OCCEFS

Manual de Mejores prácticas para la Auditoría Informática.

JUNIO 2014

INDICE

INTRODUCCIÓN

La utilización de las tecnologías de información y comunicaciones (TICs) en el procesamiento de datos y la modernización de los procesos mediante el uso de la tecnología, hacen que se optimicen los recursos en la prestación de los diferentes servicios públicos que se ofrecen a los usuarios. Adicional a los beneficios que ofrecen las TICs, se ha fomentado la aparición de nuevas formas de “Corrupción”; por lo tanto, se vuelve imprescindible controlar y fiscalizar de manera especializada la administración de los recursos tecnológicos, razón por la cual, las Entidades Fiscalizadoras Superiores (EFS) deben estar preparadas para los desafíos que implica fiscalizar las adquisiciones de bienes y servicios que se relacionan a las TICs.

La Auditoría a las Tecnologías de la información y comunicaciones (TIC), día a día se incrementa, debido a que los usurarios hacen uso de dispositivos electrónicos para consultar, enviar, pagar impuestos y realizar cualquier tipo de transacción electrónica, sin la necesidad de estar presente físicamente en un sitio especifico de las entidades públicas para llevar a cabo la transacción, por tal motivo la auditoría a las TICs requiere que el auditor se vea en la necesidad de poseer habilidades y conocimientos técnicos informáticos para una adecuada planeación de la auditoría, que les permita determinar el alcance, tamaño y características del área de Tecnología de la Información y Comunicación dentro de la entidad, la infraestructura tecnológica con la que cuentan, procesos claves sistematizados, procesos de seguridad de la información, adopción e implementación de estándares internacionales relacionados con seguridad de la información, objetivos de control interno y servicios que apoyan los procesos claves de la entidad.

Por lo tanto, es necesario el desarrollo e implementación de una guía que sirva de estándar para unificar criterios en materia de auditoría informática para la administración y fiscalización tecnológica de las entidades públicas, que permita además la identificación de los posibles riesgos que presente el proceso de la auditoria a las TICs, con el objetivo de que la capacidad de controlar y fiscalizar se mantenga al mismo ritmo en que avanzan las Tecnologías de información y comunicaciones.

OBJETIVOS DE LA GUÍA

1) Elaborar una metodología para el desarrollo de auditorías de Gestión a las Tecnologías de Información y Comunicaciones.

2) Proveer a los auditores de TICs lineamientos para la realización de una auditoría a las tecnologías de información y comunicaciones que coadyuven a la buena gestión de la disponibilidad de los servicios sistematizados prestado a la población en general, con el uso de la tecnología proporcionando seguridad, disponibilidad, confiabilidad y oportunidad de la información procesada y resguardada dentro de la entidad

MARCO LEGAL Y NORMATIVO PARA LA EJECUCION DE LAS AUDITORIAS.

1. Previsiones contenidas en la Constitución de la Republica de El Salvador.

CAPITULO V
CORTE DE CUENTAS DE LA REPUBLICA

Art. 195.- La fiscalización de la Hacienda Pública en general y de la ejecución del Presupuesto en particular, estará a cargo de un organismo independiente del Órgano Ejecutivo, que se denominará Corte de Cuentas de la República, y que tendrá las siguientes atribuciones:

1a. Vigilar la recaudación, la custodia, el compromiso y la erogación de los fondos públicos; así como la liquidación de impuestos, tasas, derechos y demás contribuciones, cuando la ley lo determine.

2a. Aprobar toda salida de fondos del Tesoro Público, de acuerdo con el presupuesto; intervenir en todo acto que de manera directa o indirecta

afecte al Tesoro Público o al Patrimonio del Estado, y refrendar los actos y contratos relativos a la deuda pública.

3a. Vigilar, inspeccionar y glosar las cuentas de los funcionarios y empleados que administren o manejen bienes públicos, y conocer de los juicios a que den lugar dichas cuentas.

4a. Fiscalizar la gestión económica de las Instituciones y empresas estatales de carácter autónomo y de las entidades que se costeen con fondos del Erario o que reciban subvención o subsidio del mismo.

5a. Examinar la cuenta que sobre la gestión de la Hacienda Pública rinda el Órgano Ejecutivo a la Asamblea, e informar a ésta del resultado de su examen.

6a. Dictar los reglamentos necesarios para el cumplimiento de sus atribuciones.

7a. Informar por escrito al Presidente de la República, a la Asamblea Legislativa y a los respectivos superiores jerárquicos de las irregularidades relevantes comprobadas a cualquier funcionario o empleado público en el manejo de bienes y fondos sujetos a fiscalización.

8a. Velar porque se hagan efectivas las deudas a favor del Estado y Municipios.

9a. Ejercer las demás funciones que las leyes le señalen.

Las atribuciones 2ª y 4ª las efectuará de una manera adecuada a la naturaleza y fines del organismo de que se trate, de acuerdo con lo que al respecto determine la Ley; y podrá actuar previamente a solicitud del organismo fiscalizado, del superior jerárquico de éste o de oficio cuando lo considere necesario.

Art. 196.- La Corte de Cuentas de la República, para el cumplimiento de sus funciones jurisdiccionales, se dividirá en una Cámara de Segunda Instancia y en las Cámaras de Primera Instancia que establezca la ley.

La Cámara de Segunda Instancia estará formada por el Presidente de la Corte y dos Magistrados, cuyo número podrá ser aumentado por la ley.

Estos funcionarios serán elegidos para un período de tres años, podrán ser reelegidos, y no podrán ser separados de sus cargos sino por causa justa, mediante resolución de la Asamblea Legislativa. La Cámara de Segunda Instancia nombrará, removerá, concederá licencias y aceptará renuncias a los Jueces de las Cámaras de Primera Instancia.

Una ley especial regulará el funcionamiento, jurisdicción, competencia y régimen administrativo de la Corte de Cuentas y Cámaras de la misma.

Art. 197.- Siempre que un acto sometido a conocimiento de la Corte de Cuentas de la República viole a su juicio alguna ley o reglamento en vigor, ha de advertirlo así a los funcionarios que en el ejercicio de sus funciones legales se lo comuniquen, y el acto de que se trate quedará en suspenso.

El Órgano Ejecutivo puede ratificar el acto, total o parcialmente, siempre que lo considere legal, por medio de resolución razonada tomada en Consejo de Ministros y comunicada por escrito al Presidente de la Corte. Tal resolución deberá ser publicada en el Diario Oficial.

La ratificación debidamente comunicada, hará cesar la suspensión del acto, siempre que las observaciones de la Corte de Cuentas no consistan en falta o insuficiencia de crédito presupuesto al cual debe aplicarse un gasto, pues, en tal caso, la suspensión debe mantenerse hasta que la deficiencia de crédito haya sido llenada.

Art. 198.- El Presidente y los Magistrados de la Corte de Cuentas deberán ser salvadoreños por nacimiento, mayores de treinta años, de honradez y competencia notorias; estar en el ejercicio de los derechos de ciudadano y haberlo estado en los tres años anteriores a su elección.

Art. 199.- El Presidente de la Corte de Cuentas rendirá anualmente a la Asamblea Legislativa un informe detallado y documentado de las labores de la Corte. Esta obligación deberá cumplirse dentro de los tres meses siguientes a la terminación del año fiscal.

El incumplimiento de esta obligación se considera como causa justa de destitución.

2. Previsiones Contenidas en la Ley que Regula el Ejercicio de la Corte de Cuentas de la Republica.

LEY DE LA CORTE DE CUENTAS DE LA REPUBLICA.
TITULO I ORGANISMO SUPERIOR DE CONTROL
CAPITULO 1 CORTE DE CUENTAS DE LA REPUBLICA

Finalidad de la Corte

Art. 1.- La Corte de Cuentas de la República, que en esta Ley podrá denominarse "La Corte", es el organismo encargado de fiscalizar, en su doble aspecto administrativo y jurisdiccional, la Hacienda Pública en general y la ejecución del Presupuesto en particular, así como de la gestión económica de las entidades a que se refiere la atribución cuarta del Artículo 195 y los incisos 4 y 5 del Artículo 207 de la Constitución de la República.

Independencia

Art. 2.- La Corte es independiente del Órgano Ejecutivo, en lo funcional, administrativo y presupuestario.

La independencia de la Corte se fundamenta en su carácter técnico, y sus actuaciones son totalmente independientes de cualquier interés particular.

Elaborará el proyecto de su presupuesto y lo remitirá al Órgano Ejecutivo para su inclusión en el Presupuesto General del Estado.

Los ajustes que la Asamblea Legislativa considere necesario introducir al referido proyecto lo hará en consulta con el Presidente de la Corte y el Ministro de Hacienda.

Jurisdicción de la Corte

Art. 3.- Están sujetas a la fiscalización y control de la Corte todas las entidades y organismos del sector público y sus servidores, sin excepción alguna. La jurisdicción de la Corte alcanza también las actividades de entidades, organismos y personas que, no estando comprendidos en el inciso anterior reciban asignaciones, privilegios o participaciones ocasionales de recursos públicos. En este caso el control se aplicará únicamente al ejercicio en que se haya efectuado el aporte o concesión y al monto de los mismos.

En el caso de entidades que estén sujetas a la vigilancia de la Superintendencia del Sistema Financiero o de la Superintendencia de Sociedades y Empresas Mercantiles, el control de la Corte podrá realizarse en coordinación con aquellas.

Competencia

Art. 4.- Es competencia de la Corte el control externo posterior de la gestión pública. La Corte podrá actuar preventivamente, a solicitud del organismo fiscalizado, del superior jerárquico de éste o de oficio cuando lo considere necesario.

La actuación preventiva consistirá en la formulación de recomendaciones de auditoría tendientes a evitar el cometimiento de irregularidades.

Atribuciones y Funciones

Art. 5.- La Corte, tendrá las atribuciones y funciones que le señala el Artículo 195 de la Constitución y, en base a la atribución novena del mismo Artículo las siguientes:

1) Practicar auditoría externa financiera y operacional o de gestión a las entidades y organismos que administren recursos del Estado;

2) Dictar las políticas, normas técnicas y demás disposiciones para:

   a) La práctica del control interno;

   b) La práctica de la auditoría gubernamental, interna o externa, financiera y operacional o de gestión;

   c) La determinación de las responsabilidades de que se trata esta Ley;

3) Examinar y evaluar los resultados alcanzados, la legalidad, eficiencia, efectividad y economía de la gestión pública;

4) Examinar y evaluar los sistemas operativos, de administración e información y las técnicas y procedimientos de control interno incorporados en ellos, como responsabilidad gerencial de cada ente público;

5) Evaluar las unidades de auditoría interna de las entidades y organismos del sector público;

6) Sin perjuicio de su responsabilidad y obligación de control, la Corte podrá: Calificar, seleccionar y contratar firmas privadas para sustentar sus auditorías en los casos que considere necesario;

7) Evaluar el trabajo de auditoría externa, efectuado por otras personas en las entidades y organismos del Estado;

8) Proporcionar asesoría técnica a las entidades y organismos del sector público, con respecto a la implantación del Sistema de Control y materias que le competen, de acuerdo con esta Ley;

9) Capacitar a los servidores de las entidades y organismos del sector público, en las materias de que es responsable; normar y coordinar la capacitación;

10) Requerir a funcionarios y empleados que hagan efectivo el cobro de las obligaciones a favor de las entidades y organismos del sector público, y que éstos cancelen las propias;

11) Declarar la responsabilidad administrativa o patrimonial, o ambas en su caso;

12) Exigir al responsable principal, por la vía administrativa el reintegro inmediato de cualquier recurso financiero indebidamente desembolsado;

13) Solicitar a la Fiscalía General de la República que proceda contra los funcionarios o empleados, y sus fiadores cuando los créditos a favor de entidades u organismos de que trata esta Ley, procedan de los faltantes de dinero, valores o bienes a cargo de dichos funcionarios o empleados;

14) Solicitar a quien corresponda la aplicación de sanciones o aplicarlas si fuera el caso y que se hagan efectivas las responsabilidades que le corresponden determinar y establecer;

15) Examinar la cuenta que sobre la gestión de la Hacienda Pública rinda el Órgano Ejecutivo a la Asamblea Legislativa e informar a ésta del resultado de su examen en un plazo no mayor de cuatro meses.

Para tal efecto la Corte practicará auditoría a los estados financieros del Órgano Ejecutivo, pronunciándose sobre la presentación y contenidos de los mismos, señalando las ilegalidades e irregularidades cometidas y toda situación que no permita a los diferentes Órganos del Estado apreciar con claridad los resultados de determinado ejercicio financiero;

16) Exigir de las entidades, organismos y servidores del sector público cualquier información o documentación que considere necesaria para el ejercicio de sus funciones; igual obligación tendrán los particulares, que por cualquier causa, tuvieren que suministrar datos o informes para aclarar situaciones.

Al servidor público o persona particular que incumpliere lo ordenado en el inciso anterior, se le impondrá una multa sin perjuicio de cualquier otra sanción a que se hiciere acreedor, todo de conformidad con la Ley;

17) Dictar las disposiciones reglamentarias, las políticas, normas técnicas y procedimientos para el ejercicio de las funciones administrativas confiadas a la Corte, y vigilar su cumplimiento;

18) Dictar el Reglamento Orgánico-Funcional de la Corte que establecerá la estructura, las funciones, responsabilidades y atribuciones de sus dependencias;

19) Ejercer las demás facultades y atribuciones establecidas por las Leyes de la República.

CAPITULO IV
AUDITORIA GUBERNAMENTAL
SECCION I
EJECUCION, CONTENIDO Y CLASES

Art. 30.- La auditoría gubernamental podrá examinar y evaluar en las entidades y organismos del sector público:

1) Las transacciones, registro, informes y estados financieros;

2) La legalidad de las transacciones y el cumplimiento de otras disposiciones;

3) El control interno financiero;

4) La planificación, organización, ejecución y control interno administrativo;

5) La eficiencia, efectividad y economía en el uso de los recursos humanos, ambientales, materiales, financieros y **tecnológicos**;

6) Los resultados de las operaciones y el cumplimiento de objetivos y metas.

En las entidades, organismos y personas a que se refiere el inciso segundo del Art. 3, la auditoría gubernamental examinará el uso de los recursos públicos.

Clases

Art. 31.- La auditoría gubernamental será interna cuando la practiquen las unidades administrativas pertinentes de las entidades y organismos del sector público; y, externa, cuando la realice la Corte o las Firmas Privadas de conformidad con el Artículo 39 de esta Ley; será financiera cuando incluya los aspectos contenidos en los numerales 1),2) y 3) del artículo anterior y, operacional cuando se refiera a alguno de los tres últimos numerales del mismo artículo. El análisis o revisión puntual de cualquiera de los numerales del artículo anterior se denominará Examen Especial.

Personal ejecutor

Art. 32.- La auditoría gubernamental será efectuada por profesionales de nivel superior, legalmente autorizados para ejercer en El Salvador. La clase de auditoría a efectuarse determinará la idoneidad de los conocimientos a exigirse. Los dictámenes sobre estados financieros serán suscritos por contadores públicos inscritos en el Consejo de Vigilancia de la Contaduría Pública y Auditoría.

Comunicación

Art. 33.- En el transcurso del examen, los auditores gubernamentales, mantendrán constante comunicación con los servidores de la entidad u organismo auditado, dándoles oportunidad para que presenten pruebas o evidencias documentadas e información verbal pertinente a los asuntos sometidos a examen.

3. Disposiciones complementarias previstas en el marco legal general y específico de la Corte de Cuentas de la Republica.

Para el uso de la Tecnología y Comunicaciones:

1. **Manual de Auditoria Gubernamental.**
   Disponer de una herramienta que facilite la práctica de Auditoría Gubernamental, por parte de los auditores de la Corte de Cuentas de la República, que en este Manual se denominará “la Corte”, cuando realicen auditorías en las entidades mencionadas en el Art. 3 de la Ley de la Corte.

2. **Normas de Auditoria Gubernamental**
   Que en el ejercicio de la Auditoría Gubernamental, la Corte de Cuentas de la República adoptó las Normas de Auditoría Gubernamental, emitidas por la Oficina de la Contraloría General de los Estados Unidos de América

   Las normas relativas a los requisitos generales y personales del auditor, tienen por objeto regular lo relativo a las aptitudes personales y profesionales que el auditor debe poseer para realizar su trabajo; se relacionan con la capacidad profesional que debe poseer todo auditor gubernamental; con la independencia, confidencialidad y cuidado profesional que debe tener y demostrar al ejecutar sus labores; con la aplicación de controles de calidad.

3. **Normas Técnicas de Control Interno de la Corte de Cuentas de la Republica. (Lo relacionado con la Tecnología de la Información y Comunicaciones TICs).**
   La presente normativa constituye el marco básico que establece la Corte de Cuentas de la República para el control interno hacia los órganos, instituciones, entidades, sociedades y empresas del sector público. De lo anterior, establece pautas generales que orientan el accionar de las entidades del sector público hacia un adecuado control interno y probidad administrativa, logrando eficiencia, efectividad, economía y transparencia en la gestión que desarrollan.

4. **Políticas Internas de Auditoria Gubernamental**
   Este reglamento contiene las políticas que deberán seguirse para agilizar los procesos de auditoría que realice la Corte de Cuentas, con el fin de garantizar el derecho de defensa tanto de servidores públicos, como de particulares que estén involucrados.

5. **Normas Técnicas de Control Interno Específicas de las entidades del Estado, aprobadas por la Corte de Cuentas de la Republica. (Lo relacionado con la Tecnología de la Información y Comunicaciones TICs).**

6. **Ley de Administración Financiera, REGISTRO CONTABLE Registro de Intangibles.**

7. **Manual Técnico del SAFI numeral C.2.5 NORMAS SOBRE INVERSIONES EN ACTIVOS INTANGIBLES.**
   Este manual tiene como objeto Proporcionar a las instituciones un instrumento Técnico Normativo para la aplicación del Sistema de Administración Integrado.

8. **Ley de Adquisiciones y Contrataciones. (desde la perspectiva adquisición y Contratación de Servicios y Equipo relacionado con la Tecnología de la Información y Comunicaciones TICs)**
   La presente Ley tiene por objeto regular las adquisiciones y contrataciones de obras, bienes y servicios, que deben celebrar las instituciones de la Administración Pública para el cumplimiento de sus fines; entendiéndose para los alcances y efectos de ésta, que la regulación comprende además los procesos enunciados en esta Ley.

9. **Ley de la Propiedad Intelectual en sus artículos 32 y 33; 85-D y E, y 89**

   La presente ley tiene por objeto asegurar una protección suficiente y efectiva de la propiedad intelectual, estableciendo las bases que la promuevan, fomenten y protejan.
   Esta ley comprende el derecho de autor, los derechos conexos y la propiedad industrial en lo relativo a invenciones, modelos de utilidad, diseños industriales y secretos industriales o comerciales y datos de prueba.

10. **Código Penal. (CAPITULO VII DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL VIOLACION DE DERECHOS DE AUTOR Y DERECHOS CONEXOS) Artículos 226, 227, 227 A y B**
    El presente Código tiene como finalidad primordial orientar nuestra normativa penal dentro de una concepción garantista, de alta efectividad para evitar la violencia social y delincuencial que vive nuestro país.

11. REGLAMENTO RELATIVO AL REGISTRO E INVENTARIO DE LAS LICENCIAS DE PROGRAMAS DE ORDENADOR (Decreto Ejecutivo Nº: 17 Fecha:20/02/2006 D. Oficial: 35 Tomo: 370 Publicación DO: 02/20/2006

El presente Reglamento tiene por objeto regular la adquisición y administración de los programas de ordenador para el uso de los organismos gubernamentales a nivel central.

Jurisprudencia Administrativa

1. Ley de Servicio Civil.
2. Ley de Asuetos, Vacaciones y Licencias de los Empleados Públicos.
3. Ley de Salarios para el año 2010, 2011 y 2012.
4. Disposiciones Generales del Presupuesto.
5. Reglamento General de Viáticos.
6. Reglamento para el uso de vehículos Nacionales, Reglamento para el uso y control de combustible, emitidos por la Corte de Cuentas de la República.
7. Ley Sobre el Enriquecimiento Ilícito de Funcionarios y Empleados Públicos.
8. Ley de Ética Gubernamental.
9. Ley del Servicio Civil.
10. Manual de Procesos para la Ejecución Presupuestaria.
11. Catálogo y tratamiento General de Cuentas del Sector Público.

Estructura y Funciones del Sistema de Control del Estado y el Gobierno.

El estado de El Salvador se compone por tres poderes, los cuales son:
Órgano Ejecutivo, Legislativo y Judicial.

Acciones dirigidas al fortalecimiento Institucional del Estado y de la sociedad civil.

La Corte de Cuentas de la Republica cuenta con un departamento de participación ciudadana (Denuncia) y Dirección de Auditoria Siete, encargada de efectuar las auditorias de gestión a las tecnologías de información y comunicaciones así como los exámenes especiales relacionados.

El Gobierno de El salvador constituyo el Instituto de Acceso de la Información y la ley de acceso a la Información Pública, creada mediante decreto legislativo No. 534 y entro en vigencia el 6 de mayo de 2012 y tiene como propósito lo siguiente:

Objeto

Art. 1. La presente ley tiene como objeto garantizar el derecho de acceso de toda persona a la información pública, a fin de contribuir con la transparencia de las actuaciones de las instituciones del Estado.

Derecho de acceso a la información pública

Art. 2. Toda persona tiene derecho a solicitar y recibir información generada, administrada o en poder de las instituciones públicas y demás entes obligados de manera oportuna y veraz, sin sustentar interés o motivación alguna.

Fines

Art. 3. Son fines de esta ley:

a. Facilitar a toda persona el derecho de acceso a la información pública mediante procedimientos sencillos y expeditos.
b. Propiciar la transparencia de la gestión pública mediante la difusión de la información que generen los entes obligados.
c. Impulsar la rendición de cuentas de las instituciones y dependencias públicas.
d. Promoción de la participación ciudadana en el control de la gestión gubernamental y la fiscalización ciudadana al ejercicio de la función pública.
e. Modernizar la organización de la información pública.
f. Promover la eficiencia de las instituciones públicas.
g. ***Promover el uso de las tecnologías de la información y comunicación y la implementación del gobierno electrónico.***
h. Proteger los datos personales en posesión de los entes obligados y garantizar su exactitud.
i. Contribuir a la prevención y combate de la corrupción.
j. Fomentar la cultura de transparencia.
k. Facilitar la participación de los ciudadanos en los procesos de toma de decisiones concernientes a los asuntos públicos.

Además se tiene un tribunal de Ética Gubernamental, y la ley de ética gubernamental.

Objeto de la Ley

Art. 1- La presente ley tiene por objeto normar y promover el desempeño ético en la función pública; salvaguardar el patrimonio del Estado, prevenir, detectar y sancionar la corrupción de los servidores públicos, que utilicen los cargos o empleos para enriquecerse ilícitamente o cometer otros actos de corrupción.

Ámbito de Aplicación

Art. 2- Esta Ley se aplica a todos los servidores públicos, permanentes o temporales, remunerados o ad-honorem, que ejerzan su cargo por elección, nombramiento o contrato emanado de la autoridad competente, que presten servicio en cualquier entidad estatal o municipal, dentro o fuera del territorio de la República.

El ejercicio de toda profesión, actividad empresarial, arte o industria es compatible con el servicio público. Las únicas incompatibilidades son las establecidas específicamente en la Constitución y las leyes.

ANTECEDENTES CORTE DE CUENTAS DE EL SALVADOR

Actualmente las entidades gubernamentales enfrentan riesgos en los controles de acceso a los sistemas de información, bases de datos, administración de servidores, codificación y resguardo de la información, prevención contra virus, malware, correo spam, fraude informático, detección y mitigación de intrusos, firma electrónica y firma digital en documentos electrónicos y rendiciones de cuentas ,entre otros.

La Corte de Cuentas de la República de El Salvador inició la auditoria a las tecnologías de información y comunicaciones el año 2005, con el propósito de evaluar la eficiencia, eficacia, economía y confiabilidad de la administración de los recursos tecnológicos que apoyan a los procesos sistematizados de las entidades públicas. Dicha experiencia nos ha llevado a identificar y definir procedimientos específicos que nos ayudan a planificar y desarrollar la auditoria a las TICs, a través del uso de buenas prácticas basadas en estándares de aceptación mundial

como COBIT e ISO27000, y el uso de las TAAC´s. Entre ellas, herramientas de software para extraer y analizar datos electrónicos, determinación de muestras, Monitoreo de las redes de datos, verificación de atributos de seguridad, integridad y confiabilidad de los sistemas de información y bases de datos, entre otros, a raíz de ello es que proponemos una metodología a seguir para la ejecución de la auditoria a las TICs, que permita verificar objetivamente la administración recursos tecnológicos.

Por esta razón, se hace necesario la implementación de una solución integral en Auditoría a la Gestión de las Tecnologías de Información y Comunicaciones, que garantice la efectividad de los procedimientos a ejecutar.

AUDITORÍA INFORMÁTICA
PANAMÁ

ANTECEDENTES

La Ley 32 de 8 de noviembre de 1984 constituye la Ley Orgánica de la Contraloría General de la República. Algunos artículos de esta Ley han sido modificados por la Ley 67 de 14 de noviembre de 2008.

La Ley Orgánica estipula que la Contraloría General de la República es un organismo estatal independiente de carácter técnico, cuya misión es fiscalizar, regular y controlar los movimientos de los fondos y bienes públicos, y examinar, intervenir y fenecer las cuentas relativas a estos. Las funciones de la Contraloría General se encuentran estipuladas en el Título III Funciones Generales.

Mediante el Decreto Núm. 101 de 22 de mayo de 1991, se crea la Dirección de Auditoría General, cuyas funciones consisten en ejercer el control posterior, a través de auditorías profesionales e independientes, de acuerdo a lo establecido en la Constitución Política y en la Ley Orgánica de la Contraloría General.

Mediante el Decreto Núm. 105-2009-DAG se formaliza la nueva Estructura Orgánica de la Dirección de Auditoría General de la Contraloría General de la República de Panamá. A través de este decreto se cambia el nombre de la Dirección de Auditoría General por Dirección Nacional de Auditoría General (DINAG); y se crea, entre otros, el Departamento Sectorial de Auditoría de Tecnologías de Información y Comunicación (DESATIC).

DESATIC tiene como objetivo fundamental revisar y evaluar, mediante un examen profesional y objetivo, los controles relacionados con los elementos y procesos del ambiente de tecnología de información y comunicaciones (TIC) y los sistemas de información de las entidades del sector público, a fin de verificar el uso, control y protección de sus activos en aras de disponer información confiable, oportuna y segura para una adecuada toma de decisiones.

Este Departamento, aunque adscrito a la Dirección Nacional de Auditoría General (DINAG), también atiende requerimientos de otras direcciones de la Contraloría General de la República como Dirección General de Fiscalización (control previo), Dirección Nacional de Auditoría Interna, Despacho Superior, etc.

ALCANCE

La Guía de procedimientos para la ejecución de la Auditoría a las Tecnologías de Información y Comunicaciones, abarcara los controles generales y específicos TIC's apoyados por recursos tecnológicos, con el propósito de mejorar la efectividad, eficiencia, economía y confidencialidad de la información.

CONTENIDO

Auditoria de Gestión a las Tecnologías de Información y Comunicaciones (TIC)

Para la fiscalización de los recursos Tecnológicos efectuamos la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones. Esta auditoria va más allá de un examen a los controles y operatividad de los elementos de hardware y software de una plataforma tecnológica.

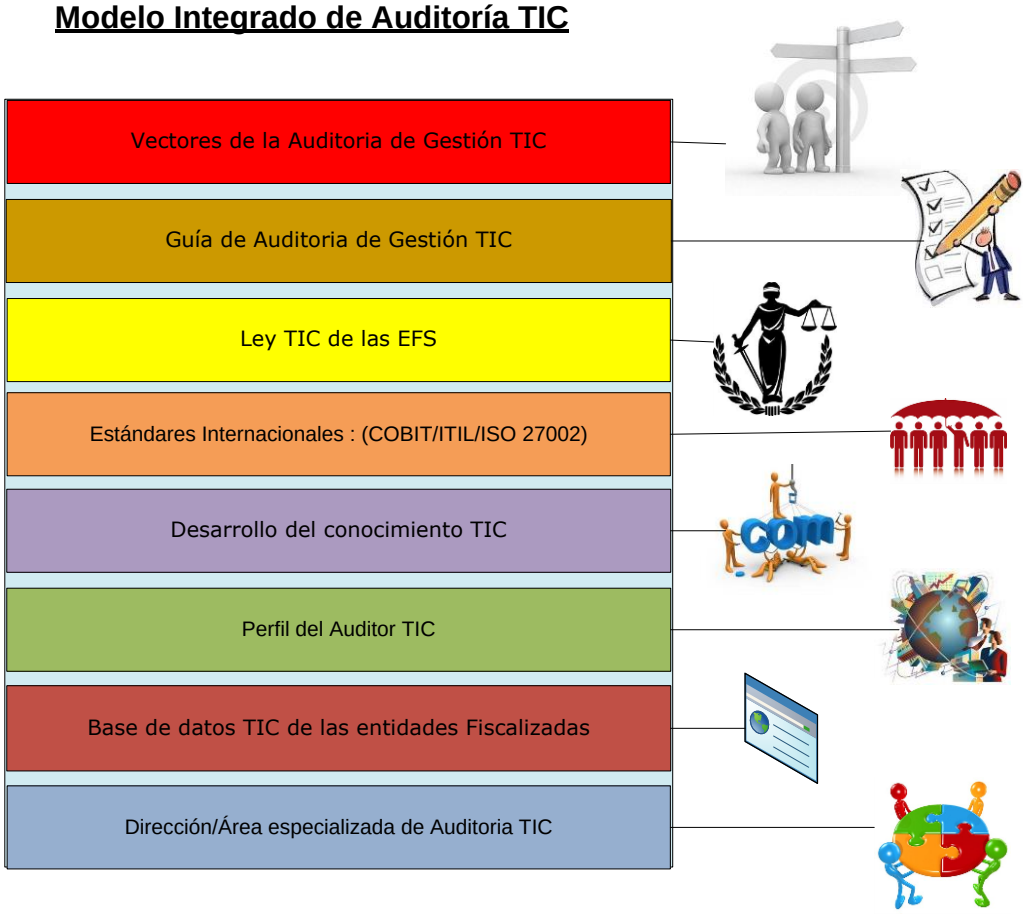
La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones se enfoca desde dos perspectivas:

a) El examen de los elementos (Hardware, software, redes y periféricos) y las técnicas utilizadas en el procesamiento, tratamiento y la transmisión de la información.

b) Como las TIC se encuentran alineadas a la consecución de los objetivos institucionales, en apoyo a la gestión de la organización, mejorando procesos y servicios en función de eficiencia, eficacia, productividad, y economía.

La solución que se presenta en esta guía, establece componentes integrados, que dependen uno del otro para funcionar, interactuando entre sí con el fin de crear un modelo estándar, secuencial y a la vez actualizable en el tiempo, para la ejecución de la auditoría a las tecnologías de la Información y comunicaciones. La cual llamamos "Torre TIC de la Auditoria".

Modelo Integrado de Auditoría TIC



Los componentes que la integran son:

1. Dirección/Área Especializada de Auditoria TIC.
2. Base de Datos TIC de las entidades Fiscalizadas.
3. Perfil del Auditor TIC

4. Desarrollo del conocimiento TIC
5. Estándares Internacionales TIC (COBIT/ITI/ISO27002).
6. Ley/Normativa TIC de las EFS
7. Guía de Auditoría de Gestión TIC
8. Vectores de la auditoria de Gestión TIC

1. **"Dirección/Área Especializada de Auditoria TIC"** Es necesario crear una área de auditoría TIC, para la ejecución de la Auditoría a las Tecnologías de Información y Comunicaciones, como instancia para la planificación, desarrollo, monitoreo y coordinación de los procesos involucrados en la auditoria.

   Facultades de la Unidad especializada de Auditoría TIC.

   - Coordinación de la ejecución de la Auditoría de Gestión a las Tecnologías de Información.
   - Investigación de las nuevas tendencias de gestión de las TIC.
   - Desarrollar e implementar un proyecto de capacitación continua en el área de TIC para sus Auditores.
   - Desarrollar y actualizar las leyes, Normas y políticas de administración TIC de las EFS.
   - Desarrollar una guía o manual de auditoria de gestión TIC.
   - Mantener actualizada la base de datos TIC de las Entidades Fiscalizadas.
   - Asesorar al gobierno en la dirección tecnológica del país.
   - Otros aspectos que las EFS superiores de la región consideren convenientes.

2. "**Base de Datos TIC de las entidades Fiscalizadas**", Es imprescindible que las EFS dedicas a la auditoria cuenten con una base de datos con información de las plataformas tecnológicas y los presupuestos anuales relacionados a las compras de bienes y servicios informáticos de cada entidad sujeta a fiscalización, esto con el fin de efectuar una planeación e integración de los profesionales idóneos para la ejecución de la auditoria.

   Contenido de la información de la base de datos de la Plataforma Tecnológica de las entidades sujetas a fiscalización.

a. Nombre de la Entidad (Dirección y teléfonos de contacto).
b. Nombre de la Máxima Autoridad de la Entidad fiscalizada.
c. Nombre del Gerente/Jefe del área que administra las TIC en la entidad fiscalizada.
d. Estructura organizativa del Área de TIC.
e. Cantidad y características técnicas de las estaciones de trabajo/equipos desktop y laptops.
f. Cantidad y Características Técnicas de Equipos Servidores.
g. Detalle de las características de las redes (LAN, WAN, WiFi) y enlaces de comunicaciones (enlaces propios o outsourcing)
h. Descripción de los dispositivos de seguridad perimetral de la Red institucional.
i. Detalle de los sistemas /aplicativos informáticos.
j. Sistemas operativos.
k. Leguajes de desarrollo.
l. Detalle de las Bases de datos.
m. La información deberá ser actualizada cada año o como mínimo en cada auditoria TIC, efectuada a la entidad fiscalizada.
n. Otros parámetros que podría contener la base de datos TIC, las cuales deberán ser definidas por cada EFS, de acuerdo a sus necesidades de información.

3. "**Perfil del auditor TIC**", La EFS deberá, a través del área o Unidad de Auditoria TIC, definir las capacidades, conocimientos y habilidades que un Auditor de TIC debe poseer, para el ejercicio de la Auditoria, identificando las especialidades a crear, de acuerdo a las características TIC de los entes a fiscalizar.

El perfil del auditor de sistemas es complejo, debido a que tiene que poseer los conocimientos de un auditor "Puro" y un Técnico o profesional en tecnologías de información, con conocimientos sobre:

- Auditoría
- Seguridad TIC
- Gobernabilidad TIC
- Bases de Datos.
- Sistemas Operativos.

- Lenguajes de Programación.
- Redes y comunicaciones.
- Infraestructura de servidores.
- Ingeniería de software.
- **Hacking ético**

Debido a que sería difícil encontrar tantos auditores con el 100% de los conocimientos necesarios para el perfil del auditor TIC. Y es por esto que introducimos dentro de dicho perfil, el concepto de **"Especialización"**.

La EFS deberá, a través del área o Unidad de Auditoria TIC, identificar las especialidades a crear, de acuerdo a las características TIC de las Organizaciones fiscalizadas, el estándar o común denominador de los elementos tecnológicos que integran a las organizaciones Gubernamentales y Privadas, así como de la información de la base de datos TIC descrito en el apartado anterior.

Se ha identificado que una organización que cuenta con infraestructura y servicios de tecnología de información y comunicaciones, posee con al menos una unidad de TIC, o servicios outsourcing, que administran las áreas siguientes:

- Soporte Técnico
- Sistemas o aplicativos informáticos
- Bases de Datos
- Redes y comunicaciones
- Infraestructura de servidores

La unidad de auditoría TIC, deberá definir las especialidades TIC de los auditores con el fin de desarrollar el talento humano enfocado a la especialidad del perfil, de los cuales se proponen los siguientes:

- Auditor TIC especializado en Redes y comunicaciones.
- Auditor TIC especializado en infraestructura de servidores y Sistemas operativos.
- Auditor TIC especializado en ingeniería de Software.
- Auditor TIC especializado en Bases de datos.

- Auditor TIC especializado en Seguridad de la información.

4. "**Desarrollo del conocimiento TIC**" La necesidad de *desarrollar las competencias del talento humano* de nuestro equipo de auditoria, bajo un esquema de "capacitación continua", basada en la especialización, con el fin de cubrir todas las áreas del conocimiento identificadas en el perfil del auditor TIC.

   El profesional en auditoria TIC, debe poseer conocimientos superiores o como mínimo, estar al mismo nivel, que el de los profesionales administradores de las plataformas tecnológicas en las entidades sujetas a fiscalización.

   Esto debido a que la EFS debe generar confianza en sus auditados, de que las personas que los auditan son competentes y "saben lo que hacen".

   En vista de la necesidad de desarrollar el talento humano **"Conocimiento TIC"** de nuestro equipo de auditoria, se recomienda, crear un esquema de **"capacitación continua",** basada en **la especialización**, con el fin de cubrir todas las áreas del conocimiento identificadas en el **perfil del auditor TIC.**

   Así mismo que dicho proyecto de capacitación continúa en TIC incorpore un proceso de investigación, para identificar nuevas tecnologías que requieran de capacitación, para que en el momento en que las entidades públicas las implementen, los auditores TIC tengan la capacidad de auditarlas.

5. "**Estándares internacionales para la auditoría de gestión TIC**", Es importante adoptar las mejores prácticas relacionadas a las TIC, tales como COBIT, ITIL, ISO 27002, para organizar, controlar y asegurar un gobierno eficaz de las actividades de control y ordenamiento de la gestión TIC, así como para la auditoria de las mismas.

   Cuando se dice adoptar las mejores prácticas, no involucra aplicar todos los componentes que posee cada estándar (COBIT, ITIL, ISO 27002, entre otros), si no, enfocar su utilización para que proporcione el mayor

beneficio a la auditoria, y sobre todo que sea adaptada a la realidad tecnológica de cada país.

6. "**Normativa TIC de las EFS**", propone y crear la normativa que establezca los criterios legales y técnicos que deben cumplirse en la gestión TIC, estos basados en estándares de aceptación mundial, así mismo deberá adaptarse a la realidad tecnológica de cada país.

   El contenido de la normativa TIC, deberá ser elaborado, de tal forma que incorpore la normativa de control utilizada por cada EFS y que además integre los estándares de aceptación mundial y mejores prácticas en la administración TIC, de los cuales se recomienda COBIT, ITIL e ISO 27002, debido a que juntos integran las características de seguridad de la información, gobierno de TIC y gestión de servicios, elementos necesarios para normar y controlar la gestión de las tecnología de información y comunicaciones en las entidades públicas. No obstante las EFS podrán adoptar cualquier otro estándar que se adapte a sus necesidades de control.

7. **"Metodología de auditoría de gestión TIC",** Proveer a los auditores lineamientos específicos para la realización de la auditoria a las TIC que ayuden a la verificación de procesos y recursos tecnológicos a través de los procedimientos de la auditoria en sus diferentes fases.

   A continuación se plantea el proceso de la práctica de la auditoría a la Gestión TIC.

1. ETAPA DE PLANIFICACIÓN

1.1 Conocimiento de la Entidad y Entorno del área de Tecnología de Información y Comunicación.

Para la ejecución de una auditoría a las TIC, es muy importante que el auditor aplique procedimientos que le permitan comprender la estructura funcional y administrativa de la entidad de manera general, Planes Estratégicos y Operativos, Ideas Rectoras, Misión y Visión de la entidad y el entorno con el propósito de identificar y analizar las entidades y

organismos que tienen relación con los procesos claves y tengan comunicación por medio de sistemas informáticos en el compartimiento de conocimientos o información que no afecte los objetivos de la entidad, de manera que le permita una adecuada planificación de su trabajo, pues ese conocimiento le brinda un marco conceptual, que le permite evaluar si la organización sigue un enfoque estructurado de gestión informática y si el mismo es adecuado.

AUDITORÍA INFORMÁTICA
PANAMÁ

FASES DE AUDITORÍA INFORMÁTICA

PLANIFICACIÓN

Antes del desarrollo de una auditoría es necesario contar con una Resolución mediante la cual se ordena la auditoría, nota de presentación del equipo auditor y la orden de trabajo. Por lineamiento de la DINAG, también se debe confeccionar una matriz de riesgo inicial y un plan de trabajo. Todos estos documentos deben ser confeccionados por el Jefe del departamento antes del inicio de la auditoría.

La Planificación en la DINAG se divide en Planificación Preliminar y Planificación Específica, se detallan:

- **Planificación Preliminar**
  En la preliminar se conoce o se obtiene una comprensión general del área de tecnología de la entidad auditada en función del objetivo de la auditoría. En esta fase se debe contar con el Programa de Planificación Preliminar, que establezca los procedimientos a realizar y como resultado se emite el Memorando de Planificación Preliminar que constituye el reporte o informe de esta planificación.

  La información recopilada en esta fase se obtiene a través de entrevistas (a quienes sean los encargados o responsables del área auditar), página web de la entidad, archivos permanentes, etc.

- **Planificación Específica**

  La planificación específica está dirigida a definir la programación y procedimientos completos de la auditoría mediante la evaluación del

ambiente de control del área de TIC, identificando y evaluando los procesos significativos y controles asociados.

En esta fase se debe tener el Programa de Planificación Específica, Memorando de Planificación Específica (reporte o informe de esta fase). Al final de la fase se debe contar con los programas de auditoría específico y cronograma de auditoría.

En esta fase se debe evaluar la estructura de control interno. Para ello DESATIC ha elaborado un cuestionario base de control interno que contiene una serie de preguntas que se seleccionan de acuerdo al objetivo de la auditoría.

En cuanto a la comunicación de los hallazgos de control interno, primero se identifican las condiciones reportables y se identifican los hallazgos. Estos se revisan por la Jefatura del Departamento y se envían para su revisión según el trámite definido por la DINAG.

1.2 Normativa Interna y Externa

Se deberá analizar la leyes, reglamentos, instructivos, normas, políticas, entre otras de la normativa que le aplica al área de Tecnología de la Información con el fin de determinar los criterios generales a utilizar en el desarrollo de la auditoria.

AUDITORÍA INFORMÁTICA
PANAMÁ

NORMATIVIDAD

Actualmente, DINAG y por ende DESATIC emplean las **Normas de Auditoría Gubernamental para la República de Panamá** emitidas mediante el Decreto 247 de 13 de diciembre de 1996. Estas normas constituyen la base conceptual y metodológica dirigida a unificar los criterios para la realización de auditorías.

La Contraloría General también cuenta con las **Normas de Control Interno Gubernamental para la República de Panamá** emitidas mediante Decreto No. 214-DGA de 8 de octubre de 1999. Estas normas constituyen el cuerpo normativo que presenta los requerimientos básicos aceptables para una estructura de control interno operativo.

Dentro de estas normas se han incluido las **Normas de Control Interno para Sistemas Computarizados** que se dividen en 8 secciones:

- Organización del área informática,
- Plan de Sistemas de Información,
- Controles de Datos Fuente, de Operación y de Salida,
- Mantenimiento de Equipos de Computación,
- Seguridad de Programas, de Datos y Equipos de Cómputo,
- Plan de Contingencias,
- Aplicación de Técnicas de Intranet,
- Gestión Óptima de Programas (software) Adquirido a la Medida por Entidades Públicas.

Como complemento, a las directrices de las Normas de Control Interno Gubernamental se emplea COBIT como marco de referencia, para la revisión del control interno de sistema.

Actualmente, la DINAG está en proceso de actualización de normas en las que se debe incluir la participación y colaboración de DESATIC.

AUDITORÍAS DESATIC

En DESATIC se realizan básicamente dos (2) tipos de trabajos:

- **Apoyos Técnicos:** se ejecutan en relación a apoyos requeridos por otros departamentos de la DINAG. Abarcan desde evaluación de control interno, uso de ACL, evaluación cumplimiento de contratos, etc. El producto final es un informe técnico.

- **Auditorías de Sistemas:** se ejecutan dentro del ciclo completo de auditoría (planificación, ejecución y comunicación de resultados). Por ahora, se han realizado auditoría de sistemas en la Autoridad de Tránsito y Transporte Terrestre y Lotería Nacional de Beneficencia.

1.3 Organización de área TIC.

El auditor debe de conocer, comprender y analizar la función del área de Tecnología de Información y Comunicaciones principalmente en aspectos como: organización, objetivos y metas operativas, Instrumentos Administrativos, infraestructura Tecnológica, Procesos sistematizados, Productos y/o Servicios, Insumos y el entorno de la función de Tecnología de Información y Comunicaciones (clientes), aplicando procedimientos generales para la conducción y el alcance de la auditoria.

Procedimientos a ejecutar

- ✓ Revisar y evaluar si la función de TIC está alineada con la misión, visión, valores, objetivos y estrategias de la organización y deberá revisar el desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.
- ✓ Revisar y evaluar la eficacia de los recursos de TIC y el desempeño de los procesos administrativos.
- ✓ Se debe utilizar un enfoque basado en riesgos para evaluar la función de TIC.
- ✓ Se deberá de revisar las áreas físicas de TIC, con el propósito identificar si está en condiciones para la operatividad de las Tecnologías de la Información y Comunicaciones.
- ✓ Se deberá de revisar las funciones de cada uno de los Técnicos para comprobar si estos cuentan con herramientas y condiciones necesarias para realizar su trabajo y de la optimización de los recursos tecnológicos.
- ✓ Se deberá de verificar y analizar si el Manual de funciones es aplicable y acorde a la realidad de las funciones desarrolladas por el capital humano del Área de Tecnología de Información y Comunicaciones.

1.4 Evaluación del Control Interno

El auditor deberá evaluar y asegurarse que el control interno diseñado e implementado por la institución garantice que las medidas de seguridad en las plataformas tecnológicas, la administración de la información y de los recursos tecnológicos, el cumplimiento de leyes, reglamentos y otras normativas aplicables estén siendo administrados de tal forma que cumplan con los propósitos para lo cual fueron diseñados y alineados con la Misión, Visión y con los objetivos estratégicos trazados institucionalmente.

Uno de los procedimientos a ejecutar para la evaluación de control Interno, es la creación de cuestionario basado en la normativa legal y técnica aplicable al área de tecnología de la información, con el propósito de obtener evidencia documental (formato electrónico) y determinar los riesgos de la auditoria y el grado de solides del control interno implementado en la entidad.

1.5 Planes de Continuidad

El auditor debe conocer y analizar el plan de contingencia y continuidad implementado por la entidad para dirigir procedimientos a ejecutar con el propósito de determinar el grado de efectividad y eficiencia para mantener la continuidad en los servicios de TIC y minimizar la probabilidad y el impacto de interrupciones en los servicios, funciones y procesos claves del negocio e incluir procedimientos a los servicios tecnológicos y de comunicaciones contratados con terceros.

1.6 Presupuesto Tecnológico.

El auditor debe ejecutar procedimientos para asegurarse que las inversiones en recursos tecnológicos hechas por la entidad, ha contribuido a maximizar el desempeño económico de la organización y es administrado adecuadamente y que toda contratación se incluya y se autorice en el plan anual de compras y evaluar el proceso de contratación, priorizando en el cumplimiento de las especificaciones técnicas, recepción del bien o servicio y utilidad de los mismos de acuerdo a las necesidades requeridas por las unidades solicitantes.

1.7 Análisis, Evaluación e Incorporación de Hallazgos de Auditoría elaborados por la Unidad de Auditoría Interna y Firmas Externas de Auditoría.

El auditor debe obtener de la entidad auditada los informes y papeles de trabajo de auditoría de tecnologías de información y comunicaciones emitidos por la Unidad de Auditoría Interna y las Firmas Externas de Auditoría, con el objetivo de analizar y evaluar los hallazgos con los respectivos atributos, su impacto, importancia relativa y la evidencia de soporte, y así determinar los hallazgos que serán incorporados en el informe de auditoría.

El proceso de análisis y evaluación deberá plasmarse en papeles de trabajo que elaborará el auditor.

Una ves el equipo de auditoria ha realizado el conocimiento y análisis general del área de tecnología de la Información, se determinan las posibles áreas criticas de examen que puedan afectar el cumplimento de la misión, visión, planes y metas proyectadas por la entidad y el área de tecnología. Se procede a elaborar informe que determinen las acciones a ejecutar, Naturaleza y alcance de la auditoria, Estrategia de la auditoría, Enfoque de la auditoria, Recursos tecnológicos y humanos, Cronograma de trabajo y la elaboración de programas de auditoría que dará inicio a la etapa siguiente (Etapa de Examen Preliminar).

2. ETAPA DE EXAMEN PRELIMINAR.

Se iniciara la etapa de examen con la agrupación de las Áreas Criticas de Examen Preliminar, estas áreas pueden ser definidas por proyectos o sistemas claves o críticos TIC, de los cuales se han determinado en la experiencia obtenida, tres áreas críticas a examinar:

- ✓Gobernabilidad y organización del área/Unidad TIC.
- ✓Administración de la infraestructura tecnológica, redes, comunicaciones y seguridad.
- ✓Operatividad de los Sistemas de Información.

Para asegurarse sobre la organización, utilización eficiente de los Sistemas, la seguridad y confiabilidad del procesamiento de la

información y base de datos y poder así proporcionar a la entidad recomendaciones viables y factibles para mejorar la administración y su gestión tecnológica.

2.1. Examen a la Gobernabilidad y Organización del área/Unidad de TIC.

El auditor debe de realizar una evaluación de la estructura organizativa y la planificación del Área de TIC, con el objetivo de verificar si las funciones, líneas de autoridad y responsabilidad de las diferentes unidades que conforman el Área de Tecnología de Información y Comunicaciones, están autorizadas y apoyan a los procesos claves que le permiten a la entidad cumplir con los planes y metas, además se debe analizar si es recomendable la ubicación actual dentro del organigrama institucional o amerite que el Área de Tecnología de Información y Comunicaciones debe estar al más alto nivel de la pirámide administrativa para cumplimiento de sus objetivos y cuente con el apoyo necesario de la máxima autoridad.

Además el auditor debe de evaluar si los usuarios internos (área de tecnología) y usuarios externos (personal que hace uso de los recursos tecnológicos dentro de la entidad) estén cumpliendo con los procedimientos de control implementados por el área de tecnología.

2.2. Administración de la Infraestructura Tecnológica, Redes, Comunicaciones y Seguridad.

El auditor deberá evaluar y analizar las actividades importantes y los controles claves para la confiabilidad y seguridad en la administración de servidores, redes, comunicaciones y el soporte técnico de la infraestructura tecnológica, verificando aspectos como los siguientes:

- ✓ Procesos y/o funciones (sustantivos, apoyo y administrativos) de la entidad, que están soportados con tecnología de información y comunicaciones.
- ✓ Plataforma de servidores y sus características de seguridad y administración.
- ✓ Administración de los Sistemas operativos.
- ✓ Administración de la Seguridad Perimetral.
- ✓ Administración de la Infraestructura de redes.

- ✓ El inventario de Hardware y Software.
- ✓ Servicios tercerizados contratados por la entidad y vinculados con la tecnología de la información y comunicaciones.
- ✓ Infraestructura eléctrica, entre otras.
- ✓ Administración de respaldos de las aplicaciones en producción y desarrollo, así como de las bases de datos.

2.2.1 Evaluación de los equipos informáticos.

El auditor debe de constatar que el Área de la Tecnología de Información y Comunicaciones ha implementado controles para determinar el nivel/grado de obsolescencia o actualización de los equipos Portátiles/Pc´s, servidores, dispositivos de la red de datos y equipos de comunicación, con las capacidades técnicas mínimas para la operatividad en el procesamiento eficiente de la información.

2.2.2 Controles en el uso de Computadoras de Escritorio y Portátiles.

Significan puntos de acceso vulnerables, de fácil acceso físico y lógico, de fácil explotación para la obtención de datos, por lo tanto los controles que se implementen ayudarán a garantizar la integridad y confidencialidad de la información.

El auditor mediante sus procedimientos de auditoría debe asegurase que el área de tecnología de información ha realizado lo siguiente:

- ✓ Control de acceso a los sistemas y caducidad automática de contraseñas.
- ✓ Mantener programas y procedimientos de detección y eliminación de virus, malware, spam, copias de software no autorizadas y control de los datos procesados en otros equipos.
- ✓ Procedimientos e informes de revisión del software contenido en el computador, para asegurarse que el software instalado cuente con la respectiva licencia de uso.
- ✓ Procesos de estandarización de sistemas operativos, software de ofimática, manejadores de base de datos y mantener actualizadas las versiones respectivas.
- ✓ Vencida la garantía de mantenimiento del proveedor del equipo se debe proporcionar mantenimiento preventivo y correctivo.

- ✓ Establecimiento de procedimientos para la realización de respaldos de la información Adquisición de equipos de protección eléctrica como reguladores de voltaje y UPS.

2.2.3 Controles de Adquisición.

El propósito es asegurar que el hardware y software adquirido a terceros proporcione mayores beneficios que cualquier otra alternativa y garantizar el costo beneficio por medio de la selección adecuada de equipos y sistemas informáticos.

Procedimientos a seguir:

- ✓ Revisión de un informe técnico en el que se justifique la adquisición del equipo, software y servicios informáticos incluyendo un estudio costo-beneficio.
- ✓ Verificar la formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación (Aplica si la legislación del país lo determina).
- ✓ Determinar si han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios informáticos. Este proceso debe enmarcarse en normas y disposiciones legales.
- ✓ Solicitar la documentación técnica de contratos de los servicios tercerizados, (hardware y software, arrendamientos de enlaces de red, Internet, entre otros) con el propósito de asegurase con el cumplimiento de lo contratado.

2.2.4 Evaluación de la Seguridad Perimetral.

Los equipos informáticos son instrumentos que procesan grandes cantidades de información, la cual es confidencial para la entidad y puede ser mal utilizada al ser divulgada a personas que hagan mal uso de esta; además existen riesgos de robos, fraudes o sabotajes que provoquen la destrucción total o parcial de los equipos que procesan y almacenan los datos.

Al auditar los sistemas de seguridad perimetral, el auditor debe verificar y constatar los aspectos siguientes:

- ✓ Que exista un diseño e implementación estructurada para la configuración de la red y equipos de seguridad, tanto de software

como de hardware, para el control, monitoreo y resguardo de la integridad de los datos que fluyen a través de la red. (ejemplo de un esquema a verificar, una DMZ, o la existencia de equipos de seguridad redundantes, etc.)

- ✓ Utilización de dispositivos físicos y lógicos de seguridad como firewalls y servidores de antivirus, para la protección de los datos e información, así como levitar el ingreso de usuarios no autorizados a la red y la restricción al acceso de la información.
- ✓ Una configuración adecuada de las políticas en los sistemas operativos y sus directorios activos en la administración de los usuarios de la red.
- ✓ Verificación de sistemas o registros auxiliares de huellas de auditoria en la red de datos, sistemas informáticos.
- ✓ Que no se tengan copias "piratas" o bien que, al conectarse a la red con otras computadoras, no exista la posibilidad de transmisión de virus.
- ✓ Implementación de seguridad física y lógica para el acceso a servidores y el ingreso a las instalaciones físicas, contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
- ✓ Verificar la elaboración y administración de respaldos de datos de información.
- ✓ Revisión de controles ambientales.
  Se hace para verificar si los equipos tienen un ambiente físico adecuado, es decir si se cuenta con aire acondicionado, fuentes de energía continua, extintores de incendios, etc.
- ✓ Revisión del plan de mantenimiento.
  Se verificará que todos los equipos principales tengan un adecuado mantenimiento que garantice su funcionamiento continuo.

2.3 Sistemas de Información y Comunicaciones.

La evaluación para esta área se hace con el objetivo de verificar las actividades importantes y controles claves en la operación y utilización eficiente de los sistemas que apoyan los procesos claves y administrativos, la seguridad y confiabilidad del procesamiento de

la información y base de datos, el soporte oportuno a los requerimientos de los usuarios

2.3.1 Evaluación de los Sistemas Informáticos.

El auditor debe de evaluar si los sistemas de Información utilizados en la entidad cumplen con los objetivos para los cuales han sido diseñados, con el propósito de determinar si los sistemas son eficientes y eficaces. Para lo cual se mencionan algunos procedimientos que puede aplicar el auditor, tales como:

- ✓ Evaluación de los diferentes sistemas informáticos en operación (flujo de información, procedimientos, documentación técnica, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).
- ✓ Evaluación del avance de los sistemas informáticos en desarrollo y congruencia con el diseño general.
- ✓ Seguridad física y lógica de los sistemas informáticos, su confidencialidad y respaldos.
- ✓ La Administración de Sistemas y Bases de Datos.
- ✓ Adopción de Metodologías de Análisis y desarrollo de Sistemas.
- ✓ Lenguajes de programación

2.3.2 Controles de Sistema en Desarrollo y Producción.

El auditor debe de evaluar y asegurarse que el Área de Tecnología de Información y Comunicaciones ha justificado que los sistemas informáticos adquiridos a terceros y desarrollados internamente han sido la mejor opción para la entidad y que proporcionen oportuna y efectiva información, también que estos se han desarrollado bajo un proceso planificado y documentado, así como la satisfacción de los usuarios en el mantenimiento y soporte oportuno a los requerimientos al sistema.

Procedimientos a seguir:

- ✓ Asegurarse que los usuarios han participado en el diseño e implantación de los sistemas informáticos, pues aportan conocimiento y experiencia de su área y esta actividad coadyuva a una mejor cultura tecnológica en el cambio de los procesos institucionales.

- ✓ Verificar que al sistema se le haya implantado de rutinas o módulos para el registro de huellas de auditoría.
- ✓ Evaluar si el desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos y que se encuentren alineados con objetivos institucionales y en general cumplan con la metodología del ciclo de vida de desarrollo de sistemas.
- ✓ Evaluar si cada fase del ciclo de vida de desarrollo de sistemas concluida esta aprobada y documentada por los usuarios mediante actas u otros mecanismos, a fin de asegurase que se esta cumpliendo con lo planificado.
- ✓ Constatar si los aplicativos antes de pasar a producción son probados con datos para concluir sobre el rendimiento de estos.
- ✓ Comprobar si todos los sistemas informáticos están debidamente documentados y actualizados.
- ✓ Verificar la existencia de bitácoras para registrar y documentar los de cambios, actualizaciones, mejoras implementados a los sistemas informáticos.
- ✓ Verificar si el sistema informático es entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos.

2.3.3 Para el procesamiento electrónico de datos en los sistemas informáticos el auditor debe de considerar:

- ✓ Evaluar la validación de datos de entrada, procesamiento y salida, este proceso es realizado en forma automática.
- ✓ Verificar que la preparación de los datos de entrada sea responsabilidad de los usuarios y consecuentemente su corrección.
- ✓ Verificar la adopción de acciones necesaria para correcciones de errores.
- ✓ Evaluación de la planificación del mantenimiento del hardware y aplicativos informáticos, tomando todas las medidas de seguridad para garantizar la integridad.
- ✓ Evaluar en general las etapas del ciclo de vida y desarrollo de los sistemas.

2.3.4 Contingencia y Continuidad de los servicios tecnológicos.

El auditor verificará si el plan de contingencia es apropiado para garantizar la continuidad del negocio, las operaciones y la recuperación de información ante contingencias humanas o naturales que puedan poner en peligro las operaciones, pérdida de información, infecciones de virus entre otras, el cual debe de contener como requisitos mínimos los siguientes:

- ✓ Considerar requerimientos de procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI.
- ✓ Cubre los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.
- ✓ Considera los requerimientos de respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.
- ✓ Se ha centrado la atención en los puntos determinados como los más críticos en el plan de continuidad para construir resistencia y establecer prioridades en situaciones de recuperación.
- ✓ Procedimientos de control de cambios, para asegurar que el plan de continuidad se mantenga actualizado y que refleje de manera continúa los requerimientos actuales del negocio.
- ✓ Mecanismos de comunicación para contactar inmediatamente a cada miembro del área TI, a través de la disposición de: direcciones de residencia, números telefónicos fijo y/o celular, correo electrónico, etc.
- ✓ Detalle de los recursos financieros.
- ✓ Análisis de los riesgos e impacto, que afecten de forma parcial o total la operatividad normal de los servicios de TIC.
- ✓ Contar con procedimientos de respaldo que permitan el resguardo y recuperación de la información identificada como critica.
- ✓ Disponibilidad de equipos informáticos de respaldo para servir de remplazo en caso de daños.

3. ETAPA DE EJECUCIÓN

Una vez concluido el análisis preliminar de las áreas antes descritas, se diseñaran programas de auditoría dirigido a las áreas de mayor vulnerabilidad y/o impacto determinadas al confrontar los riesgos versus controles tecnológicos, además se debe de obtener evidencia de las causas que originan las debilidades en la Gestión a las Tecnologías de Información y Comunicaciones, para lo cual, el auditor deberá apoyarse en las Técnicas de Auditoría Asistidas por Computadora (TAACs).

Pasos para desarrollar una TAAC.

- ✓ Definir detalladamente el objetivo de lo que se va a examinar.
- ✓ Determinar las técnicas de auditoria que deberá utilizar y la herramienta (software/Hardware) que más se adecue para obtener los resultados del objetivo establecido.
- ✓ Identifique las fuentes de los datos o los elementos de la infraestructura tecnológica (Servidores, Redes, entre otros), sobre las cuales se aplicarán las herramientas TAAC´s.
- ✓ Identifique sus atributos de la información a examinar.
- ✓ Solicite la documentación técnica del elemento TIC a examinar.
- ✓ Ejecute pruebas. Registre en una bitácora las acciones realizadas, analice y verifique los resultados.

3.1 Seguridad de datos y Técnicas de Auditoría Asistidas por Computadora.

Cuando las TAAC´s son utilizadas para extracción de información y análisis de datos, el auditor de TIC debe verificar la integridad del sistema de información y el ambiente tecnológico donde son extraídos los datos.

Las Técnicas de Auditoría Asistidas por Computadora pueden ser utilizadas para extraer información de programas o sistemas de información y datos en producción que deben ser mantenidos en forma confidencial, así como la detección de cualquier anomalía que suceda en los elementos que componen una plataforma tecnológica.

El auditor de TIC debe entender la clasificación de información de la entidad y políticas llevadas para salvaguardar adecuadamente los

programas y/o sistemas de información y datos en producción con un nivel apropiado de confidencialidad y seguridad.
El auditor de TIC debe considerar el nivel de confidencialidad y seguridad requerido por la organización propietaria de los datos y cualquier legislación pertinente, y debe consultar a otros, tanto como el consejo y administración sea necesaria.

El auditor debe utilizar y documentar los resultados de los procedimientos, para proveer sobre la marcha integridad, confiabilidad, utilidad y seguridad de la TAAC´s. Por ejemplo, esto debe incluir una revisión de programas de mantenimiento y control de cambio de programas sobre el software de auditoría para determinar que solo los cambios autorizados han sido hechos por las TAAC´s.

3.2 Evaluación y recolección de Evidencia.
El auditor en todo el proceso de la auditoria deberá obtener la certeza (evidencia) suficiente y apropiada a través de la ejecución de sus procedimientos para permitirle emitir las conclusiones viables y factibles para fundamentar su opinión sobre la operatividad de la Gestión en Tecnología de Información y Comunicaciones.

La recolección de la evidencia se entiende por suficiente, aquel nivel de evidencia que el auditor debe obtener a través de sus pruebas de auditoría, para llegar a conclusiones sobre el uso de las Tecnologías de información y comunicaciones que se someten a examen. El auditor no pretenderá obtener toda la evidencia existente, sino aquella que cumpla, a su juicio profesional, con los objetivos de su examen.

Es necesario confiar en evidencias que son más convincentes que concluyentes, por tanto, con frecuencia puede buscar evidencia de diferentes fuentes o de distinta naturaleza para apoyar un mismo hecho o dato. La evidencia es adecuada cuando sea pertinente para que el auditor emita su juicio profesional.

3.3 Evidencia adecuada.

El concepto de “adecuación” de la evidencia es la característica cualitativa, en tanto que el concepto “suficiencia” tiene carácter cuantitativo. La combinación de ambos elementos debe proporcionar al auditor el conocimiento necesario para alcanzar una base objetiva de juicio sobre los hechos sometidos a examen.

3.4 Documentación de la evidencia

La evidencia obtenida deberá documentarse en los papeles de trabajo del auditor como justificación y soporte del trabajo efectuado y para registrar todos aquellos asuntos de importancia relativa que no está conforme a la normativa técnica y legal en la operatividad y uso de las tecnologías de información y comunicaciones.

3.5 Protección y Conservación de la Evidencia.

La evidencia de auditoría deberá estar protegida contra el acceso no autorizado y la modificación.

La evidencia de auditoría debe mantenerse después de la finalización del trabajo de auditoría, mientras sea necesario para cumplir con todas las leyes aplicables, reglamentos y políticas.

3.6 Cumplimiento de Políticas y Procedimientos.

En el transcurso de la auditoría de gestión a las tecnologías de información y comunicaciones, el auditor debe cerciorarse mediante los procedimientos plasmados en los programas de auditoría, el cumplimiento de políticas y procedimientos para el uso de la información y de las tecnologías de información y comunicaciones (TICs) en la organización, y al determinar que no se están cumpliendo, el auditor lo evidenciará aplicando diferentes técnicas de auditoría y lo comunicará al funcionario público responsable del incumplimiento para determinar las causales por las cuales no se están cumpliendo con lo plasmado en la normativa interna y externa aplicable, esto a su vez le sirve al auditor para obtener documentación que respalde su juicio y su opinión profesional.

3.7 Carta de Salvaguarda.

El equipo de auditoría, deberá obtener la carta de salvaguarda, relacionada con la gestión de tecnología de información y comunicaciones, suscrita por el Titular de la Entidad o por el funcionario a quien él designe, con la finalidad que el equipo de auditores se resguarden que toda la información relacionada con las tecnologías de información y comunicaciones solicitada, ha sido prevista por la administración.

4. INFORME

4.1 Resultados Preliminares de Auditoría (Informe Previo).

Esta etapa finaliza con los procedimientos de auditoría de ejecución, y comienza con la elaboración del Informe previo de Auditoría de resultados preliminares (en algunos países se le conocen como: informe previo, pre-informe, borrador de informe, entre otros), el jefe de equipo agrupa todos los asuntos de importancia (condiciones, deficiencias, observaciones) que incumplieron las disposiciones relacionadas con aspectos de control interno y/o de cumplimiento con leyes, reglamentos legales y técnicos u otras disposiciones aplicables que dieron origen a la condición (Criterio), con la documentación que los respaldan y que los auditores determinaron al aplicar sus procedimientos de auditoría y se comunicarán a la máxima autoridad de la entidad y a los funcionarios actuantes responsables, esto se hace para garantizarse que dichos funcionarios tuvieron la oportunidad de defensa y convocándolos a una lectura de los resultados obtenidos y previos de auditoría para que emitan sus comentarios de defensa respectivos.

Para que un asunto de importancia (condiciones, deficiencias, observaciones), sea incluido en el Informe previo de Auditoría de resultados preliminares e Informe de Auditoría deberá estar estructurado con todos sus atributos (Condición, Criterio, Causa, Efecto, Comentarios de la Administración, Comentarios del Auditor y Recomendaciones).

Las recomendaciones y conclusiones hechas por los auditores deberán ser viables y factibles para que éstas sean atendidas por la administración y que sean de fácil comprensión y análisis para terceras personas y auditores que verificarán el cumplimiento en auditorias recurrentes.

El informe previo de Auditoría de resultados preliminares deberá tener un formato uniforme y estar dividido por secciones para facilitar al funcionario lector una rápida comprensión del contenido del informe, y contendrán los principios y estructuras descrita en el Informe de Auditoría.

4.2 Carta de Gerencia de Asuntos de Importancia Relativa.

Al finalizar la fase de ejecución, se elabora una carta de gerencia, en la cual se comunicará a la administración todos aquellos asuntos de menor importancia, estos asuntos de menor importancia son riesgos que pueden ser administrados y que a juicio del auditor no son de impacto en la gestión de las tecnologías de información y comunicaciones.

Este documento incluye la descripción de los asuntos de menor importancia (Condición) determinados y que no clasifican para constituirse como hallazgo y requieren de atención por parte de la administración para que en el futuro próximo no afecten el cumplimiento de la Misión, Visión, Objetivos y Metas de la entidad, al detallar estos asuntos menores, deberán incluir las disposiciones relacionadas con aspectos de control interno, leyes, reglamentos u otras disposiciones aplicables (Criterio) que se incumplieron y que originaron la condición, las cuales al ser superadas mejorarían la gestión tecnológica institucional, fortaleciendo el sistema de control interno, bajo responsabilidad de la máxima autoridad de esa Entidad.

4.3 Informe de Auditoría.

Posterior a la lectura del informe previo de Auditoría de resultados preliminares (Pre Informe, Borrador de Informe) se analizan los comentarios y documentación presentada por la administración y se elabora el Informe de Auditoría que contiene los resultados finales de la auditoría que no fuesen superados.

Se comunicarán los resultados al máximo nivel de dirección de la entidad auditada y otras instancias administrativas, así como a los funcionarios involucrados en los asuntos de importancia relativa (observaciones) que correspondan cuando esto proceda.

El informe de Auditoría debe tener un formato uniforme y estar dividido por secciones para facilitar al funcionario lector una rápida comprensión del contenido del informe.

El informe de Auditoría debe cumplir con los principios siguientes:

- ✓ Que se emita por el jefe de grupo de los auditores actuantes.
- ✓ Por escrito.
- ✓ Oportuno.
- ✓ Que sea completo, exacto, objetivo y convincente, así como claro, conciso y fácil de entender.

El hecho de que un Informe sea Conciso, no significa que su contenido sea corto, lo que se quiere es que su contenido sea breve, ya que muchos informes pueden ser amplios porque las circunstancias así lo requieren; sin embargo no deben incluir hechos impertinentes, superfluos o insignificantes.

- ✓ Que todo lo que se consigna esté reflejado en los papeles de trabajo y que responden a hallazgos relevantes con evidencias suficientes y competentes.
- ✓ Que refleje una actitud independiente.
- ✓ Que muestre la conclusión u opinión de los resultados o evaluación de la Auditoría.
- ✓ Distribución rápida y adecuada.

El informe de auditoría deberá ser estructurado y tendrá como mínimo requerido lo siguiente:

- ✓ Nombre de la organización
- ✓ Destinatario del Informe
- ✓ Alcance de la Auditoría
- ✓ Objetivos de la Auditoría
- ✓ Período auditado
- ✓ Naturaleza, plazo y extensión de las labores de auditoría
- ✓ Hallazgos
- ✓ Conclusiones
- ✓ Recomendaciones
- ✓ Seguimiento Recomendaciones de Informes de auditorías anteriores (acciones implementadas)
- ✓ Firma
- ✓ Fecha
- ✓ Distribución del Informe de acuerdo a los mecanismos de cada Contraloría

8. "Los Vectores de la Auditoria de Gestión TIC", determinan la dirección y sentido de la auditoria de gestión TICs, en la cual definimos los diferentes enfoques o áreas de importancia sobre las cuales se ejecutara la auditoria a las TIC, para que las auditorias TIC sean siempre efectivas y oportunas, al desarrollo continuo de objetivos tecnológicos actualizados. Como ejemplo podemos mencionar algunos enfoques:

1. Gobierno de TIC
2. Gobierno electrónico
3. Seguridad de la información
4. Servicios TIC
5. Adopción e Implementación de estándares internacionales TIC
6. Y otros que las EFS considere necesario para la mejor ejecución de la auditoria.

Consideraciones previas a una Auditoría de Sistemas (Gerardo Alejandro Santéliz García)

El proceso de Auditoría encomendado a cada EFS, es fundamentalmente necesario para poder medir el rendimiento, calidad de gasto y la optimización del recurso financiero para cada País; esta práctica nos ha llevado a reflexionar sobre la aplicación de las Auditorías Especializadas. En tal caso me referiré al proceso de la Auditoría de Sistemas Informáticos:

Los sistemas informáticos que surgen para la automatización de procesos y la **sistematización de los mismos requieren de una adecuada planeación que recoja** del medio las necesidades de los usuarios en base al rol de la entidad, y acá está realmente la clave:

Como ejemplo se debe analizar un sistema único de registro y control de las operaciones y transacciones financieras que utiliza un país, siendo en cada país, cada una de estas instituciones de diferentes características Entidades de

Gobierno Central, Entidades Semi Autónomas, Entidades Autónomas, Entidades Descentralizadas, Gobiernos Municipales, etcétera.

Cada módulo del Sistema Integrado de Administración Financiera (que por razón de ejemplo menciono el caso de Guatemala), deberá considerar cada una de las fases que lo sustentaran dentro del proceso…

Módulo de Contabilidad

SIAF Modulo de Presupuesto

Módulo de Tesorería

SICOIN

Sistema de Contabilidad Integrada

Definición de requerimiento: a esta fase fundamental del sustento para el desarrollo del software deberá conocerse también como Ingeniería de Requisitos (termino no generalmente reconocido en el medio), pero de transcendencia en los objetivos, misión y visión que se deseen alcanzar con el producto a desarrollarse; la responsabilidad de esta tarea deberá recaer en personas expertas de equipos multidisciplinarios que recaben y documenten cada una de las necesidades a ser automatizadas evaluando los procesos y señalando el valor agregado que se obtendrá de la implantación de un sistema. Deberán entre otras funciones considerarse lo siguiente:

· La deducción de los requisitos de usuario.

· El análisis y negociación de requisitos, para derivar requisitos adicionales.

· La documentación de los requisitos como especificación.

· La validación de los requisitos documentados contra las necesidades de usuario.

· Así como los procesos que apoyan estas actividades.

Fases de implementación

Desde un punto de vista conceptual, las actividades son de cinco clases.

· Obtener requisitos: a través de entrevistas o comunicación con clientes o usuarios, para saber cuáles son sus expectativas.

· Analizar requisitos: detectar y corregir las falencias comunicativas, transformando los requisitos obtenidos de entrevistas y requisitos, en condiciones apropiadas para ser tratados en el diseño.

· Documentar requisitos: igual que todas las etapas, los requisitos deben estar debidamente documentados.

· Verificar los requisitos: consiste en comprobar el correcto funcionamiento de un requisito en la aplicación.

· Validar los requisitos: comprobar que los requisitos implementados se corresponden con lo que inicialmente se pretendía.

Técnicas principales

La ingeniería de requisitos puede ser un proceso largo y arduo para el que se requiere de habilidades psicológicas. Los nuevos sistemas cambian el entorno y las relaciones entre la gente, así que es importante identificar a todos los actores involucrados, considerar sus necesidades y asegurar que entienden las implicaciones de los nuevos sistemas. Los analistas pueden emplear varias técnicas para obtener los requisitos del cliente.

Históricamente, esto ha incluido técnicas tales como las entrevistas, o talleres con grupos para crear listas de requisitos. Técnicas más modernas incluyen los prototipos, y utilizan casos de uso. Cuando sea necesario, el analista empleará

una combinación de estos métodos para establecer los requisitos exactos de las personas implicadas, para producir un sistema que resuelva las necesidades del negocio.

Entrevistas

Las entrevistas son un método común. Por lo general no se entrevista a toda la gente que se relacionará con el sistema, sino a una selección de personas que represente a todos los sectores críticos de la organización, con el énfasis puesto en los sectores más afectados o que harán un uso más frecuente del nuevo sistema.

Talleres

Los requisitos tienen a menudo implicaciones cruzadas desconocidas para las personas implicadas individuales y que a menudo no se descubren en las entrevistas o quedan incompletamente definidas durante la misma.

Estas implicaciones cruzadas pueden descubrirse realizando en un ambiente controlado, talleres facilitados por un analista del negocio, en donde las personas implicadas participan en discusiones para descubrir requisitos, analizan sus detalles y las implicaciones cruzadas. A menudo es útil la selección de un secretario dedicado a la documentación de la discusión, liberando al analista del negocio para centrarse en el proceso de la definición de los requisitos y para dirigir la discusión.

Forma de contrato

En lugar de una entrevista, se pueden llenar formularios o contratos indicando los requisitos. En sistemas muy complejos éstos pueden tener centenares de páginas.

Objetivos medibles

Los requisitos formulados por los usuarios se toman como objetivos generales, a largo plazo, y en cambio se los debe analizar una y otra vez desde el punto de vista del sistema hasta determinar los objetivos críticos del funcionamiento interno que luego darán forma a los comportamientos apreciables por el usuario. Luego, se establecen formas de medir el progreso en la construcción, para evaluar en cualquier momento qué tan avanzado se encuentra el proyecto.

Prototipos

Un prototipo es una pequeña muestra, de funcionalidad limitada, de cómo sería el producto final una vez terminado. Ayudan a conocer la opinión de los usuarios y rectificar algunos aspectos antes de llegar al producto terminado.

Casos de uso

Un caso de uso es una técnica para documentar posibles requisitos, graficando la relación del sistema con los usuarios u otros sistemas. Dado que el propio sistema aparece como una caja negra, y sólo se representa su interacción con entidades externas, permite omitir dichos aspectos y determinar los que realmente corresponden a las entidades externas. El objetivo de esta práctica es mejorar la comunicación entre los usuarios y los desarrolladores, mediante la prueba temprana de prototipos para minimizar cambios hacia el final del proyecto y reducir los costes finales.

Esta técnica se enfrenta a los siguientes peligros potenciales.

· A los directivos, una vez que ven un prototipo, les cuesta comprender que queda mucho trabajo por hacer para completar el diseño final.

· Los diseñadores tienden a reutilizar el código de los prototipos por temor a “perder el tiempo” al comenzar otra vez.

· Los prototipos ayudan principalmente a las decisiones del diseño y de la interfaz de usuario. Sin embargo, no proporcionan explícitamente cuáles son los requisitos.

· Los diseñadores y los usuarios finales pueden centrarse demasiado en el diseño de la interfaz de usuario y demasiado poco en producir un sistema que sirva el proceso del negocio.

Los prototipos pueden ser: diagramas, aplicaciones operativas con funcionalidades sintetizadas. Los diagramas, en los casos donde se espera que el software final tenga diseño gráfico, se realizan en una variedad de documentos de diseño gráficos y a menudo elimina todo el color del diseño del software (es decir utilizar una gama de grises). Esto ayuda a prevenir la confusión sobre la apariencia final de la aplicación.

Especificación de requisitos del software

Una especificación de requisitos del software es una descripción completa del comportamiento del sistema a desarrollar. Incluye un conjunto de casos de uso que describen todas las interacciones que se prevén que los usuarios tendrán con el software. También contiene requisitos no funcionales (o suplementarios). Los requisitos no funcionales son los requisitos que imponen restricciones al diseño o funcionamiento del sistema (tal como requisitos de funcionamiento, estándares de calidad, o requisitos del diseño).

Las estrategias recomendadas para la especificación de los requisitos del software están descritas por IEEE 830-1998. Este estándar describe las estructuras posibles, contenido deseable, y calidades de una especificación de requisitos del software.

Los requisitos se dividen en tres:

· Funcionales: son los que el usuario necesita que efectúe el software. Ej: el sistema debe emitir un comprobante al asentar la entrega de mercadería.

· No funcionales: son los "recursos" para que trabaje el sistema de información (redes, tecnología). Ej: el soporte de almacenamiento a usar debe ser Oracle Data Base.

· Empresariales u Organizacionales: son el marco contextual en el cual se implantará el sistema para conseguir un objetivo macro. Ej: abaratar costos de expedición.

Después de la descripción de esta fase para el desarrollo de Software, empieza la responsabilidad de la Auditoría Especializada en Sistemas de Informáticos, se debe requerir a la Gerencia de informática toda la documentación que sustenta el estudio de pre factibilidad del Sistema, ya sea que este sea subcontratado (outsourcing) o desarrollado en casa, para evaluar las diferentes cedulas y/o documentación de necesidades, aparte de generarnos una visión global podríamos evaluar la madurez de los sistemas o la fase en la que se encuentra el mismo, los profesionales del aérea de informática suelen llamar estas fases como Alfa, Beta y Estable o versión final.

Alfa: Es la primera versión del software generado para que los expertos hagan pruebas de cumplimiento en base a los requerimientos primarios, este proceso se conoce como proceso inestable del software, porque es susceptible de cambios y debe quedar plenamente documentado y revalidado cada vez que sea objeto de cambio, se utiliza correlación de versión.

Beta: En esta versión del software los usuarios que interactuaran con el sistema son los que generan las pruebas del mismo, generando las cargas necesarias con información real sobre un ambiente de pruebas con la finalidad de someter el

producto a pruebas de estrés y registras todos los elementos necesarios que deben ser cuidadosamente afinados para garantizar el éxito en la siguiente fase.

Sistema Estable o versión Final: Es la puesta en producción del Sistema, acá podríamos llamar al sistema versión final; es también el inicio que contabiliza la vida útil del software.

En la siguiente capsula estaremos comentando e investigando lo que se refiere al Análisis y Diseño de Software, esperando que esto sea de alguna forma útil para reforzar el conocimiento.

COMPROBACION DE LA BASE O SUSTENTO INFORMATICO (aporte CUBA)

Nuestro trabajo se centra fundamentalmente en la comprobación de la base o sustento informático, cubierto en gran medida por:

- El cumplimiento del Plan de Seguridad Informática en cada entidad. El cumplimiento de la Base Reglamentaria Interna y Externa que rigen y regulan los procesos informáticos.
- El control de los Sistemas Económico-Financieros que soportan los procesos contables y su certificación bajo el cumplimiento de las Normas Contables Cubanas.

Es por ello que hablamos de Auditoria a las TIC y no de Auditoria Informática que tiene un concepto más amplio y abarcador, llevado a cabo por un equipo de especialistas.

La Auditoria a las TIC permite centrar más el control y llevarlo a cabo con menos personal, aunque se ha previsto en las normas, la utilización de personal especializado en calidad de expertos en caso de necesidad.

Durante todo el proceso de Auditoria se comprueba el cumplimiento del Control Interno y Plan de Prevención de Riesgos, según resolución dictada por la Contraloría General de la República.

Por lo general no aplicamos las TAAC, sin desconocer que son herramientas poderosas que reducen el tiempo de auditoría y sobre todo minimizan el tema de error al poder extender el % de las muestras para un período dado. Usamos en alguna medida el IDEA, aunque debemos actualizarnos e implantarlo involucrando en ello a los auditores que son sus potenciales clientes.