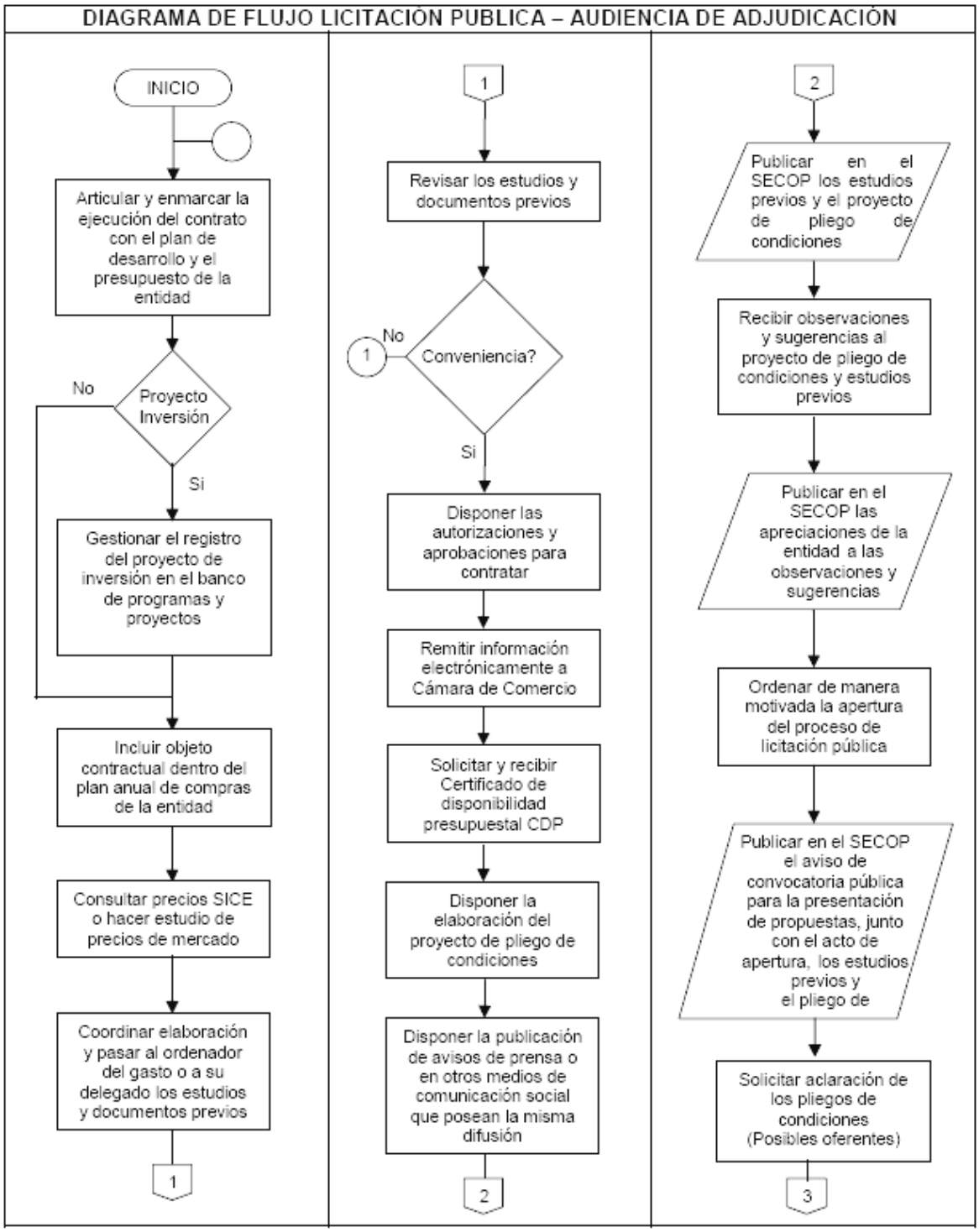


Figura 11: Licitación pública (continuación)

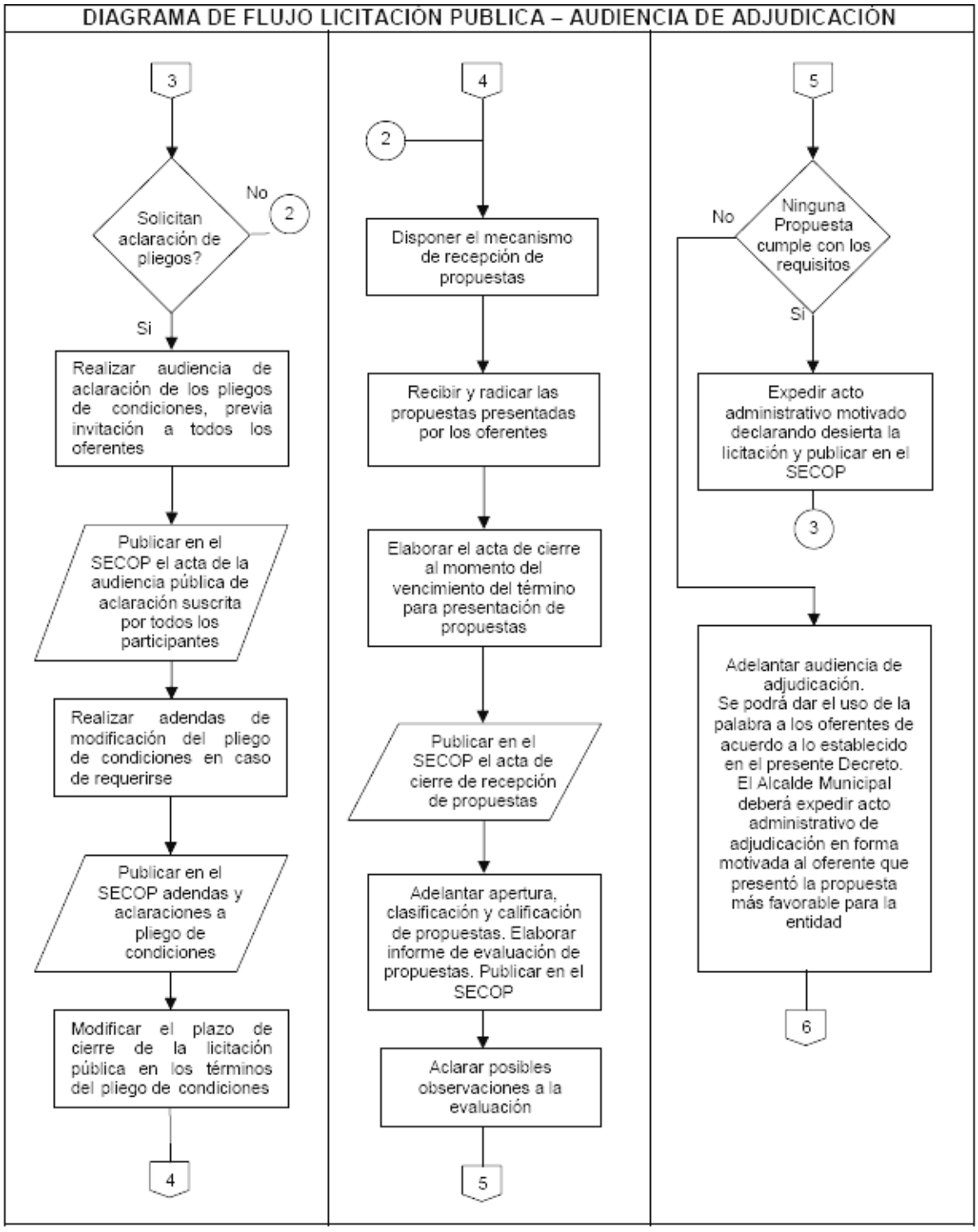


Figura 11: Licitación pública (continuación)

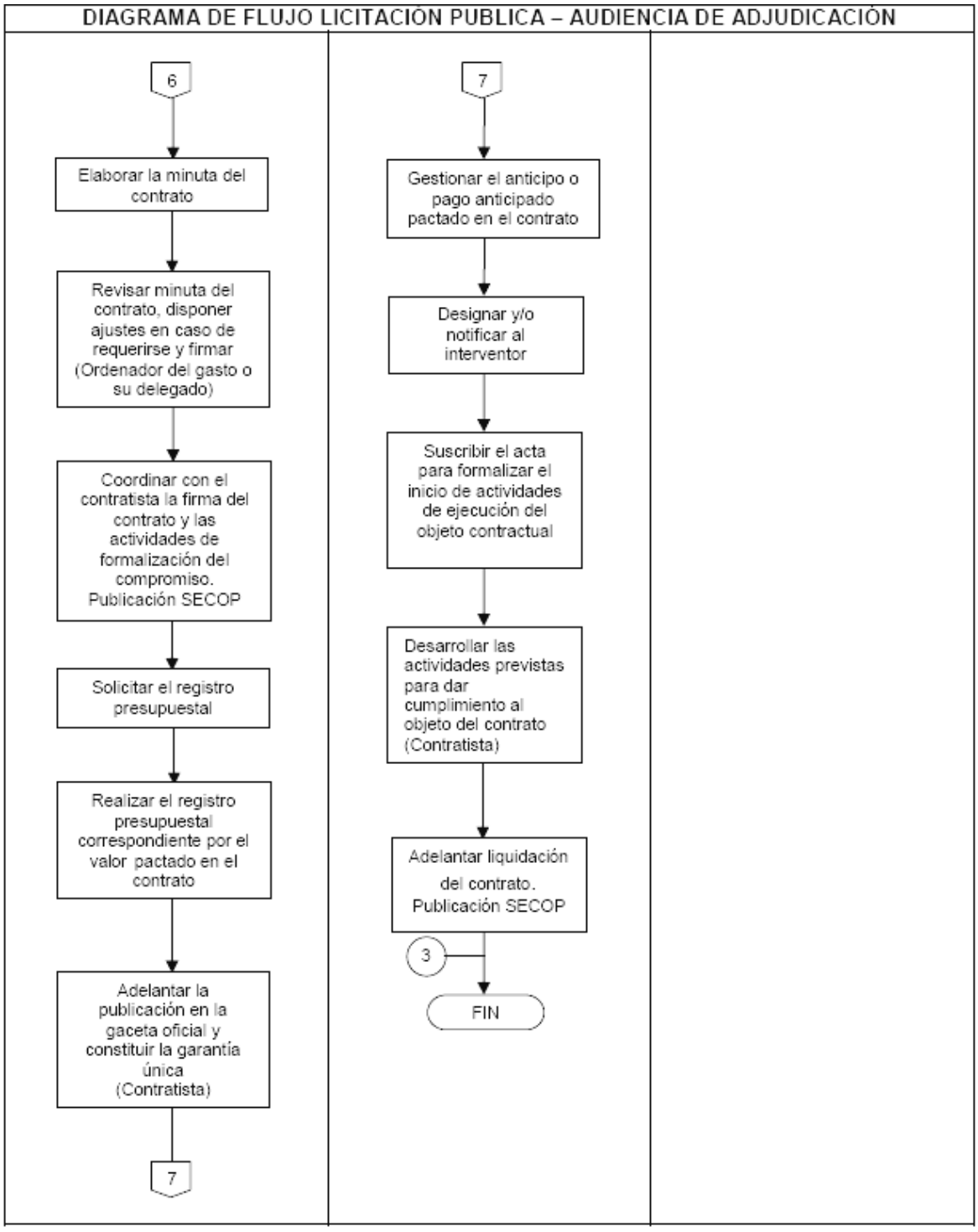


Figura 12: Menor cuantía

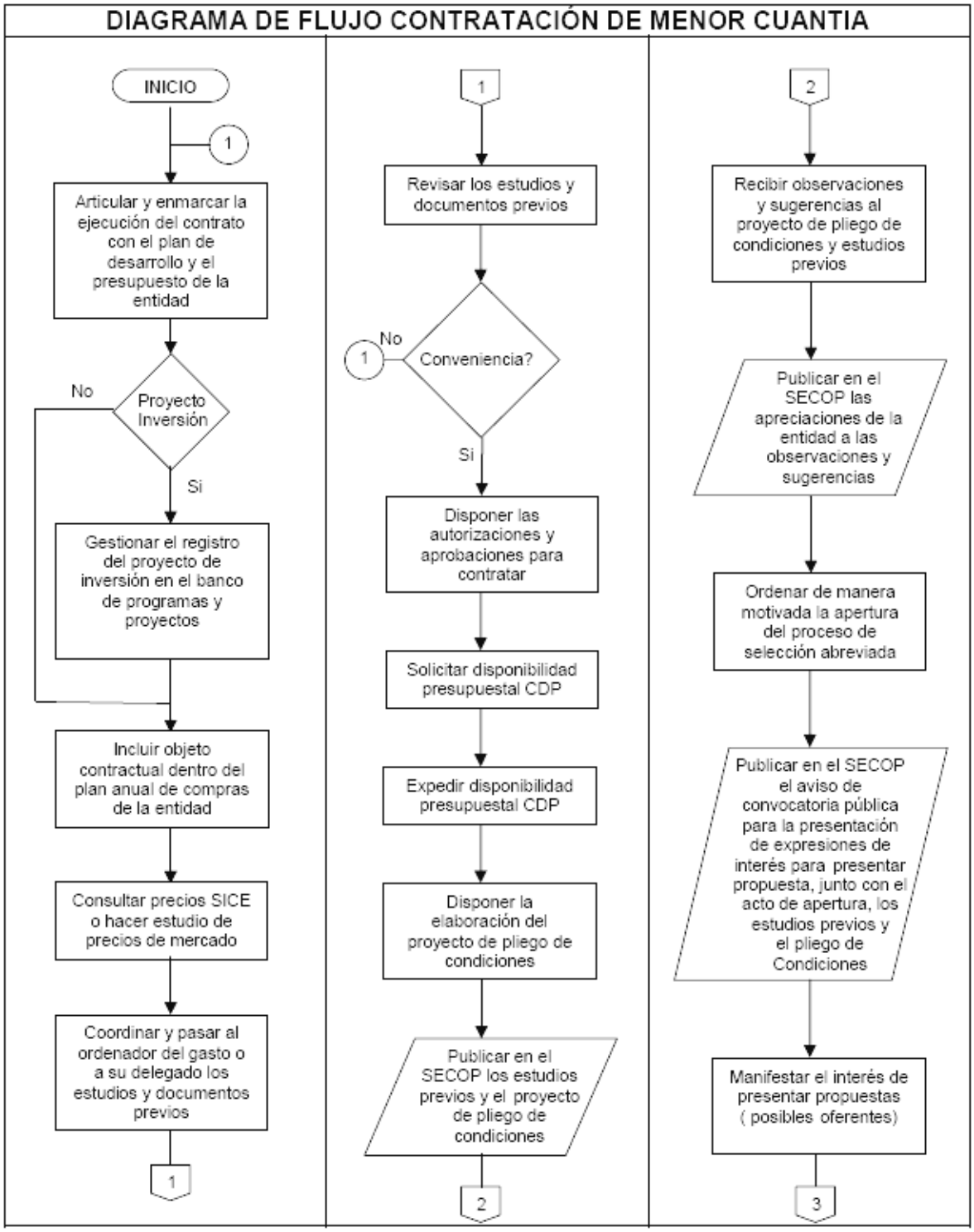


Figura 12: Menor cuantía (continuación)

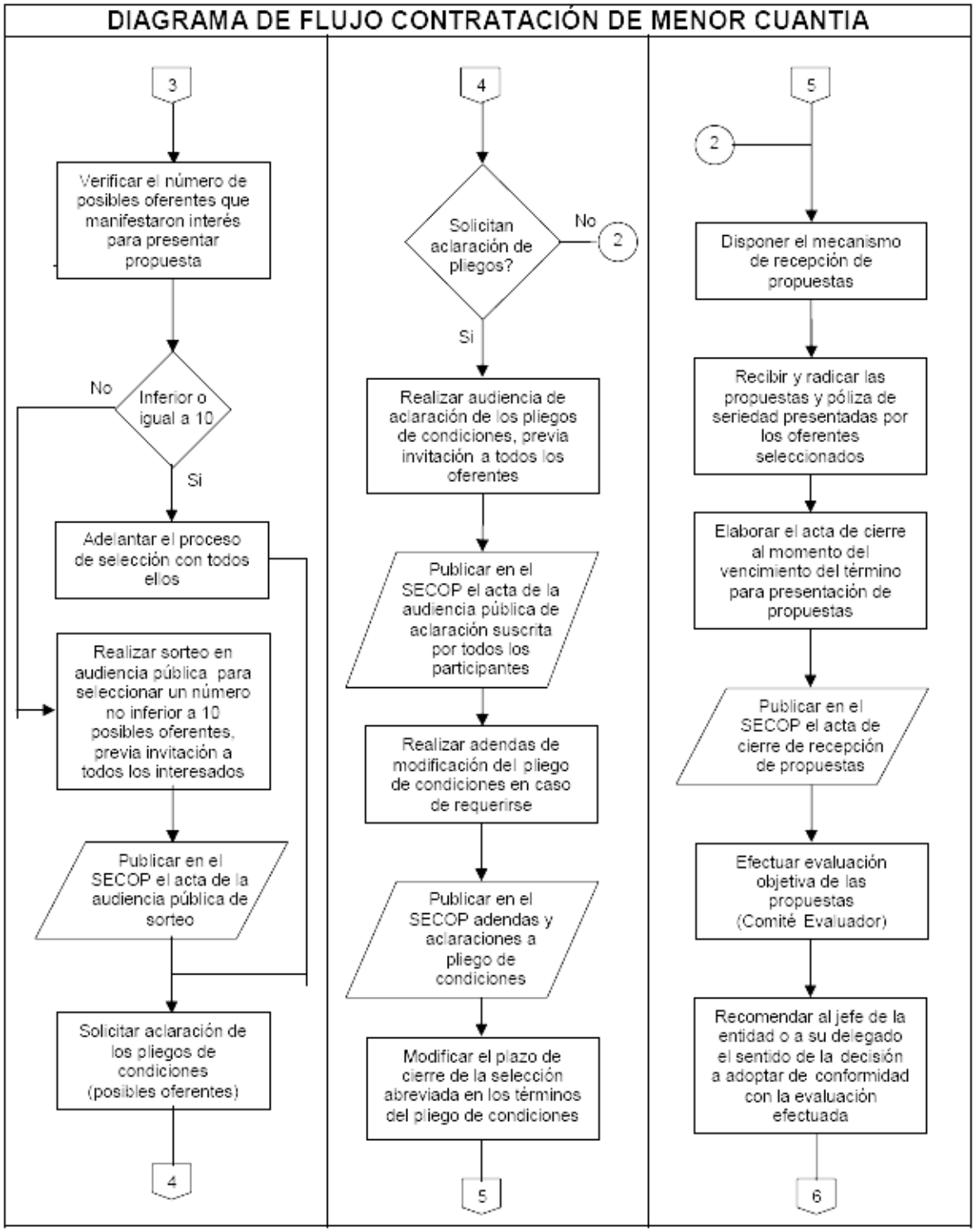
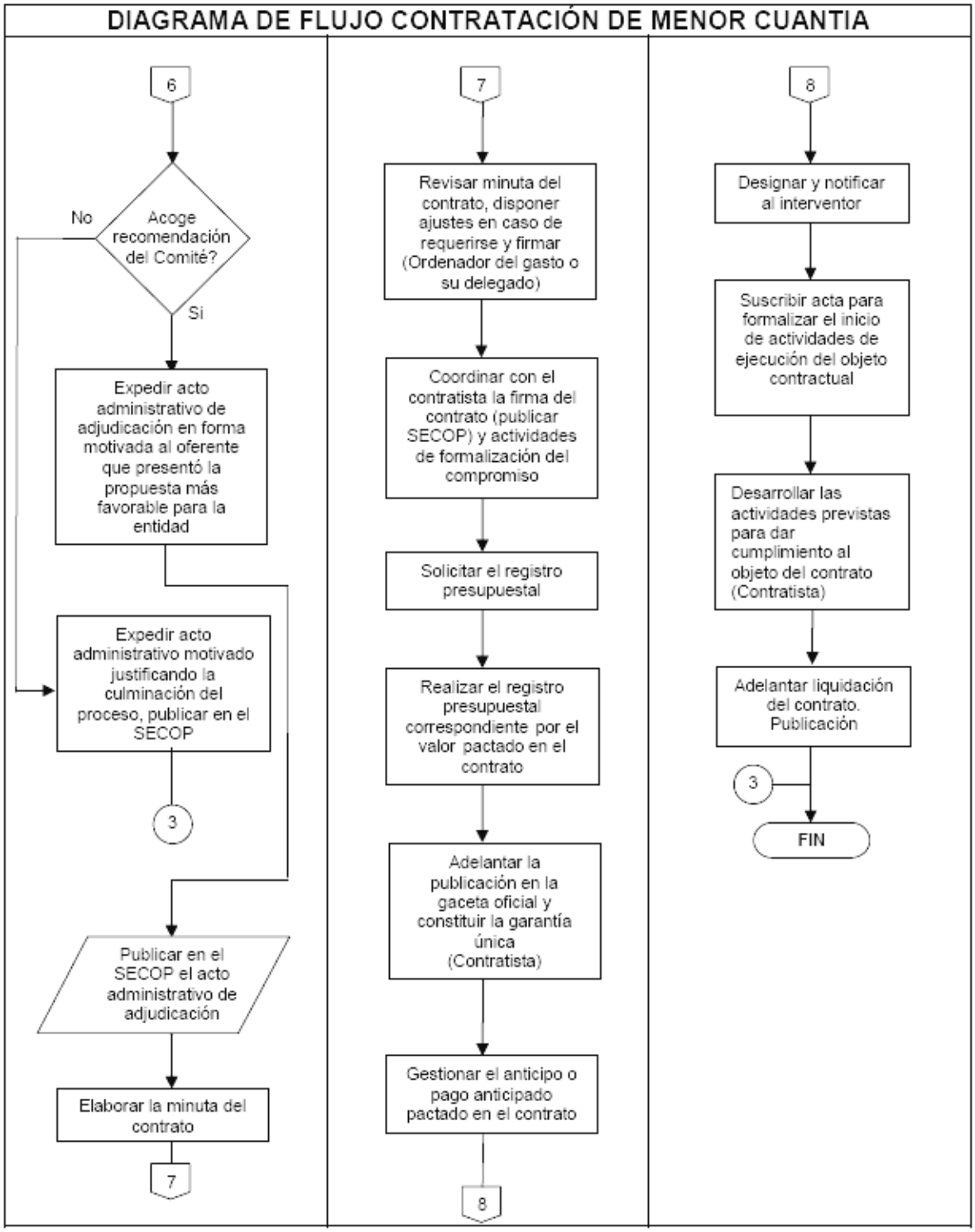


Figura 12: Menor cuantía (continuación)



3.1.2 Archivo permanente de la Alcaldía Municipal de Tangua. El archivo permanente de la Alcaldía Municipal de Tangua lo componen los siguientes elementos:

- **Ambiente general de la empresa:**

Figura 13: Simbolos de Tangua

http://tangua-narino.gov.co/

- **Nombre de la Institución:**

  ALCALDIA MUNICIPAL DE TANGUA.
  NIT: 800099151-1

- **Reseña Histórica:**

  En el año 2008 el Municipio de Tangua cumplió 168 años de su fundación oficial y 131 de su elección como Municipio, territorio que fue desmembrado del antiquísimo Municipio de Yacuanquer y su fundación se hizo mediante la Ordenanza 103 de la Asamblea del Cauca.

- **Descripción del gobierno municipal del periodo 2008:**

  ✓ JESUS ALBERTO ANDRADE MEJIA
  Alcalde Municipal
  Fecha de posesión: Enero 01 de 2008

- ✓ ANDREA ADIELA IBARRA PUCHANA
  Secretaria de Gobierno Municipal
  Fecha de posesión: Enero 01 de 2008

- ✓ JAIME HUMBERTO URBINA DE LA CRUZ
  Asesor Control Interno
  Fecha de posesión: Enero 03 de 2008

- **Entorno organizacional alcaldía de Tangua:**

  TRABAJEMOS EN MINGA PARA VOLVER A RECIPROCAR", ALCALDÍA DE TANGUA, PERIODO 2008 – 2011.

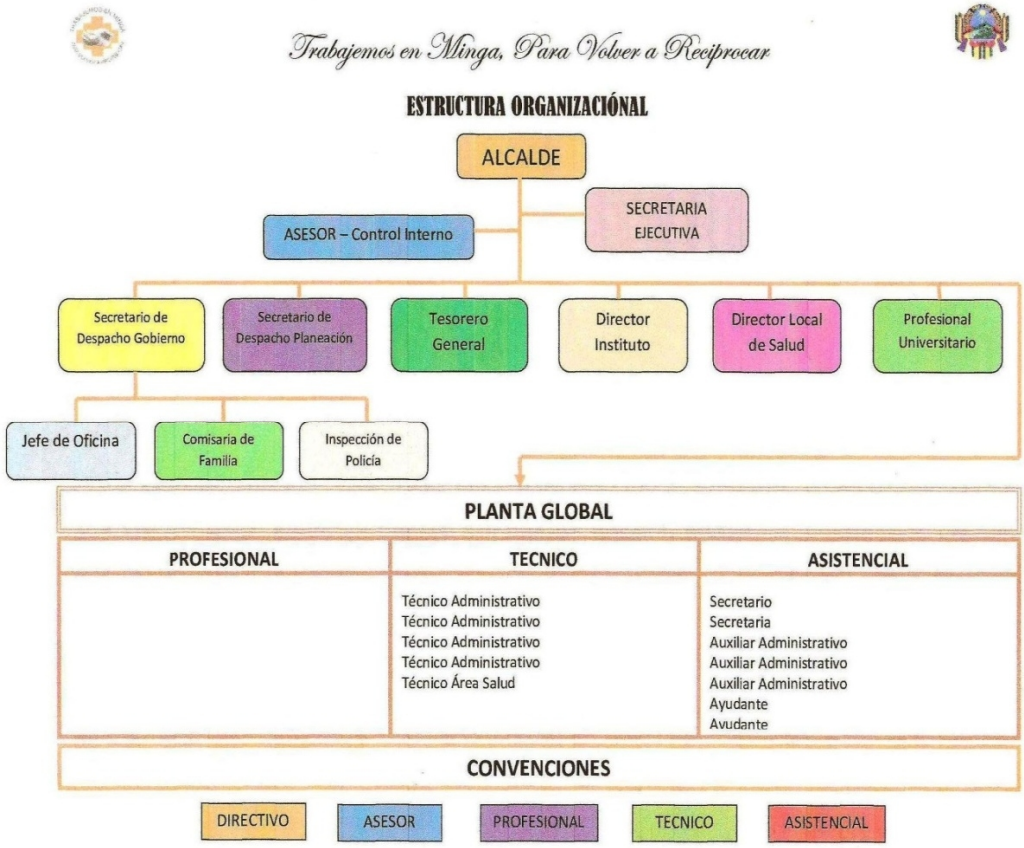
  - **Misión:** Tangua es una Municipio que se posicionará en los consensos participativos y democráticos que permitan el desarrollo cultural, religioso, político, económico, educativo, agrícola y social para el mejoramiento de la calidad de vida de los niños, mujeres, jóvenes y adultos Tangueños. E igualmente a través de la actual administración se pretende ubicarlo entre los primeros puesto a nivel Departamental y Nacional.

  - **Visión:** Tangua es un municipio participativo, sostenible, con identidad cultural y sentido de pertenencia, con desarrollo agropecuario, educativo, turístico, cultural deportivo y humano que protege el medio ambiente, logrando mejorar el bienestar de sus habitantes con una administración ágil, efectiva, eficiente, participativa y transparente. En Tangua, la participación ciudadana se constituye en la mejor alternativa para enfrentar los problemas planteados por el desarrollo territorial. Con la aplicación de los mecanismos de participación se alcanza un alto grado de compromiso de los habitantes de Tangua en la búsqueda de alternativas de solución a sus problemas internos, de mejores procesos de gestión e integración de la economía local al plano regional, departamental y nacional con un amplio margen de posibilidades de competitividad y ventajas comparativas. El Desarrollo Humano Sostenible del Municipio de Tangua conduce al crecimiento económico, a la elevación de la calidad de vida y al bienestar social, sin agotar los recursos naturales renovables en que se sustenta, ni deteriorar el medio ambiente o ahogar el derecho a las generaciones futuras. Las inversiones están encaminadas al desarrollo del talento humano, para que los habitantes del municipio alcancen un bienestar mediante el disfrute de su derecho a la salud, alimentación, nutrición, acceso a los servicios públicos, educación, cultura, recreación, y un ambiente sano, estos componentes se deben integrar para propiciar una vida más larga y saludable.

- **Objetivo general:** El Programa de Gobierno denominado Trabajemos en Minga para volver a reciprocar busca un proceso de reciprocidad con amplia participación ciudadana, donde se identifique la problemática actual, con el fin de proyectar soluciones reales y concretas al sentir de esta población, aplicando de antemano los principios fundamentales de la administración pública, con un enfoque pluralista; demostrando así la vocación deservicio, compromiso y sentido de pertenencia por nuestro municipio.

- **Organigrama**

Figura 14: Organigrama de la Alcaldía Municipal de Tangua



http://tangua-narino.gov.co/

3.1.3 Archivo permanente de la Alcaldía Municipal de Yacuanquer. El archivo permanente de la Alcaldía Municipal de Yacuanquer lo componen los siguientes elementos:

- **Ambiente general de la empresa:**

Figura 15: Organigrama de la Alcaldía Municipal de Yacuanquer

http://yacuanquer-narino.gov.co/index.shtml

- **Nombre de la institución:**

  ALCALDIA MUNICIPAL DE YACUANQUER
  NIT 800099153-6

- **Reseña Histórica:**

  En el año 2008 el Municipio de Yacuanquer cumplió 469 años de su fundación oficial, fue fundado por Lorenzo de Aldana el 10 de octubre de 1539. Posteriormente perdió la custodia sobre el municipio de Tangua mediante la Ordenanza 103 de la Asamblea del Cauca.

- **Descripción del gobierno municipal del periodo de 2008:**

  ✓ JAIME ALBERTO GUANCHA ARGOTY
  Alcalde Municipal
  Fecha de posesión: Enero 01 de 2008

  ✓ DAYANA GUERRERO JOSA
  Secretaria General

Fecha de posesión: Enero 01 de 2008

- ✓ DAYANA GUERRERO JOSA
  Control Interno
  Fecha de posesión: Enero 01 de 2008

- **Entorno Organizacional de la alcaldía de Yacuanquer:**

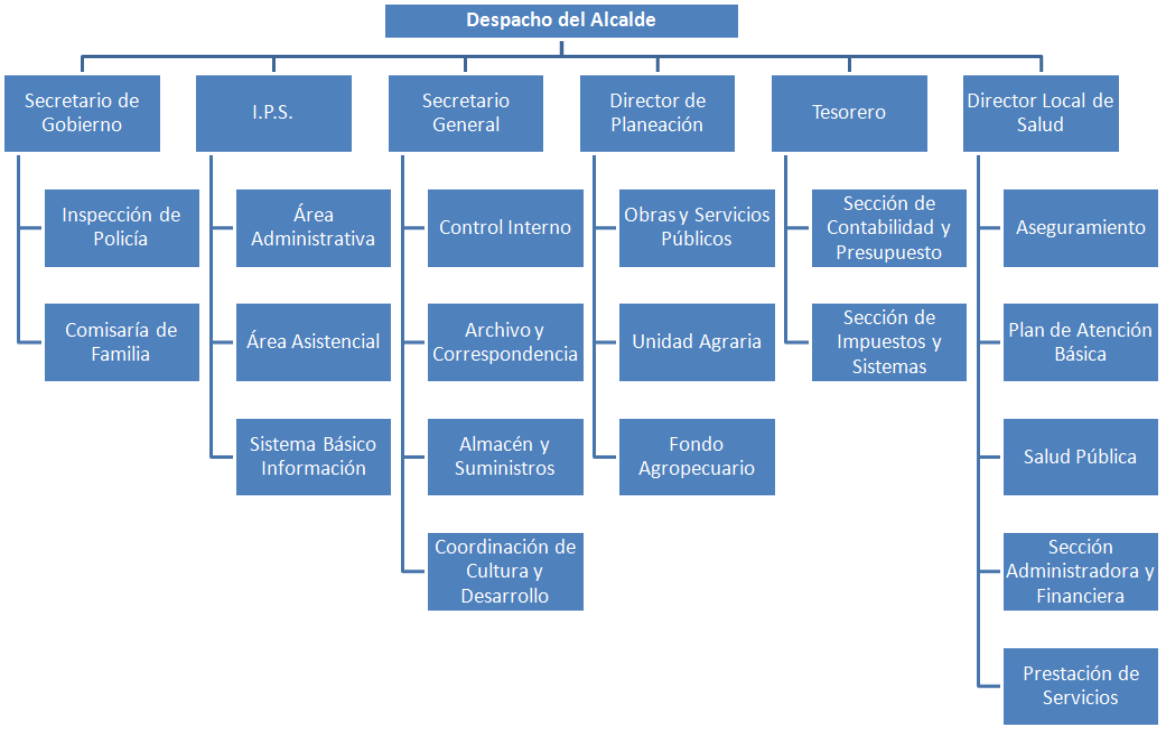
  UN YACUANQUE MAS HUMANO Y JUSTO, ALCALDIA DE YACUANQUER, PERIODO 2008 – 2011

  - **Misión:** El Municipio de Yacuanquer en cumplimiento de sus competencias normativas, propenderá por el desarrollo sostenible para brindar bienestar a su comunidad, especialmente, administrando el conjunto de asuntos municipales, planificando y ordenando los procesos locales de desarrollo en todas sus dimensiones, a través de procesos de participación ciudadana y articulación regional y subregional, ofreciendo soluciones coherentes y pertinentes a los derechos en salud, educación, saneamiento ambiental, agua potable, servicios públicos domiciliarios, vivienda, recreación, cultura, deporte, que permitan generar el progreso integral a sus habitantes, para ello serán principios rectores los de justicia, eficacia, eficiencia, transparencia, responsabilidad, imparcialidad y moralidad.

  - **Visión:** Yacuanquer es un municipio generador de su propio desarrollo económico, político, social, cultural y ambiental, contribuyendo con el bienestar y la justicia para todos sus habitantes, en donde se vive en armonía con el entorno en convivencia pacífica, vivienda digna, agua potable, salud, educación, seguridad ciudadana, desarrollo cultural y económico en comunidad con nuestras regiones hermanas; procurando la sostenibilidad de la población.

- **Organigrama:**

Figura 16: Organigrama de la Alcaldía Municipal de Yacuanquer



3.2 ARCHIVO CORRIENTE

Este archivo está conformado por una diversidad de documento, que tienen el fin de contener una documentación detallada de cada trabajo de auditoría, con el fin de que estos sean los soportes de los informes que emite el auditor y sirve de punto de partida para la siguiente auditoria.

Para la realización del proceso de auditoría en seguridad informática realizado a las alcaldías de Tangua y Yacuanquer, bajo la metodología COBIT (Objetivo de Control para la Información y Tecnologías Relacionadas), se evaluaran algunos objetivos de control que se encuentran dentro del dominio DS5 para *Garantizar la seguridad de los sistemas* y sus respectivas relaciones con otros dominios del COBIT.

3.2.1 Programa de auditoría. La determinación de los procesos COBIT involucrados dentro de la gestión de la seguridad de TI fue realizada siguiendo la organización de la nueva versión de COBIT, que a diferencia de las anteriores, en las cuales los objetivos de control que tenían que ver con un área determinada se encontraban dispersos en varios dominios y procesos. Estos objetivos de control fueron enfocados en sus respectivos procesos y dominios, al final del COBIT en el anexo V se encuentra las tablas de referencias cruzadas de las versiones anteriores y la actual.

Basándonos en esto, organizamos una matriz de riesgos potenciales y pruebas a aplicar para determinar el cumplimiento o no del objetivo de control. Esta matriz consta con el nombre del dominio, la descripción COBIT del proceso y del objetivo de control, los riesgos potenciales por el no cumplimiento de dicho objetivo y las pruebas que se realizarán.

- **Matriz de riesgos potenciales y pruebas a realizar.** A continuación se enumeran las diferentes matrices de riesgos potenciales y las pruebas a realizar de cada uno de los dominios, procesos y objetivos de control seleccionados en este plan de auditoría.

Tabla 3: Matriz de riesgos potenciales y pruebas a realizar 1

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.1 Administración de la seguridad de TI. Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.	La no existencia de un departamento o dependencia que administre el entorno TI. La no administración de riesgos a escala general de la entidad.	Solicitar y revisar el organigrama de la organización. Solicitar y revisar el manual de funciones Observación directa Entrevistar a funcionarios.

Tabla 4: Matriz de riesgos potenciales y pruebas a realizar 2

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.2 Plan de seguridad de TI. Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.	La no definición de un plan de seguridad especifico de TI. La no definición de políticas y procedimientos de seguridad.	Solicitar y revisar documento de políticas de seguridad. Entrevistar a funcionarios.

Tabla 5: Matriz de riesgos potenciales y pruebas a realizar 3

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.3 Administración de Identidad. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.	La falta o deficiencia de los mecanismos de seguridad para el control de acceso a los recursos de TI. La falta de evaluación y corrección de los mecanismos de control. La falta de registro adecuado de las actividades realizadas por los usuarios. La falta de certificación de correos de la entidad.	Solicitar y revisar el manual de procedimientos. Entrevistar a funcionarios. Observación directa.

Tabla 6: Matriz de riesgos potenciales y pruebas a realizar 4

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.4 Administración de Cuentas del Usuario. Garantizar que la Solicitar y revisar, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.	La falta de perfiles de usuario cuyos privilegios se alineen con las funciones de cada usuario. Las posibles contraseñas no seguras. La falta de control en la creación, modificación, o eliminación de las cuentas de usuario existentes. La falta de administración eficiente de perfiles y cuentas de SICE y SECOP	Solicitar y revisar las políticas de seguridad. Entrevistar a funcionarios. Observación directa.

Tabla 7: Matriz de riesgos potenciales y pruebas a realizar 5

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad. Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.	La no identificación del responsable directo o indirecto de un incidente de seguridad. La no determinación del origen, fecha y hora del incidente de seguridad. La deficiencia o inexistencia de un proceso de monitoreo periódico de las condiciones asociadas a la seguridad de TI. La falta de atención ante las alarmas de SICE y SECOP	Solicitar y revisar el histórico de vigilancia y monitoreo. Entrevistar funcionarios. Observación directa.

Tabla 8: Matriz de riesgos potenciales y pruebas a realizar 6

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.6 Definición de Incidente de Seguridad. Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.	La no notificación oportuna de los incidentes de seguridad. La pérdida o daño de información crítica. La falla o pérdida de servicios de red. La no definición de planes de contingencia.	Solicitar y revisar el manual de procedimientos. Solicitar y revisar las políticas de seguridad. Entrevistar a funcionarios. Observación directa.

Tabla 9: Matriz de riesgos potenciales y pruebas a realizar 7

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.7 Protección de la Tecnología de Seguridad Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.	La posibilidad de afectar la confiabilidad, autenticidad e integridad de los datos. La fuga de información. El acceso no autorizado a la información.	Solicitar y revisar las políticas de seguridad. Entrevistar a funcionarios. Observación directa.

Tabla 10: Matriz de riesgos potenciales y pruebas a realizar 8

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.9 Prevención, Detección y Corrección de Software Malicioso. Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).	El daño o pérdida de información. La no prevención y detección de virus tales como caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas. La no definición de políticas de actualización de software.	Solicitar y revisar de políticas de seguridad. Entrevistar funcionarios. Observación directa.

Tabla 11: Matriz de riesgos potenciales y pruebas a realizar 9

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.10 Seguridad de la Red. Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.	La no utilización de Firewalls para las conexiones con Internet u otras redes públicas en la organización. Los ataques a los recursos de la red. Los accesos no autorizados. La fuga de información.	Solicitar y revisar el mapa de red. Solicitar y revisar las políticas de seguridad de la red. Entrevistar a funcionarios. Observación directa.

Tabla 12: Matriz de riesgos potenciales y pruebas a realizar 10

DOMINIO ENTREGAR Y DAR SOPORTE		
DS5 Garantizar la seguridad de los sistemas		
El fin de este proceso es administrar la seguridad de los sistemas, para garantizar la integridad de la información y proteger los activos de TI, enfocándose en el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI, y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS5.11 Intercambio de Datos Sensitivos Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.	La intercepción o alteración de información sensible. La fuga de información por canales no seguros. La pérdida o daño de información sensible para la institución. La deficiencia o inexistencia de rutas seguras.	Solicitar y revisar las políticas de seguridad. Entrevistar funcionarios. Observación directa.

- **Entradas del proceso DS5: garantizar la seguridad de los sistemas**

Tabla 13: Matriz de riesgos potenciales y pruebas a realizar 11

PLANEAR Y ORGANIZAR		
P09. Evaluar y Administrar los Riesgos de TI.		
Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
PO9.4 Evaluación de Riesgos de TI Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.	La inadecuada evaluación de riesgos de la seguridad informática no permitirá medir el impacto de un ataque a la seguridad. La no definición de planes de contingencia para su inmediata recuperación. La no identificación de manera clara las áreas vulnerables y áreas críticas en cuando a seguridad informática tanto física como lógica. La no determinación de los costos ocasionados por los problemas de seguridad informática. La pérdida o alteración de la información.	Entrevistar funcionarios. Observación directa.

Tabla 14: Matriz de riesgos potenciales y pruebas a realizar 12

DOMINIO ENTREGAR Y DAR SOPORTE		
DS1 Definir y Administrar los Niveles de Servicio		
Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes.	La inexistencia de un departamento o dependencia que administre el entorno de TI. La no definición de funciones relacionadas con entorno de TI. La inexistencia de un marco de trabajo para los servicios de TI.	Solicitar y revisar el organigrama de la entidad Solicitar y revisar el manual de funciones Solicitar y revisar las políticas de seguridad. Entrevistar funcionarios. Observación directa.

Tabla 15: Matriz de riesgos potenciales y pruebas a realizar 13

DOMINIO ENTREGAR Y DAR SOPORTE		
DS1 Definir y Administrar los Niveles de Servicio		
Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS1.2 Definición de Servicios Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.	La no definición clara de servicios. La inexistencia de un catalogo de servicios.	Solicitar y revisar el manual de funciones Solicitar y revisar las políticas de seguridad. Entrevistar funcionarios. Observación directa.

Tabla 16: Matriz de riesgos potenciales y pruebas a realizar 14

DOMINIO ENTREGAR Y DAR SOPORTE		
DS1 Definir y Administrar los Niveles de Servicio		
Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS1.4 Acuerdos de Niveles de Operación Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima. Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.	La no definición de contratos entre los diferentes procesos y la gerencia TI. La no definición clara de las relaciones entre los diferentes procesos. La no disponibilidad del manual de contratación	Solicitar y revisar el manual de funciones Solicitar y revisar el manual de contratación Solicitar y revisar las políticas de seguridad. Entrevistar funcionarios. Observación directa.

- **Salidas del proceso DS5: garantizar la seguridad de los sistemas**

Tabla 17: Matriz de riesgos potenciales y pruebas a realizar 15

DOMINIO ENTREGAR Y DAR SOPORTE		
DS8 Administrar la Mesa de Servicio y los Incidentes.		
Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raiz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS8.1 Mesa de Servicios Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y Solicitar y revisares de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, Solicitar y revisar de servicio o Solicitar y revisar de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI	La no administración adecuada de incidentes y riesgos. El monitoreo inadecuado de incidentes. El escalamiento deficiente o inexistente de los incidentes que no se pueden resolver de forma inmediata La no notificación oportuna de los incidentes de seguridad. La pérdida o daño de información crítica. La falla o pérdida de servicios de red. La no definición de planes de contingencia.	Solicitar y revisar el manual de procedimientos Solicitar y revisar las políticas de seguridad. Entrevistar funcionarios. Observación directa.

Tabla 18: Matriz de riesgos potenciales y pruebas a realizar 16

DOMINIO ENTREGAR Y DAR SOPORTE		
DS7 Educar y Entrenar a los Usuarios.		
Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS7.1 Identificación de Necesidades de Entrenamiento y Educación Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya: • Estrategias y requerimientos actuales y futuros del negocio. • Valores corporativos (valores éticos, cultura de control y seguridad, etc.) • Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones) • Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias. • Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.	La no identificación de las necesidades de entrenamiento de los usuarios. La falta de un programa de entrenamiento para mejorar las condiciones de seguridad informática.	Entrevistar funcionarios. Observación directa.

Tabla 19: Matriz de riesgos potenciales y pruebas a realizar 17

DOMINIO ENTREGAR Y DAR SOPORTE		
DS7 Educar y Entrenar a los Usuarios.		
Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
DS7.2 Impartición de Entrenamiento y Educación Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.	El desconocimiento de riesgos de seguridad de TI por parte del personal. El desconocimiento de medidas y procedimientos adecuadas para garantizar la seguridad de TI El desconocimiento y la no aplicación de las políticas de seguridad por parte del personal.	Entrevistar funcionarios. Observación directa.

Tabla 20: Matriz de riesgos potenciales y pruebas a realizar 18

PLANEAR Y ORGANIZAR		
P09. Evaluar y Administrar los Riesgos de TI.		
Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
PO9.3 Identificación de Eventos Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.	La no identificación y registro de las amenazas y las vulnerabilidades. La no identificación de las causas y las consecuencias de las amenazas y vulnerabilidades.	Entrevistar funcionarios. Observación directa.

Tabla 21: Matriz de riesgos potenciales y pruebas a realizar 19

ADQUIRIR E IMPLEMENTAR		
AI6 Administrar Cambios		
Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.		
Objetivos de control	**Factor de riesgo**	**Descripción de la prueba**
AI6.1 Estándares y Procedimientos para Cambios Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las Solicitar y revisares (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.	La deficiente o inexistente administración de cambios de seguridad requeridos. El no seguimiento adecuado al uso de los recursos TI por parte del personal. La posible deficiencia en la identificación de responsables.	Solicitar y revisar el manual de procedimientos. Solicitar y revisar las políticas de seguridad. Entrevistar funcionarios. Observación directa.

3.2.2 Diseño de los elementos de auditoría. En el diseño de los elementos de auditoría se tuvieron en cuenta los siguientes ítems:

- **Observación Directa.** La observación directa se convierte en un poderoso aliado dentro de las auditorías, es por esto que la Contraloría Departamental de Nariño, la utiliza como herramienta de diagnostico y análisis. Sin embargo, esta debería en lo posible ir acompañada de material que constituya la evidencia de lo observado, tales como videos, fotografías, testigos, etc.

- **Entrevistas.** Las entrevistas en las entidades fueron documentadas en video y fueron realizadas por el funcionario de la Contraloría Departamental de Nariño con el apoyo del equipo auditor formado por los estudiantes Lennin Geovanny Ibarra Gonzalez y Diego Mauricio Meza García; durante la segunda visita se realizaron las entrevistas por parte del equipo auditor.

  Estas entrevistas se basaron en los Cuestionarios de verificación previamente diseñados usando COBIT y los procesos auditados del mismo.

- **Cuestionarios de Verificación.** Los Cuestionarios de verificación fueron desarrollados para servir como apoyo para las entrevistas. Su estructura es similar a la de una lista de verificación, en la cual se establece con una X si cumple o no con el ítem evaluado.

  La estructura de los Cuestionarios cuenta con los siguientes campos:

  - **REF:** Se refiere al ID o nombre del Cuestionario.

  - **ENTIDAD AUDITADA:** Se refiere al nombre de la entidad a la cual se está auditando.

  - **ÁREA AUDITADA:** Se refiere al área de TI que será objeto de estudio.

  - **PÁGINA:** Se refiere al número de página del Cuestionario.

  - **PROCESO AUDITADO:** Se refiere al nombre del proceso de la entidad que es objeto de la auditoria.

  - **RESPONSABLES:** Se refiere a los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

  - **MATERIAL DE SOPORTE:** Se refiere al material que sirvió de soporte para la realización del Cuestionario.

- **DOMINIO:** Se refiere al dominio COBIT que será auditado.
- **PROCESO:** Se refiere al proceso de COBIT que será auditado.
- **PREGUNTA:** Se refiere al listado de preguntas o ítems que serán evaluados.
- **SI / NO:** Se refiere a las posibilidades de respuesta, cumple, no cumple.
- **REF HALLAZGO:** Referencia al hallazgo que genera las diferentes preguntas, este campo contiene la identificación del hallazgo.

Figura 17: Cuestionario cualitativo

	CUESTIONARIO CUALITATIVO	REF

ENTIDAD AUDITADA				**PAGINA**	
				1	DE 1
ÁREA AUDITADA	Seguridad Física y Física y lógica	**PROCESO AUDITADO**	Contratación		
RESPONSABLES	LENNIN GEOVANNY IBARRA GONZALEZ				
	DIEGO MAURICIO MEZA GARCÍA				
MATERIAL DE SOPORTE	COBIT				
DOMINIO		**PROCESO**			

PREGUNTA	SI	NO	REF HALLAZGO

- **Hallazgos.** Los hallazgos encontrados en las entidades, serán dispuestos en similar orden al presentado en el programa de auditoría, presentando primero los objetivos de control del proceso Garantizar la seguridad de los sistemas (DS5) y posteriormente las entradas y salidas de este proceso.

  El formato de hallazgo consta de los siguientes campos:

  - **REF:** Se refiere al ID o nombre del hallazgo.

  - **PROCESO AUDITADO:** Se refiere al proceso de la entidad que fue objeto de estudio.

  - **PÀGINA:** Se refiere a la página del hallazgo.

  - **RESPONSABLE:** Se refiere a los nombres de los integrantes del grupo auditor.

  - **DESCRIPCIÓN:** Se refiere a la descripción del hallazgo encontrado, describiendo una situación perjudicial para la entidad.

  - **CONSECUENCIAS**: Se refiere a las consecuencias o el efecto que tiene el hallazgo en la entidad, además este campo será tomado como criterio para determinar el nivel de riesgo del hallazgo en la entidad.

  - **NIVEL DE RIESGO:** Se refiere a la criticidad que puede representar el hallazgo en la entidad. Hemos discriminado los hallazgos en tres niveles de criticidad:

    - ✓ **Bajo.** Este nivel no representa una amenaza grave a los recursos de TI, los objetivos y las metas de la entidad no están comprometidos, pero se pueden hacer mejoras respecto al objeto auditado. Su solución puede ser gradual y a largo plazo, dando paso a otros hallazgos de mayor prioridad.

    - ✓ **Medio.** Este nivel puede representar un riesgo a los recursos de TI, los objetivos no se ven comprometidos, pero la entidad podría fracasar en la consecución de las metas. Su solución debe ser planeada para un periodo aceptable de tiempo.

    - ✓ **Alto.** Este nivel representa un nivel crítico de riesgo. Compromete tanto la consecución de los objetivos como de las metas de la entidad. Su solución debe ser en el corto plazo y su prioridad es alta.

- **RECOMENDACIONES:** Se refiere a las acciones correctivas que puede realizar la entidad para evitar que el hallazgo persista en la entidad.

- Posterior a la exposición del hallazgo se encuentra el cuadro de **MATERIAL DE SOPORTE**, el cual brinda el fundamento del hallazgo, las evidencias y las pruebas que generaron dicho hallazgo, además este sirve también como soporte para sustentar las repuestas obtenidas en los Cuestionarios. Este cuadro contiene los siguientes campos:

  - ✓ **TIPO:** Se refiere al tipo de material de soporte del hallazgo, este puede ser un Cuestionario, un video, evidencia fotográfica, observación directa, etc.

  - ✓ **REF:** En este campo se dispone el nombre del elemento ó la descripción del mismo en caso de ser observación directa.

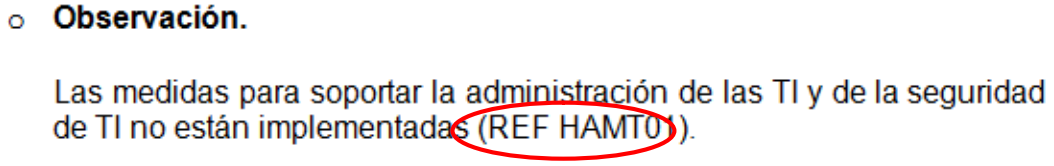
  - ✓ **UBICACIÓN:** hace referencia a la ubicación del elemento dentro de los anexos, así como puede estar dentro del archivo permanente o no aplicar en caso de ser observación directa.

- **Navegación por los hallazgos**

  Para un entendimiento de parte del lector de los hallazgos, el grupo auditor dispone a continuación los lineamientos para navegar por los hallazgos y las pruebas.

  Partiendo del informe general cada observación al final hace referencia a un hallazgo ej. REF HAMT01 (figura 18).

Figura 18: Referencia en el informe



Mediante esta referencia se puede llegar al cuadro de hallazgo en el presente documento: puntos 3.2.3 Alcaldía de Tangua ó 3.2.4 Alcaldía de Yacuanquer (figura 19).

Figura 19: Referencia en el hallazgo

4.2.3 Hallazgos Alcaldía Municipal de Tangua

Tabla 22: Hallazgo HAMT01

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	REF
		HAMT01

En el hallazgo, mediante el cuadro de MATERIAL DE SOPORTE, se puede llegar a las evidencias buscando el elemento cuyo nombre es dado por la columna REF dentro de la ubicación la cuál es brindada por la columna UBICACIÓN (figura 20).

Figura 20: Material de suporte

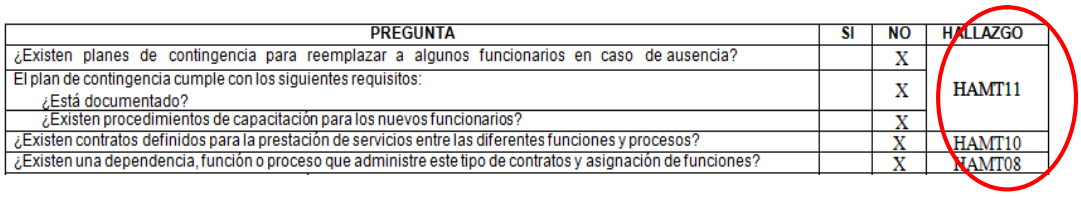
	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	REF
		HAMT01

PROCESO AUDITADO	CONTRATACIÓN	PÁGINA 2 DE 2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ	
	DIEGO MAURICIO MEZA GARCÍA	

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldía Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldía Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldía Municipal de Tangua\Evidencia
Evidencia Fotográfica	Verificación del manual de funciones	Anexos\Alcaldía Municipal de Tangua\Evidencia
Observación Directa	Verificación del organigrama	ARCHIVO PERMANENTE
Observación Directa	Verificación del sitio de trabajo	N/A

En caso de referirse a un Cuestionario cuantitativo, éste posee una columna que discrimina las preguntas según el hallazgo que se generó (figura 21).

Figura 21: Cuestionario



PREGUNTA	SI	NO	HALLAZGO
¿Existen planes de contingencia para reemplazar a algunos funcionarios en caso de ausencia?		X	
El plan de contingencia cumple con los siguientes requisitos: ¿Está documentado?		X	HAMT11
¿Existen procedimientos de capacitación para los nuevos funcionarios?		X	
¿Existen contratos definidos para la prestación de servicios entre las diferentes funciones y procesos?		X	HAMT10
¿Existen una dependencia, función o proceso que administre este tipo de contratos y asignación de funciones?		X	HAMT08

3.2.3 Hallazgos Alcaldía Municipal de Tangua. Los hallazgos de la Alcaldía Municipal de Tangua son los siguientes:

Tabla 22: Hallazgo HAMT01

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT01

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN Las medidas para soportar la administración de las TI y de la seguridad de TI no están implementadas

CONSECUENCIAS La entidad no cuenta con una adecuada administración de TI, así como tampoco de la seguridad de TI, pero aún así hace un uso intensivo y frecuente las TI. La falta de la adecuada administración TI y de su seguridad puede comprometer gravemente el cumplimiento de los objetivos y metas de la entidad.

NIVEL DE RIESGO Alto

RECOMENDACIONES La responsabilidades sobre la seguridad TI deben ser asignadas, administradas e implementadas de forma clara, para este fin se debe tomar conciencia dentro de la organización de la importancia de la administración de los recursos TI y por ende de su seguridad y para esto se deben generar una dependencia dentro de la organización, definir las funciones como mínimo de CIO y del personal de seguridad de TI dentro del manual de funciones y los procedimientos respectivos dentro del manual de procedimientos y de contratación.

Tabla 22: Hallazgo HAMT01 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT01

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldía Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldía Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldía Municipal de Tangua\Evidencia
Evidencia Fotográfica	Verificación del manual de funciones	Anexos\Alcaldía Municipal de Tangua\Evidencia
Observación Directa	Verificación del organigrama	ARCHIVO PERMANENTE
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 23: Hallazgo HAMT02

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT02

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existe un plan de seguridad TI, ni políticas de seguridad que lo sustenten

CONSECUENCIAS
La falta de planeación y definición de políticas y procedimientos pueden producir fallas y elevar los costos de las mismas, además de una falta de linealidad entre los procesos y los objetivos y metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Se deben realizar una planeación estratégica TI, en la cual se implementen estudios y análisis de seguridad, determinar los requerimientos de seguridad, identificar riesgos y establecer metas. Usando esta información crear un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.

Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

Tabla 23: Hallazgo HAMT02 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT02

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Tesorería	Anexos\Alcaldia Municipal de Tangua\Evidencia

Tabla 24: Hallazgo HAMT03

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT03

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No se define, establece y opera un proceso de administración de identidad para el acceso a los recursos TI

CONSECUENCIAS La falta de identificación de las actividades y de certificación de identidad de los usuarios (tal como la certificación de las cuentas de correo ante la contraloría) puede dificultar la verificación de responsables en caso de eventualidades, lo que atenta contra el principio de transparencia que debe manejar la entidad que se encuentra sometida a la Ley 80 de 1993.

NIVEL DE RIESGO Alto

RECOMENDACIONES Se deben definir estándares que permitan administrar la clara identificación y autorización lógica y física de todos los usuarios (internos, externos y temporales) de forma centralizada. Implementar procedimientos que permitan realizar seguimiento de las actividades de los usuarios y poder así identificar responsables. Administrar los permisos y privilegios de los usuarios para el acceso a recursos de TI por medio de cuentas de usuario, responsables de la información y niveles de acceso para casos normales, especiales y de emergencia. Estos derechos y obligaciones deben estar acordados contractualmente, así como documentados en los manuales de funciones, de procedimientos y las políticas de seguridad.

Tabla 24: Hallazgo HAMT03 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT03

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNiN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Tesorería	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 25: Hallazgo HAMT04

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT04

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNiN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existe un proceso para la administración centralizada de las cuentas y perfiles de usuario, tanto de los recursos de TI locales como de los sistemas SICE y SECOP. Los derechos y privilegios de acceso a los recursos locales por parte de los funcionarios de la entidad son inexistentes (todos pueden acceder con privilegios de administrador).

CONSECUENCIAS
La conciencia de la necesidad de seguridad y administración de cuentas y perfiles de usuario de los recursos TI locales y de las cuentas y perfiles de usuario en los sistemas SICE y SECOP en la entidad dependen principalmente del individuo, no existen procedimientos formales ni planes de contingencia que permitan una administración centralizada de esta información.

Respecto a la administración de las cuentas de SICE y SECOP el usuario de control interno, tanto como los demás, no pueden realizar una verificación de las diversas alarmas disparadas para cada tipo de usuario, por lo que afecta el cumplimiento de los objetivos de la entidad y viola el principio de transparencia establecido por el marco legal para las entidades públicas que se someten a la ley 80 de 1993.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Construir un proceso y sus respectivos procedimientos para una efectiva administración centralizada de cuentas, perfiles y permisos de acceso para los recursos de TI locales y también para los sistemas SICE y SECOP. Debe incluirse un procedimiento de aprobación que detalle la información del responsable de los recursos de TI locales y las cuentas existentes para otros funcionarios, así como también los responsables de las cuentas de los sistemas SICE y SECOP. Además deben documentarse las relaciones con otros procesos y acuerdos de operación para cada uno de los responsables.

Tabla 25: Hallazgo HAMT04 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT04

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNiN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 26: Hallazgo HAMT05

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT05

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNiN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No se monitoriza adecuadamente los incidentes de seguridad reales o potenciales

CONSECUENCIAS
La falta del adecuado seguimiento y monitoreo de incidentes puede elevar el costo de los mismos, la organización no estará preparada adecuadamente, ni podrá responder en un tiempo aceptable ante el incidente, lo cual puede retrasar el cronograma de la entidad y evitar el cumplimiento de sus metas aunque podría no afectar en gran medida al cumplimiento de los objetivos.

No se podrán identificar con claridad las causas de los incidentes, por lo que no se podrán mitigar los riesgos y disminuir la probabilidad de ocurrencia.

NIVEL DE RIESGO
Medio

RECOMENDACIONES
Se deben definir procedimientos de monitoreo y análisis de los incidentes de seguridad, tanto los reales como los potenciales, esto con el fin de garantizar un nivel de seguridad adecuado y aprobado de acuerdo con las metas preestablecidas en el plan de seguridad TI, además un correcto monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

Se deben establecer métricas para lograr medir el nivel de seguridad de forma correcta, tomar estadísticas y realizar proyecciones y correcciones.

Tabla 26: Hallazgo HAMT05 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT05

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNiN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
Evidencia fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Tangua\Material para la Contraloria
Observación Directa	Testimonio fuera de cámara	N/A
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 27: Hallazgo HAMT06

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT06

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNiN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI.

CONSECUENCIAS La falta de reportes de seguridad podría llevar a incidentes más profundos y graves que puedan comprometer la información. La falta de respuesta para resolver brechas de seguridad que pueden ser reportadas de manera informal denota una falta de atención hacia la seguridad de TI lo cual puede provocar que un incidente incremente su gravedad y nivel de riesgo comprometiendo la información de la entidad.

NIVEL DE RIESGO Medio

RECOMENDACIONES Se debe definir los incidentes de seguridad, realizar reportes detallados e informar a los interesados.

Tabla 27: Hallazgo HAMT06 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT06

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS5	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Tesorería	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 28: Hallazgo HAMT07

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT07

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
No se realiza evaluación de riesgos de seguridad de TI para el proceso de contratación; ni tampoco se toma en cuenta los impactos en la entidad asociados con las vulnerabilidades de seguridad.

CONSECUENCIAS
Si no se cuenta con una evaluación adecuada de riesgos, estos no podrán ser mitigados, ni medidos, la tasa de incidentes por riesgos no identificados podría aumentar comprometiendo la seguridad, la información, los objetivos y las metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
La entidad debe establecer el contexto de riesgo de seguridad de TI, realizar evaluaciones periódicas con el personal de seguridad de TI, establecer los planes de acción para mitigar los riesgos críticos de TI. Todo esto debe estar centralizado y los procedimientos deben estar documentados en el manual correspondiente, además las funciones que desempeñen estos procedimientos deben estar consignadas dentro del manual de funciones de la entidad.

Tabla 28: Hallazgo HAMT07 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT07

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS8	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
Evidencia fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Tangua\Material para la Contraloria
Observación Directa	Testimonio fuera de cámara	N/A
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 28: Hallazgo HAMT08

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT08

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No existe un marco de trabajo claro para los servicios de TI

CONSECUENCIAS No existe un marco de trabajo para una comunicación efectiva entre los interesados del negocio, en este caso el proceso de contratación y los que prestan el servicio de TI, y para una clara definición de los servicios prestados y sus respectivos niveles. La ausencia del marco de trabajo apropiado para los servicios de TI impide una alineación entre los servicios y los requerimientos reales de la entidad.

NIVEL DE RIESGO Medio

RECOMENDACIONES Se debe asegurar la satisfacción de los usuarios del proceso de contratación con ofertas de servicios y niveles de servicio. Desarrollar un marco de trabajo que permita administrar estos servicios de una manera efectiva y constante que facilite un entendimiento y flujo de información entre el proveedor del servicio y los usuarios finales.

Tabla 29: Hallazgo HAMT08 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT08

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS1	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del organigrama	ARCHIVO PERMANENTE
Observación Directa	Testimonio Fuera de Cámara	N/A

Tabla 29: Hallazgo HAMT09

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT09

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No existe un catálogo formal de servicios

CONSECUENCIAS La entrega de servicios por personal no capacitado puede poner a la entidad en riesgo de agravar una situación y tomar medidas innecesarias que produzcan retrasos en las metas de la entidad. Además de afectar el principio de transparencia por falta de una definición clara de responsables.

NIVEL DE RIESGO Medio

RECOMENDACIONES Se debe construir una base de servicios de TI detallado, incluyendo los servicios de seguridad de TI. Esta formalización de servicios deben ser comunicados y bien conocidos por los usuarios del proceso de contratación y deben estar almacenados y administrados de forma centralizada.

Tabla 30: Hallazgo HAMT09 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT09

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS1	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Testimonio Fuera de Cámara	N/A

Tabla 30: Hallazgo HAMT10

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT10

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN Los acuerdos de nivel de operación para los servicios de TI y seguridad TI no están definidos

CONSECUENCIAS La falta de procedimientos y estándares entendibles por el proveedor y el cliente del servicio TI que especifiquen cómo se hará entrega del mismo, puede generar brechas de seguridad, retrasos para las metas de la entidad y una baja calidad del servicio.

NIVEL DE RIESGO Medio

RECOMENDACIONES La entidad debe formalizar los convenios internos y externos alineados con los requerimientos y las capacidades de entrega del proveedor, estos deben estar documentados en los manuales de procedimientos y de funciones de TI. Se deben dar a conocer a las partes interesadas y vigilar su cumplimiento y medir su desempeño.

Tabla 31: Hallazgo HAMT10 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT10

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS1	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Testimonio Fuera de Cámara	N/A

Tabla 31: Hallazgo HAMT11

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT11

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existe un manual de contratación, ni manual de procedimientos para el proceso de contratación.

CONSECUENCIAS
La falta de los manuales de contratación y procedimientos donde se especifiquen los algoritmos a seguir para los diferentes casos dentro del proceso de contratación puede conllevar a la realización de pasos innecesarios retrasando las metas de la entidad. Además puede conllevar a violar la norma y poner en riesgo el principio de transparencia.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Construir un manual de contratación y de procedimientos que concentren los algoritmos entendibles para las partes interesadas de acuerdo a los objetivos de la entidad y del marco legal vigente.

Tabla 32: Hallazgo HAMT11 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT11

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS1	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Testimonio Fuera de Cámara	N/A

Tabla 32: Hallazgo HAMT12

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT12

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			
FECHA				

DESCRIPCIÓN
No existen procedimientos formales y documentados para el uso del sistema SICE dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma.

CONSECUENCIAS
La falta de estos procedimientos y su cumplimiento vulneran gravemente el principio de transparencia para las entidades que se rigen por la ley 80 de 1993, y violan las normas que relacionan al sistema SICE ya que esta es bien conocida y las entidades han recibido la adecuada capacitación para su uso. Además comprometen los objetivos y metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Definir claramente los procedimientos para el uso correcto y efectivo del sistema SICE, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

Tabla 33: Hallazgo HAMT12 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT12

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS1	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldia Municipal de Tangua\Evidencia
Incumplimiento de la norma	Informe de hallazgos Contraloría	Anexos\Alcaldia Municipal de Tangua\Material para la Contraloria
Observación Directa	Testimonio Fuera de Cámara	N/A

Tabla 33: Hallazgo HAMT13

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT13

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No existen procedimientos formales y documentados para el uso del sistema SECOP dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma

CONSECUENCIAS La falta de estos procedimientos y su cumplimiento vulneran gravemente el principio de transparencia para las entidades que se rigen por la ley 80 de 1993, y violan las normas que relacionan al sistema SECOP ya que esta es bien conocida y las entidades han recibido la adecuada capacitación para su uso. Además comprometen los objetivos y metas de la entidad.

NIVEL DE RIESGO Alto

RECOMENDACIONES Definir claramente los procedimientos para el uso correcto y efectivo del sistema SECOP, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

Tabla 34: Hallazgo HAMT13 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT13

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS1	Anexos\Alcaldía Municipal de Tangua\Cuestionarios
VIDEO	Control Interno	Anexos\Alcaldía Municipal de Tangua\Evidencia
Incumplimiento de la norma	Informe de hallazgos Contraloría	Anexos\Alcaldía Municipal de Tangua\Material para la Contraloría
Observación Directa	Testimonio Fuera de Cámara	N/A

Tabla 34: Hallazgo HAMT14

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT14

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
La entidad no cuenta con una mesa de servicios para la atención de incidentes de seguridad TI relacionados con el proceso de contratación.

CONSECUENCIAS
La falta de conciencia por parte de la entidad para la gestión centralizada y estandarizada de incidentes por medio de una mesa de servicios pone en riesgo los recursos de TI al dejar las responsabilidades en las manos de los usuarios (el individuo) el manejo de riesgos reales y potenciales, e incidentes. De esta forma compromete el cumplimiento de objetivos y metas de la entidad, así como también información sensible para la misma.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
La entidad debe implementar una mesa de trabajo centralizada cuyos procedimientos estén documentados y estandarizados, estos deben incluir procedimientos de clasificación (severidad e impacto) y de escalamiento (funcional y jerárquico), detectar y registrar incidentes, solicitudes de servicio o solicitudes de información. Además esta mesa de servicios se debe integrar y reconocer dentro del organigrama de la entidad, así como también en el manual de funciones.

Tabla 35: Hallazgo HAMT14 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT14

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS8	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
VIDEO	Control Interno	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 35: Hallazgo HAMT15

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT15

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
La entidad no realiza un monitoreo adecuado y constante de los incidentes que se presentan en los procesos de TI.

CONSECUENCIAS
No contar con estadísticas de los casos presentados por fallas de software, hardware o errores humanos que permitan buscar soluciones a futuro, además de conocer el tiempo de respuesta en el cual se le dio solución y el tiempo en el cual el sistema se vio interrumpido puede imposibilitar la medición, seguimiento y evaluación de la seguridad de TI, entorpeciendo el análisis y la toma de medidas preventivas y correctivas.

NIVEL DE RIESGO
Bajo

RECOMENDACIONES
Establecer procedimientos para el monitoreo y reporte de tendencias, llevar a cabo de manera regular análisis de estas tendencias y las consultas de incidentes con el fin de mitigar los riesgos y mejorar el desempeño de la mesa de servicios.

Tabla 36: Hallazgo HAMT15 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT15

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS8	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
Observación Directa	Testimonio fuera de cámara	N/A
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 36: Hallazgo HAMT16

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMT16

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
No existe un escalamiento adecuado en caso de presentarse incidentes.

EFECTO
La falta de un escalamiento adecuado en caso de incidentes puede producir que se interrumpan por completo los procedimientos dentro del proceso de contratación que dependen de las TI afectadas por el incidente comprometiendo el cumplimiento de las metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Definir procedimientos y criterios de escalamiento claros por parte de la mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente, evitando la interrupción de procedimientos dentro del proceso de contratación y esperando resolverlos de forma rápida dentro de un proceso estructurado de escalamiento.

Tabla 37: Hallazgo HAMT16 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT16

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS8	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 37: Hallazgo HAMT17

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT17

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
La entidad no cuenta con un programa de entrenamiento relacionado con las herramientas de TI y la seguridad de TI para los usuarios de TI involucrados en el proceso de contratación. Las necesidades de entrenamiento no han sido identificadas ni reconocidas.

CONSECUENCIAS
La falta de un programa de entrenamiento y la identificación y categorización de las necesidades de entrenamiento para los usuarios de TI, expone a la entidad a una baja productividad, un posible rechazo ante la intrusión de nuevas tecnologías, bajo desempeño, baja calidad de resultados y compromete el cumplimiento de objetivos y metas de la entidad.

NIVEL DE RIESGO
Alta

RECOMENDACIONES
La entidad debe garantizar el uso apropiado y un optimo desempeño de los recursos y soluciones de TI, identificar y categorizar las necesidades de capacitación de los usuarios, basándose en esto construir un programa de capacitación que además incluya temáticas de seguridad de TI, la comunicación de las políticas de seguridad vigentes, procedimientos y dar a conocer los manuales existentes.

Tabla 38: Hallazgo HAMT17 (Continuacón)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT17

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALES			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS7	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
Observación Directa	Verificación del sitio de trabajo	N/A
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 38: Hallazgo HAMT18

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT18

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
Los usuarios de TI involucrados en el proceso de contratación no cuentan con entrenamiento en el uso eficiente y efectivo de TI, así como tampoco en la seguridad de TI. El entrenamiento depende de la necesidad y la iniciativa del individuo.

CONSECUENCIAS
La falta de una adecuada capacitación de los usuarios de TI podría provocar una tasa de incidentes mayor, mayores riesgos y un aumento en las brechas de seguridad, además de la carencia de capacidad de respuesta ante los incidentes reales. Esto podría causar un retraso en las metas de la entidad y comprometer sus objetivos.

NIVEL DE RIESGO
Alta

RECOMENDACIONES
Realizar las actividades de capacitación, intrusión y concienciación, teniendo en cuenta un programa de entrenamiento, del adecuado manejo TI para disminuir tasa de incidentes y riesgos potenciales, así como también instruirlos en seguridad de TI con el fin de disminuir las posibles brechas de seguridad y darles una capacidad de respuesta primaria

Tabla 39: Hallazgo HAMT18 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT18

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALES			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTDS7	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
Observación Directa	Verificación del sitio de trabajo	N/A
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 39: Hallazgo HAMT19

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF** HAMT19

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALES			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No existe un proceso para administrar, registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio en los requerimientos de seguridad de las TI.

CONSECUENCIAS Al no haber un control de cambio adecuado, la entidad se podría volver inflexible ante los cambios en el entorno, esto puede afectar el flujo de información, producir cambios no autorizados, forzar a decisiones que violarán las medidas de seguridad y de esa forma comprometer la integridad de la información.

NIVEL DE RIESGO Bajo

RECOMENDACIONES Se deben definir las políticas y procedimientos de cambio incluyendo cambios de emergencia y parches, así como evaluar, priorizar y autorizar dichos cambios. Realizar registro detallado de los cambios y guardar un histórico de dichos cambios.

Tabla 40: Hallazgo HAMT19 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMT19

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALES			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCTAI6	Anexos\Alcaldia Municipal de Tangua\Cuestionarios
VIDEO	Tesoreria	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Tangua\Evidencia
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Tangua\Evidencia

3.2.4 Hallazgos Alcaldía Municipal de Yacuanquer. Los hallazgos de la Alcaldía Municipal de Yacuanquer son los siguientes:

Tabla 40: Hallazgo HAMY01

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF**
		HAMY01

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN Las medidas para soportar la administración de las TI y de la seguridad de TI no están implementadas

CONSECUENCIAS La entidad no cuenta con una adecuada administración de TI, así como tampoco de la seguridad de TI, pero aún así hace un uso intensivo y frecuente las TI. La falta de la adecuada administración TI y de su seguridad puede comprometer gravemente el cumplimiento de los objetivos y metas de la entidad.

NIVEL DE RIESGO Alto

RECOMENDACIONES La responsabilidades sobre la seguridad TI deben ser asignadas, administradas e implementadas de forma clara, para este fin se debe tomar conciencia dentro de la organización de la importancia de la administración de los recursos TI y por ende de su seguridad y para esto se deben generar una dependencia dentro de la organización, definir las funciones como mínimo de CIO y del personal de seguridad de TI dentro del manual de funciones y los procedimientos respectivos dentro del manual de procedimientos y de contratación.

Tabla 41: Hallazgo HAMY01 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY01

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Verificación del organigrama	ARCHIVO PERMANENTE
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 41: Hallazgo HAMY02

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY02

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No existe un plan de seguridad TI, ni políticas de seguridad que lo sustenten

CONSECUENCIAS La falta de planeación y definición de políticas y procedimientos pueden producir fallas y elevar los costos de las mismas, además de una falta de linealidad entre los procesos y los objetivos y metas de la entidad.

NIVEL DE RIESGO Alto

RECOMENDACIONES Se deben realizar una planeación estratégica TI, en la cual se implementen estudios y análisis de seguridad, determinar los requerimientos de seguridad, identificar riesgos y establecer metas. Usando esta información crear un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

Tabla 42: Hallazgo HAMY02 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY02

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 42: Hallazgo HAMY03

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY03

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No se define, establece y opera un proceso de administración de identidad para el acceso a los recursos TI

CONSECUENCIAS
La falta de identificación de las actividades y de certificación de identidad de los usuarios (tal como la certificación de las cuentas de correo ante la contraloría) puede dificultar verificación de responsables en caso de eventualidades, lo que atenta contra el principio de transparencia que debe manejar la entidad que se encuentra sometida a la Ley 80 de 1993.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Se deben definir estándares que permitan administrar la clara identificación y autorización lógica y física de todos los usuarios (internos, externos y temporales) de forma centralizada. Implementar procedimientos que permitan realizar seguimiento de las actividades de los usuarios y poder así identificar responsables. Administrar los permisos y privilegios de los usuarios para el acceso a recursos de TI por medio de cuentas de usuario, responsables de la información y niveles de acceso para casos normales, especiales y de emergencia. Estos derechos y obligaciones deben estar acordados contractualmente, así como documentados en los manuales de funciones, de procedimientos y las políticas de seguridad.

Tabla 43: Hallazgo HAMY03 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY03

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 43: Hallazgo HAMY04

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	REF
		HAMY04

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existe un proceso para la administración centralizada de las cuentas y perfiles de usuario, tanto de los recursos de TI locales como de los sistemas SICE y SECOP. Los derechos y privilegios de acceso a los recursos locales por parte de los funcionarios de la entidad son inexistentes (todos pueden acceder con privilegios de administrador).

CONSECUENCIAS
La conciencia de la necesidad de seguridad y administración de cuentas y perfiles de usuario de los recursos TI locales y de las cuentas y perfiles de usuario en los sistemas SICE y SECOP en la entidad dependen principalmente del individuo, no existen procedimientos formales ni planes de contingencia que permitan una administración centralizada de esta información.

Respecto a la administración de las cuentas de SICE y SECOP el usuario de control interno, tanto como los demás, no pueden realizar una verificación de las diversas alarmas disparadas para cada tipo de usuario, por lo que afecta el cumplimiento de los objetivos de la entidad y viola el principio de transparencia establecido por el marco legal para las entidades públicas que se someten a la ley 80 de 1993.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Construir un proceso y sus respectivos procedimientos para una efectiva administración centralizada de cuentas, perfiles y permisos de acceso para los recursos de TI locales y también para los sistemas SICE y SECOP. Debe incluirse un procedimiento de aprobación que detalle la información del responsable de los recursos de TI locales y las cuentas existentes para otros funcionarios, así como también los responsables de las cuentas de los sistemas SICE y SECOP. Además deben documentarse las relaciones con otros procesos y acuerdos de operación para cada uno de los responsables.

Tabla 44: Hallazgo HAMY04 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY04

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria

Tabla 44: Hallazgo HAMY05

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY05

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No se monitoriza adecuadamente los incidentes de seguridad reales o potenciales

CONSECUENCIAS La falta del adecuado seguimiento y monitoreo de incidentes puede elevar el costo de los mismos, la organización no estará preparada adecuadamente, ni podrá responder en un tiempo aceptable ante el incidente, lo cual puede retrasar el cronograma de la entidad y evitar el cumplimiento de sus metas aunque podría no afectar en gran medida al cumplimiento de los objetivos. No se podrán identificar con claridad las causas de los incidentes, por lo que no se podrán mitigar los riesgos y disminuir la probabilidad de ocurrencia.

NIVEL DE RIESGO Medio

RECOMENDACIONES Se deben definir procedimientos de monitoreo y análisis de los incidentes de seguridad, tanto los reales como los potenciales, esto con el fin de garantizar un nivel de seguridad adecuado y aprobado de acuerdo con las metas preestablecidas en el plan de seguridad TI, además un correcto monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. Se deben establecer métricas para lograr medir el nivel de seguridad de forma correcta, tomar estadísticas y realizar proyecciones y correcciones.

Tabla 45: Hallazgo HAMY05 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY05

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 45: Hallazgo HAMY06

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY06

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	1
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI.

CONSECUENCIAS La falta de reportes de seguridad podría llevar a incidentes más profundos y graves que puedan comprometer la información. La falta de respuesta para resolver brechas de seguridad que pueden ser reportadas de manera informal denota una falta de atención hacia la seguridad de TI lo cual puede provocar que un incidente incremente su gravedad y nivel de riesgo comprometiendo la información de la entidad.

NIVEL DE RIESGO Medio

RECOMENDACIONES Se debe definir los incidentes de seguridad, realizar reportes detallados e informar a los interesados.

Tabla 46: Hallazgo HAMY06 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY06

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
Observación Directa	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 46: Hallazgo HAMY07

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY07

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existe un marco de trabajo claro para los servicios de TI

CONSECUENCIAS
No existe un marco de trabajo para una comunicación efectiva entre los interesados del negocio, en este caso el proceso de contratación y los que prestan el servicio de TI, y para una clara definición de los servicios prestados y sus respectivos niveles. La ausencia del marco de trabajo apropiado para los servicios de TI impide una alineación entre los servicios y los requerimientos reales de la entidad.

NIVEL DE RIESGO
Medio

RECOMENDACIONES
Se debe asegurar la satisfacción de los usuarios del proceso de contratación con ofertas de servicios y niveles de servicio. Desarrollar un marco de trabajo que permita administrar estos servicios de una manera efectiva y constante que facilite un entendimiento y flujo de información entre el proveedor del servicio y los usuarios finales.

Tabla 47: Hallazgo HAMY07 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY07

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
VIDEO	Asesor jurídico	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Verificación del organigrama	ARCHIVO PERMANENTE
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 47: Hallazgo HAMY08

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	REF
		HAMY08

PROCESO AUDITADO	CONTRATACIÓN	PÁGINA		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existe un catálogo formal de servicios

CONSECUENCIAS
La entrega de servicios por personal no capacitado puede poner a la entidad en riesgo de agravar una situación y tomar medidas innecesarias que produzcan retrasos en las metas de la entidad. Además de afectar el principio de transparencia por falta de una definición clara de responsables.

NIVEL DE RIESGO
Medio

RECOMENDACIONES
Se debe construir una base de servicios de TI detallado, incluyendo los servicios de seguridad de TI. Esta formalización de servicios deben ser comunicados y bien conocidos por los usuarios del proceso de contratación y deben estar almacenados y administrados de forma centralizada.

Tabla 48: Hallazgo HAMY08 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY08

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 48: Hallazgo HAMY09

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY09

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN Los acuerdos de nivel de operación para los servicios de TI y seguridad TI no están definidos

CONSECUENCIAS La falta de procedimientos y estándares entendibles por el proveedor y el cliente del servicio TI que especifiquen cómo se hará entrega del mismo, puede generar brechas de seguridad, retrasos para las metas de la entidad y una baja calidad del servicio.

NIVEL DE RIESGO Medio

RECOMENDACIONES La entidad debe formalizar los convenios internos y externos alineados con los requerimientos y las capacidades de entrega del proveedor, estos deben estar documentados en los manuales de procedimientos y de funciones de TI. Se deben dar a conocer a las partes interesadas y vigilar su cumplimiento y medir su desempeño.

Tabla 49: Hallazgo HAMY09 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY09

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 49: Hallazgo HAMY10

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY10

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN No existe un manual de contratación disponible, ni manual de procedimientos para el proceso de contratación.

CONSECUENCIAS La falta de los manuales de contratación y procedimientos donde se especifiquen los algoritmos a seguir para los diferentes casos dentro del proceso de contratación puede conllevar a la realización de pasos innecesarios retrasando las metas de la entidad. Además puede conllevar a violar la norma y poner en riesgo el principio de transparencia.

NIVEL DE RIESGO Alto

RECOMENDACIONES Construir un manual de contratación y de procedimientos que concentren los algoritmos entendibles para las partes interesadas de acuerdo a los objetivos de la entidad y del marco legal vigente.

Tabla 50: Hallazgo HAMY10 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF**
		HAMY10

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Incumplimiento de la Norma	Hallazgos Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 50: Hallazgo HAMY11

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	REF
		HAMY11

PROCESO AUDITADO	CONTRATACIÓN	PÁGINA		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existen procedimientos formales y documentados para el uso del sistema SICE dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma.

CONSECUENCIAS
La falta de estos procedimientos y su cumplimiento vulneran gravemente el principio de transparencia para las entidades que se rigen por la ley 80 de 1993, y violan las normas que relacionan al sistema SICE ya que esta es bien conocida y las entidades han recibido la adecuada capacitación para su uso. Además comprometen los objetivos y metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Definir claramente los procedimientos para el uso correcto y efectivo del sistema SICE, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

Tabla 51: Hallazgo HAMY11 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY11

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Incumplimiento de la Norma	Hallazgos Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria

Tabla 51: Hallazgo HAMY12

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	REF
		HAMY12

PROCESO AUDITADO	CONTRATACIÓN	PÁGINA		
		1	DE	1
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

DESCRIPCIÓN
No existen procedimientos formales y documentados para el uso del sistema SECOP dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma

CONSECUENCIAS
La falta de estos procedimientos y su cumplimiento vulneran gravemente el principio de transparencia para las entidades que se rigen por la ley 80 de 1993, y violan las normas que relacionan al sistema SECOP ya que esta es bien conocida y las entidades han recibido la adecuada capacitación para su uso. Además comprometen los objetivos y metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Definir claramente los procedimientos para el uso correcto y efectivo del sistema SECOP, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

Tabla 52: Hallazgo HAMY12 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY12

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Incumplimiento de la Norma	Hallazgos Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria

Tabla 52: Hallazgo HAMY13

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY13

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
No se realiza evaluación de riesgos de seguridad de TI para el proceso de contratación; ni tampoco se toma en cuenta los impactos en la entidad asociados con las vulnerabilidades de seguridad.

CONSECUENCIAS
Si no se cuenta con una evaluación adecuada de riesgos, estos no podrán ser mitigados, ni medidos, la tasa de incidentes por riesgos no identificados podría aumentar comprometiendo la seguridad, la información, los objetivos y las metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
La entidad debe establecer el contexto de riesgo de seguridad de TI, realizar evaluaciones periódicas con el personal de seguridad de TI, establecer los planes de acción para mitigar los riesgos críticos de TI. Todo esto debe estar centralizado y los procedimientos deben estar documentados en el manual correspondiente, además las funciones que desempeñen estos procedimientos deben estar consignadas dentro del manual de funciones de la entidad.

Tabla 53: Hallazgo HAMY13 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY13

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYPO9	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 53: Hallazgo HAMY14

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMY14

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
La entidad no cuenta con un programa de entrenamiento relacionado con las herramientas de TI y la seguridad de TI para los usuarios de TI involucrados en el proceso de contratación. Las necesidades de entrenamiento no han sido identificadas ni reconocidas.

CONSECUENCIAS
La falta de un programa de entrenamiento y la identificación y categorización de las necesidades de entrenamiento para los usuarios de TI, expone a la entidad a una baja productividad, un posible rechazo ante la intrusión de nuevas tecnologías, bajo desempeño, baja calidad de resultados y compromete el cumplimiento de objetivos y metas de la entidad.

NIVEL DE RIESGO
Alta

RECOMENDACIONES
La entidad debe garantizar el uso apropiado y un optimo desempeño de los recursos y soluciones de TI, identificar y categorizar las necesidades de capacitación de los usuarios, basándose en esto construir un programa de capacitación que además incluya temáticas de seguridad de TI, la comunicación de las políticas de seguridad vigentes, procedimientos y dar a conocer los manuales existentes.

Tabla 54: Hallazgo HAMY14 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY14

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
Observación Directa	Verificación del sitio de trabajo	N/A
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 54: Hallazgo HAMY15

	HALLAZGOS: ALCALDIA MUNICIPAL DE TANGUA	**REF**
		HAMY15

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
Los usuarios de TI involucrados en el proceso de contratación no cuentan con entrenamiento en el uso eficiente y efectivo de TI, así como tampoco en la seguridad de TI. El entrenamiento depende de la necesidad y la iniciativa del individuo.

CONSECUENCIAS
La falta de una adecuada capacitación de los usuarios de TI podría provocar una tasa de incidentes mayor, mayores riesgos y un aumento en las brechas de seguridad, además de la carencia de capacidad de respuesta ante los incidentes reales. Esto podría causar un retraso en las metas de la entidad y comprometer sus objetivos.

NIVEL DE RIESGO
Alta

RECOMENDACIONES
Realizar las actividades de capacitación, intrusión y concienciación, teniendo en cuenta un programa de entrenamiento, del adecuado manejo TI para disminuir tasa de incidentes y riesgos potenciales, así como también instruirlos en seguridad de TI con el fin de disminuir las posibles brechas de seguridad y darles una capacidad de respuesta primaria

Tabla 55: Hallazgo HAMY15 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY15

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
Observación Directa	Verificación del sitio de trabajo	N/A
Observación Directa	Testimonio fuera de cámara	N/A

Tabla 55: Hallazgo HAMY16

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY16

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
La entidad cuenta con un proceso para atender incidentes, pero este no es estandarizado y sólo brinda soporte reactivo. Además los procedimientos no se encuentran documentados y no existe ninguna relación del proceso en el manual de funciones ni en el organigrama de la entidad.

CONSECUENCIAS
La falta de una gestión centralizada y estandarizada de incidentes por medio de una mesa de servicios pone en riesgo los recursos de TI al brindar un soporte reactivo incapaz de adaptarse a un entorno cambiante y desestima los riesgos potenciales. Esto puede reducir el desempeño de los sistemas, la calidad de resultados y presentar una baja productividad.

NIVEL DE RIESGO
Medio

RECOMENDACIONES
La entidad debe desarrollar conciencia de la importancia de los recursos de TI, el papel que juega dentro del proceso de contratación es vital, por tal razón se debe realizar la instalación y operación de una mesa de servicios que provee todo el soporte técnico para registrar, atender, comunicar y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información por parte de los usuarios relacionados con el proceso de contratación. Sólo de esta forma se puede garantizar un funcionamiento óptimo de TI y así reducir los incidentes y brechas de seguridad.

Tabla 56: Hallazgo HAMY16 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY16

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Testimonio fuera de cámara	N/A
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 56: Hallazgo HAMY17

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY17

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
La entidad no realiza un monitoreo adecuado y constante de los incidentes que se presentan en los procesos de TI.

CONSECUENCIAS
No contar con estadísticas de los casos presentados por fallas de software, hardware o errores humanos que permitan buscar soluciones a futuro, además de conocer el tiempo de respuesta en el cual se le dio solución y el tiempo en el cual el sistema se vio interrumpido puede imposibilitar la medición, seguimiento y evaluación de la seguridad de TI, entorpeciendo el análisis y la toma de medidas preventivas y correctivas.

NIVEL DE RIESGO
Bajo

RECOMENDACIONES
Establecer procedimientos para el monitoreo y reporte de tendencias, llevar a cabo de manera regular análisis de estas tendencias y las consultas de incidentes con el fin de mitigar los riesgos y mejorar el desempeño de la mesa de servicios.

Tabla 57: Hallazgo HAMY17 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY17

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Evidencia Fotográfica	Informe preliminar Contraloría	Anexos\Alcaldia Municipal de Yacuanquer\Material para la Contraloria
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 57: Hallazgo HAMY18

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY18

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCIA			

DESCRIPCIÓN:
No existe un escalamiento adecuado en caso de presentarse incidentes.

EFECTO
La falta de un escalamiento adecuado en caso de incidentes puede producir que se interrumpan por completo los procedimientos dentro del proceso de contratación que dependen de las TI afectadas por el incidente comprometiendo el cumplimiento de las metas de la entidad.

NIVEL DE RIESGO
Alto

RECOMENDACIONES
Definir procedimientos y criterios de escalamiento claros por parte de la mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente, evitando la interrupción de procedimientos dentro del proceso de contratación y esperando resolverlos de forma rápida dentro de un proceso estructurado de escalamiento.

Tabla 58: Hallazgo HAMY18 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF**
		HAMY18

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA**		
		2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Verificación del sitio de trabajo	N/A

Tabla 58: Hallazgo HAMY19

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY19

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 1	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			
FECHA				

DESCRIPCIÓN No existe un proceso para administrar, registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio en los requerimientos de seguridad de las TI.

CONSECUENCIAS Al no haber un control de cambio adecuado, la entidad se podría volver inflexible ante los cambios en el entorno, esto puede afectar el flujo de información, producir cambios no autorizados, forzar a decisiones que violarán las medidas de seguridad y de esa forma comprometer la integridad de la información.

NIVEL DE RIESGO Bajo

RECOMENDACIONES Se deben definir las políticas y procedimientos de cambio incluyendo cambios de emergencia y parches, así como evaluar, priorizar y autorizar dichos cambios. Realizar registro detallado de los cambios y guardar un histórico de dichos cambios.

Tabla 59: Hallazgo HAMY19 (Continuación)

	HALLAZGOS: ALCALDIA MUNICIPAL DE YACUANQUER	**REF** HAMY19

PROCESO AUDITADO	CONTRATACIÓN	**PÁGINA** 2	DE	2
RESPONSABLE	LENNIN GEOVANNY IBARRA GONZALEZ			
	DIEGO MAURICIO MEZA GARCÍA			

MATERIAL SOPORTE		
TIPO	**REF**	**UBICACIÓN**
CUESTIONARIO	CCYDS5	Anexos\Alcaldia Municipal de Yacuanquer\Cuestionarios
VIDEO	Primera Visita	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia
Observación Directa	Verificación del manual de funciones	Anexos\Alcaldia Municipal de Yacuanquer\Evidencia

3.2.4. Informe de Auditoria. El informe final de la auditoría es el siguiente:

- **Objetivos.** Realizar Auditoria de Sistemas a las entidades públicas: Alcaldía Municipal de Tangua y Alcaldía Municipal de Yacuanquer para evidenciar vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información manejada en el proceso de contratación.

- **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.

  - 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.

  - Auditar el sitio Web de las entidades públicas del Departamento de Nariño tomadas como caso de estudio en conformidad al decreto 1151 de gobierno en línea, así como parámetros de calidad y usabilidad.

  - 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.

- **Limitaciones.** Teniendo en cuenta que el grupo auditor se debía ceñir al trabajo realizado por la Contraloría Departamental de Nariño, sus normas y metodologías, las visitas autorizadas fueron mínimas y no se pudieron aplicar algunas de las técnicas de auditoría especificadas en el estado del arte este documento.

- **Alcance de la Auditoría.** El alcance de la auditoría buscó cumplir con los siguientes puntos:

  - Conocer los aspectos fundamentales que intervienen en los procedimientos que involucran recursos de TI, dentro del proceso de contratación.

  - Determinar y valorar las amenazas y vulnerabilidades de la seguridad de TI dentro del proceso de contratación utilizando el marco de trabajo COBIT.

- Proponer mejoras y recomendaciones para mitigar los riesgos y subsanar las vulnerabilidades en la seguridad de TI.

- Resultados de la Auditoría COBIT

  - **Alcaldía Municipal de Tangua**

  En conformidad con la auditoría realizada, la recolección de pruebas y basándonos en el marco de trabajo COBIT, el grupo auditor, logró definir las siguientes observaciones en la entidad y recomienda tomar las respectivas acciones correctivas para garantizar la seguridad de TI dentro del proceso de contratación de la entidad.

  ✓ **Proceso principal COBIT auditado. DS5 Garantizar la seguridad de los sistemas.** En este apartado se presenta un informe con las observaciones y recomendaciones del proceso COBIT principal que fue auditado, el cual es el que hace referencia a la seguridad de los sistemas.

  o **Observación.** Las medidas para soportar la administración de las TI y de la seguridad de TI no están implementadas (REF HAMT01).

  o **Recomendaciones.** La responsabilidades sobre la seguridad TI deben ser asignadas, administradas e implementadas de forma clara, para este fin se debe tomar conciencia dentro de la organización de la importancia de la administración de los recursos TI y por ende de su seguridad y para esto se deben generar una dependencia dentro de la organización, definir las funciones como mínimo de CIO y del personal de seguridad de TI dentro del manual de funciones y los procedimientos respectivos dentro del manual de procedimientos y de contratación.

  o **Observación.** No existe un plan de seguridad TI, ni políticas de seguridad que lo sustenten (REF HAMT02).

  o **Recomendaciones.** Se deben realizar una planeación estratégica TI, en la cual se implementen estudios y análisis de seguridad, determinar los requerimientos de seguridad, identificar riesgos y establecer metas. Usando esta información crear un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.

  Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

- **Observación.** No se define, establece y opera un proceso de administración de identidad para el acceso a los recursos TI (REF HAMT03).

- **Recomendaciones.** Se deben definir estándares que permitan administrar la clara identificación y autorización lógica y física de todos los usuarios (internos, externos y temporales) de forma centralizada. Implementar procedimientos que permitan realizar seguimiento de las actividades de los usuarios y poder así identificar responsables. Administrar los permisos y privilegios de los usuarios para el acceso a recursos de TI por medio de cuentas de usuario, responsables de la información y niveles de acceso para casos normales, especiales y de emergencia. Estos derechos y obligaciones deben estar acordados contractualmente, así como documentados en los manuales de funciones, de procedimientos y las políticas de seguridad.

- **Observación.** No existe un proceso para la administración centralizada de las cuentas y perfiles de usuario, tanto de los recursos de TI locales como de los sistemas SICE y SECOP. Los derechos y privilegios de acceso a los recursos locales por parte de los funcionarios de la entidad son inexistentes (todos pueden acceder con privilegios de administrador (REF HAMT04).

- **Recomendaciones.** Construir un proceso y sus respectivos procedimientos para una efectiva administración centralizada de cuentas, perfiles y permisos de acceso para los recursos de TI locales y también para los sistemas SICE y SECOP. Debe incluirse un procedimiento de aprobación que detalle la información del responsable de los recursos de TI locales y las cuentas existentes para otros funcionarios, así como también los responsables de las cuentas de los sistemas SICE y SECOP. Además deben documentarse las relaciones con otros procesos y acuerdos de operación para cada uno de los responsables.

- **Observación.** No se monitoriza adecuadamente los incidentes de seguridad reales o potenciales (REF HAMT05).

- **Recomendaciones.** Se deben definir procedimientos de monitoreo y análisis de los incidentes de seguridad, tanto los reales como los potenciales, esto con el fin de garantizar un nivel de seguridad adecuado y aprobado de acuerdo con las metas preestablecidas en el plan de seguridad TI, además un correcto monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

Se deben establecer métricas para lograr medir el nivel de seguridad de forma correcta, tomar estadísticas y realizar proyecciones y correcciones.

- **Observación.** No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI (REF HAMT06).

- **Recomendaciones.** Se debe definir los incidentes de seguridad, realizar reportes detallados e informar a los interesados.

✓ **Procesos COBIT de entrada al proceso DS5**. Las entradas del proceso DS5, son las relaciones con otros dominios, procesos y objetivos de control externos al proceso DS5 que deben entregarle información a éste para un adecuado funcionamiento.

Los procesos COBIT de entrada que el grupo auditor determinó aplicaban al proceso de contratación de la entidad fueron los que se describirán a continuación.

Dominio planear y organizar. Proceso COBIT P09 Evaluar y Administrar los Riesgos de TI.

- **Observación.** No se realiza evaluación de riesgos de seguridad de TI para el proceso de contratación; ni tampoco se toma en cuenta los impactos en la entidad asociados con las vulnerabilidades de seguridad (REF HAMT07).

- **Recomendaciones.** La entidad debe establecer el contexto de riesgo de seguridad de TI, realizar evaluaciones periódicas con el personal de seguridad de TI, establecer los planes de acción para mitigar los riesgos críticos de TI. Todo esto debe estar centralizado y los procedimientos deben estar documentados en el manual correspondiente, además las funciones que desempeñen estos procedimientos deben estar consignadas dentro del manual de funciones de la entidad.

  Dominio entregar y dar soporte. Proceso COBIT DS1 Definir y Administrar los Niveles de Servicio.

- **Observación.** No existe un marco de trabajo claro para los servicios de TI (REF HAMT08).

- **Recomendaciones.** Se debe asegurar la satisfacción de los usuarios del proceso de contratación con ofertas de servicios y niveles de

servicio. Desarrollar un marco de trabajo que permita administrar estos servicios de una manera efectiva y constante que facilite un entendimiento y flujo de información entre el proveedor del servicio y los usuarios finales.

- **Observación.** No existe un catálogo formal de servicios (REF HAMT09).

- **Recomendaciones.** Se debe construir una base de servicios de TI detallado, incluyendo los servicios de seguridad de TI. Esta formalización de servicios deben ser comunicados y bien conocidos por los usuarios del proceso de contratación y deben estar almacenados y administrados de forma centralizada.

- **Observación.** Los acuerdos de nivel de operación para los servicios de TI y seguridad TI no están definidos (REF HAMT10).

- **Recomendaciones.** La entidad debe formalizar los convenios internos y externos alineados con los requerimientos y las capacidades de entrega del proveedor, estos deben estar documentados en los manuales de procedimientos y de funciones de TI. Se deben dar a conocer a las partes interesadas y vigilar su cumplimiento y medir su desempeño.

- **Observación.** No existe un manual de contratación, ni manual de procedimientos para el proceso de contratación (REF HAMT11).

- **Recomendaciones.** Construir un manual de contratación y de procedimientos que concentren los algoritmos entendibles para las partes interesadas de acuerdo a los objetivos de la entidad y del marco legal vigente.

- **Observación.** No existen procedimientos formales y documentados para el uso del sistema SICE dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma (REF HAMT12).

- **Recomendaciones.** Definir claramente los procedimientos para el uso correcto y efectivo del sistema SICE, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

- **Observación.** No existen procedimientos formales y documentados para el uso del sistema SECOP dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma (REF HAMT13).

- **Recomendaciones.** Definir claramente los procedimientos para el uso correcto y efectivo del sistema SECOP, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

✓ **Procesos COBIT de salida al proceso DS5.** Las salidas del proceso DS5, son las relaciones con otros dominios, procesos y objetivos de control externos al proceso DS5 a los que el proceso DS4 debe entregarle información para su adecuado funcionamiento.

Los procesos COBIT de salida que el grupo auditor determinó aplicaban al proceso de contratación de la entidad fueron los que se describirán a continuación.

Dominio planear y organizar. Proceso COBIT P09 Evaluar y Administrar los Riesgos de TI.

- **Observación.** No se realiza evaluación de riesgos de seguridad de TI para el proceso de contratación; ni tampoco se toma en cuenta los impactos en la entidad asociados con las vulnerabilidades de seguridad (REF HAMT07).

- **Recomendaciones.** La entidad debe establecer el contexto de riesgo de seguridad de TI, realizar evaluaciones periódicas con el personal de seguridad de TI, establecer los planes de acción para mitigar los riesgos críticos de TI. Todo esto debe estar centralizado y los procedimientos deben estar documentados en el manual correspondiente, además las funciones que desempeñen estos procedimientos deben estar consignadas dentro del manual de funciones de la entidad.

  Dominio entregar y dar soporte. Proceso COBIT DS7 Educar y Entrenar a los Usuarios.

- **Observación.** La entidad no cuenta con un programa de entrenamiento relacionado con las herramientas de TI y la seguridad de TI para los usuarios de TI involucrados en el proceso de contratación. Las necesidades de entrenamiento no han sido identificadas ni reconocidas (REF HAMT14).

- **Recomendaciones.** La entidad debe garantizar el uso apropiado y un optimo desempeño de los recursos y soluciones de TI, identificar y categorizar las necesidades de capacitación de los usuarios, basándose en esto construir un programa de capacitación que además incluya temáticas de seguridad de TI, la comunicación de las políticas de seguridad vigentes, procedimientos y dar a conocer los manuales existentes.

- **Observación.** Los usuarios de TI involucrados en el proceso de contratación no cuentan con entrenamiento en el uso eficiente y efectivo de TI, así como tampoco en la seguridad de TI. El entrenamiento depende de la necesidad y la iniciativa del individuo (REF HAMT15).

- **Recomendaciones.** Realizar las actividades de capacitación, intrusión y concienciación, teniendo en cuenta un programa de entrenamiento, del adecuado manejo TI para disminuir tasa de incidentes y riesgos potenciales, así como también instruirlos en seguridad de TI con el fin de disminuir las posibles brechas de seguridad y darles una capacidad de respuesta primaria

  Dominio entregar y dar soporte. Proceso COBIT DS8 Administrar la Mesa de Servicio y los Incidentes.

- **Observación.** La entidad cuenta con un proceso para atender incidentes, pero este no es estandarizado y sólo brinda soporte reactivo. Además los procedimientos no se encuentran documentados y no existe ninguna relación del proceso en el manual de funciones ni en el organigrama de la entidad (REF HAMT16).

- **Recomendaciones.** La entidad debe desarrollar conciencia de la importancia de los recursos de TI, el papel que juega dentro del proceso de contratación es vital, por tal razón se debe realizar la instalación y operación de una mesa de servicios que provee todo el soporte técnico para registrar, atender, comunicar y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información por parte de los usuarios relacionados con el proceso de contratación. Sólo de esta forma se puede garantizar un funcionamiento óptimo de TI y así reducir los incidentes y brechas de seguridad.

- **Observación.** La entidad no realiza un monitoreo adecuado y constante de los incidentes que se presentan en los procesos de TI (REF HAMT17).

- **Recomendaciones.** Establecer procedimientos para el monitoreo y reporte de tendencias, llevar a cabo de manera regular análisis de estas tendencias y las consultas de incidentes con el fin de mitigar los riesgos y mejorar el desempeño de la mesa de servicios.

- **Observación.** No existe un escalamiento adecuado en caso de presentarse incidentes (REF HAMT18).

- **Recomendaciones.** Definir procedimientos y criterios de escalamiento claros por parte de la mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente, evitando la interrupción de procedimientos dentro del proceso de contratación y esperando resolverlos de forma rápida dentro de un proceso estructurado de escalamiento.

  Dominio adquirir e implementar. Proceso COBIT AI6 Administrar Cambios.

- **Observación.** No existe un proceso para administrar, registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio en los requerimientos de seguridad de las TI (REF HAMT19).

- **Recomendaciones.** Se deben definir las políticas y procedimientos de cambio incluyendo cambios de emergencia y parches, así como evaluar, priorizar y autorizar dichos cambios. Realizar registro detallado de los cambios y guardar un histórico de dichos cambios.

✓ **Evaluación del nivel de madurez para el proceso DS5 Garantizar la Seguridad de los Sistemas.** Basándose en las evaluaciones y los análisis realizados, los cuales se sustentan mediante la evidencia recolectada y los hallazgos encontrados podemos concluir que para las entidades auditadas el nivel de madurez es 1 Inicial / Ad Hoc, dado que cumple con la descripción de CobIT:

La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

Además basándose en los factores de riesgos descritos podemos decir que las entidades auditadas cumplen con los siguientes atributos de madurez:

Tabla 59: Atributos de madurez Tangua

Conciencia y comunicación	Políticas, Estándares y Procedimientos	Herramientas y automatización	Habilidades y experiencia	Responsabilidad y rendición de cuentas	Establecimiento y medición de metas
Surge el reconocimiento de la necesidad del proceso. Existe comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de	No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.	No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva	Las metas no están claras y no existen las mediciones

herramientas

- **Alcaldía Municipal de Yacuanquer**

  En conformidad con la auditoría realizada, la recolección de pruebas y basándonos en el marco de trabajo COBIT, el grupo auditor, logró definir las siguientes observaciones en la entidad y recomienda tomar las respectivas acciones correctivas para la garantizar la seguridad de TI dentro del proceso de contratación de la entidad.

  - ✓ **Proceso COBIT principal auditado. DS5 Garantizar la seguridad de los sistemas.** En este apartado se presenta un informe con las observaciones y recomendaciones del proceso COBIT principal que fue auditado, el cual es el que hace referencia a la seguridad de los sistemas.

    - o **Observación.** Las medidas para soportar la administración de las TI y de la seguridad de TI no están implementadas (REF HAMY01).

    - o **Recomendaciones.** La responsabilidades sobre la seguridad TI deben ser asignadas, administradas e implementadas de forma clara, para este fin se debe tomar conciencia dentro de la organización de la importancia de la administración de los recursos TI y por ende de su seguridad y para esto se deben generar una dependencia dentro de la organización, definir las funciones como mínimo de CIO y del personal de seguridad de TI dentro del manual de funciones y los procedimientos respectivos dentro del manual de procedimientos y de contratación.

    - o **Observación.** No existe un plan de seguridad TI, ni políticas de seguridad que lo sustenten (REF HAMY02).

    - o **Recomendaciones.** Se deben realizar una planeación estratégica TI, en la cual se implementen estudios y análisis de seguridad, determinar los requerimientos de seguridad, identificar riesgos y establecer metas. Usando esta información crear un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.

      Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

    - o **Observación.** No se define, establece y opera un proceso de administración de identidad para el acceso a los recursos TI (REF HAMY03).

- **Recomendaciones.** Se deben definir estándares que permitan administrar la clara identificación y autorización lógica y física de todos los usuarios (internos, externos y temporales) de forma centralizada. Implementar procedimientos que permitan realizar seguimiento de las actividades de los usuarios y poder así identificar responsables. Administrar los permisos y privilegios de los usuarios para el acceso a recursos de TI por medio de cuentas de usuario, responsables de la información y niveles de acceso para casos normales, especiales y de emergencia. Estos derechos y obligaciones deben estar acordados contractualmente, así como documentados en los manuales de funciones, de procedimientos y las políticas de seguridad.

- **Observación.** No existe un proceso para la administración centralizada de las cuentas y perfiles de usuario, tanto de los recursos de TI locales como de los sistemas SICE y SECOP. Los derechos y privilegios de acceso a los recursos locales por parte de los funcionarios de la entidad son inexistentes (todos pueden acceder con privilegios de administrador (REF HAMY04).

- **Recomendaciones.** Construir un proceso y sus respectivos procedimientos para una efectiva administración centralizada de cuentas, perfiles y permisos de acceso para los recursos de TI locales y también para los sistemas SICE y SECOP. Debe incluirse un procedimiento de aprobación que detalle la información del responsable de los recursos de TI locales y las cuentas existentes para otros funcionarios, así como también los responsables de las cuentas de los sistemas SICE y SECOP. Además deben documentarse las relaciones con otros procesos y acuerdos de operación para cada uno de los responsables.

- **Observación.** No se monitoriza adecuadamente los incidentes de seguridad reales o potenciales (REF HAMY05).

- **Recomendaciones.** Se deben definir procedimientos de monitoreo y análisis de los incidentes de seguridad, tanto los reales como los potenciales, esto con el fin de garantizar un nivel de seguridad adecuado y aprobado de acuerdo con las metas preestablecidas en el plan de seguridad TI, además un correcto monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

  Se deben establecer métricas para lograr medir el nivel de seguridad de forma correcta, tomar estadísticas y realizar proyecciones y correcciones.

- **Observación.** No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. (REF HAMY06).

- **Recomendaciones.** Se debe definir los incidentes de seguridad, realizar reportes detallados e informar a los interesados.

✓ **Procesos COBIT de entrada al proceso DS5.** Las entradas del proceso DS5, son las relaciones con otros dominios, procesos y objetivos de control externos al proceso DS5 que deben entregarle información a éste para un adecuado funcionamiento.

Los procesos COBIT de entrada que el grupo auditor determinó aplicaban al proceso de contratación de la entidad fueron los que se describirán a continuación.

Dominio planear y organizar. Proceso COBIT P09 Evaluar y Administrar los Riesgos de TI.

- **Observación.** No se realiza evaluación de riesgos de seguridad de TI para el proceso de contratación; ni tampoco se toma en cuenta los impactos en la entidad asociados con las vulnerabilidades de seguridad (REF HAMY13).

- **Recomendaciones.** La entidad debe establecer el contexto de riesgo de seguridad de TI, realizar evaluaciones periódicas con el personal de seguridad de TI, establecer los planes de acción para mitigar los riesgos críticos de TI. Todo esto debe estar centralizado y los procedimientos deben estar documentados en el manual correspondiente, además las funciones que desempeñen estos procedimientos deben estar consignadas dentro del manual de funciones de la entidad.

  Dominio entregar y dar soporte. Proceso COBIT DS1 Definir y Administrar los Niveles de Servicio.

- **Observación.** No existe un marco de trabajo claro para los servicios de TI (REF HAMY07).

- **Recomendaciones.** Se debe asegurar la satisfacción de los usuarios del proceso de contratación con ofertas de servicios y niveles de servicio. Desarrollar un marco de trabajo que permita administrar estos servicios de una manera efectiva y constante que facilite un entendimiento y flujo de información entre el proveedor del servicio y los usuarios finales.

- **Observación.** No existe un catálogo formal de servicios (REF HAMY08).

- **Recomendaciones.** Se debe construir una base de servicios de TI detallado, incluyendo los servicios de seguridad de TI. Esta formalización de servicios deben ser comunicados y bien conocidos por los usuarios del proceso de contratación y deben estar almacenados y administrados de forma centralizada.

- **Observación.** Los acuerdos de nivel de operación para los servicios de TI y seguridad TI no están definidos (REF HAMY09).

- **Recomendaciones.** La entidad debe formalizar los convenios internos y externos alineados con los requerimientos y las capacidades de entrega del proveedor, estos deben estar documentados en los manuales de procedimientos y de funciones de TI. Se deben dar a conocer a las partes interesadas y vigilar su cumplimiento y medir su desempeño.

- **Observación.** No existe un manual de contratación, ni manual de procedimientos para el proceso de contratación (REF HAMY10).

- **Recomendaciones.** Construir un manual de contratación y de procedimientos que concentren los algoritmos entendibles para las partes interesadas de acuerdo a los objetivos de la entidad y del marco legal vigente.

- **Observación.** No existen procedimientos formales y documentados para el uso del sistema SICE dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma (REF HAMY11).

- **Recomendaciones.** Definir claramente los procedimientos para el uso correcto y efectivo del sistema SICE, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

- **Observación.** No existen procedimientos formales y documentados para el uso del sistema SECOP dentro de la entidad. Los procedimientos son informales e intuitivos y a veces no se cumplen según la norma (REF HAMY12).

- **Recomendaciones.** Definir claramente los procedimientos para el uso correcto y efectivo del sistema SECOP, así como modificar el manual de funciones y especificar las responsabilidades y obligaciones dentro de las funciones del personal a cargo. Estos procedimientos deben ser estándar y centralizados. Se deben comunicar a todos los interesados estos procesos. Realizar acuerdos de operación si son necesarios para establecer los requerimientos del proveedor y el cliente. Vigilar el cumplimiento de estos procedimientos de acuerdo a la normatividad vigente.

✓ **Procesos COBIT de salida al proceso DS5.** Las salidas del proceso DS5, son las relaciones con otros dominios, procesos y objetivos de control externos al proceso DS5 a los que el proceso DS4 debe entregarle información para su adecuado funcionamiento.

Los procesos COBIT de salida que el grupo auditor determinó aplicaban al proceso de contratación de la entidad fueron los que se describirán a continuación.

Dominio planear y organizar. Proceso COBIT P09 Evaluar y Administrar los Riesgos de TI.

- **Observación.** No se realiza evaluación de riesgos de seguridad de TI para el proceso de contratación; ni tampoco se toma en cuenta los impactos en la entidad asociados con las vulnerabilidades de seguridad (REF HAMY13).

- **Recomendaciones.** La entidad debe establecer el contexto de riesgo de seguridad de TI, realizar evaluaciones periódicas con el personal de seguridad de TI, establecer los planes de acción para mitigar los riesgos críticos de TI. Todo esto debe estar centralizado y los procedimientos deben estar documentados en el manual correspondiente, además las funciones que desempeñen estos procedimientos deben estar consignadas dentro del manual de funciones de la entidad.

  Dominio entregar y dar soporte. Proceso COBIT DS7 Educar y Entrenar a los Usuarios.

- **Observación.** La entidad no cuenta con un programa de entrenamiento relacionado con las herramientas de TI y la seguridad de TI para los usuarios de TI involucrados en el proceso de contratación. Las

necesidades de entrenamiento no han sido identificadas ni reconocidas (REF HAMY14).

- **Recomendaciones.** La entidad debe garantizar el uso apropiado y un optimo desempeño de los recursos y soluciones de TI, identificar y categorizar las necesidades de capacitación de los usuarios, basándose en esto construir un programa de capacitación que además incluya temáticas de seguridad de TI, la comunicación de las políticas de seguridad vigentes, procedimientos y dar a conocer los manuales existentes.

- **Observación.** Los usuarios de TI involucrados en el proceso de contratación no cuentan con entrenamiento en el uso eficiente y efectivo de TI, así como tampoco en la seguridad de TI. El entrenamiento depende de la necesidad y la iniciativa del individuo (REF HAMY15).

- **Recomendaciones.** Realizar las actividades de capacitación, intrusión y concienciación, teniendo en cuenta un programa de entrenamiento, del adecuado manejo TI para disminuir tasa de incidentes y riesgos potenciales, así como también instruirlos en seguridad de TI con el fin de disminuir las posibles brechas de seguridad y darles una capacidad de respuesta primaria

Dominio entregar y dar soporte. Proceso COBIT DS8 Administrar la Mesa de Servicio y los Incidentes.

- **Observación.** La entidad cuenta con un proceso para atender incidentes, pero este no es estandarizado y sólo brinda soporte reactivo. Además los procedimientos no se encuentran documentados y no existe ninguna relación del proceso en el manual de funciones ni en el organigrama de la entidad (REF HAMY16).

- **Recomendaciones.** La entidad debe desarrollar conciencia de la importancia de los recursos de TI, el papel que juega dentro del proceso de contratación es vital, por tal razón se debe realizar la instalación y operación de una mesa de servicios que provee todo el soporte técnico para registrar, atender, comunicar y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información por parte de los usuarios relacionados con el proceso de contratación. Sólo de esta forma se puede garantizar un funcionamiento óptimo de TI y así reducir los incidentes y brechas de seguridad.

- **Observación.** La entidad no realiza un monitoreo adecuado y constante de los incidentes que se presentan en los procesos de TI (REF HAMY17).

- **Recomendaciones.** Establecer procedimientos para el monitoreo y reporte de tendencias, llevar a cabo de manera regular análisis de estas tendencias y las consultas de incidentes con el fin de mitigar los riesgos y mejorar el desempeño de la mesa de servicios.

- **Observación.** No existe un escalamiento adecuado en caso de presentarse incidentes (REF HAMY18).

- **Recomendaciones.** Definir procedimientos y criterios de escalamiento claros por parte de la mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente, evitando la interrupción de procedimientos dentro del proceso de contratación y esperando resolverlos de forma rápida dentro de un proceso estructurado de escalamiento.

  Dominio adquirir e implementar. Proceso COBIT AI6 Administrar Cambios.

- **Observación.** No existe un proceso para administrar, registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio en los requerimientos de seguridad de las TI (REF HAMY19).

- **Recomendaciones.** Se deben definir las políticas y procedimientos de cambio incluyendo cambios de emergencia y parches, así como evaluar, priorizar y autorizar dichos cambios. Realizar registro detallado de los cambios y guardar un histórico de dichos cambios.

✓ **Evaluación del nivel de madurez para el proceso DS5 Garantizar la Seguridad de los Sistemas.** Basándose en las evaluaciones y los análisis realizados, los cuales se sustentan mediante la evidencia recolectada y los hallazgos encontrados podemos concluir que para las entidades auditadas el nivel de madurez es 1 Inicial / Ad Hoc, dado que cumple con la descripción de CobIT:

La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

Además basándose en los factores de riesgos descritos podemos decir que las entidades auditadas cumplen con los siguientes atributos de madurez:

Tabla 60: Atributos de madurez Yacuanquer

Conciencia y comunicación	Políticas, Estándares y Procedimientos	Herramientas y automatización	Habilidades y experiencia	Responsabilidad y rendición de cuentas	Establecimiento y medición de metas
Surge el reconocimiento de la necesidad del proceso. Existe comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de	No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.	No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva	Las metas no están claras y no existen las mediciones

herramientas

- **Resultados de la Auditoría de la Página Web.** La auditoría realizada a la página web se realizó confrontando el manual de implementación del Decreto 1151 contra la página actual, construyendo una lista de verificación para evaluar el cumplimiento de las fases de gobierno en línea que deberían estar implementadas hasta el 31 de diciembre de 2008.

  Finalmente se aplica la técnica de scoring, se evalúa la usabilidad y algunos parámetros de calidad de la página.

  - **Evaluación del Decreto 1151 para la Alcaldía Municipal de Tangua.**

    ✓ **Fase Preliminar**

Tabla 61: Comité de Gobierno en Línea

COMITÉ DE GOBIERNO EN LINEA	
Característica	**Cumple (Sí/No)**
El comité de gobierno en línea fue conformado	**si**
Existe un líder de gobierno en línea	**si**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de planeación	**si**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de atención al ciudadano	**no**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de comunicaciones y/o prensa	**si**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de control interno	**si**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de sistemas y/o informática	**si**
Se invitaron a los representantes de la dirección de gestión de calidad y el jefe de responsable de jurídica	**no**

Tabla 62: Plan de Acción

PLAN DE ACCIÓN 2009 - 2012 (plazo de entrega: primera semana de noviembre de 2008)	
Característica	**Cumple (Sí/No)**
Se generó un plan de acción con el fin de garantizar la implementación de la Estrategia de Gobierno En Línea	**si**
El plan tiene un marco estratégico en el que se identifiquen las políticas de la entidad y su relación con los objetivos de la Estrategia de Gobierno En Línea	**no**
Un diagnóstico del estado de la entidad a la fecha de elaboración del Plan, con respecto al cumplimiento de los diferentes criterios en cada una de las Fases de Gobierno En Línea	**no**
Un esquema que identifique las acciones necesarias para el cumplimiento de cada uno de los criterios en cada fase y su plazo de implementación	**no**
Un marco de acción, que comprenda la identificación de los proyectos tendientes a garantizar la implementación de la Estrategia de Gobierno En Línea el cumplimiento de los objetivos misionales de cada entidad	**no**
Una ficha por cada proyecto que se desarrollará, identificando los objetivos, las actividades, los beneficios e impacto, las metas, los recursos señalando las líneas presupuestales que respaldan dichos recursos, los responsables y los plazos de ejecución.	**no**

✓ Información mínima a publicar

Tabla 63: Sitio web principal

PARA EL SITIO WEB PRINCIPAL		
Característica	**Cumple (Sí/No)**	**Observaciones**
Acerca de la entidad		
Información básica en el Portal del Estado Colombiano	**Si**	
Misión y Visión	**Si**	
Objetivos y funciones	**si**	No presenta los objetivos
Organigrama	**Si**	
Localización Física (Incluyendo todas las sedes o sucursales)	**Si**	
Teléfonos y/o líneas gratuitas y fax.	**Si**	
Correo electrónico de contacto	**Si**	
Horarios y días de atención al público	**Si**	
Directorio de los funcionarios principales	**si**	Se da uso de correos comerciales.
Directorio de las entidades	**si**	
Directorio de agremiaciones y asociaciones	**si**	
Normatividad		
Leyes/Ordenanzas/acuerdos	**no**	Los documentos no cumplen con el plazo de 5 días para su publicación
Decretos	**no**	
Resoluciones y/u otros actos administrativos de carácter general	**no**	
Proyectos de normatividad	**N/R**	
Presupuesto		
Presupuesto aprobado en ejercicio	**si**	
Información histórica de presupuestos	**si**	
Políticas, planes, programas y proyectos institucionales		
Políticas, planes y/o líneas estratégicas	**si**	

Tabla 63: Sitio web principal (Continuación)

Característica	Cumple (Sí/No)	Observaciones
Programas, proyectos en ejecución	**si**	
Contacto con dependencia responsable	**si**	
Trámites y Servicios		
Listado de trámites	**si**	No existe enlace al suit
Listado de servicios	**si**	No existe enlace al suit
Contratación		
Información sobre la contratación	**si**	
Control y rendición de cuentas		
Entes de control que vigilan a la entidad	**si**	La información está incompleta (procuraduría y contraloría)
Informes de gestión	**no**	Información escasa e incompleta
Metas, indicadores de desempeño y/o gestión, y resultados	**no**	
Plan de mejoramiento	**no**	No contiene información
Servicios de Información		
Información para niños	**si**	Está desactualizada
Preguntas y respuestas frecuentes	**si**	No existe información
Boletines y publicaciones	**no**	No existen boletines y publicaciones muy desactualizada
Noticias	**no**	No existe
Calendario de actividades	**si**	
Glosario	**si**	
Política de privacidad y condiciones de uso	**si**	

Tabla 64: Sitios adicionales

PARA SITIOS ADICIONALES AL SITIO WEB PRINCIPAL		
Característica	**Cumple (Sí/No)**	**Observaciones**
Acerca de la entidad		
Objetivos y funciones	**si**	
Localización Física (Incluyendo todas las sedes o sucursales)	**si**	
Teléfonos y/o líneas gratuitas y fax.	**si**	
Correo electrónico de contacto	**si**	
Horarios y días de atención al público	**si**	
Equipo de trabajo	**si**	Falta la foto de la mayoría de funcionarios y se utilizan correos comerciales
Directorio de los funcionarios principales	**si**	
Directorio de las entidades	**si**	
Directorio de agremiaciones y asociaciones	**si**	
Normatividad		
Leyes/Ordenanzas/acuerdos	**si**	
Decretos	**si**	
Resoluciones y/u otros actos administrativos de carácter general	**si**	
Proyectos de normatividad	**no**	
Líneas estratégicas y proyectos institucionales		
Programas, proyectos en ejecución	**si**	Varios no presentan información
Contacto con dependencia responsable	**si**	
Control y rendición de cuentas		
Informes de gestión	**si**	
Metas, indicadores de desempeño y/o gestión, y resultados	**si**	
Servicios de Información		
Bolentines y publicaciones	**no**	
Noticias	**si**	

Tabla 64: Sitios adicionales (Continuación)

Calendario de actividades	**si**	
Glosario	**si**	
Política de privacidad y condiciones de uso	**si**	

Tabla 65: Entidades estatales

PARA GOBERNACIONES Y ALCALDIAS		
Característica	**Cumple (Sí/No)**	**Observaciones**
Sobre el departamento o el municipio		
Presentación	**si**	
Información general	**si**	
Territorios	**si**	
Mapas	**si**	
Indicadores	**si**	
Documentos del municipio	**si**	
Álbum o galería de fotos	**si**	
Turismo	**si**	

✓ Estándares de navegación

Tabla 66: Navegación sitio principal

PARA EL SITIO WEB PRINCIPAL	
Característica	**Cumple (Sí/No)**
Acerca de la entidad	
Identidad Visual	si
Enlace al portal del Estado Colombiano	si
Fecha de última actualización	si
División de los contenidos	si
Uso de colores	si
Uso de marcos	si
Manejo de Vínculos	si
Estándares de Funcionalidad	
Mapa del sitio	si

Tabla 66: Navegación sitio principal (Continuación)

Característica	Cumple (Sí/No)
Acceso a la página de inicio	si
Acceso al menú principal	si
Estándares Técnicos	
Nombre del dominio	si
Marcación y/o Etiquetado	si
Tiempo de despliegue	si
Parpadeo	si

- ✓ **Conclusiones y observaciones.**

  Aunque el comité de gobierno en línea fue creado mediante acto administrativo, el proceso de creación de planes de acción como lo determina el decreto 1151 no es el adecuado.

  Respecto a la información mínima, la Alcaldía Municipal de Tangua cumple con la mayoría de los ítems, sin embargo, algunos de ellos están incompletos o simplemente vacios.

- **Estudio de usabilidad para análisis de la página web de la Alcaldía Municipal de Tangua**

Tabla 67: Evaluación de usabilidad Tangua

20%		**1. Usabilidad**	**7**	**1,4819**
	40%	**1.1 Comprensibilidad Global del Sitio**	**6,458**	**2,5833**
		1.1.1 Esquema de Organización Global	**7,667**	
		1.1.1.1 Mapa del Sitio	8	
		1.1.1.2 Índice Global (por Temas, etc.)	7	
		1.1.1.3 Tabla de Contenidos	8	
		1.1.2 Calidad en el Sistema de Etiquetado	**4,5**	
		1.1.2.1 Etiquetado Textual	8	
		1.1.2.2 Etiquetado con Iconos	1	
		1.1.3 Página Principal	**5,667**	
		1.1.3.1 Navegabilidad de la página principal	7	
		1.1.3.2 Impacto de la página principal	4,333	
		1.1.3.2.1 La página principal refleja la idea del sitio	6	
		1.1.3.2.2 La página principal deja claro que puedo hacer en el sitio	6	
		1.1.3.2.3 La página principal se ve bien al deshabilitar las imágenes	1	
		1.1.4 Consistencia de la navegación	**8**	
	10%	**1.2 Mecanismos de Ayuda y Retroalimentación en línea**	**8**	**0,75**
		1.2.1 Calidad de la Ayuda	**9**	
		1.2.1.1 Ayuda Explicatoria acerca del sitio	8	
		1.2.1.2 Ayuda de la Búsqueda	10	
		1.2.2 Indicador de Ultima Actualización	**10**	
		1.2.2.1 Global (de todo el sitio Web)	10	
		1.2.2.2 Restringido (subsitio o página)	10	
		1.2.2.3 Por noticias (Solo ultimas noticias)	10	
		1.2.3 Directorio de Enlaces	**10**	
		1.2.3.1 Enlaces a sitios de Interés	10	
		1.2.3.2 Enlaces a asociaciones de interés	10	
		1.2.4 Facilidad FAQ	**1**	
	10%	**1.3 Aspectos de Interfaces y Estéticos**	**7,167**	**0,7167**
		1.3.1 Cohesividad al Agrupar los Objetos de Control Principales	**6**	
		1.3.2 Permanencia y Estabilidad en la Presentación de los Controles Principales	**8,667**	
		1.3.2.1 Permanencia de Controles Directos	10	
		1.3.2.2 Permanencia de Controles Indirectos	8	
		1.3.2.3 Estabilidad	8	

Tabla 67: Evaluación de usabilidad Tangua (Continuación)

		1.3.3 Preferencia Estética	**7**	
		1.3.4 Uniformidad en el Estilo del sitio	**7**	
	10%	**1.4 Misceláneas**	**8,333**	**0,8333**
		1.4.1 Soporte a Lenguaje Extranjero	**5**	
		1.4.2 Descarga de contenidos	**10**	
		1.4.2.1 Descarga de contenidos	10	
		1.4.3 Intrusión publicitaria	**10**	
	15%	**1.5 Usabilidad de los Textos**	10	**15%**
		1.5.1 Textos adaptados para la Web	**10**	
		1.5.1.1 Textos breves	10	
		1.5.1.3 Estilo de escritura conciso	10	
	15%	**1.6 Clasificación de la información**	5	**0,75**
		1.6.1 Categorías	5	
		1.6.1.1 Claridad de las categorías	5	
		1.6.1.2 Cohesión de las categorías	5	
10%		**2. Accesibilidad**	**8,083**	**0,8083**
	70%	**2.1 Accesibilidad para usuarios con discapacidades**	**4,25**	**2,975**
		2.1.1 Discapacidades visuales	**3,5**	
		2.1.1.1 Posibilidad de modificar el tamaño de las fuentes	1	
		2.1.1.2 Combinaciones de color (para usuarios con ceguera al color)	5	
		2.1.1.3 Markup claro para poder ser leído por un lector de pantalla	7	
		2.1.1.4 Etiquetas ALT en todas las imágenes	1	
		2.1.2 Discapacidades auditivas	**5**	
	15%	**2.2 Acceso a navegadores no gráficos**	**10**	**1,5**
	15%	**2.3 Acceso Multidispositivo**	**10**	**1,5**
15%		**3. Funcionalidad**	**6,75**	**1,0125**
	50%	**3.1 Aspectos de Búsqueda**	**6,5**	**3,25**
		3.1.1 Mecanismo de Búsqueda en el Sitio	**3**	
		3.1.1.1 Búsqueda Restringida (por secciones)	1	
		3.1.1.2 Búsqueda Global	5	
		3.1.2 Búsqueda siempre disponible	**10**	
	50%	**3.2 Aspectos de Navegación y Exploración**	**7**	**3,5**
		3.2.1 Navegabilidad Local (de subsitio)	**7,5**	
		3.2.1.1 Nivel de Interconexión	7	
		3.2.1.2 Orientación	8	
		3.2.1.2.1 Indicador del Camino	8	
		3.2.1.2.2 Etiqueta de la Posición Actual	8	
		3.2.2 Navegabilidad Global	**10**	
		3.2.2.1 Acoplamiento entre Subsitios	10	
		3.2.3 Objetos de Control Navegacional	**7,5**	

Tabla 67: Evaluación de usabilidad Tangua (Continuación)

		3.2.3.2 Nivel de Desplazamiento	7,5	
		3.2.3.2.1 Desplazamiento Vertical	5	
		3.2.3.2.2 Desplazamiento Horizontal	10	
		3.2.4 Predicción Navegacional	**4**	
		3.2.4.1 Enlace con Título (enlace con texto explicatorio)	7	
		3.2.4.2 Calidad de la Frase del Enlace	1	
		3.2.5 Funciones Misceláneas y Específicas del Dominio	**6**	
40%		**4 Contenidos**	**5,538**	**2,2153**
	50%	**4.1 Información Institucional**	**5,233**	**2,6167**
		4.1.1 Información sobre el municipio	**6**	
		4.1.2 Presupuesto y finanzas	**4**	
		4.1.2.1 Presupuesto en vigencia	7	
		4.1.1.2 Presupuestos anteriores	1	
		4.1.3 Información sobre la organización de la entidad	**4,5**	
		4.1.3.1 Mecanismos de control interno	6	
		4.1.3.2 mecanismos de control externo	3	
		4.1.4 Valores institucionales	**7,333**	
		4.1.4.1 Misión y Visión	10	
		4.1.4.2 Reglamentos	5	
		4.1.4.3 Historia de la Entidad	7	
		4.1.5 Información sobre la contratación realizada por la entidad	4,333	
		4.1.5.1 Contratación de mínima cuantía	1	
		4.1.5.2 Contratos publicados en el Portal Único de Contratación	5	
		4.1.5.3 medios de Participación ciudadana	7	
	20%	**4.2 Información sobre la dirección de la entidad**	**7**	**1,4**
		4.2.1 hoja de vida del Alcalde	**8**	
		4.2.1.1 Plan de gobierno	10	
		4.2.1.2 Formación	5	
		4.2.2 Información de contacto	**6**	
		4.2.2.1 Dirección	**10**	
		4.2.2.2 Teléfono	5	
		4.2.2.3 Mail	3	
	10%	**4.4 Información sobre los dependencias**	**6,25**	**0,625**
		4.4.1 Objetivos	**6**	
		4.4.2 Contenidos	**7**	
		4.4.3 Evaluación	**5**	
		4.4.4 Funciones	**7**	
		4,4,5 Funcionarios		
	10%	**4.5 Información de contacto de la Institución**	**5,208**	**0,5208**
		4.5.1 Ubicación	**5,667**	
		4.5.1.1 Como llegar (transportes, distancias, etc.)	5	
		4.5.1.2 Mapa geográfico	6	

Tabla 67: Evaluación de usabilidad Tangua (Continuación)

		4.5.1.3 Mapa interno	6	
		4.5.2 Contacto con responsables y asesores	4,75	
		4.5.2.1 Nombre	6	
		4.5.2.2 Correo	3	
		4.5,2.3 Teléfono	5	
		4.5.2.4 Fax	5	
	10%	4.6 Información para empleados nuevos	4	
		4.6.1 manuales de Funciones	10	
		4.6.2 Codigo de Etica	1	
		4.6.3 Reglamento	1	
7.5%		5. Confiabilidad	8,593	0,64444
	50%	5.1 Ausencia de Deficiencias y Errores	8,778	4,3889
		5.1.1 Errores de Enlaces	10	
		5.1.1.1 Enlaces Rotos	10	
		5.1.1.2 Enlaces Inválidos	10	
		5.1.1.3 Enlaces no Implementados	10	
		5.1.2 Errores o Deficiencias Varias	6,333	
		5.1.2.1 Deficiencias o cualidades ausentes debido a diferentes navegadores	10	
		5.1.2.2 Nodos Web Muertos (sin enlaces de retorno)	8	
		5.1.2.3 Nodos Destinos (inesperadamente) en Construcción	1	
		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 Actualización periódica de la información	7	1,75

7.5%		6. Eficiencia	4,9	0,3675
	60%	6.1 Accesibilidad de Información	3,75	2,25
		6.1.1 Soporte a Versión sólo Texto	2	
		6.1.2 Legibilidad al desactivar la Propiedad Imagen del Browser	5,5	
		6.1.2.1 Imagen con Título	6	
		6.1.2.2 Legibilidad Global	5	
	20%	6.2 Rendimiento	8,5	2
	20%	6.3 Tiempo de descarga	8,5	1,7

- **Informe de evaluación de usabilidad**

  El fin de este trabajo es proponer un modelo de evaluación de usabilidad para entidades públicas como son las alcaldías municipales.

  Uno de los objetivo principales es la evaluación de la usabilidad del sitio, pero también se tendrán en cuanta los contenidos de esta.

  Los aspectos que se tienen en cuenta en la evaluación de usabilidad de la página web son:

  - ✓ Usabilidad: La usabilidad evalúa aspectos referentes a la facilidad de uso del portal web.

  - ✓ Accesibilidad: En esta sección se evalúa que tan amigable es el acceso al sitio en ambientes diferentes al normal. (Navegadores no gráficos, acceso a discapacitados).

  - ✓ Funcionalidad: Aquí se evalúa la funcionalidad del portal web, teniendo en cuenta la búsqueda, navegación y exploración.

  - ✓ Contenidos: Es de gran importancia evaluar los contenidos del portal web, en este caso centraremos nuestra atención en los contenidos referentes a la institución que estamos evaluando. La evaluación permitirá verificar si la información publicada es de importancia para la comunidad o los entes de control.

    Este es el criterio de mayor peso en la evaluación, dado que es el aspecto fundamental y diferencial del sitio: este no es un sitio de venta, comercial, es un portal web del estado y su información debe ser clara, verdadera, de carácter público, y verificable.

  - ✓ Confiabilidad: El usuario del portal web debe sentir una sensación de confiabilidad, debe existir ausencia de errores, la utilización de estándares y la existencia de vínculos externos a entidades de prestigio.

  - ✓ Eficiencia: Aquí evaluaremos lo que se refiere a la eficiencia del sitio, la accesibilidad de la información, rendimiento y tiempo de descarga.

  Los criterios para la evaluación que se tuvieron en cuenta fueron:

  - ✓ Cada uno de los parámetros se califica de 1 a 10 puntos

- ✓ Los parámetros que no apliquen no se califican y no cuentan en la evaluación final.

- ✓ En los “parámetros hoja”, se indica la calificación sobre 10.

- ✓ En los “parámetros padre”, se indica la media de sus hijos y el valor después de realizar la ponderación del punto.

Teniendo en cuenta los aspectos y criterios mencionados anteriormente la calificación de la página en cuanto a la evaluación de usabilidad es de 6,5301 de 10 posibles

- ✓ **Inconsistencia y errores del sitio evaluado.**

  Existen vínculos que no contiene información desorientando al usuario (figura 22 y figura 23).

Figura 22: Vínculos sin información

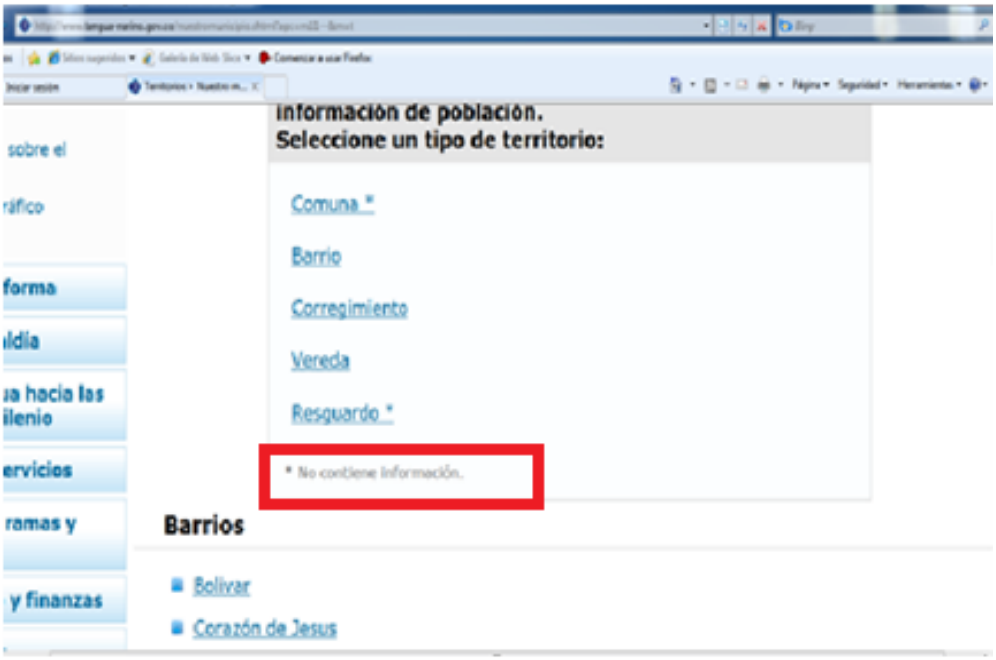


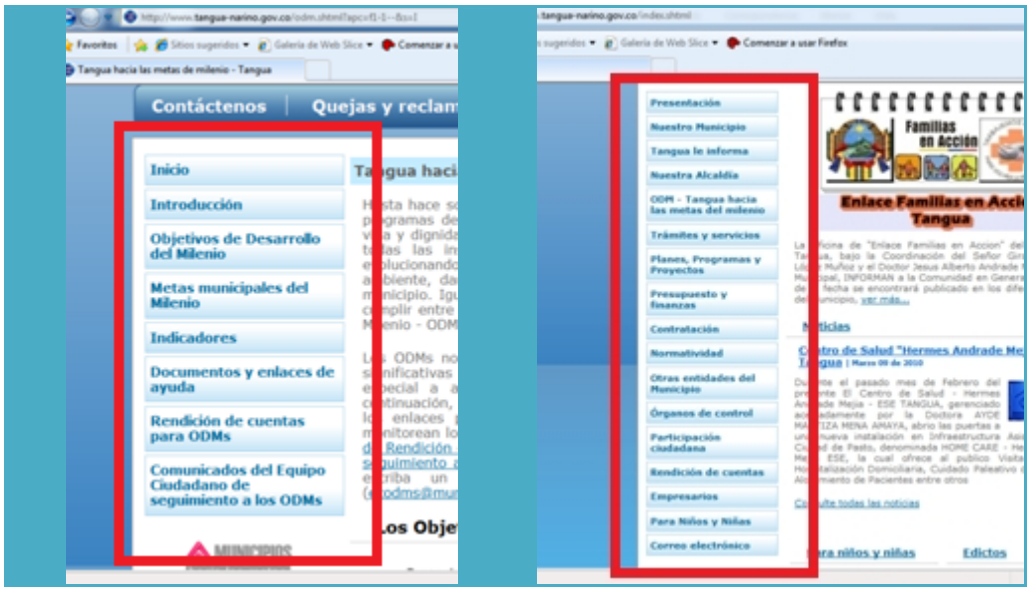
Figura 23: Vínculos sin información 2

Existen atajos descritos por etiquetas ALT para acceder a los menús pero estos no funcionan (figura 24).

Figura 24: Etiquetas ALT

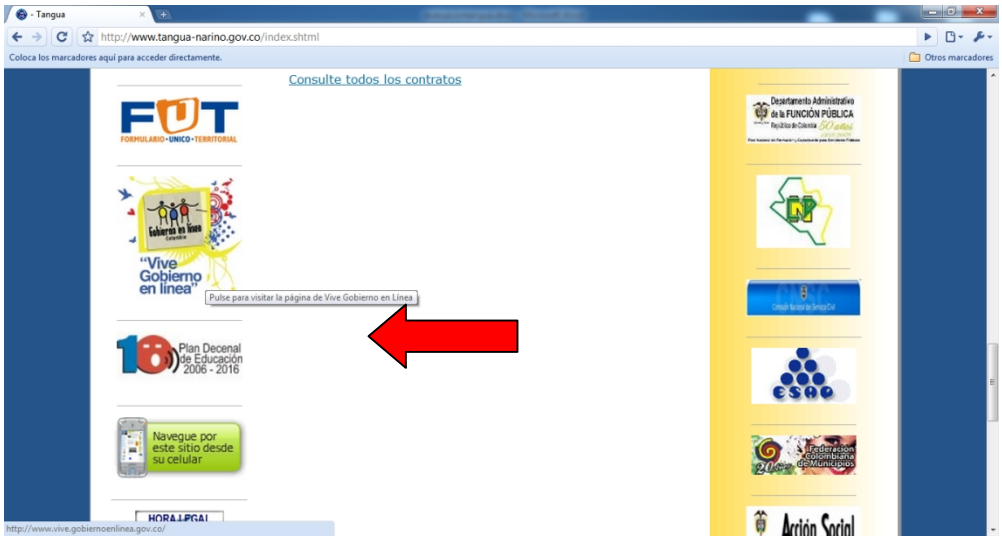
Cambio de menú principal al ingresar a metas del milenio desorientando al usuario (figura 25).

Figura 25: Cambio de menú



Se produce el efecto llamado “mistery meat navigation” por vincent flanders en, lo cual hace que no se pueda saber que hacer cada botón hasta posar el mouse sobre él (figura 26).

Figura 26: Mistery meat navigation



Presentación de la página sin imágenes (figura 27).

Figura 27: Sin imágenes

Existe información que no está citada, ni referenciada, violando los derechos de autor (figura 28).

Figura 28: Sin referenciación

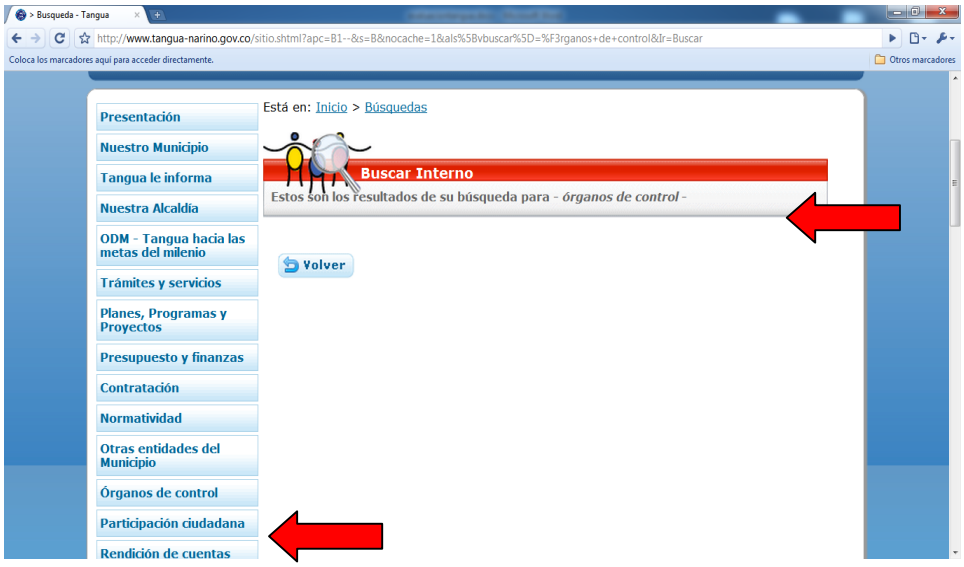

Nuestros derechos y deb...
http://www.tangua-narino.gov.co/paraaprender.shtml?apc=j1-1--&x=1809191
Coloca los marcadores aquí para acceder directamente.
Otros marcadores
Servicios
Noticias
Eventos
Para aprender
Otros sitios relacionados
Nuestros derechos y deberes
Pisarrón
Juegos
Comunícate con la alcaldía
Nuestros derechos y deberes
Nuestros derechos y deberes
Todos los niños y niñas tenemos derecho a
1. "Debemos respetar a nuestros semejantes, sin importar su sexo, nivel socioeconómico, religión, nacionalidad o sus impedimentos físicos y mentales."
2. "Debemos respetar a nuestros padres, maestros y a todas las personas, pues entre todos nos ayudan a encontrar el camino que conduce de la infancia a la vida adulta."
3. "Debemos aprender a respetar las opiniones y costumbres de los demás, aunque no sean iguales a las nuestras."
4. "Debemos respetar las leyes que rigen la sociedad, tener buena conducta en la escuela y portarnos bien en casa."
5. "Debemos respetarnos a nosotros mismos. Nuestro cuerpo, nuestro pensamiento y nuestros sentimientos son lo más importante que tenemos."
6."Debemos hablar siempre con la verdad y cumplir lo que prometemos."
7. "Debemos respetar y cuidar el medio ambiente."
8. "Debemos respetar nuestra patria. Ella nos da alimento, hogar, educación y todo lo que tenemos. En nuestras manos está convertirnos en buenos ciudadanos que hagan de nuestro país del que todos estemos orgullosos."
Normas básicas de seguridad para los niños en INTERNET
1ª. No des nunca información personal sobre ti, tu colegio o tu casa. No envíes fotografías sin el permiso de sus padres.
2ª. No respondas nunca a mensajes o tablones de anuncios en los que se incluyan mensajes agresivos, obscenos, amenazantes o que te hagan sentir mal.
3ª. Mucho cuidado cuando alguien te ofrezca algo por nada en Internet, y te de una dirección a la que acercarte a por un regalo. Si asistes debe ser con tus padres.
4ª. Cuando recibas o encuentres una información que te haga sentir incómodo/a díselo inmediatamente a tus padres.
5ª. No quedes con nadie desconocido sin el permiso de tus padres y sin su presencia.
6ª. Recuerda que la gente que navega por internet no siempre es lo que parece, porque no puedes verles ni oirles. Por ejemplo : cuando alguien te está diciendo por Internet que es una niña de 12 años, puede ser un señor de 45.
7ª. Conoce a tus amigos de internet de la misma forma que conoces a tus otros amigos. No les permitas cosas que no les permitirías a los que tienes ahora.
Fecha de última actualización: Marzo 02 de 2009

La presentación de la página principal cambia en las páginas interiores (figura 29).

Figura 29: Cambio de interfaz

La búsqueda de la página no tiene una funcionalidad óptima, no presenta algunos resultados existentes, además no permite restringir las búsquedas (figura 30).

Figura 30: Búsqueda

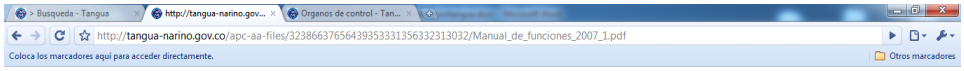


La opción de descargar archivos desorienta al usuario ya que abre el archivo en el mismo explorador y al cerrar este se cierra el explorador sacando al usuario del portal web (figura 31).

Figura 31: Descarga de archivos

Existen vínculos los cuales al dar click no presentan información (figura 32).

Figura 32: Vínculos sin funcionalidad

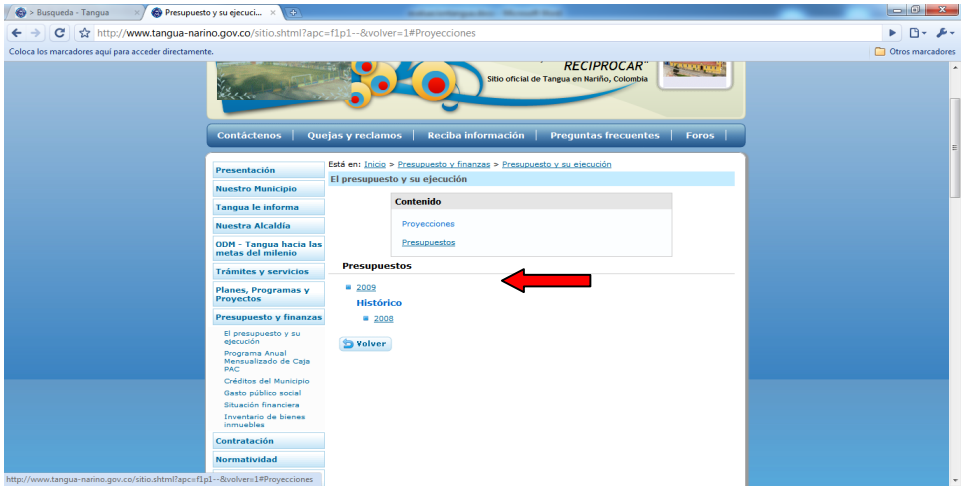


La Información publicada es incompleta (figura 33).

Figura 33: Información incompleta

Enlaces rotos no llevan a ninguna parte (figura 34).

Figura 34: Enlaces rotos

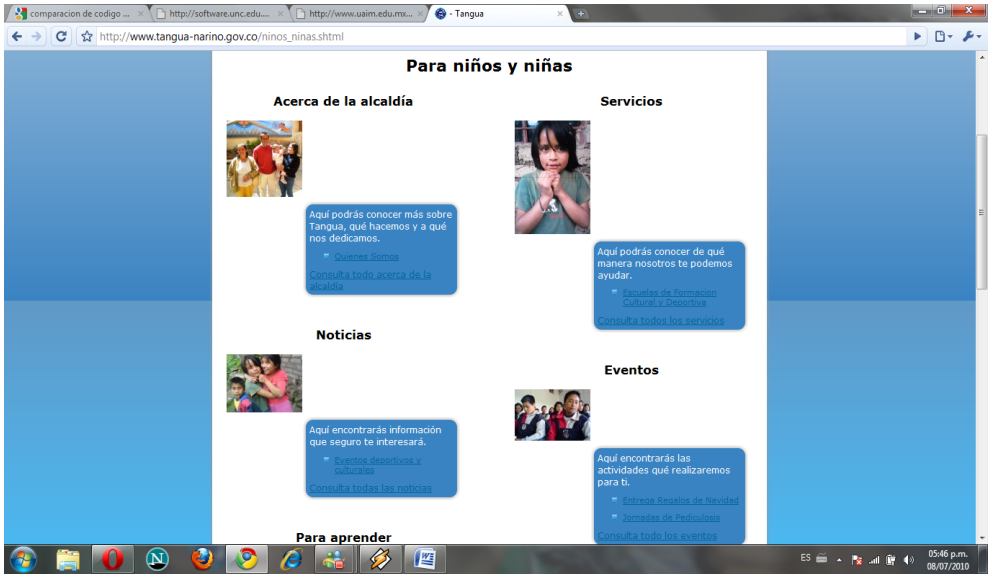


Se entrega Información incompleta a la ciudadanía (figura 35).

Figura 35: Información a la ciudadanía

El contraste entre fondo y textos no presenta legibilidad al momento de leer la información (figura 36).

Figura 36: Contraste



- **Evaluación del Decreto 1151 para la Alcaldía Municipal de Yacuanquer**

  ✓ **Fase Preliminar**

Tabla 68: Comité de Gobierno en Línea Yacuanquer

COMITÉ DE GOBIERNO EN LINEA	
Característica	**Cumple (Sí/No)**
El comité de gobierno en línea fue conformado	**sí**
Existe un líder de gobierno en línea	**sí**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de planeación	**sí**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de atención al ciudadano	**sí**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de comunicaciones y/o prensa	**sí**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de control interno	**sí**
Fueron incluidos en el comité el jefe o delegado de la oficina responsable de sistemas y/o informática	**sí**
Se invitaron a los representantes de la dirección de gestión de calidad y el jefe de responsable de jurídica	**no**

Tabla 69: Plan de acción Yacuanquer

PLAN DE ACCIÓN 2009 - 2012 (plazo de entrega: primera semana de noviembre de 2008)	
Característica	**Cumple (Sí/No)**
Se generó un plan de acción con el fin de garantizar la implementación de la Estrategia de Gobierno En Línea	**No**
El plan tiene un marco estratégico en el que se identifiquen las políticas de la entidad y su relación con los objetivos de la Estrategia de Gobierno En Línea	**No**
Un diagnóstico del estado de la entidad a la fecha de elaboración del Plan, con respecto al cumplimiento de los diferentes criterios en cada una de las Fases de Gobierno En Línea	**No**
Un esquema que identifique las acciones necesarias para el cumplimiento de cada uno de los criterios en cada fase y su plazo de implementación	**No**
Un marco de acción, que comprenda la identificación de los proyectos tendientes a garantizar la implementación de la Estrategia de Gobierno En Línea el cumplimiento de los objetivos misionales de cada entidad	**No**
Una ficha por cada proyecto que se desarrollará, identificando los objetivos, las actividades, los beneficios e impacto, las metas, los recursos señalando las líneas presupuestales que respaldan dichos recursos, los responsables y los plazos de ejecución.	**No**

✓ **Información mínima a publicar**

Tabla 70: Sitio web principal Yacuanquer

PARA EL SITIO WEB PRINCIPAL		
Característica	**Cumple (Sí/No)**	**Observaciones**
Acerca de la entidad		
Información básica en el Portal del Estado Colombiano	**Sí**	
Misión y Visión	**Sí**	
Objetivos y funciones	**Sí**	La información está incompleta, los objetivos de la entidad como tal no están.
Organigrama	**No**	
Localización Física (Incluyendo todas las sedes o sucursales)	**Sí**	
Teléfonos y/o líneas gratuítas y fax.	**Sí**	
Correo electrónico de contacto	**Sí**	
Horarios y días de atención al público	**Sí**	
Directorio de los funcionarios principales	**Sí**	No se puede confrontar con el organigrama, Se utilizan correos comerciales
Directorio de las entidades	**No**	Presenta sólo un listado. No se muestra información de cada entidad
Directorio de agremiaciones y asociaciones	**Sí**	
Normatividad		
Leyes/Ordenanzas/acuerdos	**Sí**	No cumplen con el plazo de 5 días para su publicación en la página
Decretos	**Sí**	
Resoluciones y/u otros actos administrativos de carácter general	**Sí**	
Proyectos de normatividad		

Tabla 70: Sitio web principal Yacuanquer (Continuación)

Presupuesto		
Característica	**Cumple (Sí/No)**	**Observaciones**
Presupuesto aprobado en ejercicio	**No**	
Información histórica de presupuestos	**No**	
Políticas, planes, programas y proyectos institucionales		
Políticas, planes y/o líneas estratégicas	**Sí**	
Programas, proyectos en ejecución	**Sí**	Falta información
Contacto con dependencia responsable	**Sí**	
Trámites y Servicios		
Listado de trámites	**Sí**	
Listado de servicios	**Sí**	
Contratación		
Información sobre la contratación	**No**	
Control y rendición de cuentas		
Entes de control que vigilan a la entidad	**Sí**	Sólo cumple para la personería de Yacuanquer, para la contraloría y contaduría falta especificar la forma en la cual un particular puede comunicar una irregularidad.
Informes de gestión	**No**	No se publican los informes de gestión del período en vigencia y el histórico del período inmediatamente anterior, presentados a la Contraloría, al Concejo, etc., así como tampoco el informe semestral de Gobierno En Línea y demás entes que vigilan la gestión de la entidad.
Metas, indicadores de desempeño y/o gestión, y resultados	**No**	no presenta ninguno

Tabla 70: Sitio web principal Yacuanquer (Continuación)

Plan de mejoramiento	**No**	
Servicios de Información		
Característica	**Cumple (Sí/No)**	**Observaciones**
Información para niños	**Sí**	
Preguntas y respuestas frecuentes	**No**	no presenta ítems
Boletines y publicaciones	**No**	no presenta información
Noticias	**Sí**	la redacción no cumple con los estándares de una noticia y son difíciles de entender
Calendario de actividades	**Si**	
Glosario	**Si**	
Política de privacidad y condiciones de uso	**Si**	

Tabla 71: Navegación sitio principal Yacuanquer

PARA EL SITIO WEB PRINCIPAL	
Característica	**Cumple (Sí/No)**
Acerca de la entidad	
Identidad Visual	Si
Enlace al portal del Estado Colombiano	Si
Fecha de última actualización	Si
División de los contenidos	Si
Uso de colores	si
Uso de marcos	si
Manejo de Vínculos	si
Estándares de Funcionalidad	
Mapa del sitio	si
Acceso a la página de inicio	si
Acceso al menú principal	si
Estándares Técnicos	
Nombre del dominio	si
Marcación y/o Etiquetado	si
Tiempo de despliegue	
Parpadeo	No

- ✓ **Conclusiones y observaciones.**

  Aunque el comité de gobierno en línea fue creado mediante acto administrativo, el proceso de creación de planes de acción como lo determina el decreto 1151 no es el adecuado.

  Respecto a la información mínima, la Alcaldía Municipal de Tangua cumple con la mayoría de los ítems, sin embargo, algunos de ellos están incompletos o simplemente vacios.

  La falta de indicadores de gestión e informes de gestión compromete el cumplimiento de la entidad con el principio de transparencia. Además se han incumplido con algunas metas impuestas por la norma.

- **Estudio de usabilidad para análisis de la página web de la Alcaldía Municipal de Tangua**

Tabla 72: Evaluación de usabilidad Yacuanquer

20%		1. Usabilidad	6	1,1447
	40%	1.1 Comprensibilidad Global del Sitio	6,9583	2,7833
		1.1.1 Esquema de Organización Global	8,6667	
		1.1.1.1 Mapa del Sitio	9	
		1.1.1.2 Índice Global (por Temas, etc.)	8	
		1.1.1.3 Tabla de Contenidos	9	
		1.1.2 Calidad en el Sistema de Etiquetado	4	
		1.1.2.1 Etiquetado Textual	7	
		1.1.2.2 Etiquetado con Iconos	1	
		1.1.3 Página Principal	6,1667	
		1.1.3.1 Navegabilidad de la página principal	7	
		1.1.3.2 Impacto de la página principal	5,3333	
		1.1.3.2.1 La página principal refleja la idea del sitio	8	
		1.1.3.2.2 La página principal deja claro que puedo hacer en el sitio	6	
		1.1.3.2.3 La página principal se ve bien al deshabilitar las imágenes	2	
		1.1.4 Consistencia de la navegación	9	
	10%	1.2 Mecanismos de Ayuda y Retroalimentación en línea	6,3333	0,6333
		1.2.1 Calidad de la Ayuda	8,5	
		1.2.1.1 Ayuda Explicatoria acerca del sitio	8	
		1.2.1.2 Ayuda de la Búsqueda	9	
		1.2.2 Indicador de Ultima Actualización	7,3333	
		1.2.2.1 Global (de todo el sitio Web)	10	
		1.2.2.2 Restringido (subsitio o página)	2	
		1.2.2.3 Por noticias (Solo ultimas noticias)	10	
		1.2.3 Directorio de Enlaces	8,5	
		1.2.3.1 Enlaces a sitios de Interes	8	
		1.2.3.2 Enlaces a asociaciones de interes	9	
		1.2.4 Facilidad FAQ	1	
	10%	1.3 Aspectos de Interfaces y Estéticos	7,0667	0,7067
		1.3.1 Cohesividad al Agrupar los Objetos de Control Principales	9	
		1.3.2 Permanencia y Estabilidad en la Presentación de los Controles Principales	9,3333	
		1.3.2.1 Permanencia de Controles Directos	10	
		1.3.2.2 Permanencia de Controles Indirectos	9	
		1.3.2.3 Estabilidad	9	

Tabla 72: Evaluación de usabilidad Yacuanquer (Continuación)

		1.3.3 Preferencia Estética	**8**	
		1.3.4 Uniformidad en el Estilo del sitio	**9**	
	10%	**1.4 Misceláneas**	**7**	**0,7**
		1.4.1 Soporte a Lenguaje Extranjero	**5**	
		1.4.2 Descarga de contenidos	**8**	
		1.4.2.1 Descarga de contenidos	8	
		1.4.3 Intrusión publicitaria	**8**	
	15%	**1.5 Usabilidad de los Textos**	**6,5**	**15%**
		1.5.1 Textos adaptados para la Web	**6,5**	
		1.5.1.1 Textos breves	7	
		1.5.1.3 Estilo de escritura conciso	6	
	15%	**1.6 Clasificación de la información**	**5**	**0,75**
		1.6.1 Categorías	**5**	
		1.6.1.1 Claridad de las categorías	4	
		1.6.1.2 Cohesión de las categorías	6	
10%		**2. Accesibilidad**	**2,3625**	**0,2363**
	70%	**2.1 Accesibilidad para usuarios con discapacidades**	**3,375**	**2,3625**
		2.1.1 Discapacidades visuales	**6,75**	
		2.1.1.1 Posibilidad de modificar el tamaño de las fuentes	1	
		2.1.1.2 Combinaciones de color (para usuarios con ceguera al color)	7	
		2.1.1.3 Markup claro para poder ser leído por un lector de pantalla	9	
		2.1.1.4 Etiquetas ALT en todas las imágenes	10	
		2.1.2 Discapacidades auditivas	**0**	
	15%	**2.2 Acceso a navegadores no gráficos**		**0**
	15%	**2.3 Acceso Multidispositivo**		**0**
15%		**3. Funcionalidad**	**8,425**	**1,2638**
	50%	**3.1 Aspectos de Búsqueda**	**7,75**	**3,875**
		3.1.1 Mecanismo de Búsqueda en el Sitio	**5,5**	
		3.1.1.1 Búsqueda Restringida (por secciones)	1	
		3.1.1.2 Búsqueda Global	10	
		3.1.2 Búsqueda siempre disponible	**10**	
	50%	**3.2 Aspectos de Navegación y Exploración**	**9,1**	**4,55**
		3.2.1 Navegabilidad Local (de subsitio)	**8,5**	
		3.2.1.1 Nivel de Interconexión	9	
		3.2.1.2 Orientación	8	
		3.2.1.2.1 Indicador del Camino	7	
		3.2.1.2.2 Etiqueta de la Posición Actual	9	
		3.2.2 Navegabilidad Global	**8**	
		3.2.2.1 Acoplamiento entre Subsitios	8	
		3.2.3 Objetos de Control Navegacional	**10**	

Tabla 72: Evaluación de usabilidad Yacuanquer (Continuación)

		3.2.3.1 Nivel de Desplazamiento	10	
		3.2.3.1.1 Desplazamiento Vertical	10	
		3.2.3.1.2 Desplazamiento Horizontal	N/A	
		3.2.4 Predicción Navegacional	**9**	
		3.2.4.1 Enlace con Título (enlace con texto explicatorio)	10	
		3.2.4.2 Calidad de la Frase del Enlace	8	
		3.2.5 Funciones Misceláneas y Específicas del Dominio	**10**	
40%		**4 Contenidos**	**5,2517**	**2,1007**
	50%	**4.1 Información Institucional**	**3,8**	**1,9**
		4.1.1 Información sobre el municipio	**5**	
		4.1.2 Presupuesto y finanzas	**1**	
		4.1.2.1 Presupuesto en vigencia	1	
		4.1.1.2 Presupuestos anteriores	1	
		4.1.3 Información sobre la organización de la entidad	**4**	
		4.1.3.1 Mecanismos de control interno	3	
		4.1.3.2 mecanismos de control externo	5	
		4.1.4 Valores institucionales	**5,6667**	
		4.1.4.1 Misión y Visión	10	
		4.1.4.2 Reglamentos	5	
		4.1.4.3 Historia de la Entidad	2	
		4.1.5 Información sobre la contratación realizada por la entidad	3,3333	
		4.1.5.1 Contratación de mínima cuantía	1	
		4.1.5.2 Contratos publicados en el Portal Único de Contratación	3	
		4.1.5.3 medios de Participación ciudadana	6	
	20%	**4.2 Información sobre la dirección de la entidad**	**8**	**1,6**
		4.2.1 hoja de vida del Alcalde	**8**	
		4.2.1.1 Plan de gobierno	10	
		4.2.1.2 Formación	5	
		4.2.2 Información de contacto	**8**	
		4.2.2.1 Dirección	**10**	
		4.2.2.2 Teléfono	6	
		4.2.2.3 Mail	8	
	10%	**4.4 Información sobre los dependencias**	**6,25**	**0,625**
		4.4.1 Objetivos	**6**	
		4.4.2 Contenidos	**6**	
		4.4.3 Evaluación	**5**	
		4.4.4 Funciones	**8**	
		4,4,5 Funcionarios	**8**	
	10%	**4.5 Información de contacto de la Institución**	**3,875**	**0,3875**
		4.5.1 Ubicación	**4**	
		4.5.1.1 Como llegar (transportes, distancias, etc.)	5	

Tabla 72: Evaluación de usabilidad Yacuanquer (Continuación)

		4.5.1.2 Mapa geográfico	6	
		4.5.1.3 Mapa interno	**1**	
		4.5.2 Contacto con responsables / asesores	**3,75**	
		4.5.2.1 Nombre	6	
		4.5.2.2 Correo	3	
		4.5,2.3 Teléfono	5	
		4.5.2.4 Fax	**1**	
	10%	**4.6 Información para empleados nuevos**	**4,3333**	
		4.6.1 manuales de Funciones	**10**	
		4.6.2 Código de Ética	**1**	
		4.6.3 Reglamento	**2**	
7.5%		**5. Confiabilidad**	**8,6296**	**0,6472**
	50%	**5.1 Ausencia de Deficiencias y Errores**	**8,8889**	**4,4444**
		5.1.1 Errores de Enlaces	**8,6667**	
		5.1.1.1 Enlaces Rotos	10	
		5.1.1.2 Enlaces Inválidos	10	
		5.1.1.3 Enlaces no Implementados	6	
		5.1.2 Errores o Deficiencias Varias	**8**	
		5.1.2.1 Deficiencias o cualidades ausentes debido a diferentes navegadores	9	
		5.1.2.2 Nodos Web Muertos (sin enlaces de retorno)	10	
		5.1.2.3 Nodos Destinos (inesperadamente) en Construcción	5	
		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 Actualización periódica de la información**	**7**	**1,75**

7.5%		**6. Eficiencia**	**4,9**	**0,3675**
	60%	**6.1 Accesibilidad de Información**	**9,5**	**5,7**
		6.1.1 Soporte a Versión sólo Texto	**N/A**	
		6.1.2 Legibilidad al desactivar la Propiedad Imagen del Browser	**9,5**	
		6.1.2.1 Imagen con Título	10	
		6.1.2.2 Legibilidad Global	9	
	20%	**6.2 Rendimiento**	**8**	**2**
	20%	**6.3 Tiempo de descarga**	**7**	**1,4**

- **Informe de evaluación de usabilidad**

  El fin de este trabajo es proponer un modelo de evaluación de usabilidad para entidades públicas como son las alcaldías municipales.

  Uno de los objetivo principales es la evaluación de la usabilidad del sitio, pero también se tendrán en cuanta los contenidos de esta.

  Los aspectos que se tienen en cuenta en la evaluación de usabilidad de la página web son:

  - ✓ Usabilidad: La usabilidad evalúa aspectos referentes a la facilidad de uso del portal web.

  - ✓ Accesibilidad: En esta sección se evalúa que tan amigable es el acceso al sitio en ambientes diferentes al normal. (Navegadores no gráficos, acceso a discapacitados).

  - ✓ Funcionalidad: Aquí se evalúa la funcionalidad del portal web, teniendo en cuenta la búsqueda, navegación y exploración.

  - ✓ Contenidos: Es de gran importancia evaluar los contenidos del portal web, en este caso centraremos nuestra atención en los contenidos referentes a la institución que estamos evaluando. La evaluación permitirá verificar si la información publicada es de importancia para la comunidad o los entes de control.

    Este es el criterio de mayor peso en la evaluación, dado que es el aspecto fundamental y diferencial del sitio: este no es un sitio de venta, comercial, es un portal web del estado y su información debe ser clara, verdadera, de carácter público, y verificable.

  - ✓ Confiabilidad: El usuario del portal web debe sentir una sensación de confiabilidad, debe existir ausencia de errores, la utilización de estándares y la existencia de vínculos externos a entidades de prestigio.

  - ✓ Eficiencia: Aquí evaluaremos lo que se refiere a la eficiencia del sitio, la accesibilidad de la información, rendimiento y tiempo de descarga.

  Los criterios para la evaluación que se tuvieron en cuenta fueron:

  - ✓ Cada uno de los parámetros se califica de 1 a 10 puntos

- ✓ Los parámetros que no apliquen no se califican y no cuentan en la evaluación final.

- ✓ En los “parámetros hoja”, se indica la calificación sobre 10.

- ✓ En los “parámetros padre”, se indica la media de sus hijos y el valor después de realizar la ponderación del punto.

Teniendo en cuenta lo presentado en el apartado anterior la calificación de la página en cuanto a la evaluación de usabilidad es de 5,7601 de 10 posibles.

- ✓ **Inconsistencia y errores del sitio evaluado.**

  Los Atajos de navegación que pudieran servir en algunos casos de accesibilidad para personas con necesidades especiales no funcionan. Debería ponerse en funcionamiento o quitar el texto ALT que ofrece al usuario la función de atajo (figura 37).

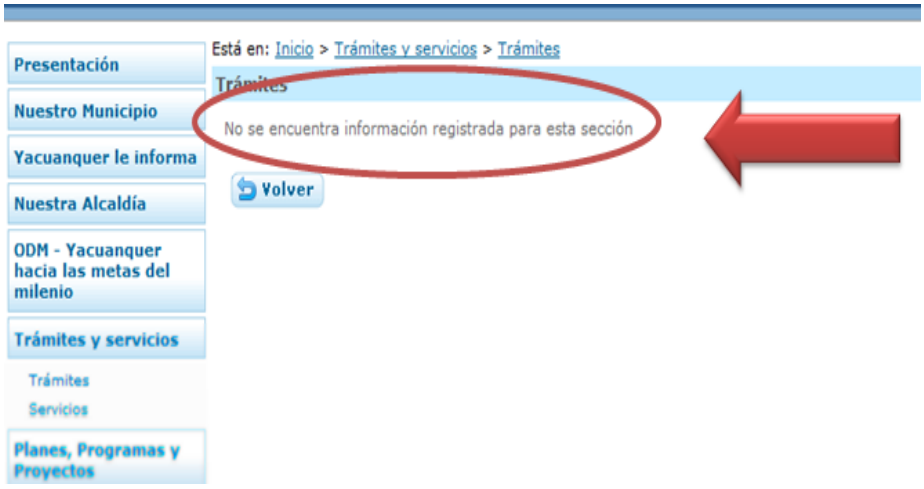
Figura 37: Atajos ALT

Existe un cambio de menú al seleccionar la opción de ODM Metas del Milenio. Esto desorienta al usuario, y no permite acceder a las demás opciones, debería presentarse en forma de submenú como las demás opciones (figura 38).

Figura 38: Cambio de menú

Existen secciones sin contenido. Estas deberían ser eliminadas de los menús ó actualizar su contenido (figura 39).

Figura 39: Sección sin contenido



Se produce el efecto llamado “Mistery Meat Navigation” por *Vincent Flanders* , lo cual hace que no se pueda saber que hace cada botón hasta posar el mouse sobre él. Además estos iconos carecen de etiquetas (figura 40).

Figura 40: Mistery meat navigation

Algunos contenidos se presentan incompletos y aunque los enlaces están en la página, estos no funcionan (figura 41).

Figura 41: Contenidos incompletos

La interfaz de la página cambia cuando se accede a una de las opciones del menú (figura 42).

Figura 42: Cambio de interfaz

Algunos enlaces existen sin ninguna información y al hacer click no funcionan, ni se visualiza alguna información de error o del enlace vacio (figura 43).

Figura 43: Enlaces sin información

Si se deshabilitan las imágenes, algunas partes se vuelven de difícil navegación (figura 44).

Figura 44: Difícil navegación

La búsqueda no se puede refinar o restringir ni antes ni después de la misma, además la línea del mapa del sitio muestra “Está en: Inicio” cuando en realidad está en los resultados de la página (figura 45).

Figura 45: Búsqueda

4. CONCLUSIONES

- COBIT es un marco de referencia para la gerencia y directivos que permite realizar una adecuada administración de los recursos TI, COBIT está enfocado en el control y por esto, se transforma también en una valiosa herramienta para el auditor de TI; su organización por diferentes dominios y procesos facilita el enfoque del auditor o la gerencia en un área en particular, ya que la nueva versión de COBIT ha sufrido una evaluación y mejora respecto a la convergencia y relaciones de los objetivos de control con otras áreas de la empresa y otros procesos.

- El decreto 1151 de 2008 acerca de las estrategias de gobierno en línea es un claro compromiso con las tecnologías de información, se reconoce su necesidad y utilidad, además busca involucrar a la ciudadanía en la vigilancia y control de los procesos de las entidades estatales en un intento de garantizar el principio de transparencia; sin embargo si las entidades no aprecian realmente los recursos de TI y lo ven como algo que simplemente deben cumplir, no se logrará un avance significativo en este campo.

- Atendiendo estos retos la Contraloría Departamental de Nariño pretendió con el trabajo realizado, generar conciencia por la adecuada gestión de los recursos de TI, su importancia y la dependencia de los objetivos y metas de la entidad.

- Tras realizar la auditoría el grupo auditor logró observar que la conciencia de la importancia de los recursos de TI en las entidades evaluadas surge sólo cuando se presentan inconvenientes o riesgos reales contra los recursos de TI, y sólo entonces se logra ver el gran grado de dependencia de los procesos hacia las TI.

- Gracias a COBIT se logró establecer la relevancia de la seguridad de TI dentro de los procesos de gerencia de TI, pues tras la evaluación y conclusiones del trabajo de auditoría a la seguridad informática de las entidades, el grupo auditor determinó que ésta es uno de los ejes y pilares de la gerencia de TI.

- Además el grupo auditor descubrió que existe casi un total desinterés por parte de las entidades hacía los procedimientos que incluyen las tecnologías de información, como son por ejemplo, algunos procedimientos en los que se involucran los sistemas SICE y SECOP. Estos muchas veces son omitidos deliberadamente, a pesar de que se cuenta con conocimiento de la norma y está dentro de los objetivos y metas de las entidades públicas. Observando esta situación desde una perspectiva diferente a la que encierra el marco legal

y las sanciones que pueden caer sobre las entidades y funcionarios, esto representa una advertencia no sólo para las entidades de control, sino también para las entidades educativas, los ingenieros de sistemas, pues nos propone una problemática general, enfrentándonos a nuevos retos, la búsqueda de soluciones más efectivas para el usuario común y su fatiga tecnológica.

- De similar forma que en el párrafo anterior sucede para el cumplimiento con las estrategias de gobierno en línea. Para la mayoría de las entidades estatales, tales como las auditadas, el Ministerio de las tecnologías de información y comunicaciones provee un gestor de contenido que no requiere desarrollo alguno por parte de las alcaldías y así estas se limiten a gestionar el contenido sin perder tiempo en el desarrollo o diseño de sus sitios web, además provee servicio de internet para aquellas entidades que no lo tengan, todo esto para garantizar el uso de las TIC por parte de las mismas para un mejor servicio a la comunidad. Aún así las entidades presentan un total desinterés por la gestión de estos contenidos, comprometiendo sus objetivos, el principio de transparencia, las políticas del gobierno y el progreso de los municipios.

RECOMENDACIONES

- Se recomienda establecer políticas que garanticen la realización periódica de auditorías a los diferentes departamentos.

- Se recomienda realizar procesos de capacitación a los usuarios de los diferentes procesos, en donde se puedan apropiarse de las tecnologías de información y la seguridad informática.

- Se recomienda realizar pruebas de seguridad lógica de la red, en relación al mapeo de puertos, sniffer propios de redes inalámbricas, pruebas por inyección de SQL para acceso a la base de datos, e intrusiones al servidor, con el fin de encontrar las debilidades y poder sugerir e implementar los controles respectivos.

BIBLIOGRAFIA

APPIGNANESI L., CASTAÑO P. et al. Software de Auditoria [en línea], s.l., s.f., s.f., disponible en: http://cs.uns.edu.ar/~mc/Auditoria/downloads/Exposiciones/Software%20de%20%20auditoria%20(handouts).pdf

AuditSoftware, TopCAATs [en línea], s.l., s.f., s.f., disponible en: http://www.auditsoftware.net/documents/TopCAATs.pdf

BRITO JIMMY, "Análisis y aprovechamiento de los sistemas de información para una eficiente auditoría y control de gestión" [en línea], Guayaquil (Ecuador), 2004, s.f., disponible en: http://www.dspace.espol.edu.ec/bitstream/123456789/4158/1/6686.pdf

CALVO-MANZANO J., CARRILLO J, CUEVAS G, SAN FELIU T, TOVAR E, "Introducción a la Auditoría Informática", Facultad de Informática de Madrid, 2002.

ECHENIQUE GARCIA José A., Auditoría en informática, 2ª Ed., Mc GRAW-HILL, México D.F., 2005.

Expansión, Control Interno, Auditoría y Seguridad Informática. Tomos II-IV, 1996.

Grupo Eniac, ACL Business Assurance Analytics [en línea], s.l., s.f., s.f., disponible en: 3. http://www.eniac.com/productos/download/acl_ge.pdf.

IT Governance Institute, Cobit 4.1 [en línea], Rolling Meadows (IL, EEUU), 2007, s.f., disponible en: http://www.itsor.net/pdf/ITSOR_COBIT_Brochure_VE.pdf.

Newman Byron, ACL Edición de Desktop/Red [en línea], s.l., s.f., s.f., disponible en: http://www.datasec-soft.com/archivos/sp/folletos/acl/ACL_Desktop_Data_Sheet-es.pdf

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.
PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995.

L. ZAVARO Y C. MARTÍNEZ, Auditoría informática, las técnicas de auditoría asistidas por computadora (CAAT).

GOVINDAN, MARSHAL, JOHN Y. PICARD, Manifest on Information Systems Control and Management, McGraw-Hill, 1990.

ANEXOS

Los anexos están dispuestos en un DVD. Estos constan de gran parte de la información obtenida en la investigación, evidencias y el material de base para los hallazgos e informes de este documento.

Existen tres carpetas:

- Alcaldía Municipal de Tangua. Consta de la información para la Alcaldía Municipal de Tangua.

- Alcaldía Municipal de Yacuanquer. Consta de la información para la Alcaldía Municipal de Yacuanquer.

- Material de consulta. Consta del material de consulta para este documento así como de algunas leyes y decretos relevantes.

Las carpetas referentes a las entidades constan de otra división más que comprenden:

- Cuestionarios. Contiene los Cuestionarios diseñados y distribuidos según el proceso COBIT.

- Evaluación de la página. Contiene la evaluación de la página presente en este documento.

- Evidencias. Parte de las evidencias (videos) obtenidas en las alcaldías.

- Hallazgos. Contienen los hallazgos presentados en este informe distribuidos según su proceso COBIT.

- Material para la contraloría. Contiene material relevante para la contraloría, la información que se solicitó e informes presentados con la evidencia restante (imágenes y pantallazos).