UNIVERSIDAD FRANCISCO GAVIDIA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

TRABAJO DE GRADUACIÓN

Tesis:

MANUAL DE AUDITORÍA DE SISTEMAS PARA LA EVALUACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN - MASTI

PRESENTADO POR

Calderón Trinidad, Osbaldo Antonio

Para optar al grado académico de:
INGENIERO EN CIENCIAS DE LA COMPUTACIÓN.

FEBRERO DE 2007

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

AUTORIDADES

RECTOR
ING. MARIO ANTONIO RUIZ RAMÍREZ

VICERECTORA
DRA. LETICIA ANDINO DE RIVERA

SECRETARIA GENERAL
LICDA. TERESA DE JESÚS GONZÁLEZ DE MENDOZA

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO
ING. ROBERTO ARISTEDES CASTELLON MURCIA

ORGANIZACIÓN DEL TRABAJO DE GRADUACIÓN

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO
ING. ROBERTO ARISTEDES CASTELLON MURCIA

ASESOR

ING. KARLA REGINA PÉREZ

JURADO EVALUADOR

PRESIDENTE:
ING. NELSON ANTONIO TESORERO VALENCIA

VOCAL:
ING. LUIS ENRIQUE VALENCIA

VOCAL:
LIC. JOSÉ SALVADOR OLIVARES

No. 28274

Universidad Francisco Gavidia

ACTA DE LA DEFENSA DE TRABAJO DE GRADUACION

Acta No.368. Mes de Febrero de 2007

En la Sala de Defensa Número Tres del Quinto Nivel del Edificio "Administrativo", de la Universidad Francisco Gavidia, a las diez horas y cero minutos del día tres de febrero de dos mil siete; siendo estos el día y la hora señalada para el análisis y la defensa del trabajo de graduación "MANUAL DE AUDITORÍA DE SISTEMAS PARA LA EVALUACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN-MASTI". Presentado por el estudiante: Osbaldo Antonio Calderón Trinidad. De la Carrera de: INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN.

Y estando presentes los interesados y el Tribunal Calificador, se procedió a dar cumplimiento a lo estipulado, habiendo llegado el Tribunal, después del interrogatorio y las deliberaciones correspondientes, a pronunciarse por este fallo:

Aprobado por unanimidad

Osbaldo Antonio Calderón Trinidad

Y no habiendo más que hacer constar, se da por terminada la presente.

Presidente/a

Ing. Nelson Antonio Tesorero Valencia

Vocal

Ing. Luis Enrique Reyes Valencia

Vocal

Lic. José Salvador Olivares

Alumno

Osbaldo Antonio Calderón Trinidad

AGRADECIMIENTOS

DIOS PADRE, la gloria y la honra sea para ti.
Gracias.

El temor de Jehová es el principio de la sabiduría y
el conocimiento del Santísimo es la inteligencia**.**
Proverbios 9:10-11

TABLA DE CONTENIDO

CONTENIDO **Pág.**

CAPÍTULO II

CONTENIDO **Pág.**

CAPÍTULO III

CONTENIDO **Pág.**

CAPÍTULO IV

CONTENIDO **Pág.**

CONTENIDO

CONTENIDO

RESUMEN

La información es uno de los activos más importantes de las organizaciones por ello cada día las entidades dependen más de la información y de la tecnología, los Sistemas Informáticos se han constituido en las herramientas principales para materializar uno de los conceptos significativos y necesarios para cualquier Organización, sin dejar a un lado las nuevas tecnologías en el creciente uso de las mismas, como herramienta de competencia y desarrollo de sus operaciones electrónicas. En tal sentido, la auditoría de sistemas es de vital importancia para el buen desempeño de los sistemas de información, ya que valida la efectividad de los controles, en virtud para que éstos sean confiables y seguros, las empresas a través de los auditores de sistemas tienen que tomar medidas que permitan un crecimiento o desarrollo adecuado de este tipo de operaciones, así como establecer mecanismo idóneo para la administración y regulación del riesgo tecnológico.

En virtud de lo expuesto, se presenta el *Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información*, conocido como "MASTI", el cual agrupa las siguientes divisiones: a) Planificación y Organización: Comprende las decisiones estratégicas y planes operativos definidos por la Administración, esto incluye el entorno organizacional, elementos que contribuirán al logro de los objetivos planeados por la Entidad. b) Plataforma Tecnológica: La práctica de las estrategias definidas por la Organización, obligan a la directriz responsable de TI a cumplir bajo soluciones integrales y tecnológicas a proporcionar un mejor servicio ante el crecimiento y demanda que la institución requiere generando su confianza en los sistemas informáticos. c) Soporte: Mantenimiento, control y seguridad son factores a considerar como complemento de los procesos de TI debido a que deben ser evaluados regularmente, en calidad como cumplimiento, ya que es parte fundamental para la continuidad del servicio. d) Subcontratación: Un acuerdo de subcontratación es aquel que se establece entre una entidad y un proveedor de servicios, en el que este último realiza una actividad, función, proceso o administra los recursos de TI del negocio solicitante.

Las divisiones en referencia se agrupan en 30 áreas de control y estas a la vez se subdividen en 541 actividades seccionadas las cuales conforman los programas de auditoría. El Marco Referencial de MASTI proporciona al auditor de sistemas una metodología que le permite guiarlo sobre los puntos importantes a evaluar dentro de la Organización, no obstante la experiencia del auditor, podrá hacer la ampliación o reducción del mismo, estando sujeto a la responsabilidad y la objetividad que defina los lineamientos de la Administración de la cual depende. Los programas de auditoría descritos en MASTI, permitirán a la Administración tener una evaluación de carácter técnico sobre el ambiente de TI, así como mejorar el servicio tecnológico en: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, todo ello encaminado a que la tecnología apoye el logro de los objetivos estratégicos institucionales.

INTRODUCCION

Los Sistemas Informáticos se han constituido en las herramientas poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial. La Informática de hoy está relacionada en la gestión integral de la empresa bajo normas y estándares propiamente informáticos.
Es aclarar que la Informática no gestiona la empresa, ayuda a la toma de decisiones, pero no decide por sí misma.
No debemos olvidar la incorporación de nuevas tecnologías en el quehacer diario de las empresas y el creciente uso de las mismas como herramienta de competencia y desarrollo de sus operaciones electrónicas y de nuevos esquemas de negocios que están generando un entorno competitivo radicalmente distinto al tradicional. En tal sentido las empresas a través de los auditores de sistemas, tienen que tomar medidas que permitan un crecimiento o desarrollo adecuado de este tipo de operaciones y que al final podamos establecer mecanismo idóneo para la administración y regulación del riesgo tecnológico.

Además, la calidad de información que se maneja es importante para todas aquellas personas que las necesitan, y de nada sirve la información incorrecta e irrelevante; este tipo de información no hace más que ocasionar pérdidas de tiempo y recursos a las empresas que la reciben. En base a lo anterior se expresa que "La calidad de la información descansa sobre tres pilares: exactitud, oportunidad y relevancia a los cuales son los atributos claves de toda buena información". Exactitud, quiere decir que la información tiene que reflejar exactamente lo que significa: libre de errores y ambigüedades, tiene que representar claramente el sentido de los datos de manera que el receptor comprenda de forma inmediata lo que se quiere transmitir, en cuanto a la oportunidad; la información tiene que llegar a manos del receptor justo cuando la necesite, .el tercer punto es la relevancia de la información; el cual trata sobre si la información recibida es importante o no.

Las premisas anteriores nos permiten visualizar la necesidad de presentar el "Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información", al cual nombraremos como "MASTI", formado por cuatro capítulos detallados así:

Capítulo uno. Se explica los conceptos básicos de Auditoría de Sistemas, así como los objetivos del manual, alcances, antecedentes que permitan conocer la evolución de la disciplina.

Capítulo dos. Se mencionan y describe de forma breve los puntos importantes del riesgo tecnológico y el rol del auditor de sistemas.

Capítulo tres. Se hace referencia a la metodología de investigación de campo y el resultado de las encuestas con su respectivo análisis.

Capítulo cuatro. Describe la metodología que debe de seguir el auditor para implementar la auditoría, así mismo detalla el contenido del manual de auditoría de sistemas para la evaluación de la tecnología de información (MASTI), mostrando las actividades orientadas a objetivos de control que forman cada División, siendo estas: Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación.
También incluye las herramientas que le permiten al auditor apoyarse para la evaluación automática de datos, así como software para el control de tráfico en la red.

CAPÍTULO I
1. DESCRIPCIÓN DEL PROYECTO

1.1 OBJETIVOS DEL PROYECTO

1.1.1 OBJETIVO GENERAL

Diseñar un manual de Auditoría de Sistemas que permita realizar el proceso de evaluación de la Tecnología de Información, considerando cuatro divisiones específicas de control: Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación.

1.1.2 OBJETIVOS ESPECIFICOS

a. Definir un marco conceptual que proporcione una visión general de la auditoría en el área de Tecnología de Información.

b. Diseñar un instrumento de auditoría de sistemas que identifique las áreas a evaluar y el alcance del examen de forma que le permita a los profesionales del área, facilitar y homogenizar el desarrollo de la auditoría de sistemas con base a una metodología.

c. Elaborar guías de auditoría de sistemas para las divisiones de Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación, orientadas a minimizar el riesgo tecnológico.

d. Proporcionar a las instituciones un instrumento que permita evaluar los sistemas de información y el entorno tecnológico de la empresa.

e. Realizar un Diagnóstico de la Tecnología de Información de forma que permita identificar si los resultados obtenidos están alineados con los objetivos estratégicos de la empresa.

f. Permitir al auditor de sistemas emitir una opinión sobre las áreas evaluadas con base en los resultados obtenidos de la aplicación del instrumento diseñado en este trabajo.

1.2 ALCANCES Y LIMITACIONES DEL PROYECTO

1.2.1 ALCANCES DEL PROYECTO

a) El manual comprenderá cuatro Divisiones denominadas: Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación.

b) El manual comprenderá una lista de verificaciones de los principales aspectos a evaluar en cada una de las divisiones, los cuáles podrán aplicarse independientemente de la plataforma e infraestructura tecnológica de la empresa.

c) La investigación de campo se aplicará al sector privado, específicamente a la mediana y gran empresa de El Salvador.

1.2.2 LIMITACIONES DEL PROYECTO

a) El manual es de carácter general, no está orientado a una plataforma específica.

b) El manual deberá ser actualizado periódicamente por los auditores, con las nuevas tendencias tecnológicas existentes en el mercado informático.

1.3 ANTECEDENTES

1.3.1 RESEÑA HISTÓRICA SOBRE TECNOLOGÍA DE INFORMACIÓN (TI)

La información es uno de los activos más importantes de las organizaciones y de modo especial en el sector productivo, por ello cada día las entidades dependen más de la información y de la tecnología, hace unos años atrás, la protección de la información era fácil, con plataformas y arquitecturas centralizadas y terminales fuera de línea, actualmente los entornos son complejos, con diversidad de plataformas y expansión de redes internas y externas, con enlaces internacionales. Los Sistemas Informáticos se han constituido como las herramientas más poderosas para materializar los conceptos vitales que conforman la organización empresarial.

La Informática de hoy forma parte de la gestión integral de las empresas, habiéndose establecido normas y estándares propiamente informáticos, en consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado "Tecnología de la Información (TI)". La Informática proporciona la versatilidad a las empresas y administra los datos para la toma de decisiones, pero no decide por sí misma. Por lo tanto, la importancia de la auditoria de sistemas informáticos debe considerarse como parte de la Gestión Organizacional.

La palabra auditoría proviene del latín *auditorius,* y de esta proviene auditor, que se refiere a todo aquel que tiene la virtud de oír y revisar cuentas, el cual es orientado a un objetivo específico y facultar al auditor para que exprese una opinión respecto al objetivo de su revisión en todos sus aspectos significativos de acuerdo a estándares, sin embargo, con el agregado de la palabra Informática podemos expresar; que auditoría en TI es la revisión y la evaluación de los controles, sistemas, procedimientos de informática, equipos de cómputo, su utilización, eficiencia y seguridad de la organización a fin de que por medio de lo señalado concluya respecto a su razonabilidad y exactitud.

La auditoría de sistemas es de vital importancia para el buen desempeño de los sistemas de información, ya que valida la efectividad de los controles, en virtud para

que éstos sean confiables y seguros. Por otra parte, la evaluación y revisión de la auditoría se define como el conjunto de métodos y procedimientos técnicos que se aplican a los sistemas, con el fin de verificar el cumplimiento de las políticas y normas que existen en las instituciones, determinando el grado de confianza, así como llevar a cabo las acciones procedentes con objeto de mejorar la gestión.

1.3.2 CARACTERÍSTICAS GENERALES DE LA AUDITORIA

Los sistemas de información son recursos de vital importancia para las empresas de hoy, entonces el auditor tiene la responsabilidad de hacer que el uso de los recursos de la empresa se administre correctamente para llegar a tener conocimiento pleno de la actividad informática. Por ello es importante, pues la utilizan para realizar la gestión de negocios en forma óptima con la finalidad de obtener los beneficios económicos y de costes deseados. De acuerdo a todo esto los sistemas de información están sujetos a un control permanente y se toman en cuenta tanto como otros órganos de la empresa o entidad a la que se está haciendo la auditoría.

El hecho de realizar una Auditoría de Sistemas es importante debido a que las herramientas que se utilizan pueden definir o marcar la diferencia con respecto a la competencia o al momento en que se está viviendo. El mal diseño de los sistemas puede ser perjudicial, porque puede traer consecuencias desastrosas para la organización debido a que las máquinas sólo reciben órdenes de forma incuestionable, y el perfil de las organizaciones se encuentra supeditada al buen funcionamiento de estas, las cuales materializan los sistemas de información, entonces la empresa no puede permitir que el software, el hardware, los datos y la documentación presenten deficiencias porque va en contra de sus propios intereses y de la gestión de crecimiento que proyecta la empresa dentro de su plan estratégico.

Todos sabemos que las computadoras pueden tener fallas en la información elaborada y arrojar resultados erróneos, pero si es que dichos datos son igualmente erróneos. Tal situación se da frecuentemente cuando las instituciones pierden de vista la naturaleza y calidad de la información que ingresan a sus sistemas de consulta, con el peligro de que otros sistemas que son independientes se vean

afectados por este hecho, por ello la necesidad de realizar una auditoría de sistemas es importante para las empresas, por que les permitirá conocer la capacidad que tienen, a nivel informático.

La Auditoría debe ser independiente, no toma acciones pero da sugerencias, y sus conclusiones deben considerarse en la toma de decisiones, previa también a una evaluación de las partes involucradas. La auditoría se apoya de herramientas de análisis, verificación y exposición conformando así elementos de juicio, los cuales permitirán determinar las debilidades y fortalezas.

Con todos los elementos de juicio recolectados, el Auditor podrá emitir un informe en el cual expresará el estado en el que ha encontrado los sistemas, expondrá las debilidades para su mejora. En cuanto a la información recolectada, esta es estrictamente confidencial, es propiedad de la empresa y para la empresa auditada, tendrá una importancia especial, además esta información es considerada como un activo real.

Por su independencia la auditoría de sistemas ocupa dentro de la estructura organizacional un nivel jerárquico que le permite llevar a cabo su trabajo, sin que las áreas auditadas puedan incidir en el alcance de la revisión.

Funcionalmente el auditor de sistemas podrá ser parte de la Dirección de Auditoría Interna a nivel de Staff, reportando directamente a la estructura de la cual depende.

La ejecución de la auditoria de sistemas será íntegra, es decir obtener un conocimiento pleno de la actividad informática, las normas y parámetros establecidos por la empresa verificando su cumplimiento, y la gestión de los recursos humanos y materiales.

El trabajo de la auditoría debe ser objetivo, respondiendo a la metodología propuesta en el presente documento; el auditor de sistemas deberá planear su trabajo obteniendo un conocimiento pleno de TI, evaluando controles, determinando áreas críticas y diseñando las pruebas a realizar teniendo en cuenta el riesgo de la existencia de errores y/o irregularidades, los resultados de la auditoría de sistemas serán de carácter confidencial y de interés del organismo de dirección, las observaciones deberán ser planteadas a las partes involucradas y el auditor deberá

estimar las oportunas argumentaciones de la conclusión del examen y divulgación de los resultados.

En la ejecución de la auditoría de sistemas deberá considerarse la adecuación de la dirección de informática a estándares y normas técnicas vigentes; en concordancia con el grado tecnológico alcanzado, en cuanto a infraestructura y tamaño de la organización.

1.3.3 RAZONES PARA EFECTUAR UNA AUDITORÍA DE SISTEMAS

La Alta Dirección de la organización deberá considerar la realización de una auditoría de sistemas, cuando se presente más de una de las siguientes razones.

a. Aumento considerable e injustificado del presupuesto de Procesamiento de Datos.
b. Desconocimiento en el nivel directivo de la situación informática de la empresa.
c. Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
d. Descubrimiento de fraudes efectuados con la computadora.
e. Falta de una planificación informática.
f. Organización que no funciona correctamente por falta de: políticas, objetivos, normas, metodología y adecuada administración del Recurso Humano.
g. Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.
h. Los promedios conseguidos no se habitúan a los estimados por lo que concesiones de productividad no son respetados y sufren un desvío en su calidad.
i. Los resultados periódicos no son entregados en los plazos establecidos.
j. Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento y continuidad de los sistemas liberados en producción.

1.4 PLANTEAMIENTO DEL PROBLEMA

La auditoría no es una actividad esencialmente mecánica que afecte la aplicación de algunos procedimientos cuyos resultados una vez llevados a cabo, son de carácter indudable. La auditoría requiere de un ejercicio de juicio profesional, sólido y de razón para realizar seguimiento a los resultados obtenidos. Por ello la auditoría nace como una unidad de control de algunas organizaciones, a la cual se sujeta que la función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones, queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades, aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades mencionadas con anterioridad; estas sugerencias plasmadas en el informe final reciben el nombre de Recomendaciones.

Las funciones de análisis y revisión que el auditor informático realiza, puede contraponer con la psicología del auditado, ya que es un informático u operativo, aunado a la necesidad de realizar sus tareas con racionalidad y eficiencia, la resistencia del auditado es comprensible y, en ocasiones fundamentada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los cortos plazos en tiempo de los que suelen disponer para realizar su tarea. Además, la evaluación de los Sistemas, el auditor somete al auditado a una serie de puntos de control, la concatenación y secuencia de los referidos puntos, llamados “Programas de Auditoría” o “Guía de Objetivos específicos de control” que le permitirán brindar las opiniones.

Con base a las referencias en mención y la investigación realizada, se comprobó que las empresas necesitan fortalecer el control interno en el área de tecnología información (TI), debido a que se observó que los programas o puntos de control se encuentran deficientes o débiles en su contenido y alcance.

1.4.1 MODELO DE LA CAJA NEGRA

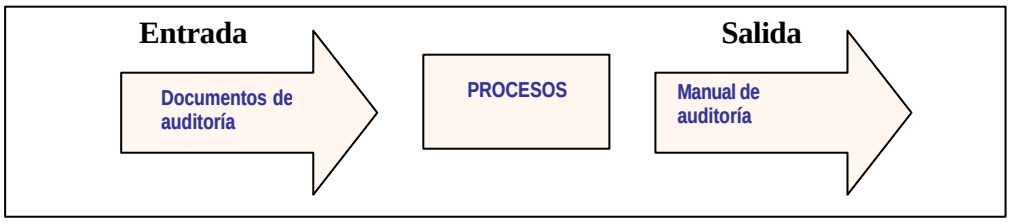
Un problema puede formularse verbal o de forma teórica y esquemáticamente. Para ello el Método de la Caja Negra[1], permite visualizar un problema en forma esquemática cuyo objetivo es visualizar un conjunto de variables de entrada que a través de un proceso se conviertan en la solución al problema planteado.

ENUNCIADO DEL PROBLEMA

No se dispone en el medio de un manual que permita evaluar a través de la auditoría la totalidad de la tecnología de información (TI), bajo un esquema de objetivos específicos enfocado a riesgo tecnológico.

ESTABLECIMIENTO DE UNA ESTRATEGIA DE SOLUCIÓN

La elaboración de un manual que facilite y optimice el proceso de la realización de auditoria en tecnología.



Dificultad de encontrar un documento completo que presente una guía de los aspectos a evaluar de las principales áreas de Tecnología de Información.		Se dispondrá de un manual que será una guía de los aspectos a evaluar de las principales áreas de Tecnología de Información.
Falta de un instrumento teórico que permita identificar los riesgos tecnológicos a los que están expuestas las empresas en el área de Tecnología de Información.		Se tendrá a disposición un instrumento teórico práctico que permita identificar los riesgos tecnológicos a los que están expuestas las empresas en el área de Tecnología de Información.

[1] Tomado de Introducción a la Ingeniería y al diseño en la Ingeniería. 2da. Edición, Krick,Edward .

Programas de auditoría de sistemas incompletos y propiedad de cada empresa en particular.		Se tendrá a disposición guías técnicas completas de aplicación para cualquier organización.
Falta de base conceptual en el área de Auditoría de Sistemas.		Establecer una base conceptual de Auditoría de Sistemas.
Falta de herramienta de evaluación en el área de auditoría de sistemas.		Proporcionar una herramienta de evaluación para el área de auditoría de sistemas.

1.5 JUSTIFICACIÓN DEL PROYECTO

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la Información y de la Tecnología de Información (TI). En esta sociedad global, donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad, sustenta la creciente dependencia en información y la creciente vulnerabilidad de los sistemas de información. Por ello para muchas organizaciones la información y la tecnología que la soporta representan los activos más valiosos de la empresa. Por lo que se hace necesario que la alta administración incluya dentro de su estructura un área de Auditoría de Sistemas, la cual es de vital importancia para el buen desempeño de los sistemas informáticos, considerando la revisión y evaluación de las Divisiones siguientes: Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación. Partiendo de las premisas anteriores para el buen desempeño y cumplimiento de la auditoría se requiere de un manual que reúna las principales divisiones que conforman la Tecnología de Información, el cual contenga las guías de trabajo para desarrollarlas.

MASTI (Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información) es el documento propuesto, debido a que en la actualidad no existe un manual completo que reúna estas condiciones. Al respecto, la propuesta de MASTI será guía práctica de aplicación para profesionales en Auditoría de Sistemas en el área de Tecnología de Información y para los docentes será un documento de apoyo para la enseñanza universitaria de dicha área.

1.5.1 ESTUDIO DE FACTIBILIDAD

La factibilidad de MASTI se determinó por dos factores: Operativo y Económico por la naturaleza del proyecto, cabe mencionar que después de haber realizado el estudio preliminar y la investigación de campo se obtuvo como resultado la continuidad y factibilidad del mismo.

1.5.1.1 FACTIBILIDAD OPERATIVA

Debido a la carencia en el medio de un manual de auditoria de sistemas generado bajo objetivos específicos, la creación del referido manual es de beneficio para la aplicación de los profesionales en el área, debido a que su uso les permitirá tener una relativa certeza sobre la opinión a emitir con relación a los sistemas de información. Por otra parte la objetividad, el criterio y la experiencia de los auditores en el área es de importancia para la implementación del manual, factores que se han visualizado con el personal involucrado.

1.5.1.2 FACTIBILIDAD ECONÓMICA

La inversión de la empresa al implementar MASTI será de un bajo costo, debido a que los beneficios que se obtienen al aplicar el presente manual de auditoria superan la inversión, ya que el costo mayor está cubierto en el desarrollo de este proyecto . (Anexo B)

1.6 METODOLOGÍA Y TÉCNICAS DE LA INVESTIGACIÓN.

1.6.1 METODOLOGÍA

Todo desarrollo implica estructurar el entorno de la información interna y externa de un requerimiento, por ello la metodología que se va a utilizar en este proyecto es el modelo del Ciclo de Vida clásico o también llamado Modelo de Cascada. Este modelo define el estado de las fases a través de las cuales se mueve un proyecto. También intenta determinar el orden de las etapas involucradas y los criterios de transición asociadas entre estas etapas.

Los modelos del Ciclo de vida de los Sistemas por una parte suministran una guía para aquellos usuarios que desean ordenar las diversas actividades técnicas que conforman un proyecto, así mismo suministran un marco para la administración del desarrollo y el mantenimiento, en el sentido en que permiten estimar recursos, definir puntos de control intermedios, monitorear el avance, etc.

Con base a lo anterior podemos afirmar que un sistema es simplemente un conjunto de componentes que interactúan para alcanzar un objetivo y de hecho los sistemas es todo aquello que rodea al ser humano. Sin embargo queremos también demostrar que el uso base de esta metodología y con algunas variaciones en sus etapas es posible el desarrollo del presente manual.

1.6.1.1 INVESTIGACIÓN PRELIMINAR

La solicitud para recibir ayuda de un sistema de información puede originarse por un usuario, cuando se formula la solicitud comienza la primera actividad del sistema, por lo que antes de considerar cualquier investigación esta debe examinarse. Al respecto, si bien es cierto que en Internet existen manuales de auditoria, estos no se encuentran de forma completa o se presentan demasiado generalizados los cuales es difícil su aplicación o integración con otras áreas, de igual forma ocurre con algunos libros que se encuentran en el medio, por lo que las situaciones en referencia nos incentivan a la creación de MASTI.

1.6.1.2 ANÁLISIS DE LOS DATOS

La información recopilada en la fase anterior nos permite como consecuencia establecer el alcance, los objetivos y requisitos del manual de auditoria, examinando con ello las posibles alternativas de fortalecimiento del control interno de los sistemas de información.

1.6.1.3 DISEÑO DE LAS DIVISIONES

El diseño de las divisiones corresponde al esquema que tendrá MASTI al agrupar las áreas y las actividades que la conforman, orientando dichas actividades a los objetivos de control, el manual cumplirá con los requerimientos identificados durante la fase de análisis y la creación de la estructura de las divisiones las cuales corresponden a la Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación.

1.6.1.4 DESARROLLO DE LAS GUÍAS

Cada división contendrá una guía de objetivos de control y/o de actividades que permitan identificar las fortalezas ó debilidades de cada división en el área de la tecnología de información, la finalidad de las guías es aumentar la exactitud, integridad y confianza de la información.

1.6.1.5 PRUEBAS Y CORRECCIÓN

Se emplea de manera experimental para asegurarse que el manual no tenga fallas en la aplicación, es decir que funcione correctamente en las áreas a evaluar.

1.6.1.6 DOCUMENTACIÓN

Esta fase nos permitirá agrupar cada actividad u objetivo de control al dominio que la deriva, asimismo estará relacionado a las sub actividades que la conforman.

1.6.2 TÉCNICAS DE INVESTIGACIÓN

Las técnicas tienen como objeto reunir datos relacionados con los requerimientos, entre estos se incluyen la entrevista, el cuestionario, la revisión de los registros y la observación, por ello la fase de investigación preliminar nos permitirá profundizar en cada técnica de acuerdo a la complejidad de la misma.

Técnica Documental: La cual será posible recolectar todos los formatos de programas y documentación relacionada a la auditoria, asimismo nos permite conocer procedimientos y la aplicación de políticas y normas en el área.

Técnica de observación: Es aquella mediante la cual el investigador tiene la capacidad de observar los eventos y las acciones que permitan analizar la situación desde un punto óptico y de forma adecuada. Con ello comprobamos que muchas empresas carecen de programas de auditoria integrados bajo objetivos específicos de control.

La Entrevista: Es aquella mediante la cual existe una interrelación entre el investigador y las personas que componen el objeto de estudio, el propósito de esta técnica es conversar de una manera formal sobre algunos aspectos establecidos con anterioridad y a su vez recolectar información que permita conocer la situación actual del punto a tratar. Esta técnica nos permitió conocer información con funcionarios de las instituciones a las cuales se entrevistó sobre los procesos y métodos utilizados en la evaluación de los sistemas de información, también intercambiar experiencias.

La Encuesta: Permite realizar una medición sobre aspectos relacionados a la investigación que se ejecuta, arrojando datos fehacientes, debido a que las preguntas utilizadas fueron de forma estructurada, sobre la aplicación de auditoria de sistemas en el área específica de informática, es la encuesta la que nos permite tener una visión más amplia de la situación actual en que se desarrollan dichas actividades.

1.7 RESULTADOS ESPERADOS

La elaboración de un manual de auditoría de sistemas para la evaluación de las principales áreas de Tecnología de Información, traerá en su aplicación beneficios inherentes, tales como:

a. Proporcionar guías técnicas orientadas al riesgo tecnológico para evaluar los sistemas de información de una empresa con el fin de garantizar niveles de seguridad adecuados para proteger la información que actualmente se considera uno de los activos más valiosos de una empresa.

b. Determinar si las operaciones inmersas en los sistemas de información se desarrollan eficientemente dentro del marco normativo y legal, así como las políticas internas de cada empresa.

c. Proporcionar a la Alta Administración de la empresa una opinión que garantice que la información generada por los sistemas de información utilizados para la toma de decisiones es confiable y oportuna ó se presenta de forma razonable.

d. Los profesionales involucrados en el área se verán favorecidos al contar con un manual que les permita planificar en un tiempo definido el alcance de las áreas a evaluar de acuerdo a los objetivos del examen de auditoría

CAPITULO II

2. MARCO TEÓRICO

2.1 RIESGOS DE TECNOLOGÍA

Considerando la definición de riesgo como la posibilidad de que los acontecimientos o eventos esperados o imprevistos puedan tener un impacto negativo sobre el servicio y uso de la tecnología, así como puede afectar las ganancias y el capital de la empresa. Consecuentemente por ello, la alta administración de cada institución debe estar consciente de esta perspectiva y crear mecanismos que le permitan anticiparse a los cambios que se están produciendo en la tecnología, debido a que las operaciones vía electrónica facilitan el acceso y disminuye los costos operativos, por lo que puede rápidamente convertirse en un servicio de uso masivo, incidiendo en el incremento de los riesgos en que incurren las organizaciones.

Las diversas ofertas de soluciones tecnológicas que pueden ser utilizadas por las entidades en sus operaciones, hacen que permitan al menos identificar el control de los riesgos inherentes al uso de la tecnología. En consecuencia, el presente trabajo permitirá a las instituciones tener una autorregulación y control de los riesgos asociados al riesgo tecnológico, por eso es de interés conocer la funcionalidad que la tecnología ha aportado al crecimiento de la sociedad moderna y a la empresa misma, y como consecuencia, se ha presenciado un ambiente de cambio importante orientado a la búsqueda de la aplicación del conocimiento apoyado sobre un medio de mayor efectividad para el procesamiento de las funciones diarias del ser humano. Esta situación es de especial énfasis en todos y cada uno de los sectores, e incluso ha permitido la extensión de las fronteras culturales, operativas, legales y gubernamentales.

Ante las diversas ofertas de soluciones tecnológicas que pueden ser utilizadas por las entidades comerciales, es de suma importancia que la auditoría de sistemas esté en plena capacidad y objetividad de establecer las evaluaciones a seguir para manejar el impacto tecnológico que estas causan.

Todos y cada uno de los factores que conforman a cada empresa deberán contribuir

a la reducción de estos riesgos, adoptando las medidas que permitirán a los auditores prevenir, detectar y corregir las irregularidades que se puedan presentar en el desarrollo de las operaciones diarias de las empresas.

2.1.1 ADMINISTRACIÓN DEL RIESGO

Las actividades tecnológicas pueden permitir que las entidades amplíen sus nichos de producción para las actividades tradicionales y que ofrezcan productos y servicios nuevos que consoliden su competitividad junto a los existentes, reduciendo los costos en las transacciones y propiciando una reducción importante en sus gastos operativos a la vez que proporcionan una mayor facilidad de acceso para los clientes. En este contexto, los auditores de sistemas tienen que cumplir dos papeles principales en el proceso de administración de riesgos: a) Establecer parámetros uniformes para limitar los riesgos en su conjunto. b) Asegurar que la entidad a que pertenece posee elementos del entorno que permitan minimizar el riesgo.

2.1.2 IDENTIFICACIÓN DEL RIESGO

Debido a los rápidos cambios en tecnología de la información, ninguna lista de riesgos puede ser exhaustiva. Los riesgos específicos a que hacen frente las empresas se involucran en actividades que se pueden agrupar según las categorías de riesgo.

Los riesgos básicos generados por actividades de cada entidad, pueden ser: Operativo, Legal, Reputación y sistemas entre otros.

2.1.3 RIESGO OPERACIONAL

El riesgo operacional es la posibilidad de que deficiencias significativas en la confiabilidad del sistema de información o en su integridad puedan resultar en pérdidas financieras y afectar las ganancias y el capital de la empresa. También es conocido como riesgo de transacción y surge de problemas en la entrega de servicios o productos ofrecidos a través del uso transacciones. El riesgo operacional puede también presentarse de uso erróneo de los sistemas por parte del cliente, así como de aplicaciones electrónicas con diseño no adecuado puestas en ejecución.

Como la mayor parte de los riesgos se desarrollan durante el proceso de las transacciones, es conveniente definir los riesgos asociados al riesgo operacional o transaccional:

2.1.3.1 SEGURIDAD

El riesgo de seguridad se presenta con respecto a los controles sobre el acceso a las operaciones internas de la empresa y sus sistemas de control de amenazas. El acceso a los sistemas se ha vuelto cada vez más complejo debido a las amplias capacidades de las computadoras, a la dispersión geográfica de los puntos de acceso y al uso de varias trayectorias de comunicación, incluyendo redes públicas, el acceso no autorizado por parte de empleados a los sistemas puede conducir a pérdidas directas, asumir responsabilidades de parte de la empresa, además de ataques externos.

2.1.3.2 CONFIDENCIALIDAD

Este es uno de los riesgos más sensibles, ya que si no se adoptan medidas de seguridad, las transferencias de datos viajan abiertas a través de la red, dejando la posibilidad de que se coloquen a la puerta de un servidor donde se realicen operaciones y se obtenga información.

2.1.3.3 INTEGRIDAD DE LOS DATOS

Se refiere a la posibilidad de que los datos de una operación puedan ser modificados en el momento de ser transferidos o mientras se hallan almacenados en un sistema informático, por personas ajenas a las partes involucradas, generando conflicto de intereses por una variación en los datos registrados en los sistemas.

2.1.3.4 AUTENTICACIÓN

Es un factor fundamental para la legitimidad de una operación, la ausencia de ella posibilita que a partir de una serie de técnicas, un usuario pueda ocultar su identidad o asumir la de otro.

2.1.3.5 NO REPUDIO

Si no existen medios para demostrar la intervención de las partes en una transacción electrónica, se genera el riesgo de que cualquiera de ellas pueda rechazar los cargos que se deriven del negocio subyacente o simplemente se niegue la participación en el mismo. Este riesgo es el resultado de la falta de mecanismos que permitan la identificación y autenticación absoluta del cliente.

2.1.3.6 PROGRAMAS DE BÚSQUEDA DE FISURAS

Existen programas que permiten localizar los puntos débiles de la seguridad de un servidor. Aunque su utilidad esencial es preventiva, ello no impide que sean utilizados con intención de lanzar ataques contra el sistema, lo que se traduce en un potencial riesgo cuando se use en contra de la empresa.

2.1.3.7 POLÍTICAS

La ausencia de control y políticas de acceso a los sistemas y servicios puede constituirse en un riesgo que podría afectar las operaciones de la empresa.

2.1.3.8 AGUJEROS DE SEGURIDAD

Cuando se localiza un fallo de seguridad en un sistema operativo, navegador, Firewall, o cualquier otro elemento del sistema, se produce una inmediata difusión a través de Internet, lo cual permite alertar a los administradores del servidor, pero también es una posibilidad de que se produzca un ataque antes de subsanar el problema, por tal razón este tipo de lagunas en la seguridad incrementan el riesgo de transacción.

2.1.3.9 USO ERRÓNEO DE SERVICIOS

El uso erróneo de los productos y servicios por parte del cliente, sea este intencional o inadvertido, es otra fuente del riesgo operacional. El riesgo puede ser aumentado

cuando la empresa no educa adecuadamente a sus clientes sobre las precauciones de la seguridad.

2.1.4 RIESGO DE REPUTACIÓN

El riesgo de reputación es el que resulta de la opinión pública negativa y trae como resultado una pérdida en las ganancias o el capital. Este riesgo se presenta cuando los sistemas o los productos no trabajan según lo esperado y causan una reacción pública negativa extensa. El riesgo reputación también puede presentarse si las acciones que realiza la empresa causa una pérdida importante en la confianza pública y afectan su capacidad para cumplir con sus funciones y operaciones críticas.

2.1.5 RIESGO LEGAL

Es el riesgo que enfrentan las ganancias o el capital que surge de violaciones o de incumplimiento a leyes, normas, regulaciones y prácticas reglamentarias vigentes, o cuando los derechos y las obligaciones de las partes no han sido establecidas en una transacción electrónica.

El riesgo legal y reglamentario puede exponer a la empresa a sanciones o multas, pago de daños o invalidación de contratos, entre otros. Por ejemplo quebrantamiento a ley de propiedad intelectual, IVA, renta, etc.

2.1.6 RIESGO DE DEPENDENCIA TECNOLÓGICA

Se refiere al riesgo de pérdida en el capital, por un mal desempeño de los proveedores de sistemas tecnológicos, o por debilidades en los contratos de estos servicios. También, puede resultar de un bajo desempeño con relación a las expectativas futuras de la empresa.

Varias empresas se inclinan por confiar en proveedores y consultores externos para la implementación y ejecución de sus sistemas. Tal confianza puede ser deseable porque permite operar bajo los aspectos de un “outsourcing”, la confianza en la subcontratación expone a una empresa a los riesgos de dependencia operacional.

2.1.7 MEDICIÓN DEL RIESGO

El esquema de medición del riesgo que adopte la empresa debe tener una herramienta de soporte para determinar el método apropiado, ya que medir el riesgo es un elemento crítico en un proceso efectivo de administración del riesgo tecnológico. Esto se debe a que la medición permite a la gerencia priorizar, controlar y verificar el riesgo, y en función de ello, tomar las medidas correspondientes oportunamente.

2.1.8 SEGUIMIENTO DEL RIESGO

Las actividades de seguimiento del riesgo deben estar apoyadas por sistemas de información que provean a la Alta Administración la condición financiera, resultados operativos y exposición al riesgo de la organización en su conjunto.

2.1.9 CONTROL DEL RIESGO

Los controles son los procedimientos establecidos por la empresa para mitigar los riesgos. La empresa tiene que diseñar y poner en funcionamiento un sistema de gestión sobre las transacciones electrónicas acorde con su tamaño, volumen de operaciones y su perfil de riesgo. El sistema deberá contemplar una adecuada separación de funciones y la asignación de responsabilidades al personal. También para que el control de los riesgos sea efectivo la entidad tiene que establecer políticas, procedimientos y controles internos por escrito, donde se identifiquen los tramos de control interno que corresponden a cada nivel, atendiendo a la naturaleza de las transacciones que se realicen, muy especialmente en lo referente a medidas de seguridad, transferencias e integridad de los datos, las normas de autenticación y control de acceso.

2.2 DILIGENCIA PROFESIONAL DEL AUDITOR DE SISTEMAS

Los Auditores deberán proceder con el debido cuidado y diligencia profesional al planear y ejecutar las auditorías, preparar los informes correspondientes y dar

seguimiento a las recomendaciones formuladas por las instancias de la cual depende.

El auditor debe de considerar según el caso, las normas, políticas y su Código de Conducta Profesional y demás elementos aplicables a las auditorías. Además, deberán emplear objetivamente su juicio profesional para determinar el alcance de la auditoría, seleccionar las técnicas y procedimientos que habrán de aplicarse, practicar dichas pruebas y procedimientos, evaluar los resultados de la auditoría e informar al respecto.

2.2.1 ELEMENTOS PRINCIPALES DE LA OPERATIVIDAD

El auditor debe tener en consideración algunos elementos que le permita fortalecer el desarrollo de su actividad:

a) Los objetivos de la auditoría.
b) La importancia y el riesgo de las áreas o materias por revisar.
c) La suficiencia de los controles internos.
d) La magnitud y complejidad del trabajo por realizar.
e) Los recursos humanos disponibles y los plazos en que deberán presentarse los informes respectivos.

Por tanto, la calidad del trabajo y de los informes de auditoría dependerá de las consideraciones siguientes:

a) El alcance de la revisión y las pruebas y demás procedimientos de auditoría que se apliquen permitirán tener una seguridad razonable de que se cumplirán sus objetivos.
b) Los resultados y recomendaciones que se presenten en los informes estén claramente sustentados en una evaluación objetiva de la evidencia obtenida en la auditoría.
c) La evidencia obtenida en la auditoría sea suficiente y competente.
d) La auditoría se haya ejecutado conforme a las normas aplicables.
e) Se supervise debidamente el trabajo de los auditores.

Por ello el personal de la Auditoría deberá estar libre de impedimentos para proceder con entera autonomía en todos los asuntos relacionados con las auditorías a su cargo, en ese sentido impone a los auditores la responsabilidad de preservar su independencia a fin de que sus opiniones, juicios y recomendaciones sean imparciales y así sean considerados por terceros.

La credibilidad de los informes de resultados emitidos por la Auditoría está sustentada en su autonomía de criterio, que es indispensable para el cumplimiento de sus responsabilidades de fiscalización. Así mismo es de suma importancia el seguimiento a las observaciones realizadas con la finalidad que estas sean subsanadas, por ello el auditor deberá realizar las pruebas y verificaciones correspondientes, en tal sentido que las correcciones no impliquen maquillaje superficial en los sistemas, si más bien considere la naturalidad y raíz de la incidencia, error o deficiencia, sean estos con o sin el conocimiento de los especialistas que brindan el soporte y mantenimiento.

2.2.2 NORMAS DE EJECUCIÓN

Las normas de ejecución se refieren a la necesidad de planear y supervisar debidamente todo el proceso de auditoría; estudiar y evaluar el control interno con objeto de determinar tanto el alcance de la revisión como la naturaleza, extensión y oportunidad de las pruebas de auditoría y demás procedimientos que habrán de aplicarse; y obtener evidencia suficiente y competente para sustentar debidamente los resultados de la auditoría.

2.2.3 ATRIBUTOS DE LOS RESULTADOS DE AUDITORÍA DE SISTEMAS

Los resultados de auditoría deberán ser relevantes en cuanto a monto, incidencia, objetivos y metas del rubro sujeto a revisión, y habrán de ser congruentes con el objetivo y el alcance de la revisión, lo cual estará sujeto al auditor, conforme a las leyes, reglamentos, decretos, acuerdos y demás normativas aplicable al ente auditado.

En los resultados, no se deben incluir descripciones largas y detalladas, ya que el lector perderá la visión del conjunto, además, los comentarios no le servirán para formarse un criterio objetivo sobre una situación específica.

Para precisar un resultado de auditoría, es necesario que el auditor identifique los siguientes atributos:

ATRIBUTOS	DESCRIPCION
CRITERIO	Se puede establecer con base a: Leyes, reglamentos, decretos, acuerdos, manuales, procedimientos, prácticas, normas, políticas, etc.
CONDICION	Es la representación objetiva del hallazgo como consecuencia de la aplicación de procedimientos de auditoría, lo que es representado por la observación o resultado la cual debe sustentarse de forma eficiente y competente
CAUSA	Origen de la condición, puede derivarse de una deficiencia del control interno ó una inobservancia de un proceso, cada condición podrá tener una ó más causas que involucren la actividad o el proceso
EFECTO	La diferencia entre lo que es y el deber ser, por ello el auditor identificará si la diferencia es significativa en términos cuantitativos y cualitativos
RECOMENDACION	Acciones necesarias para prevenir y corregir los efectos referidos a las causas

Cuando estos atributos no se identifican claramente, el resultado se convierte en un conjunto de datos sin sentido que poco o nada aportan al informe de auditoría. En cambio, si los atributos se precisan, el lector del informe comprenderá la posición asumida por los auditores.

Una vez que el auditor de sistemas haya identificado el resultado de acuerdo con los lineamientos anteriores procederá a determinar el atributo que soporta cada parte de la evidencia obtenida; asimismo cada dato asentado en los papeles de trabajo tendrá que estar relacionado con el tipo de atributo que le corresponda.

CAPITULO III

3. GENERALIDADES Y METODOLOGIA DE LA INVESTIGACION

3.1 INTRODUCCION A LA METODOLOGIA DE INVESTIGACION

El vocablo *método,* proviene de las raíces: *meth,* que significa meta, y *odos*, que significa vía. Por tanto, el método es la vía para llegar a la meta. Método y metodología son dos conceptos diferentes. El método es el *procedimien*to para lograr los objetivos. Metodología es el *estudio del método.*

Según Kerlinger: "La investigación científica es sistemática, controlada, empírica y crítica, de proposiciones hipotéticas sobre las relaciones supuestas entre fenómenos naturales[...]: sistemática y controlada para tener confianza crítica en los resultados[...]; empírica, al depositar su confianza en una prueba ajena a él".

Afirma Rojas Soriano: "La investigación es una búsqueda de conocimientos ordenada, coherente, de reflexión analítica y confrontación continua de los datos empíricos y el pensamiento abstracto, a fin de explicar los fenómenos de la naturaleza". También explica: "Para descubrir las relaciones e interconexiones básicas a que están sujetos los procesos y los objetos, es necesario el pensamiento abstracto, cuyo producto (conceptos, hipótesis, leyes, teorías) debe ser sancionado por la experiencia y la realidad concreta..."

Investigar supone aplicar la inteligencia a la exacta comprensión de la realidad objetiva, a fin de dominarla. Sólo al captar la esencia de las cosas, al confrontarla con la realidad, se cumple la labor del investigador por lo que la consecuencia de tal proceso incrementará la objetividad del presente estudio.

3.2 GENERALIDADES

El estudio de campo es un trabajo creativo y sistemático que tiene como fin la aplicación del conocimiento científico con el objetivo de producir y obtener nueva información, cualidades del proceso o sistema para la elaboración de uno nuevo o la mejora de uno ya existente.

En el estudio de campo se obtiene información acerca de las necesidades de los usuarios, los problemas que tienen para realizar su trabajo, y una serie de parámetros que ayudan a la comprensión de diferentes procesos.

Con la interacción directa de los usuarios en la determinación de los requerimientos de información se puede lograr un sistema mas completo.

El objetivo del estudio de campo:

Determinar el grado de aceptación y la calidad en estructura y contenido de los programas o guías actuales de auditoría, que tiene la mediana y gran empresa a través de la información recopilada.

3.3 METODOLOGÍA DE LA INVESTIGACIÓN

3.3.1 TIPO DE INVESTIGACIÓN

La investigación desarrollada es de tipo descriptiva y de campo. Es descriptiva porque los métodos y técnicas aplicadas buscan desarrollar una imagen o fiel representación del fenómeno estudiado a partir de sus características a través de información acerca de la presencia o ausencia de algo, la frecuencia con que ocurre, quién, cómo y dónde sucede determinado evento. También es de campo porque la recopilación de la información se efectuó en las empresas que proporcionaron lo referente al área de auditoría, con la salvedad de no ser identificadas por el compromiso adquirido de confidencialidad.

3.3.2 DATOS PRIMARIOS

Están conformados por la información obtenida a través de la observación directa en las empresas visitadas, así como las entrevistas realizadas a personal con conocimientos de informática o auditoría. Los referidos instrumentos se utilizaron con la finalidad de obtener información relacionada al uso , aplicación y procedimientos de la auditoría de sistemas.

3.3.3 DATOS SECUNDARIOS

Esta información se obtuvo por medio de informes, programas, guías y apuntes de auditorías utilizados por las empresas en las evaluaciones informáticas.

3.3.4 PERSONAL PARTICIPATIVO

Los funcionarios que fueron partícipes en la investigación de la mediana y gran empresa, se detallan:

- Gerente General
- Gerente de Informática
- Auditor Interno
- Auditor Senior
- Auditor de Sistemas

3.4 DETERMINACIÓN DEL MARCO MUESTRAL

3.4.1 TÉCNICA DE INVESTIGACIÓN DE LOS DATOS IMPRESOS (REGISTROS)

Es de gran importancia el examen de diferentes tipos de documentos impresos que proporcionan información que no se encuentra disponible por ningún otro método de recopilación de datos. Aquí se examinan los datos impresos identificados en informes ejecutivos, informes preliminares, papeles de trabajo, anexos, programas, guías u otros documentos que permitan identificar importancia, debido a estos pueden ser un

indicador de qué esta sucediendo, así como muestran la forma en que se desarrollan las actividades en la realidad dentro de la organización.

3.4.2 TÉCNICA DE LA OBSERVACIÓN DIRECTA

Observar es advertir los hechos tal y como se presentan en la realidad y consignarlos por escrito, confirmar que eso está ocurriendo o dejar constancia de lo que ocurre. El fundamento científico de la observación reside en la comprobación del fenómeno que se tiene frente a la vista. La observación se convierte en método o una técnica en la medida en que cumple una serie de objetivos o requisitos.

3.4.3 TÉCNICA DE LA ENTREVISTA PERSONAL

Las entrevistas permiten descubrir áreas mal comprendidas, información que no se ha encontrado en la documentación proporcionada. Las entrevistas permiten encontrar datos cualitativos (opiniones, políticas, descripciones subjetivas de actividades y problemas) y está diseñada para ser una conversación dirigida con un propósito específico que usa un formato de preguntas y respuestas. La técnica que se aplicó en el presente estudio es entrevista abierta, en la que el entrevistado participó de forma extensiva, objetiva y crítica en la conversación. (Anexo C)

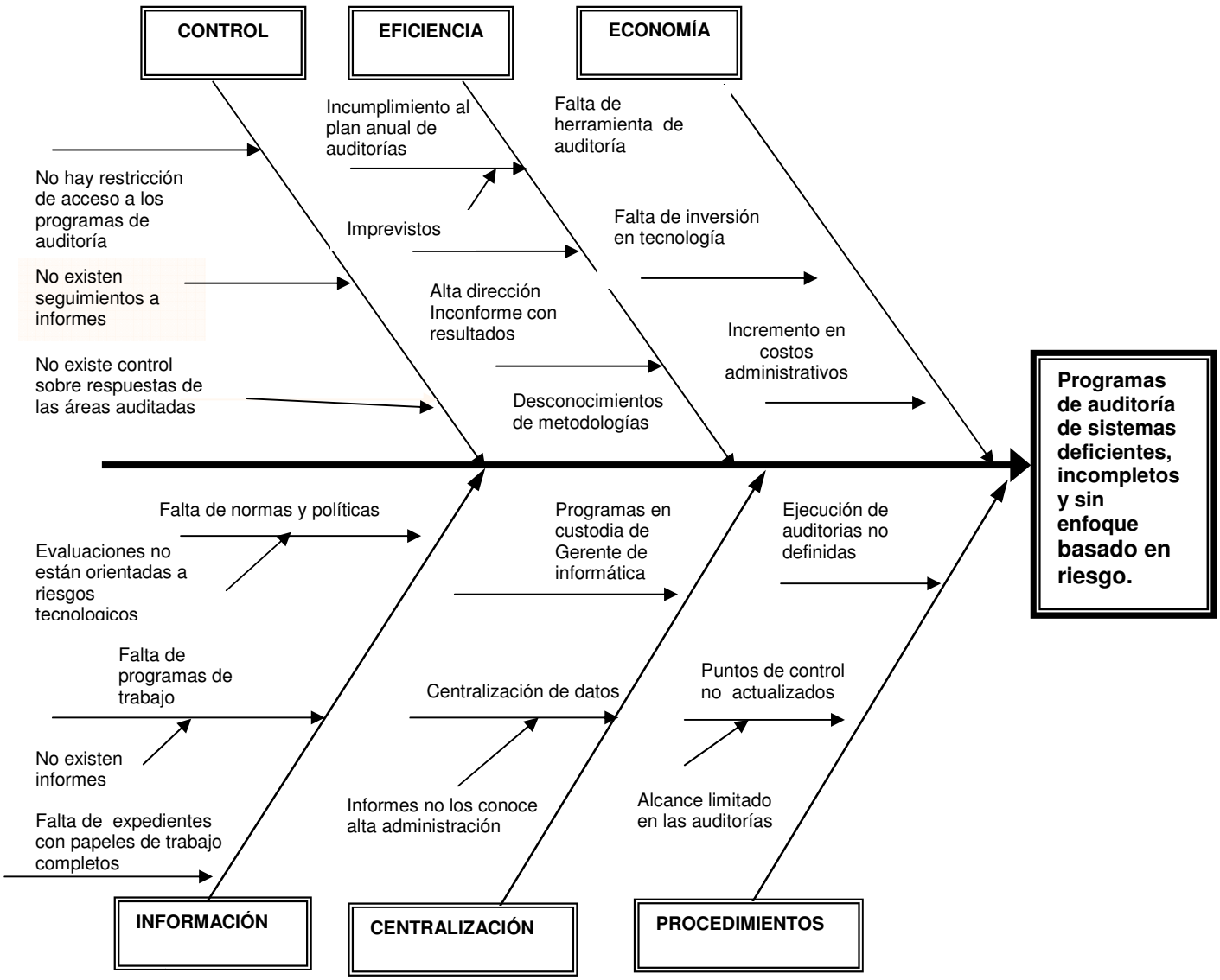
3.4.4 INSTRUMENTOS DE INVESTIGACIÓN

Tal como se hace referencia en el capítulo I, los instrumentos utilizados para esta investigación consistieron en la revisión documental sobre información impresa que permitió conocer la magnitud de los expedientes y papeles de trabajo. No obstante, la observación (no participante) por su parte nos permite identificar algunos procedimientos utilizados, por su parte la entrevista y encuesta, también fueron instrumentos de valiosa utilidad.

3.5 ANÁLISIS DE LA INVESTIGACIÓN DE CAMPO

3.5.1 DIAGRAMA CAUSA EFECTO

El diagrama de Ishikawa, o **Diagrama Causa-Efecto**, es una herramienta que ayuda a identificar, clasificar y poner de manifiesto posibles causas, tanto de problemas específicos como de características de calidad. En la que se ilustra gráficamente las relaciones existentes entre un resultado dado (efectos) y los factores (causas) que influyen en ese resultado. Como producto de las entrevistas e investigación de campo podemos presentar el esquema siguiente:



3.5.2 MUESTREO E INVESTIGACIÓN DE DATOS

Para realizar el cálculo del tamaño de la muestra a estudiar se utilizó el método probabilístico, mediante la fórmula estadística para la población finita y variable discreta, debido a que el universo se considera de naturaleza finita, aplicada el sector privado de este país, compuesta así: 7,077 empresas medianas y 2,572 grandes. [1]

La investigación se realizó por medio del método probabilístico simple debido que el personal entrevistado de las diferentes empresas son usuarios reales o potenciales del referido estudio, de acuerdo con el ámbito de la investigación y conociendo el universo o población que es de carácter finita, se utilizó la siguiente formula:

$$N = \frac{Z^2.P.Q.N}{(N-1)e^2+Z^2.P.Q}$$

DONDE:

N: Tamaño de la muestra
e : Error muestral e= 5% (0.05)
Z : Desviación estándar
P : Probabilidad de éxito de la variable. P= 0.5
Q : Probabilidad de no éxito de la variable. Q = 0.5
N : Universo o Población (10649 = 7077 + 2572)
(N-1) : Factor de Corrección por finitud (población finita)

$$\mathbf{N = \frac{(1.96)^2(0.5)\,(0.5)\,(10649)}{(10649-1)(0.05)^2 + (1.96)^2\,(0.5)\,(0.5)}}$$

$$\mathbf{N = \frac{10{,}227.2996}{27.5829}}$$

N= 370 número de encuestas

[1]. Cifras proporcionadas por el Ministerio de Hacienda de El Salvador, datos a diciembre 2005

3.5.2.1 TABULACIÓN Y ANÁLISIS DE ENCUESTAS

Después de haber recolectado los datos por medio de las encuestas (Anexo D), se procedió a tabular los datos en cuadro representativo, con sus respectivos gráficos y para su mayor comprensión de los datos obtenidos se describe un análisis por cada gráfico, para el tamaño de la muestra de 370 que representa el número de empresas encuestadas del sector privado, a las cuales se les realizó el trabajo de investigación de este documento.

Para analizar los cuestionarios se han resumido las respuestas obtenidas por cada pregunta mostrando solo aquellas que tienen relevancia para investigación tal y como se muestran en las gráficas siguientes:

PREGUNTA N° 1

¿Tiene evaluaciones de auditoría Externa en el área de Tecnología de Información?

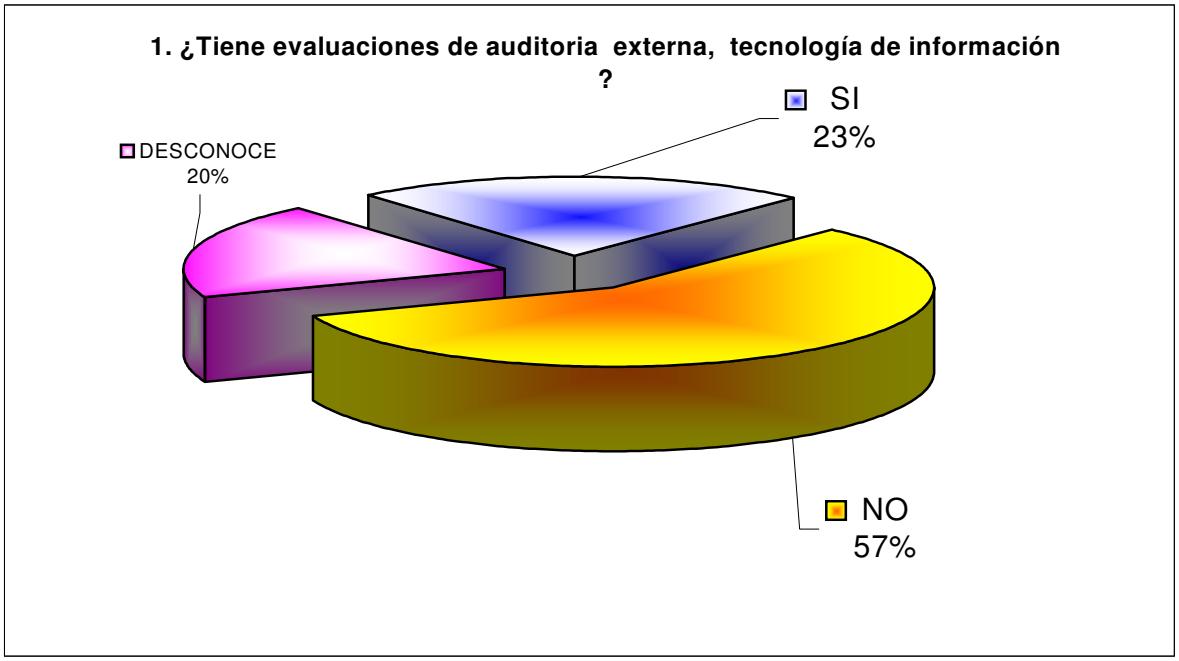
OBJETIVO:

Determinar el grado de contratación de servicios de auditoría externa en las empresas encuestadas

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
SI	30	55	85	23
NO	65	147	212	57
DESCONOCE	28	45	73	20
	123	247	370	100
Total de encuestas	123	247	370	

ANALISIS DE LOS DATOS

Como se puede observar el 57% de las empresas encuestadas no contratan los servicios de auditoría externa en área de tecnología. Es de aclarar que una parte de la mediana empresa reconocen como servicio externo la consultoria y mantenimiento, por lo que el porcentaje del 23% podría ser menor.



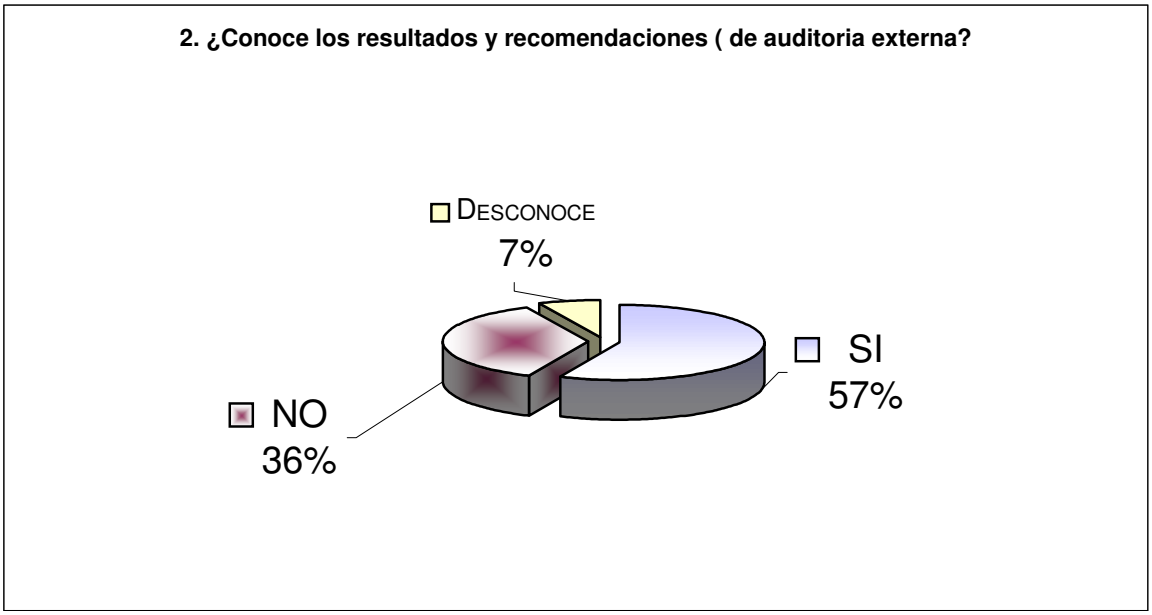
PREGUNTA N° 2
¿Conoce los resultados y recomendaciones formuladas por la auditoría externa?

OBJETIVO:
Determinar si el personal del área de auditoría de sistemas, de las empresas que contratan servicios de auditoría externa conocen el resultado de la evaluación.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
SI	18	30	48	57
NO	9	22	31	36
DESCONOCE	3	3	6	7
	30	**55**	**85**	**100**
Total de encuestas	**30**	**55**	**85**	

ANALISIS DE LOS DATOS

Como se observa en la gráfica el 36% de los entrevistados no conocen las recomendaciones realizadas por auditoría externa, un 7% no se entera sobre los resultados, y un 57 categoricamente expresò que SI.



PREGUNTA N° 3
¿Existe Centro de Cómputo en la Empresa?

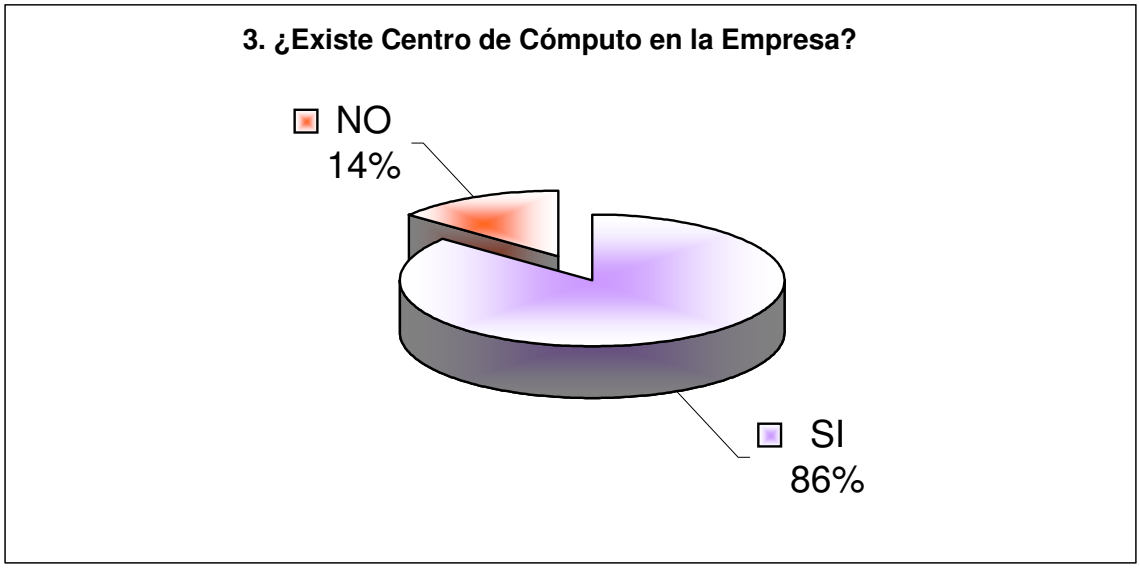
OBJETIVO:

Determinar la existencia de un centro de procesamiento de datos en las empresas entrevistadas.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
SI	90	228	318	86
NO	33	19	52	14
	123	**247**	**370**	**100**
Total de encuestas	**123**	**247**	**370**	

ANALISIS DE DATOS

Como se observa el 86% de los entrevistados afirma que disponen de un centro de cómputo en sus empresas, y el porcentaje restante no poseen o no sabe responder.



PREGUNTA N° 4

¿Qué nivel tiene el centro de cómputo dentro de la estructura organizacional?

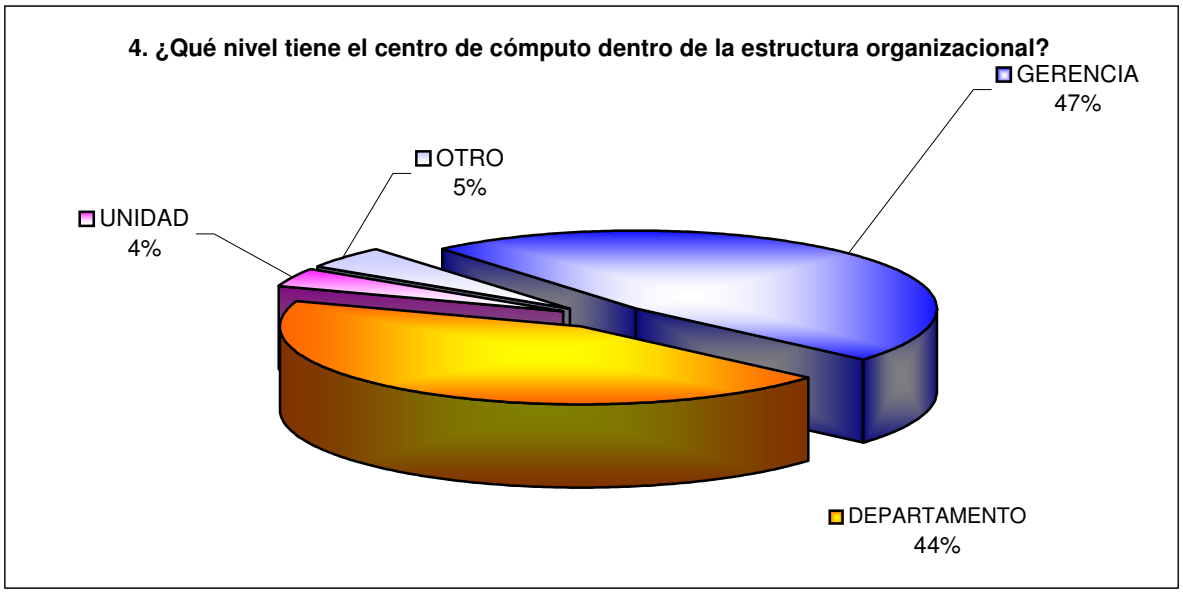
OBJETIVO:

Determinar que nivel jerárquico tiene el centro de cómputo dentro de la organización.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
GERENCIA	3	148	151	47
DEPARTAMENTO	69	71	140	44
UNIDAD	7	5	12	4
OTRO	11	4	15	5
	90	**228**	**318**	**100**
Total de encuestas	**90**	**228**	**318**	

ANALISIS DE DATOS

De la informacion obtenida de los entrevistados se observó que en la mediana empresa predomina el "departamento" y en la gran empresa la "Gerencia", y en una minoria la "unidad"



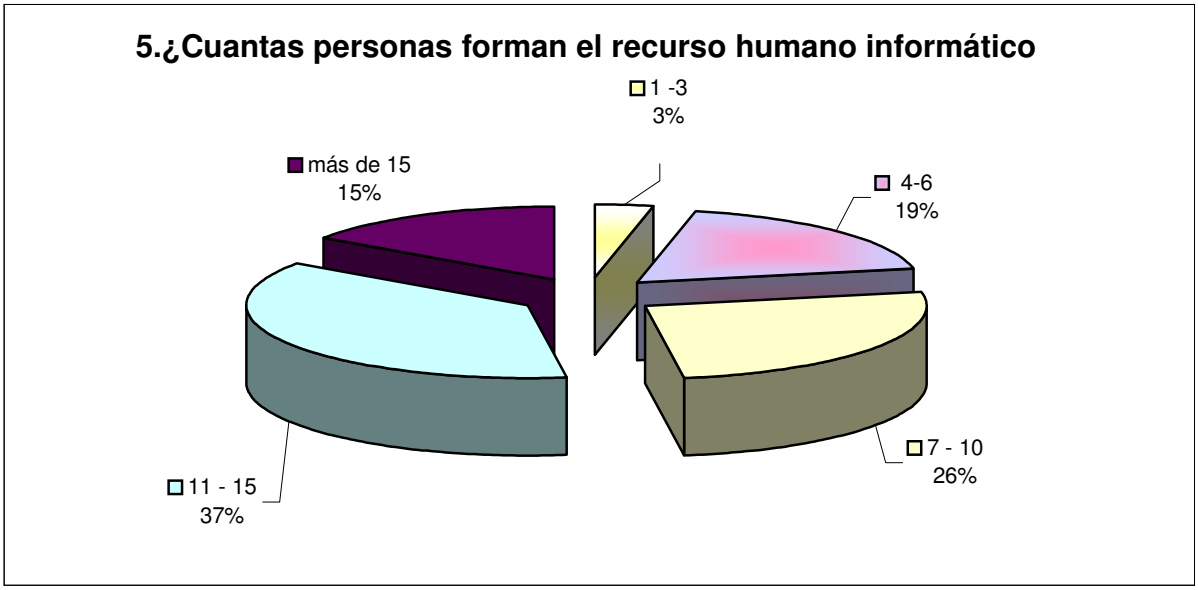
PREGUNTA N° 5
¿Cuántas personas forman el recurso humano informático ?

OBJETIVO:

Determinar e identificar la cantidad de recurso humano en el PED

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
1 -3	9	2	11	3
4 - 6	32	27	59	19
7 - 10	44	39	83	26
11 - 15	4	112	116	37
más de 15	1	48	49	15
	90	228	318	100
Total de encuestas	90	228	318	

ANALISIS DE DATOS
Como se observa en la grafica, el promedio de personas que conforman el recurso humano informàtico en la mediana empresa se encuentra en el rango 7 - 10 personas y en la gran empresa de 11 a 15 personas.



PREGUNTA N° 6

¿En su opinión que porcentaje hace uso de las computadoras para desempeñar sus actividades?

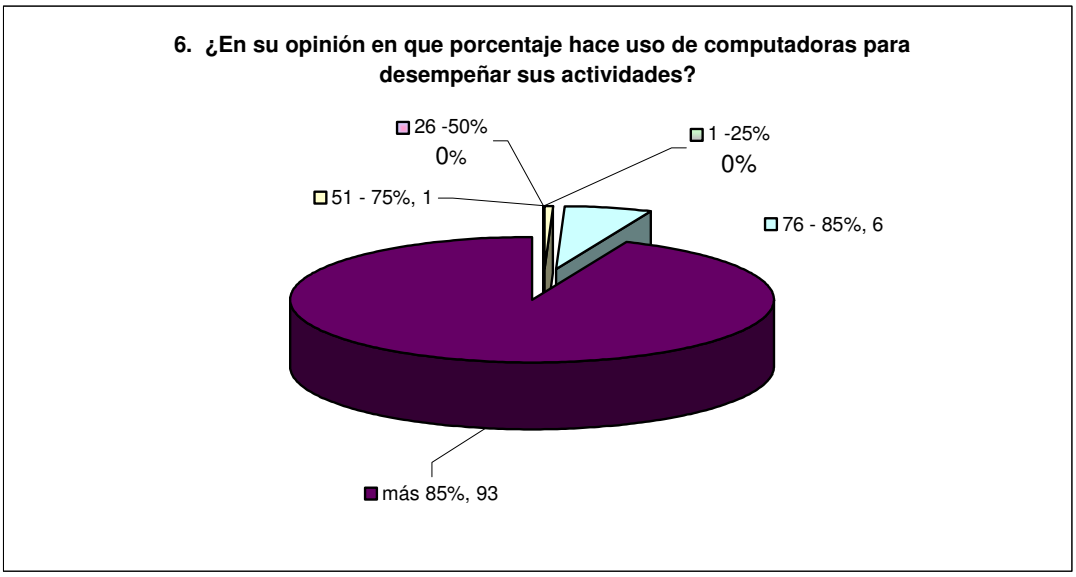
OBJETIVO:

Estimar un porcentaje dado por el entrevistado del uso que hace de las computadoras en sus actividades laborales.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
1 - 25%	0	0	0	0
26 - 50%	0	0	0	0
51 - 75%	2	0	2	1
76 - 85%	7	11	18	6
más 85%	81	217	298	93
	90	228	318	100
Total de encuestas	90	228	318	

ANALISIS DE DATOS

Uno de los aspectos relevantes que los entrevistados proporcionaron es que para el 94% de ellos la informacion procesada en sus computadoras representa màs del 85%, lo cuál manifiesta que el desarrollo de las actividades laborales depende en gran medida de la tecnología y el PED.



PREGUNTA N° 7

¿Cuántos sistemas tiene la empresa en funcionamiento?

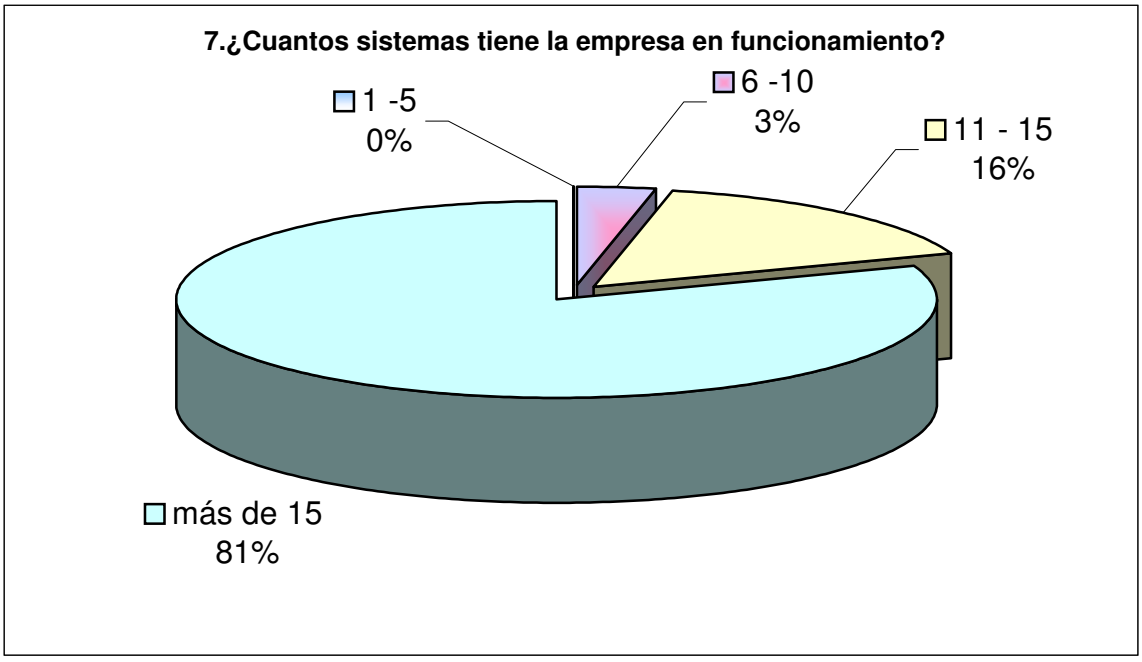
OBJETIVO:

Determinar el número de sistemas o aplicativos que tienen las empresas para apoyar las actividades laborales diarias.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
1 -5	0	0	0	0
6 -10	9	2	11	3
11 - 15	9	42	51	16
más de 15	72	184	256	81
	90	228	318	100
Total de encuestas	90	228	318	

ANALISIS DE DATOS

Como se observa, la tendencia en la mayoría de las empresas, el 81% es la automatización de los procesos de trabajo, apoyados en diversos sistemas o aplicaciones informáticas, por lo que existe una alta dependencia de la tecnología.



PREGUNTA N° 8

¿Existe en la empresa personal interno que realice auditoría de sistemas?

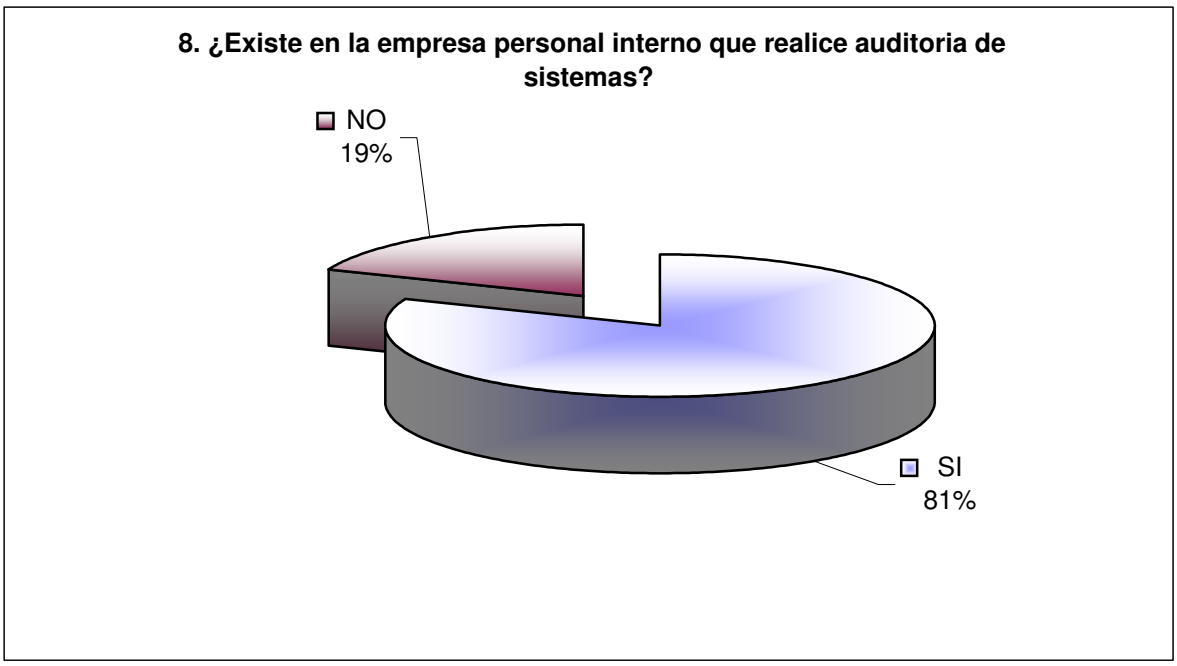
OBJETIVO:

Determinar si existe dentro de la empresa personal que realice auditoría de sistemas.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
SI	67	191	258	81
NO	23	37	60	19
	90	228	318	100
Total de encuestas	90	228	318	

ANALISIS DE DATOS

Como se observa en la grafica el 81% de las empresas manifestó que cuentan con personal que realiza auditoría de sistemas dentro de la empresa.



PREGUNTA N° 9

¿De quién depende jerárquicamente ó a quién reporta auditoría de sistemas?

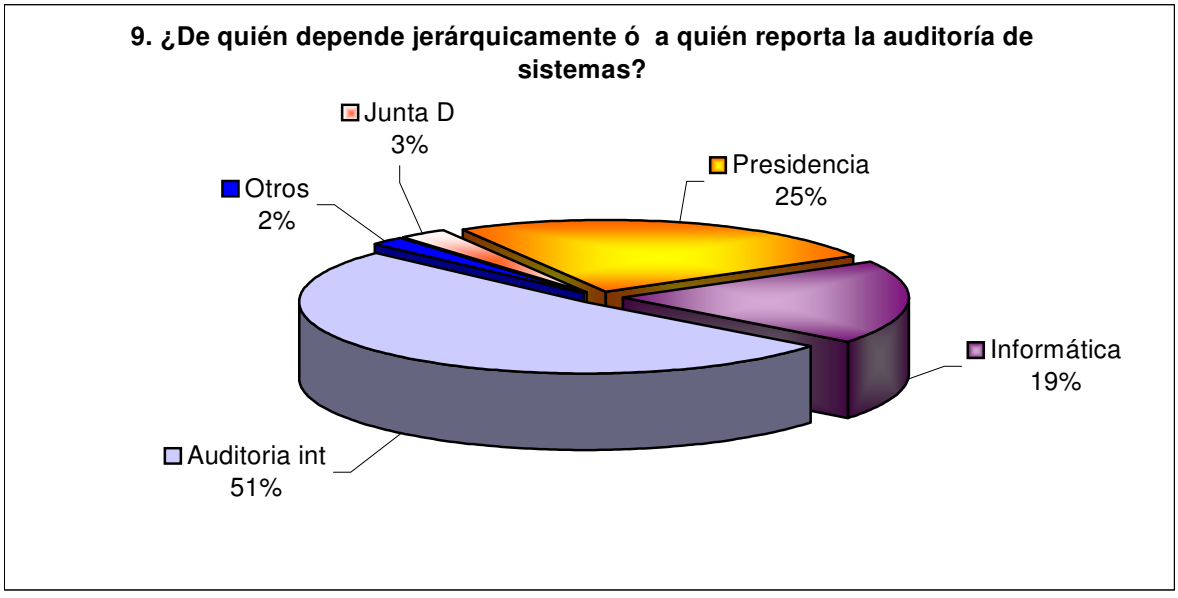
OBJETIVO:

Determinar el nivel de dependencia jerárquica de auditoría de sistemas dentro de la organización.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
Junta Directiva	2	5	7	3
Presidencia	25	39	64	25
Informática	15	34	49	19
auditoría Interna	24	109	133	51
Otros	1	4	5	2
	67	**191**	**258**	**100**
Total de encuestas	**67**	**191**	**258**	

ANALISIS DE DATOS

Como la gráfica nos indica el 51% de los entrevistados respondieron que auditoría de sistemas reporta a auditoría interna, y en segundo lugar reportan a la presidencia, lo que evidencia que los dictámenes de auditoría pueden tener cierto grado de independencia para emitir los hallazgos encontrados.



PREGUNTA N° 10

¿Se ha implementado en la empresa alguna metodología de auditoría de sistemas?

OBJETIVO:

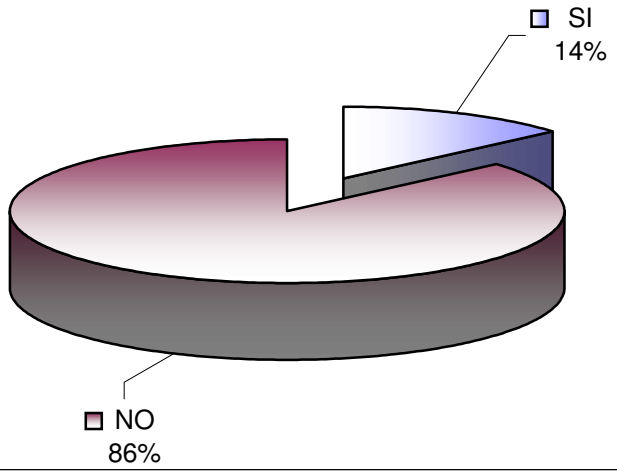
Determinar si en las empresas encuestadas se ha implementado alguna metodología de auditoría de sistemas.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
SI	22	13	35	14
NO	45	178	223	86
	67	**191**	**258**	**100**
Total de encuestas	**67**	**191**	**258**	

ANALISIS DE DATOS

De la totalidad de las empresas encuestadas, el 86% no han implementado alguna metodología de auditoría de sistemas.

10. ¿Se ha implementado alguna metodología de auditoría de sistemas?



PREGUNTA N° 11

¿Poseen programas de auditorías de sistemas, para la evaluación de la tecnología?

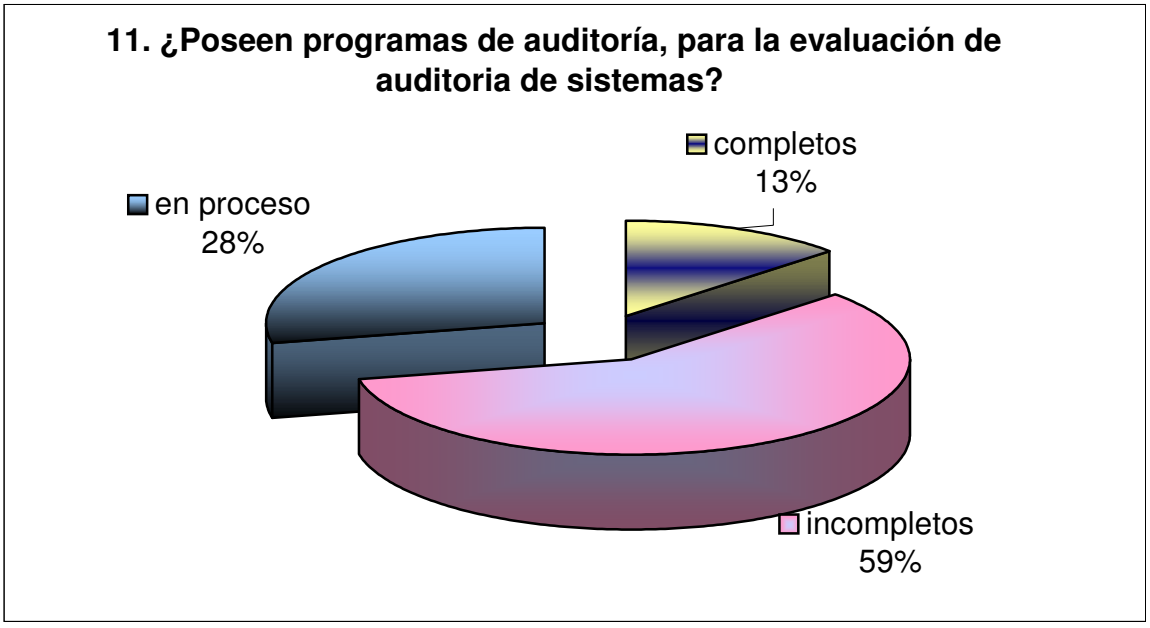
OBJETIVO:

Determinar la existencia de programas de auditoría de sistemas para evaluar el área de tecnología.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
completos	7	27	34	13
incompletos	39	112	151	59
en proceso	21	52	73	28
	67	**191**	**258**	**100**
Total de encuestas	**67**	**191**	**258**	

ANALISIS DE DATOS

El 87% de las empresas encuestadas requieren programas de auditoría, debido que los que poseen actualmente estan incompletos o en proceso.



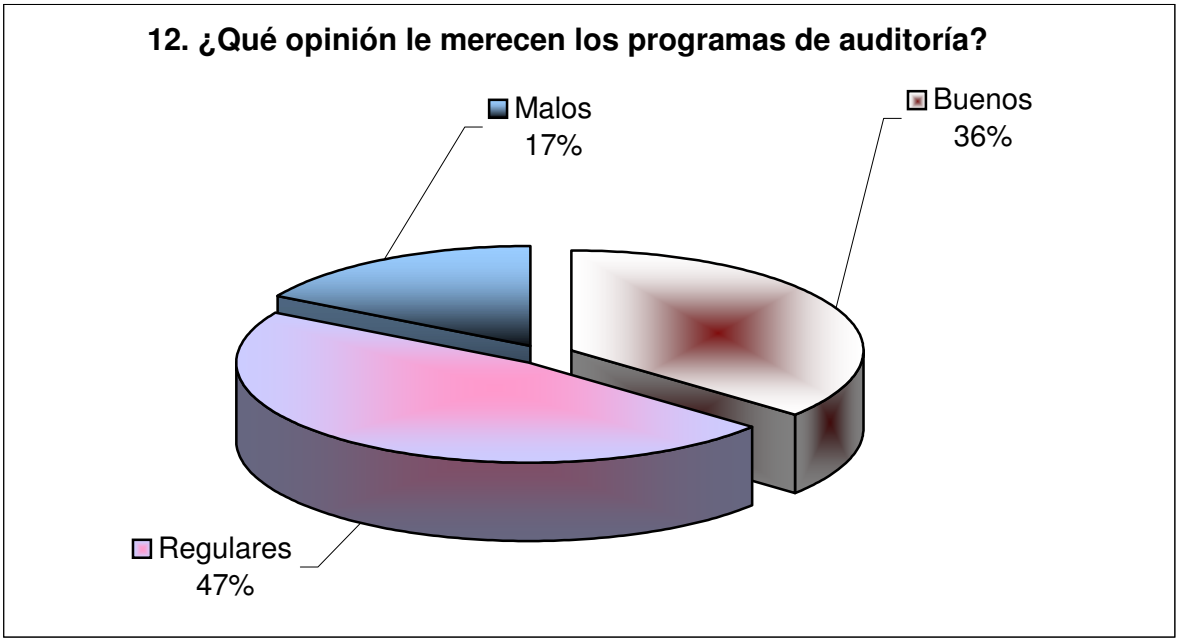
PREGUNTA N° 12
¿Qué opinion le merecen los programas actuales de auditoría?

OBJETIVO:

Comprobar cual es el nivel de aceptación de los programas actuales de auditoría en la aplicación a los sistemas que se encuentran en producción.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
Buenos	22	71	93	36
Regulares	10	112	122	47
Malos	35	8	43	17
	67	**191**	**258**	**100**
Total de encuestas	**67**	**191**	**258**	

ANALISIS DE DATOS
La mayoría de los entrevistados afirma que a pesar de disponer de programas, el 64% los consideran regulares o malos en cuanto a su contenido y aplicabilidad.



PREGUNTA N° 13
¿Cómo Califica el contenido de estos programas de auditoría?

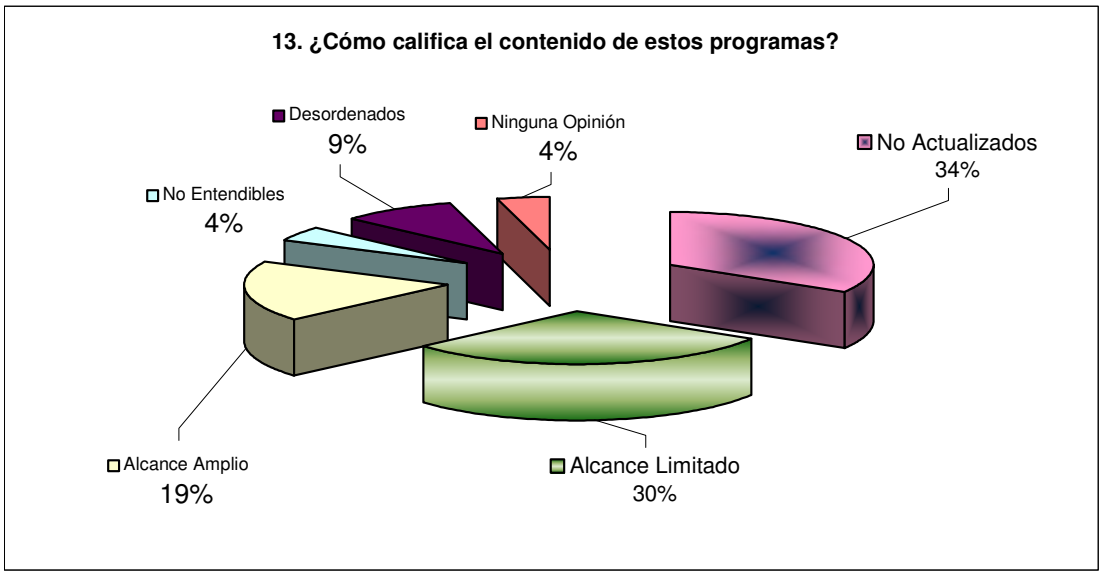
OBJETIVO:

Identificar cual es la opinión sobre los programas de auditoría.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
No actualizados	12	73	85	34
Alcance Limitado	20	58	78	30
Alcance Amplio	12	37	49	19
No Entendibles	4	7	11	4
Desordenados	13	11	24	9
Ninguna Opinión	6	5	11	4
	67	**191**	**258**	**100**
Total de encuestas	**67**	**191**	**258**	

ANALISIS DE DATOS

De la misma forma se observa que el 96% de los entrevistados afirmaron que los programas no se encontraban actualizados, el alcance es limitado, no son entendibles o estan desordenados; lo que evidencia la necesidad de desarrollar programas de auditoría de sistemas completos y entendibles, facíl y de amplio alcance



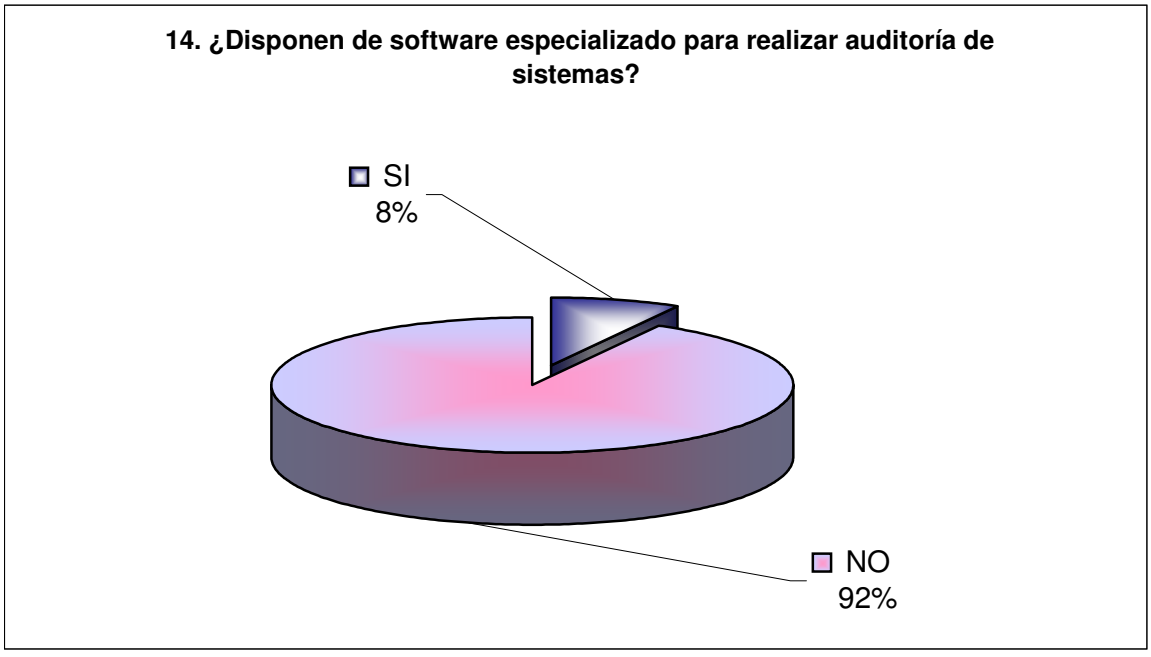
PREGUNTA N° 14
¿Disponen de software especializado para realizar auditoría de sistemas ?

OBJETIVO:

Conocer si poseen un software que apoye el desarrollo de los exámenes de auditoría de sistemas

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
SI	7	19	26	8
NO	85	210	295	92
	92	229	321	100
Total de encuestas	92	229	321	

ANALISIS DE DATOS
El 92% de los entrevistados no dispone de software especializado para realizar los examenes de auditoría de sistemas



PREGUNTA N° 15

¿Qué opiníon le merece el software de auditoría?

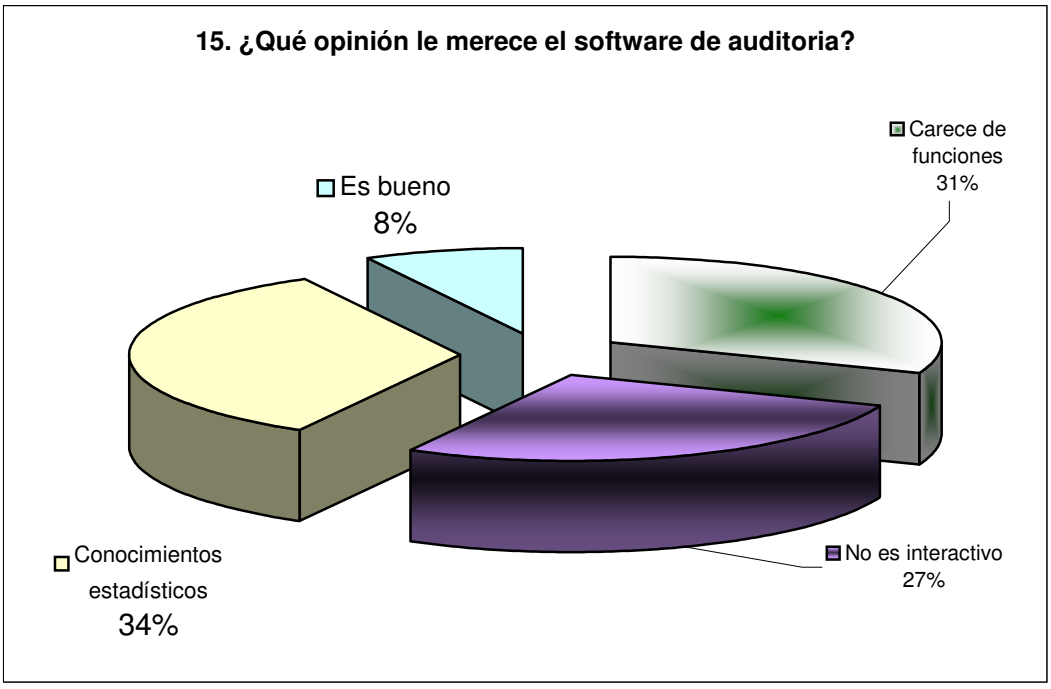
OBJETIVO:

Identificar la opinion que tiene el personal que utiliza el software de auditoría sobre su funcionalidad.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Mediana	Grande		
Carece de funciones	2	6	8	31
No es interactivo	2	5	7	27
Conocimientos estadísticos	3	6	9	34
Es bueno	1	1	2	8
	8	**18**	**26**	**100**
Total de encuestas	**8**	**18**	**26**	

ANALISIS DE DATOS

El 92% de los usuarios que respondieron que la empresa posee software de auditoría de sistemas, considera que no es totalmente funcional, lo cuál evidencia la necesidad del desarrollo de programas de auditoría de sistemas como complemento al uso de este software.



PREGUNTA N° 16

¿Le gustaria disponer de un manual de auditoría de sistemas enfocada a riesgos que le permita evaluar la tecnología de información e identificar segmentos y objetivos definidos?

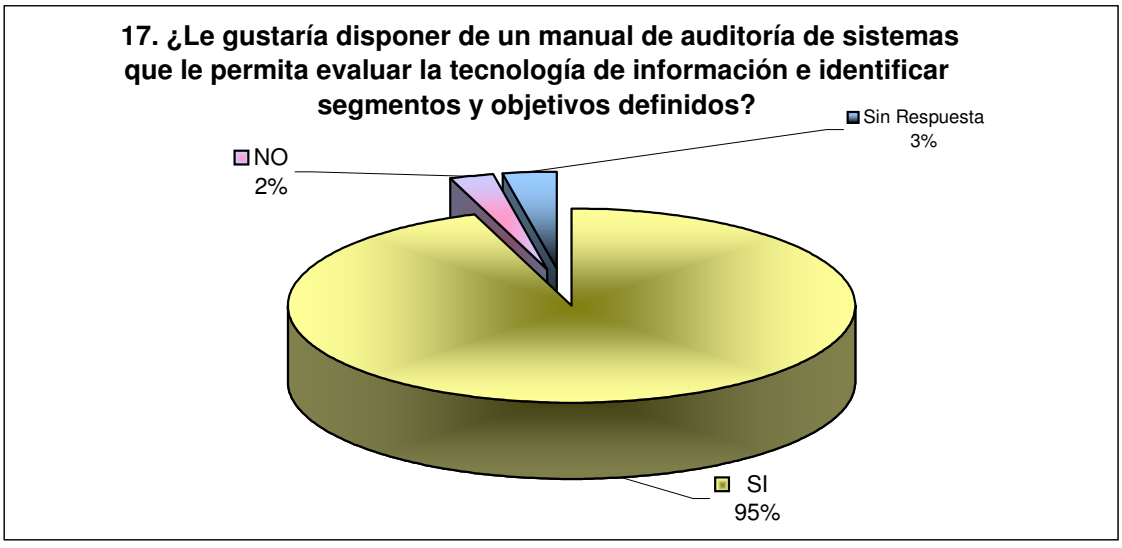
OBJETIVO:

Conocer si los entrevistados estan interesados en una guía de auditoría de sistemas para facilitar la evaluación del área de tecnología de la empresa en donde labora.

Alternativas	DATOS DE CLASIFICACION		Total de respuestas	%
	Medina	Grande		
Si	63	181	244	95
No	2	4	6	2
Sin Respuesta	2	6	8	3
	67	191	258	100
Total de encuestas	67	191	258	

ANALISIS DE DATOS

De los 258 entrevistados, el 95% manifestó que está interesado en un manual de auditoría de sistemas que contenga las áreas a revisar y sus objetivos de forma que facilite la evaluación del área de tecnología de la empresa en la que labora.



3.5.2.2 CONCLUSIONES DE LAS ENCUESTAS

1. De acuerdo a los resultados de la investigación, existe una necesidad no satisfecha por la falta de un manual de auditoría de sistemas enfocado en riesgo tecnológico que apoye la realización de los exámenes de auditoría , de forma que el alcance y aspectos a evaluar en el área de tecnología queden cubiertos. Prueba de ello tenemos el resumen de los puntos siguientes:

    1.1 Que el 43% de 85 empresas que respondieron disponer de auditoría externa de sistemas, pero desconocen de los resultados, situación que debe ser superada por la Alta Administración, con la finalidad de fortalecer el área de TI.

    1.2 Que el 86% de 370 empresas encuestadas su información se administra en equipo informático, así mismo manifestaron que los módulos puestos en producción tienen un 100% de dependencia tecnológica.

    1.3 Siendo 258 (81%) empresas de un universo 318 encuestadas, manifestaron tener dentro de su estructura auditoría de sistemas, no obstante 224 no disponen de programas de auditoría actualizados y bajo ese contexto el 47% los considera regulares y un 17% malos.

2. Otra de las circunstancias observadas es la debilidad del control interno de las instituciones, ya que se pudo identificar que al no disponer de un manual de auditoría o de programas actualizados, podría ser perjudicial para lograr los objetivos previstos, debido a que la eficiencia y eficacia del servicio se ven afectadas.

3. Los porcentajes identificados en la investigación de campo, demuestran que el control interno de las empresas demandan mayor atención y fortalecimiento, para ello deben de identificar los siguientes factores:

   3.1 El ambiente de control, le permite a la empresa influir en el recurso humano la conciencia laboral y el conocimiento del sentido del control interno. El ambiente de control incluye factores de integridad, valores éticos, competencia, filosofía de la administración y cumplimiento de políticas.

   3.2 La evaluación del Riesgos es la identificación, análisis y seguimiento para determinar como deben ser manejados.

   3.3 Actividades de control, concierne a las políticas y procedimientos que ayudan a garantizar la conducción y la administración en los recursos de TI.

   3.4 La información emitida y administrada por TI, debe ser manejada con prudencia y responsabilidad, debido a que forma parte de los activos de la empresa.

   3.5 La tecnología y su entorno necesita ser supervisada, con la finalidad de garantizar el cumplimiento de los objetivos.

CAPÍTULO IV
4. AUDITORÍA DE SISTEMAS

4.1 INTRODUCCIÓN

El nivel académico en armonía con la tecnología, la capacidad y experiencia son elementos importantes para el buen desarrollo de la auditoría en TI, asimismo el responsable de ejecutar la evaluación debe considerar escenarios de posibles "supuestos" que permitan ampliar o profundizar las pruebas para minimizar los riesgos, por ello el proceso de auditoría exige que el auditor de TI reúna evidencia, evalúe fortalezas y debilidades de los controles existentes, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la Administración o Gerencia de la cual depende. Asimismo el auditor debe ser portador de independencia y autoridad para realizar su examen.

Como primer paso, la planificación es necesaria para realizar auditorías de TI. El auditor debe comprender el ambiente del negocio en el que se ha de realizar la auditoría, así como los riesgos del negocio y control asociado. Por ello el auditor antes de aplicar los programas de trabajo debe tener en cuenta las siguientes consideraciones.

Al planificar una auditoría, el auditor de TI debe tener una comprensión suficiente del ambiente total que se revisa, debe incluir una idea general de las diversas prácticas comerciales y funciones relacionadas con el tema de la auditoría, así como los tipos de sistemas que se utilizan. El auditor de TI también debe comprender el ambiente normativo en el que opera el negocio.

4.2 PERFIL DEL AUDITOR DE SISTEMAS Y NORMAS BÁSICAS DE APLICACIÓN

Cada empresa tiene establecido los criterios, condiciones y obligaciones que deben ser respetados por el personal que labora en ella, esto obedece a que son aspectos vigentes que regulan la actuación de quienes administran la empresa, por tanto, es compromiso del auditor apegarse a las normas o políticas establecidas, sean estas

internas o externas en el ejercicio del servicio profesional, auditoria de sistemas debe de exigir el cumplimiento de normas básicas o principios generales aceptados.
En cualquier ámbito laboral existen necesidades que cumplir, el primer requisito que debe poseer quien se dedica a esta profesión, es estar totalmente libre de cualquier tipo de influencia; es decir debe ser autónomo en su actuación y no permitir ningún tipo de injerencia, ya sea de cualquier carácter, sean estas; laborales, morales, conducta, independencia y conocimiento profesional. El segundo requisito son los conocimientos computacionales que debe tener, con un amplio cúmulo de nociones en áreas vinculadas al trabajo, métodos, herramientas y técnicas de auditoría a fin de que pueda realizar sus tareas con eficiencia y eficacia.

Sin embargo, este debe poseer otras características personales que son representativas del auditor tales como: honradez, valores, confianza, tenacidad, capacidad analítica, en ese contexto también lo ideal es la experiencia profesional para el buen desempeño del trabajo dentro de la Organización. Así mismo debe el auditor de sistemas manejar otros factores que contribuyen y se encuentran ligados a su profesión, tales como: a) El auditor debe de aprender a manejar adecuadamente las relaciones personales, profesionales y laborales entre él y el auditado. b) Como profesional de auditoría debe utilizar la misma metodología, procedimientos, herramientas y técnicas que se hayan establecido para la revisión de las áreas. c) Los resultados que obtiene el auditor forman evidencias en las que se respalda, para emitir el dictamen .d) Es obligación profesional, moral y personal del auditor respetar la confidencialidad de dicha información y no divulgarla. d) Mantener y aplicar la equidad, en virtud que trata de igualar la justicia, ponderación y emisión de juicios; la imparcialidad que evita las preferencias injustas y la razonabilidad que es la capacidad del individuo para emitir un juicio.

La sociedad misma identifica una serie de aspectos fundamentales que debe de tener el profesional dedicado a la auditoría, a fin de que identifique y cumpla con los principios y valores del auditor, citando algunos de ellos:

4.2.1 INDEPENDENCIA

La independencia supone una actitud mental que permite al auditor actuar con libertad respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad en la consideración objetiva de los hechos, así como en la formulación de sus conclusiones.
Para ser independiente, el auditor no debe tener intereses ajenos a los profesionales, ni estar sujeto a influencias susceptibles de comprometer tanto la solución objetiva de los asuntos que le son sometidos, como la libertad de expresar su opinión profesional.

4.2.2 INTEGRIDAD

La integridad debe entenderse como la rectitud intachable en el ejercicio profesional, que le obliga a ser honesto y sincero en la realización de su trabajo y en la emisión de su informe. En consecuencia, todas y cada una de las funciones que realice han de estar regidas por una honradez profesional irreprochable.

4.2.3 OBJETIVIDAD

La objetividad implica el mantenimiento de una actitud imparcial en todas las funciones del auditor. Para ello, debe gozar de una total independencia en sus relaciones con la entidad auditada. Debe ser justo y no permitir ningún tipo de influencia o prejuicio.

4.2.4 COMPETENCIA PROFESIONAL

Es la obligación de mantener su nivel de competencia a lo largo de toda su carrera profesional, así como de mantener sus conocimientos y sus habilidades a un nivel adecuado para asegurar que la evaluación será la adecuada.

4.2.5 CONFIDENCIALIDAD

El Auditor deberá respetar la confidencialidad respecto a la información que reúna en el desarrollo de su trabajo y no deberá revelar ninguna información a terceros sin la autorización específica, a menos que tenga el derecho o la obligación profesional o legal de hacerlo. También tiene la obligación de garantizar que el personal bajo su control respete fielmente el principio de la confidencialidad.

El principio de confidencialidad es más amplio que la revelación de la información; incluye el hecho de que un auditor que obtenga información en el curso de la prestación de sus servicios, no debería usarla ni aparentar usarla para su beneficio personal o para terceros.

4.2.6 RESPONSABILIDAD

Se mantiene como responsabilidad el hecho de aceptar el compromiso que implica la toma de decisiones y las consecuencias previstas por las acciones y omisiones en el cumplimiento del trabajo.

4.2.7 CONDUCTA PROFESIONAL

Actuar de acuerdo con la buena reputación de la profesión y evitar cualquier conducta que pueda desacreditarla. Esto requiere que las normas de ética tengan en cuenta las responsabilidades profesionales.

4.2.8 NORMAS TÉCNICAS

El auditor deberá conducir una auditoría conforme las Normas y Políticas, locales o internacionales. Estas deberán contener principios básicos y procedimientos esenciales junto con lineamientos relativos y asociados a las funciones del auditor.

Los elementos referenciados con anterioridad se encuentran integrados en normas llamadas código de ética, aplicadas para el auditor de sistemas, siendo estos utilizados y difundidos por instituciones nacionales e internacionales. (Anexo E)

4.3 RIESGO Y MATERIALIDAD DE AUDITORÍA

Se pueden definir los riesgos de auditoría como aquellos riesgos en que la información pueda tener errores materiales o que el auditor de TI no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera:

- **Riesgo inherente:** Cuando un error material no se puede evitar que suceda por que no existen controles compensatorios relacionados que se puedan establecer.
- **Riesgo de control:** Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno.
- **Riesgo de detección:** Es el riesgo en que el auditor realiza pruebas exitosas a partir de un procedimiento inadecuado. El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad existen. La palabra "material" utilizada con cada uno de estos componentes o riesgos, se refiere a un error que debe considerarse significativo cuando se lleva a cabo una auditoría.

En una auditoría de TI, la definición de riesgos materiales depende del tamaño o importancia del ente auditado, así como de otros factores. Una auditoría tal vez no detecte cada uno de los potenciales errores en el universo. Pero, si cuando el tamaño de la muestra es lo suficientemente grande, o se utiliza procedimientos estadísticos adecuados se llega a minimizar la probabilidad del riesgo de detección. De manera similar al evaluar los controles internos, el auditor de TI debe percibir que en un sistema dado, se puede detectar un error mínimo, pero ese error combinado con otros, puede convertirse en un error material para todo el sistema.

Aunque siempre debe prevalecer el deber del secreto profesional del auditor, conviene recordar que en el caso de detectar fraude durante el proceso de auditoría

procede actuar en consecuencia con la debida prudencia que aconseja, sobre todo si afecta a los administradores de la organización. Ante un caso así, conviene consultar con la Alta Administración o el Comité creado para tal fin, así mismo con el asesor jurídico, e identificar leyes afines para tal efecto, por ejemplo: Código Penal, Código Civil, Código de Comercio, Ley de Propiedad Intelectual y otras disposiciones. Al determinar qué áreas funcionales o temas de auditoría deben auditarse, el auditor puede enfrentarse ante una gran variedad de temas, por ello debe evaluar esos riesgos y determinar cuales de esas áreas de alto riesgo deben ser auditadas.

4.3.1 EVIDENCIA

La evidencia es la base razonable de la opinión del Auditor de TI, esto es parte complementaria del Informe, la evidencia tiene una serie de calificativos:

- La evidencia relevante, que tiene una relación lógica con los objetivos de la Auditoría.
- La evidencia fiable, que es válida y objetiva, aunque con nivel de confianza.
- La evidencia suficiente, que es de tipo cuantitativo para soportar la opinión profesional del auditor.
- La evidencia adecuada, que es de tipo cualitativo para afectar a las conclusiones del auditor.

4.4. HERRAMIENTAS DE SOPORTE

4.4.1 SOFTWARE PARA AUDITORÍA

EL auditor de sistemas puede auxiliarse con herramientas alternas que existen en el medio creadas para dicho fin, por ejemplo: para evaluar las Bases de Datos, estas permiten medir la consistencia, coherencia y calidad de los datos, para evaluar redes; estas permiten monitorear la seguridad y la continuidad del servicio. Al respecto podemos mencionar algunas de ellas:

4.4.1.1 ACL

ACL es un software para la solución de auditoría y análisis de datos, siendo su significado “Lenguaje de Control para Auditoría”, es un producto reconocido en el mundo por su excepcional servicio y soporte técnico, siendo un valor agregado para las empresas por sus ventajas de generación de reportes que se almacenan como papeles de trabajo. El software es un producto eficiente según las características siguientes:

a) Funcionalidad incorporada para; auditar y analizar datos mediante poderosos comandos tales como: estratificar, muestreo y duplicados.
b) Facilidad para el análisis interactivo; aplicando cualquier metodología de auditoría, analizando sus datos de forma que los resultados son inmediatos no importando la cantidad de registros que contenga el archivo, por su manejo de alta capacidad y velocidad en el proceso.
c) Facilidad de uso; su interfaz amigable que incluye facilidades como: menús, barras de herramientas y comandos.
d) Análisis universal de datos; una vez que se accede los datos, ACL los puede leer en su formato nativo, utilizando un solo producto en una herramienta para leer cualquier plataforma tecnológica, incluyendo bases de datos que cumplan con las especificaciones de ODBC, archivos de longitud variable, archivos de texto y muchos mas.
e) Procesamiento de varios archivos; trabaja simultáneamente con varios archivos, para hacer análisis y reportes mas complejos.
f) Identifica tendencias y señala excepciones y áreas que requieren atención.
g) Localiza errores y posibles irregularidades, comprobando y analizando los datos según los criterios del auditor.
h) Verifica integridad de datos en los archivos.
i) Emite cálculos estadísticos y analíticos para realizar proyecciones.
j) Despliegue de Gráficos de Barra

4.4.1.2 IDEA

Datos Interactivos Extracción y Análisis (IDEA) es una herramienta para auditores, contadores y administradores financieros que necesitan auditar, revisar, analizar, extraer y evaluar información contenida en sistemas, base de datos y cualquier archivo electrónico.

Este software permite la ejecución de procesos como consultas a archivos de datos, calcular totales o promedios, encontrar cuantas transacciones o registros cumplen un criterio dado o buscar campos inusuales. La interfaz del software está orientada hacia los usuarios finales, de manera que su uso y aplicación resulta amigable con el usuario, el software presenta algunas características:

a) Análisis de información: IDEA permite realizar una serie de funciones de análisis sobre los datos extraídos, mejorando la confianza y la exactitud de la información utilizada por el auditor.
b) Ordenamiento de registros: IDEA permite ordenar registros hasta por ocho llaves de ordenamiento concatenado, ascendente o descendente.
c) Gráficos de barra: permite visualizar de modo gráfico la información que está analizando.
d) Estadísticas de un campo: muestra una variedad de información estadística de un campo numérico y puede actuar hasta para 32 campos Simultáneamente.
e) Comparación de dos archivos: permite comparar dos archivos similares e identificar eventuales diferencias entre ambos.
f) Detección de errores de secuencia: permite detectar errores de secuencia en un archivo, como por ejemplo en un archivo de cheques emitidos.
g) Detección de llaves duplicadas: permite detectar campos duplicados que deberían ser únicos.

4.4.1.3 TEAM-MATE

Es un software que dispone de un sistema administrador de usuarios de la Base de Datos, de manera que cada usuario tiene diferentes niveles de acceso. Está diseñado para ser utilizado por todos los sectores, comerciales, industriales, financiero; así como para todo tipo de auditoría, como financiera, de cumplimiento, procedimientos, operacionales, investigaciones y auditoría de TI, dispone de integrar el programa de auditoría con las observaciones o comentarios afines para luego poderlo relacionar al papel de trabajo no importando su formato, ello le permite la flexibilidad y manejo operativo del mismo. También dispone de módulo de evaluación de riesgos, basada en la metodología ORCA (Objetivos, Riesgos, Controles y Alineación), esta enfocada en cómo una organización, unidad de negocio, proceso de negocio o individuo define y prioriza sus estrategias y objetivos. La metodología ORCA determina el impacto del riesgo en el objetivo y su probabilidad de ocurrencia. También dispone de Team Risk el cual permite la evaluación de riesgos, determinando el universo de riesgo con objetivos y controles que pueden ser editados durante el proceso de evaluación. Team Risk permite determinar la fórmula de puntuación y las bandas de puntuación (scoring), las métricas de puntuación, como impacto y probabilidad que mejor describan su forma de determinar el riesgo, las dimensiones de las métricas para ver los factores de riesgo antes y después del control o ambos.

4.4.1.4 MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (MAGERIT). Está compuesto por: Aproximación a la Seguridad de los Sistemas de Información, Procedimientos, Técnicas, Desarrolladores de Aplicaciones, Responsables del Dominio, Legales y Técnicas, Arquitectura de la Información y especificaciones de la interfaz para el intercambio de datos.

El modelo normativo de MAGERIT se apoya en tres sub modelos: Componentes, Eventos y Procesos, la metodología permite estudiar los riesgos que soporta un sistema de información y el entorno asociado a él, por ello propone la realización de

un análisis de los riesgos que implica la evaluación del impacto que una falta en la seguridad que tiene la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

Los Criterios de Seguridad de normalización y conservación recogen los requisitos y recomendaciones relativos a la implantación de las medidas de seguridad organizativa y técnica para asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en el diseño, desarrollo, implantación y explotación de las aplicaciones que la Administración General del Estado utiliza para el ejercicio de sus potestades. Estos criterios pueden ser, por tanto, complemento de MAGERIT para la identificación y selección de funciones y mecanismos de salvaguarda.

En cuanto al derecho de utilización, MAGERIT es una metodología usada por el Gobierno Español y es de carácter público, perteneciente al Ministerio de Administraciones Públicas. Su utilización requiere autorización previa del MAP. MAGERIT es una opción para poderse aplicar en el sector gubernamental y por consiguiente con algunas adaptaciones conforme a las leyes del país.

4.4.1.5 OTROS

Para el monitoreo, seguimiento y control de Base de Datos puede auxiliarse por ejemplo de Spotlight el cual permite operar en tiempo real, identifica problemas de entrada y salida, mantiene historia y relaciones de hechos, realiza calibraciones de la base, alarmas audibles , tiempo y espacio de cpu, disponibilidad de memoria principal, disponibilidad de discos, tiempo y espacio de procesos, otra opción de software es NimBUS que se utiliza para monitorear bases de datos e indica la disponibilidad y rendimiento de los servidores de bases de datos. Además, soporta múltiples plataformas de bases de datos: Oracle, Sybase, DB2, MS SQL, e Informix. Otras características*:* evalúa clusters de bases de datos, bitácoras de eventos, usuarios activos, consumo de recursos, opciones flexibles de notificación de alarmas

(SMS, PDA, consola, web, email, etc) alertas e indicadores de rendimiento, análisis de entradas en tablas para la generación de alertas e informes de tendencia, entre otros.

Por otra parte conforme al conocimiento del auditor y la plataforma tecnológica con la que cuenta la Organización, el auditor de sistemas puede apoyarse con software de soporte para el desarrollo de sus evaluaciones, por ejemplo: Visual Fox, Visual Basic, Sql, e inclusive los procedimientos definidos en la línea de comandos de un AS-400 ó cualquier otro lenguaje que le permita filtrar, definir, seleccionar y evaluar los datos, con la finalidad de brindar opinión sobre la calidad, coherencia y existencia de la información almacenada.

Así mismo se recomienda que el auditor pueda identificar aquellos procedimientos o consultas que demanden la creación de sentencias o líneas de código fuente, sabiendo que estas se utilizarán más de una vez, en el sentido que le permita disponer de un respaldo de los mismos, para que en futuras evaluaciones sean ejecutados.

4.5 SOFTWARE DE MONITOREO PARA REDES

La seguridad se hace posible con el desarrollo de negocios a través de Internet y debe ser un componente fundamental de cualquier estrategia de comercio electrónico. A medida que las empresas abren sus redes a más usuarios y aplicaciones, las exponen a mayores riesgos. Por ello las organizaciones o personas que comparten información y que ingresan con sus equipos a una red por cualquier clase de motivo, es prácticamente imprescindible usar algún Corta Fuego (Firewall) y de herramientas que le permitan monitorear la red, sobre todo sí comparte archivos a través de Internet, utiliza un servidor Web, utiliza algún tipo de herramienta de control remoto como PC Anywhere, Laplink o Servicios de Terminal de Microsoft o desea estar protegido ante ataques de denegación de servicio (DoS) o intrusiones. Al respecto presentamos a manera de ejemplos algún software que pueden servir de soporte para ejercer auditoría en las redes de comunicaciones:

SOFTWARE	DESCRIPCION
CISCO	Dispone de una variedad de productos para la seguridad y confiabilidad del servicio de red.
DEFENDER	Es un sistema contra hacker, explora el DSL, módem de cable, o conexión de marcado manual del Internet que busca actividad del hacker. Cuando detecta una intrusión, bloquea automáticamente el tráfico de esa fuente, evitando a intrusos tener acceso a su sistema. Tiene como punto fuerte combinar dos programas de seguridad en uno, un Firewall y un Analizador de red. El Firewall funciona de la misma manera que la mayoría de Firewall, bloquea o permite el tráfico según las preferencias del usuario, y el analizador de red intenta determinar la naturaleza de los paquetes.
DTK	(ToolKit) es una caja de herramientas de engaño diseñada para dar ventaja a los usuarios propietarios, para dar órdenes de engaño a los atacantes.
ETHEREAL	Es un sistema capaz de obtener datos de múltiples Sniffers de sistema, desde ficheros o directamente de la red. En este último caso, puede ser usado en redes de tipo Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, IP sobre ATM e interfaces de loopback. Con este analizador se puede diseccionar a más de 700 protocolos de red, pudiendo guardar la información obtenida en ficheros, así como filtrar la información mostrada en pantalla.
PGP	Es un programa que da aislamiento al correo electrónico, hace esto cifrando su correo de modo que únicamente la persona prevista pueda leerlo, también es absolutamente capaz de resistir incluso las formas más sofisticadas de análisis dirigidas leyendo el texto cifrado.
RETINA	Es un producto de seguridad para red que explora, monitorea, y dispone alarmas, y fija automáticamente vulnerabilidades de la seguridad de la red.
SAINT	Es la herramienta integrada de red para el administrador de seguridad, recopila tanta información sobre los ordenadores principal remotos y las redes como sea posible examinando los servicios de red tales como "finger", el NFS, el NIS, el FTP y el REXD y otros servicios.
SATAN	(the Security Administrator Tool for Analyzing Networks) es una herramienta de prueba que recolecta una variedad de información acerca de Host de red y fue considerada una de las mejores en su

	momento. Fue diseñado para ayudar a los administradores de sistemas a automatizar el proceso de prueba de sus sistemas frente a vulnerabilidades conocidas que pueden ser explotadas por la red. SATAN esta escrito mayoritariamente en PERL y utiliza un navegador Web como Netscape, Mosaic o Lynx.
SNIFFER	Es un analizador robusto del protocolo de red o "succionador" de paquetes, su función es escuchar básicamente el tráfico de la red y produce el análisis basado en el tráfico y/o traduce los paquetes a un cierto nivel de la forma legible humana.
SNORT	Es un paquete basado Sniffer/logger que se puede utilizar como sistema ligero para la detección de intrusión en la red.
StoneGate	Combina seguridad y continuidad en una sola plataforma, soluciones de Firewall, VPN e IPS, análisis y detección de intrusión, gestión centralizada, escalabilidad y continuidad, con la tecnología multilink, que le permite conectar StoneGate a diferentes ISPs y seleccionar el ISP de menor tiempo de respuesta, asegurando la conectividad y rapidez.
TOOLS NMAP	Es un utilitario para las redes grandes de la exploración, control y verificación de puertos.
ZoneAlarm	Su categoría es optimizar la configuración por defecto y de manera automática.

4.6 VERIFICACIÓN DEL CONTROL INTERNO

El siguiente programa es un resumen (listado de verificación) de las actividades propuestas en MASTI, en ese sentido se pretende medir el control interno de los sistemas tecnológicos de información a la brevedad posible, debido a que es un formato que recolecta una respuesta cerrada (SI/NO) por parte del auditado, al cual se le demanda honestidad en las respuestas, el consolidado de ambas respuestas le daría una opinión de juicio y análisis al auditor y en este contexto podría tener una idea previa de las fortalezas y debilidades de TI:

INSTITUCIÓN:	**FECHA FIN:**
AUDITOR:	**FIRMA:**

Áreas / Actividades	**Número de Referencia**

PUNTOS DE CONTROL INTERNO

Evaluar cuáles son los mecanismos que dispone la alta administración para velar por la estabilidad y la eficiencia de la empresa, en relación a: los sistemas, los equipos, la seguridad, la utilización y los controles aplicados al Área de Tecnología de Información. Verificar con el área responsable de informática el conocimiento y disposición de los siguientes elementos:

1. Documentación

1.1	Organigrama	Si ☐ No ☐
1.2	Manual de Puestos	Si ☐ No ☐
1.3	Inventario de aplicativos puestos en producción	Si ☐ No ☐
1.4	Inventario de programas con su respectiva descripción	Si ☐ No ☐
1.5	Inventario de archivos con su respectiva descripción	Si ☐ No ☐
1.6	Inventario de hardware	Si ☐ No ☐
1.7	Inventario de software	Si ☐ No ☐
1.8	Diccionario de Datos	Si ☐ No ☐
1.9	Diagramas de Red	Si ☐ No ☐
1.10	Diagramas de relación	Si ☐ No ☐
1.11	Evaluación de sistemas por parte de auditoría externa	Si ☐ No ☐
1.12	Evaluación de sistemas por parte de auditoría interna	Si ☐ No ☐
1.13	Plan estratégico	Si ☐ No ☐
1.14	Plan de capacitación para el personal	Si ☐ No ☐
1.15	Presupuesto anual	Si ☐ No ☐
1.16	Políticas y normas que regulen la administración de TI	Si ☐ No ☐
1.17	Políticas de Seguridad	Si ☐ No ☐
1.18	Políticas de calidad de datos	Si ☐ No ☐
1.19	Políticas de Mantenimiento del software	Si ☐ No ☐
1.20	Contrato de mantenimiento del hardware	Si ☐ No ☐
1.21	Políticas de respaldo	Si ☐ No ☐
1.22	Estudios de Factibilidad de los proyectos	Si ☐ No ☐
1.23	Plan de trabajo (período actual)	Si ☐ No ☐

2. Servicios con Terceros

2.1	Existe contrato de servicios	Si ☐ No ☐
2.2	Existe dentro del contrato cláusula de confidencialidad	Si ☐ No ☐
2.3	El proveedor ha dado cumplimiento a lo pactado	Si ☐ No ☐
2.4	Existen controles para el servicio	Si ☐ No ☐

INSTITUCIÓN:	**FECHA FIN:**	
AUDITOR:	**FIRMA:**	
Áreas / Actividades		**Número de Referencia**
3. Seguridad		
3.1 Control de acceso al personal a la sala de cómputo	Si ☐ No ☐	
3.2 Identifican, autentican y autorizan el acceso a la Base de Datos	Si ☐ No ☐	
3.3 Pared de fuego (Firewall)	Si ☐ No ☐	
3.4 Restringen el tráfico hacia dentro y fuera de la red	Si ☐ No ☐	
3.5 Software para prevenir, detectar y corregir virus	Si ☐ No ☐	
3.6 Regulan el correo electrónico	Si ☐ No ☐	
3.7 Evaluación técnica de infraestructura del edificio	Si ☐ No ☐	
3.8 Control en las condiciones ambientales	Si ☐ No ☐	
3.9 Control en los ambientes de desarrollo y producción	Si ☐ No ☐	
3.10 Controles para la medición de calidad de datos	Si ☐ No ☐	
3.11 Software para monitorear / analizador redes	Si ☐ No ☐	
3.12 Herramientas para administrar la seguridad de las Bases de Datos	Si ☐ No ☐	
3.13 Existen censores (fuego, humo, movimiento)	Si ☐ No ☐	
4. Redes		
4.1 Evalúan la capacidad y desempeño del hardware.	Si ☐ No ☐	
4.2 Evalúan la capacidad de la red.	Si ☐ No ☐	
4.3 Evalúan al proveedor de servicio de comunicaciones.	Si ☐ No ☐	
4.4 Evalúan la calidad de las operaciones en Internet.	Si ☐ No ☐	
4.5 Evalúan periódicamente los equipos de comunicación	Si ☐ No ☐	

4.7 PLAN DE IMPLEMENTACIÓN

El plan de implementación estará sujeto a las instrucciones de la evaluación dadas por la Alta Administración, así como el objetivo y alcance a desarrollar, por ello el auditor de sistemas debe considerar antes de realizar la evaluación los siguientes elementos para su aplicación: planeación, factores de entorno, supervisión, solicitud de requerimientos, programas de auditoría, papeles de trabajo, memorando e informe y el seguimiento.

4.7.1 PLANEACIÓN

Las auditorías deberán planearse adecuadamente para asegurarse que se cumplan sus objetivos, y que las revisiones se efectúen conforme a la normatividad aplicable, con la debida oportunidad, eficiencia y eficacia que le corresponde.

Planear la auditoría implica determinar y plasmar en un cronograma de trabajo algunas variables, tales como: aplicativo, rubro por auditar, alcance, objetivos de la revisión, naturaleza, extensión, procedimientos, personal que debe intervenir en el trabajo y el tiempo estimado para cubrir o realizar cada fase de la auditoría. Este cronograma de trabajo deberá revisarse durante la auditoría y en caso necesario, deberá ser ajustado.

El auditor deberá planear su trabajo de modo que la auditoría sea desarrollada de una manera efectiva. Planeación significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperado de la auditoría. La planeación adecuada del trabajo de auditoría ayuda a asegurar que se presta atención a las áreas importantes de la auditoría, y que los problemas potenciales son identificados y que el trabajo es completado en forma oportuna. La planeación también ayuda a la apropiada asignación de trabajo a los auxiliares y para la coordinación del trabajo realizado por otros auditores y técnicos, el tiempo asignado para el desarrollo de la auditoría estará basado en el alcance y objetivos previstos por la administración.

El grado de detalle de planeación variará de acuerdo con el tamaño de la entidad, la complejidad de la auditoría y la experiencia del auditor con la entidad y conocimiento de la actividad del cliente.

Adquirir conocimiento de la actividad del cliente es una parte importante de la planeación del trabajo. El auditor puede desear discutir elementos del plan global de auditoría y algunos procedimientos de auditoría con el comité de auditoría,

administración y personal de la entidad, para mejorar la efectividad, por ello debe de tener en cuenta los siguientes puntos de control:

a. Reconocer el origen de la auditoría
b. Establecer el objetivo de la auditoría
c. Definir el alcance.
d. Determinar las áreas a evaluar
e. Elaborar un cronograma en tiempo versus actividades
f. Elaborar presupuesto según el caso
g. Asignar recursos tecnológicos.
h. Definir el uso de herramientas de auditoría.

4.7.2 RECONOCIMIENTO DE FACTORES DEL ENTORNO

El auditor deberá desarrollar y documentar el alcance y conducción esperados según el caso a evaluar, por lo que tendrá que considerar:

a. Factores económicos generales y condiciones de la industria que afectan la empresa.
b. El nivel general de competencia de la administración.
c. Experiencia previa con la entidad y su industria.
d. Evaluación del informe de auditoría anterior.
e. Discusión con personal de auditoría interna y/o externa.
f. Discusión con otros auditores y con asesores legales o de otro tipo que hayan proporcionado servicios a la entidad.
g. Legislación y reglamentos que afecten en forma importante a la Organización.
h. Los términos del trabajo y cualquier responsabilidad estatutaria.

4.7.3 SUPERVISIÓN

La auditoría deberá supervisarse en cada una de sus fases y en todos los niveles del personal para garantizar el cumplimiento de sus objetivos.

El responsable de la supervisión deberá ser cuidadoso y tener siempre presente que en los trabajos de auditoría se deben aplicar las normas de auditoría y que la opinión que se vaya a emitir esté justificada y debidamente sustentada por el trabajo realizado.

La supervisión es esencial para asegurarse de que se cumplan los objetivos de la auditoría y el trabajo se ejecute con la calidad necesaria.

4.7.4 SOLICITUD DE REQUERIMIENTOS

El auditor debe considerar e identificar algunos requerimientos que le permitirán realizar la auditoría, estos requerimientos deberán ser enviados de forma escrita a la persona responsable o de enlace en la empresa, de forma anticipada estableciendo un plazo de tiempo para la entrega, estos deberán ser proporcionados por el auditado en medios electrónicos o en medios impresos, según el caso, por ejemplo: manual de organización, políticas de seguridad, plan de contingencia, manuales de usuario, diccionario de datos, diagramas de relación, archivos de datos, listado de usuarios, etc.

4.7.5 PROGRAMAS DE AUDITORÍA

El auditor deberá aplicar, mejorar y documentar los programas de auditoría propuestos en MASTI, así mismo definirá la naturaleza, oportunidad y alcance de los procedimientos de auditoría planeados que se requieren para implementar la evaluación. El programa de auditoría sirve como un conjunto de instrucciones a los auditores involucrados en la auditoría y como un medio para el control y registro de la ejecución apropiada del trabajo. El programa de auditoría puede también contener los objetivos de la auditoría para cada área y un estimado de horas hombre a invertir en las diversas áreas o procedimientos de auditoría a desarrollar.

Al preparar y modificar el programa de auditoría, el auditor debería considerar las evaluaciones específicas de los riesgos inherentes y de control y el nivel requerido de certeza que tendrán que proporcionar los procedimientos sustantivos. La

coordinación de cualquier ayuda esperada de la entidad, la disponibilidad de los auxiliares y la inclusión de otros auditores o expertos.
Al conocer el alcance del trabajo, queda a juicio del auditor aplicar la totalidad o parcialidad de las actividades definidas en cada área de control de MASTI.

4.7.6 PAPELES DE TRABAJO

Los papeles de trabajo son el conjunto de documentos que contienen la información obtenida por el auditor en su revisión, así como los resultados de los procedimientos y pruebas de auditoría aplicados; con ellos se sustentan las observaciones, recomendaciones, opiniones y conclusiones contenidas en el informe correspondiente. Todos los resultados y recomendaciones de la auditoría deberán sustentarse con evidencia obtenida en la auditoría, deberá documentarse debidamente en los papeles de trabajo, principalmente con el objeto de: Contar con una fuente de información y en su caso, efectuar aclaraciones con el ente auditado u otras partes interesadas y dejar constancia del trabajo realizado para futura consulta y referencia. Los auditores deberán considerar que el contenido y disposición de sus papeles de trabajo reflejarán el grado de su competencia y experiencia, estos deberán ser completos y detallados que pueda servirse de ellos para conocer el trabajo en que se sustente el informe de auditoría.

En conclusión la evidencia debe ser suficiente y apropiada en la auditoría para poder extraer conclusiones razonables sobre las cuales basa su informe, en ese contexto la **evidencia en la auditoría:** Significa la información obtenida por el auditor para llegar a las conclusiones, asimismo comprenderá documentos fuentes, la evidencia en la auditoría se obtiene de una mezcla apropiada de pruebas de control, de procedimientos sustantivos, análisis de proyecciones y análisis de indicadores y las **pruebas de control**: Significa pruebas realizadas para obtener evidencia en la auditoría sobre lo adecuado del diseño y operación efectiva de los sistemas, control interno, el cumplimiento de las metas y objetivos propuestos y el grado de eficacia, economía y eficiencia y el manejo de la entidad.

Para obtener las conclusiones de la auditoría, el auditor normalmente examina toda la información disponible, con base a los siguientes factores:

a. Nivel del riesgo.
b. Naturaleza de los sistemas y el control interno.
c. Evaluación del riesgo de control.
d. Experiencia obtenida en auditorías previas
e. Resultados de procedimientos de auditoría, incluyendo fraude o error que puedan haberse encontrado.
f. Fuente y confiabilidad de información disponible.

Por tanto, los papeles de trabajo estarán bajo la custodia de Auditoría de Sistemas ó de la instancia a la que pertenece, por contener la evidencia de trabajos de auditoría realizados por su personal.

La confidencialidad está ligada al cuidado y diligencia profesional con que deberán proceder los auditores, el uso y consulta de los papeles de trabajo estarán vedados por el secreto profesional a personas ajenas al área, salvo requerimiento o mandato de la autoridad jerárquica o legal de su competencia.

4.7.6.1 OBTENCIÓN PARA LA EVIDENCIA EN LA AUDITORÍA

El auditor de sistemas obtiene evidencia en la auditoría por uno o más de los siguientes procedimientos:

a. La inspección consiste en examinar registros, documentos, o activos tangibles. La inspección de registros y documentos proporciona evidencia en la auditoría de grados variables de confiabilidad dependiendo de su naturaleza y fuente y de la efectividad de los controles internos sobre su procesamiento.

b. La observación consiste en mirar un proceso o procedimiento que está siendo realizado por otros, incluye toma fotográfica.

c. La revisión consiste en buscar la información adecuada, dentro o fuera de la Organización, estas podrán variar dependiendo la información a recolectar.

d. La entrevista consiste en la respuesta a una pregunta o solicitud para corroborar la información obtenida en la investigación.

e. Los procedimientos analíticos consisten en el análisis de índices, indicadores y tendencias significativas incluyendo la investigación resultante de fluctuaciones y relaciones que son inconsistentes con otra información relevante.

4.7.6.2 FORMA Y CONTENIDO DE LOS PAPELES DE TRABAJO

El auditor deberá preparar papeles de trabajo que sean suficientemente completos y detallados para proporcionar una comprensión global de la auditoría.

La extensión de los papeles de trabajo es un caso de juicio profesional, ya que dependiendo la naturaleza de la Organización y el alcance determinarán el volumen o profundidad de los papeles, estos a su vez podrán ser:

a. Información referente a la estructura organizacional de la entidad.
b. Extractos o copias de documentos legales importantes, convenios u otro texto.
c. Resumen de las principales leyes, reglamentos y normas que debe cumplir la entidad.
d. Información concerniente a la industria, entorno económico y entorno legislativo dentro de los que opera la entidad.
e. Evidencia del proceso de planeación incluyendo programas de auditoría y cualesquier cambio al respecto.
f. Evidencia de las pruebas realizadas en el control interno.
g. Evidencia de evaluaciones de los riesgos inherentes y de control y cualesquiera revisiones al respecto.

h. Evidencia de la consideración del auditor del trabajo de auditoría interna y las conclusiones alcanzadas.
i. Análisis de transacciones.
j. Análisis de tendencias, índices importantes e indicadores económicos.
k. Una indicación sobre quién desarrolló los procedimientos de auditoría y cuándo fueron desarrollados
l. Copias de documentación sobre comunicaciones con otros auditores, expertos y terceras partes.

4.7.6.3 MARCAS PARA LOS PAPELES DE TRABAJO

La finalidad principal de las marcas en los papeles de trabajo es para identificarlos mejor, su utilidad radica en que tienen un significado preciso ya que destacan aspectos importantes de los papeles de trabajo que ha medida se van revisando, con el uso de estos símbolos se evita el abuso en la recopilación de copias inútiles de papeles de evaluación, por otra parte las referencias en los papeles de trabajo tienen la finalidad de facilitar y de relacionar la observación con el informe.

4.7.7 EL MEMORANDO (INFORME PRELIMINAR)

No es una práctica recomendable, aunque sí usual en algunos casos, ya que el Informe de Auditoría es por principio, un informe de conjunto. Sin embargo, en el caso de detección de irregularidades significativas, tanto errores como fraudes, sobre todo se requiere una actuación inmediata según la normativa legal y profesional, independientemente del nivel jerárquico afectado dentro de la estructura.

La finalidad principal del memorando, informe preliminar o borrador de informe no es formal sino que es representación de comunicar al auditado de manera inmediata las observaciones identificadas, con base en los resultados que se vayan obteniendo en el proceso de la auditoría, es decir que son avances sobre las observaciones para corrección, queda a criterio del auditor también poderlas enviar vía correo electrónico o impreso, todo esto es con el objetivo de dejar en el informe final aquellas que no fueron posible corregirlas durante el proceso de evaluación, con relación a las

observaciones que fueron superadas, estas se documentan y se señalan en el informe.

4.7.8 EL INFORME FINAL

Una vez que se ha detectado los hallazgos u observaciones, es obligación del auditor comentarlas de forma directa y abierta con los responsables asignados, a fin de que conozcan, acepten, aclaren, complementen y/o las modifiquen con detalles y pruebas.

Un informe final con su dictamen u opinión sobre los resultados, deberán ser superados por las áreas involucradas de la Organización, en el tiempo según la importancia y exigencia de cada observación.

El informe de auditoría de sistemas puede definirse como un documento formal y oficial que utiliza el auditor para informar por escrito y de manera oportuna, precisa, completa, sencilla y clara, sobre los resultados que obtuvo después de haber aplicado las técnicas, métodos y procedimientos apropiados al tipo de revisión que realizó, para fundamentar con ellos su opinión respecto a la auditoría realizada y estar en condiciones de poder emitir un dictamen correcto sobre el comportamiento de la tecnología de información. El informe de auditoría debe contener, como mínimo las siguientes secciones:

4.7.8.1 CARTA EJECUTIVA (OFICIO DE PRESENTACIÓN)

Es la primera parte del informe de auditoría y es un documento de carácter oficial que sirve como presentación consolidada del informe, mediante al cual se le expone a la Alta Administración de la empresa o a la jefatura correspondiente a quien reporte el auditor, un resumen general de los hallazgos. Esta carta contiene los siguientes aspectos: (anexo F modelo de carta ejecutiva)

a. Logotipo de identificación.

   Se trata de poner el logotipo, emblema o símbolo que permita identificar a la empresa o al área al cual pertenece auditoría de sistemas.(no es mandatario)

b. Nombre de la empresa.

Si la evaluación la realizó una entidad externa se coloca el nombre de la empresa, caso contrario se coloca el nombre del área al cual depende auditoría de sistemas.

c. Ubicación física y fecha de emisión de la carta

Esto identifica el lugar y la fecha que se emite la carta ejecutiva.

d. Identificación del área o empresa auditada

Se coloca el área, departamento, sistema al cual fue evaluado.

e. Nombre del personal receptor de la carta ejecutiva.

Por lo general, este informe se remite a un ejecutivo de alto nivel de la empresa o al jefe a quién reporta el auditor de sistemas (los grados académicos son reglas de cortesía)

f. Período de evaluación.

En esta parte se anotan las fechas de inicio y finalización de la auditoría; con esto se busca darle a conocer al receptor del informe el tiempo que comprendió la evaluación.

g. Contenido.

Es una breve descripción de los puntos que fueron evaluados y de los aspectos que integran el informe, su redacción debe ser precisa, esquemática y clara.

h. Responsable de emitir el dictamen.

En esta parte se anota el nombre del profesional responsable de emitir la carta ejecutiva, o el nombre del auditor de sistemas, según políticas internas de cada institución.

i. Firma.

En esta parte se pone la firma autógrafa del responsable de la auditoría, que es la persona que adquiere el compromiso de avalar lo reportado.

4.7.8.2 PRESENTACIÓN DEL INFORME.

Se consideran al inicio los mismos literales de la carta ejecutiva “a,b,c,d,e” este permite de una forma más amplia las observaciones identificadas en la evaluación, así mismo está formada por los siguientes elementos: (anexo G modelo de Informe)

a. Breve introducción al Informe.

En esta parte se anotan las razones que dieron origen a la auditoría, quién la ordenó, área o sistemas a revisar, actividades sujetas a evaluación, estos elementos permiten fundamentar las razones del porqué se realizó la auditoría.

b. Contenido del informe.

Se hace una breve descripción de los puntos que fueron evaluados, describiendo en forma clara, los aspectos que se consideran como observaciones o desviaciones sobre los puntos de los programas de auditoría.

c. Listado de observaciones.

Se describen las observaciones o situaciones que necesitan mejorarse; queda a criterio del auditor presentarlas de importancia mayor a importancia menor, cabe señalar que cada observación se encuentra relacionada o referenciada a un papel de trabajo.

d. Recomendaciones.

Después de haber señalado la observación, el auditor puede recomendar de manera objetiva, libre de cualquier influencia y con estricto apego a las pruebas y resultados observados durante la evaluación.

e. Responsable.

Se deja el nombre, puesto y titulo del responsable de emitir el informe, además de su firma autógrafa.

4.7.9 SEGUIMIENTO

Consiste en realizar un monitoreo o seguimiento a las observaciones señaladas en el informe con la finalidad de identificar el estado de estas, las cuales pueden llegar a ser: superadas, no superadas, en proceso o no aplica al proceso actual. Independientemente del estado que presenten las observaciones, estas deben ser evaluadas por el auditor de sistemas con la finalidad de fortalecer el área tecnológica. Con relación al tiempo de iniciar el seguimiento queda a juicio del auditor o jefatura a la cual reporta.

4.7.10 FECHA DEL INFORME

El período de realización del examen puede ser flexible, la fecha del Informe es importante, no sólo por la cuantificación de honorarios y el cumplimiento con el cliente, sino para conocer la magnitud del trabajo y sus implicaciones. Conviene precisar las fechas de inicio y conclusión del trabajo de campo, como períodos probables para la toma de decisiones. No obstante algunas ocasiones la fecha de finalización puede verse afectada debido a los hallazgos y al grado de riesgo identificado, al respecto, será decisión de la Alta Administración la ampliación ó reducción del tiempo estipulado.

4.8 COMPOSICIÓN DE MASTI

El Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información, conocido como "MASTI", agrupa las siguientes divisiones:

Planificación y Organización:
Comprende las decisiones estratégicas y planes operativos definidos por la Administración, esto incluye el entorno organizacional, elementos que contribuirán al logro de los objetivos planeados por la Entidad.

Plataforma Tecnológica:
La práctica de las estrategias definidas por la Organización, obligan a la directriz responsable de TI a cumplir bajo soluciones integrales y tecnológicas, proporcionar un mejor servicio ante el crecimiento y demanda que la institución requiere, todo ello con la finalidad de hacer posible la continuidad de las operaciones, descargando su confianza en los sistemas informáticos.

Soporte:
El mantenimiento, control y seguridad son factores a considerar como complemento de los procesos de TI debido a que deben ser evaluados regularmente, tanto en calidad como cumplimiento, ya que es parte fundamental para la continuidad del servicio.

Subcontratación.
Un acuerdo de subcontratación es aquel que se establece entre una entidad y un proveedor de servicios, en el que este último realiza una actividad, función, proceso o administra los recursos de TI del negocio solicitante. Las razones para que una empresa requiera de subcontratación están en función del alcance, naturaleza, ubicación, proveedor, calidad, recursos, oportunidad, servicios, etc.

4.9. APLICACIÓN DE MASTI

Los programas de auditoría podrían llegar a aparentar la facilidad de su aplicación, sin embargo, podemos decir que no es una actividad plenamente mecánica sino que es necesario tener conocimientos y la capacidad de medir el alcance debido a que esta es una actividad de análisis crítico, la cual no implica que existan fallas en la entidad auditada sino más bien fortalecer y mejorar el servicio de TI.

El Marco Referencial de MASTI "Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información", proporciona al auditor de sistemas una herramienta que le permite guiarlo sobre los puntos importantes a evaluar dentro de la Organización, no obstante la experiencia de éste, podrá hacer la ampliación o reducción del mismo, estando sujeto a la responsabilidad y la objetividad que defina los lineamientos de la Administración de la cual depende.

En nuestra opinión tenemos la certeza que los recursos de TI deben ser segmentados en divisiones, y éstas compuestas en áreas más específicas. Como producto de ello presentamos cuatro principales divisiones en las que se sustenta el presente manual: Planificación y Organización, Plataforma Tecnológica, Soporte y Subcontratación. Las divisiones en referencia se agrupan en **30** áreas de control y estas a la vez se subdividen en **541** actividades seccionadas las cuales conforman los programas de auditoría. La numeración correlativa de las actividades descritas en los referidos programas no representan, ni obedecen un orden de importancia, más bien es un numero correlativo, asimismo las actividades en comento no son obligatorias en su totalidad para la aplicación de cada una de estas, debido a que son de carácter general, de forma que permita la aplicación en cualquier tipo de organización, este enfoque resultó como producto de las pruebas realizadas del trabajo de aplicación en el campo.

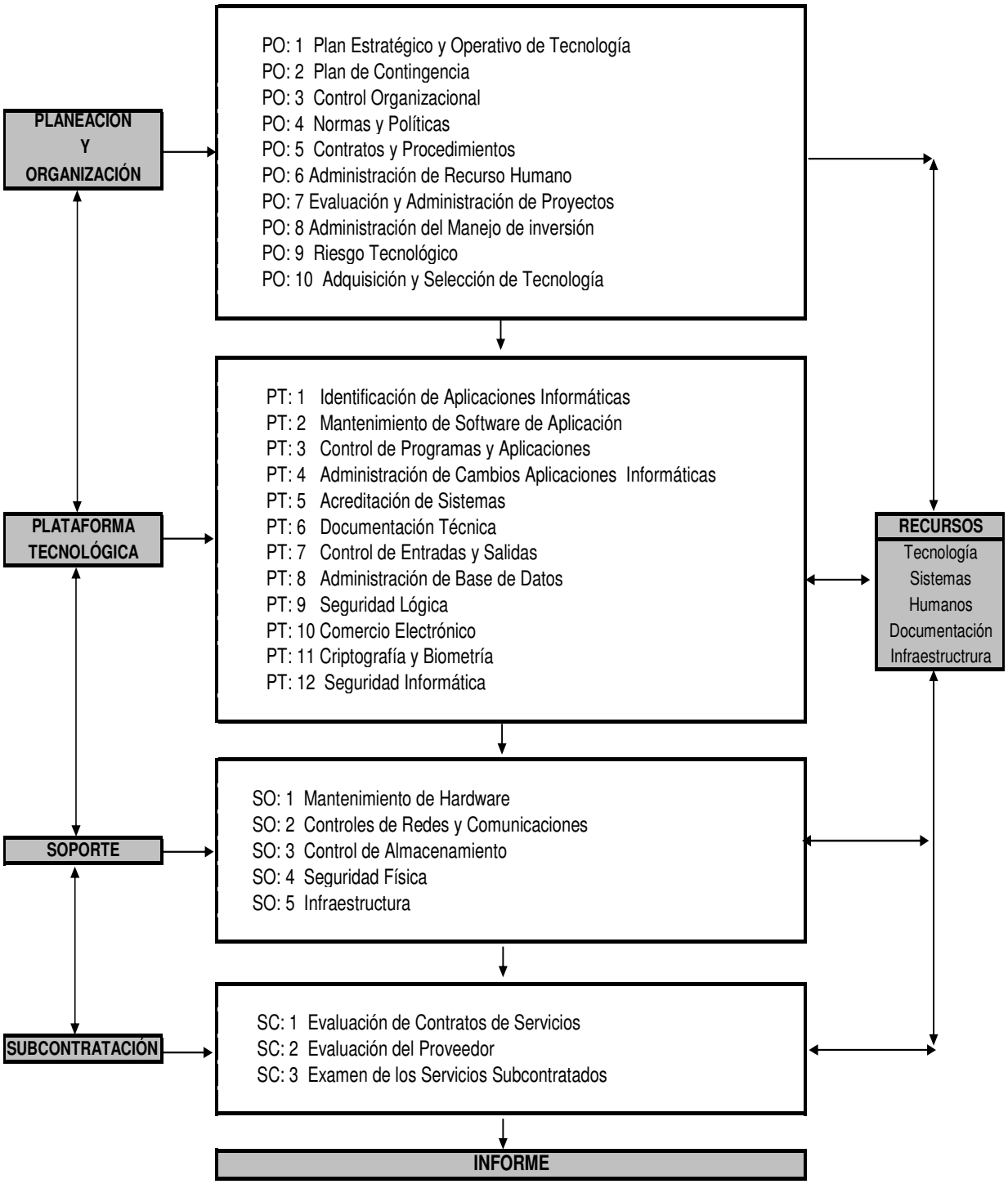
Los programas de auditoría descritos en MASTI, se encuentran orientados a objetivos de control en TI, que permitirán a la Administración tener una evaluación de carácter técnico sobre el ambiente de TI en la Organización y los riesgos asociados a esta actividad y los resultados obtenidos que permita mejorar el

servicio tecnológico en: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, todo ello encaminado a que la tecnología apoye el logro de los objetivos estratégicos institucionales.

4.10 ESQUEMA DE MASTI

El siguiente esquema representa el proceso que indica al auditor de sistemas, el flujo interactivo que pueden efectuar al realizar la evaluación, donde se observa que las cuatro divisiones están ligadas y se retroalimentan o se complementan con las actividades que dependen de cada una de ellas, el proceso en referencia estará bajo el juicio y el conocimiento que el auditor quiera profundizar en el alcance y objetivo previsto, esto requerirá la necesidad de disponer o involucrar para el desarrollo algunos recursos tales como: tecnológicos, de sistemas, recursos humanos, documentación técnica operativa y administrativa e infraestructura tecnológica.

ESQUEMA DE FLUJO PARA LA APLICACIÓN DE MASTI



4.11 MANUAL DE AUDITORÍA DE SISTEMAS PARA LA EVALUACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN. (MASTI)

(Ver Manual de Auditoría)

ÁREAS Páginas

MANUAL DE AUDITORÍA DE SISTEMAS PARA LA EVALUACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN.

(MASTI)

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PLANEACION Y ORGANIZACIÓN (PO)	
PO1: PLAN ESTRATÉGICO Y OPERATIVO DE TECNOLOGÍA.	
1. Verificar si en el plan estratégico institucional se encuentra incluido el plan estratégico de TI.	
2. Verificar si las actividades y metas del plan estratégico de TI están alineados, con los objetivos estratégicos institucionales y dar seguimiento al cumplimiento de los proyectos a largo plazo.	
3. Verificar la existencia de un plan operativo de TI para dar seguimiento al cumplimiento de metas de los proyectos a corto plazo.	
4. Verificar las actividades, períodos, grado de avance y responsables de ejecución de las actividades del plan estratégico.	
5. Verificar que el plan estratégico de TI sea traducido periódicamente en planes a corto plazo.	
6. Verificar si la Alta Administración o Auditoría Interna realiza monitoreo sobre el desarrollo e implementación de los Planes de TI a Corto y Largo Plazo, para contribuir al cumplimiento de los objetivos y metas de dichos planes.	
7. Verificar si en el proceso de planificación se han considerado factores internos y externos que afectan a la institución y su entorno por ejemplo: la distribución geográfica, la evolución tecnológica, los costos administrativos y operativos, los requerimientos legales, las regulaciones y leyes que rigen el funcionamiento de la Entidad.	
8. Evaluar si la institución tiene los recursos tecnológicos y humanos suficientes para el desarrollo del proyecto bajo las condiciones establecidas inicialmente.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
9. Verificar los insumos o fuentes de información que se utilizarán como base para la elaboración de la planeación estratégica de TI.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO2: PLAN DE CONTINGENCIA 1. Identificar la existencia del plan de contingencia y obtener una copia, así mismo verificar la fecha de vigencia, última actualización y funcionario responsable de autorización. 2. Verificar que el plan hace referencia a normas y políticas dictadas por tecnología. 3. Verificar si el plan está orientado a superar procesos críticos e imprevistos en el menor tiempo posible. 4. Verificar si la estructura y lenguaje del documento general es entendible y comprensible para su aplicación. 5. Verificar que en el plan se encuentren definidas las tareas a realizar para cada una de las personas involucradas en el plan. 6. Verificar que en el plan se hayan considerado pruebas para distintos escenarios y los mecanismos para la solución, por ejemplo: fallas en servidores centrales, fallas en servidores de servicio, fallas en el suministro eléctrico, fallas en los enlaces de comunicación, falta de insumos, respaldos no actualizados, etc. 7. Verificar que las jefaturas dispongan de una copia actualizada del plan. 8. Identificar si el plan incluye o describe la participación de un comité de administración de desastres o del equipo de emergencia. 9. Verificar si existe un servidor de contingencia para todas las aplicaciones críticas. 10. Verificar que el plan disponga de un anexo con los nombres del personal de soporte, administrativo y proveedores de servicio, el cargo, número telefónico fijo y móvil.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
11. Realizar llamadas telefónicas a parte del personal involucrado en el plan con la finalidad de verificar que los números son correctos y están actualizados. 12. Verificar que el plan se haya probado al menos dos veces al año, con la finalidad de fortalecer las áreas no funcionales. 13. Entrevistar al personal para identificar si conocen las responsabilidades que tienen asignadas en una situación de desastre. 14. Verificar si existen procedimientos definidos para actualizar el manual. Asimismo si aplican y distribuyen las actualizaciones a los usuarios involucrados. 15. Verificar que el plan contenga los planos del centro de cómputo, diagramas de cableado eléctrico, diagramas de red, diagramas de ductos e inventarios de hardware. 16. Verificar que exista una copia de datos actualizados, programas y documentación técnica del sistema que almacene en un lugar externo a la empresa. 17. Verificar que el personal involucrado tiene el conocimiento de los procedimientos establecidos para la continuidad de las operaciones en caso de desastres. 18. Evaluar si el centro de cómputo alterno o para la continuidad de operaciones reúne las condiciones mínimas de seguridad física tales como: controles de acceso, piso elevado o protegido, controles de humedad, controles de temperatura, circuitos especializados, fuente interrumpida de energía, dispositivos de detección de agua, detectores de humo y un sistema adecuado de extinción de incendios.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO3: CONTROL ORGANIZACIONAL 1. Solicitar el organigrama de la empresa e identificar la ubicación de TI, analizar su estructura jerárquica y que esté conforme a la situación actual. Así mismo verificar su vigencia y aprobación. 2. Verificar si la estructura actual está encaminada a los logros de los objetivos del área de TI. 3. Verificar si los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área de TI. 4. Verificar si se consideran adecuados los departamentos y áreas en que está dividida la estructura de TI. 5. Solicitar los manuales de puestos del área de TI y verificar que las funciones descritas correspondan con las que ejecuta cada empleado de TI. 6. Evaluar el manual de puestos, su claridad en la delegación de autoridades, y que deben ir acompañadas de definiciones de las habilidades técnicas necesarias, para utilizarse como base para la evaluación del desempeño. 7. Verificar si los puestos actuales son adecuados a la necesidad que tiene el área para cumplir con sus funciones. 8. Verificar que mecanismo utiliza la administración para resolver los conflictos por las cargas de trabajo desequilibradas. 9. Identificar las causas de incumplimiento de las funciones y objetivos previstos por la Administración, como por ejemplo: falta de personal, personal no capacitado, cargas de trabajo excesivas, realización de otras actividades, planificación y la forma en que se desarrollan.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar que la posición de la unidad de tecnología esté en un nivel suficientemente alto para garantizar su independencia de los departamentos usuarios. 11. Verificar si en los manuales de reclutamiento de personal, consideran la educación, la experiencia y los riesgos de trabajo pertinentes para los requerimientos del puesto y del grado de responsabilidad. 12. Verificar que exista una separación adecuada de tareas entre los operadores de la computadora, los programadores de la Aplicación y los analistas de sistemas. 13. Verificar que existan controles externos apropiados de manera que el personal administrativo, operativo y técnico esté informado e involucrado en las actividades ya definidas. 14. Asegurar una adecuada separación de deberes entre la preparación manual de los datos y las funciones de transferencia de los datos a la computadora, grabación manual en cinta o disco magnético, etc. 15. Verificar que exista un plan de capacitación y que éste responda a las necesidades de la institución en cumplimiento al plan estratégico de TI. 16. Verificar que todo el personal tome un mínimo de cinco días consecutivos de vacaciones, de manera que alguien mas pueda ejecutar las funciones específicas de un puesto determinado. 17. Verificar que exista una política o norma apropiada para la separación de funciones y esta sea auditada. 18. Revisar las descripciones de los puestos por cada departamento o unidad, de tal manera asegurar que cada una de ellas está conforme al cargo.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO4: NORMAS Y POLÍTICAS 1. Solicitar inventario de políticas y normas establecidas para TI. 2. Verificar que la Administración o la Gerencia de TI sea responsable de la formulación, desarrollo, documentación, divulgación y el control de las políticas; y que todas ellas estén por escrito y debidamente autorizadas y actualizadas. 3. Verificar que la Gerencia de TI haya creado mecanismos de divulgación que permitan asegurar que las políticas sean comunicadas y comprendidas por todo el personal involucrado directa o indirecta con el área de TI. 4. Verificar que las políticas o normas emitidas sean actualizadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional, para garantizar que sean funcionales y aplicables. 5. Verificar si las políticas o normas son del conocimiento y aceptadas por el personal de TI. 6. Verificar la existencia de política o normas sobre reserva y confidencialidad de información. 7. Verificar que las normas y políticas estén autorizadas por la alta administración y que presenten fecha de vigencia. 8. Verificar que exista una participación de las áreas especializadas de la institución en la creación y regulación de las normas y políticas.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO5: CONTRATOS Y PROCEDIMIENTOS ADMINISTRATIVOS. 1. Verificar que los procedimientos de trabajo ejecutados por los operadores del centro de cómputo estén documentados por escrito. 2. Verificar que los procedimientos escritos definan los horarios de trabajo para los operadores del centro de cómputo, considerando los cierres semanales, mensuales y anuales. 3. Verificar si existe un control para restringir el acceso al personal externo a TI en días y horarios de procesos especiales. 4. Verificar que exista un control manual o automático de la información que entra y sale del área TI. 5. Verificar si existe un responsable oficial encargado de la oficina de control de la información para toda la organización, teniendo como una de sus funciones principales ser el enlace de la información entre TI y el resto de la organización. 6. Verificar la existencia de procedimientos a utilizar por los operadores del centro de cómputo, de forma que permitan identificar el inicio, proceso y final de cada actividad. 7. Verificar la existencia de una póliza de seguro con cobertura para la pérdida de equipo de computación y medios de proceso de datos. 8. Solicitar las hojas de vida de los principales puestos de TI para evaluar la capacidad y experiencia para desarrollar su puesto.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO6. ADMINISTRACIÓN DEL RECURSO HUMANO. 1. Verificar que se considera en el proceso de selección de personal el nivel educativo, y la experiencia laboral en el puesto para el cual está participando. 2. Verificar si existe evaluación del personal para garantizar un nivel aceptable de desempeño y cumplimiento de metas del área de TI. 3. Verificar si existe un plan de capacitación y si está orientado al giro de la institución y la plataforma tecnológica con que cuenta la institución. 4. Verificar si la Gerencia de TI ha considerado pruebas de entrenamiento cruzado, con la finalidad de disponer con personal de respaldo ante posible ausencia de personal clave. 5. Verificar que la Gerencia de TI considere acciones oportunas y apropiadas con respecto a cambios de puestos y despidos. 6. Verificar que exista la suficiente formación del personal, con capacitación continua que ayude a mantener su conocimiento técnico, sus destrezas y habilidades. 7. Verificar si el desempeño de los empleados se evalúa contra los estándares establecidos. 8. Verificar si los puestos actuales son adecuados a la necesidad que tiene el área para llevar a cabo sus funciones. 9. Verificar si el número de empleados que trabajan actualmente en el área de TI es adecuado para cumplir con las funciones encomendadas. 10. Verificar si las cargas de trabajo están distribuidas de forma equitativa para todo el personal de TI.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
11. Verificar si son adecuadas las condiciones ambientales con respecto a: espacio, iluminación, ventilación, equipo de oficina, mobiliario, ruido, etc.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO7: EVALUACIÓN Y ADMINISTRACIÓN DE PROYECTOS. 1. Verificar si existe un comité técnico evaluador de proyectos e identificar los miembros que la integran; asimismo verificar si existe un libro de actas de los acuerdos y decisiones tomadas sobre los proyectos. 2. Verificar si existe documentación histórica sobre la ejecución de los proyectos finalizados o en proceso. 3. Verificar la existencia de cumplimientos de las normas internas para la formulación de proyectos. 4. Verificar si la institución cuenta con controles para evaluar periódicamente la ejecución del proyecto, de forma que permita evaluar la situación actual y efectuar las medidas correctivas necesarias, como cambios en el entorno del negocio y en la tecnología, para lograr la finalización del proyecto cumpliendo con las metas y objetivos requeridos. 5. Verificar que la Gerencia de TI haya establecido una metodología de Administración de Proyectos que defina como mínimo, la asignación de responsabilidades, el detalle completo de las tareas, el cronograma de trabajo, los recursos, los diversos puntos de revisión y los procedimientos para las aprobaciones. 6. Verificar que para los proyectos de TI considerados importantes para la institución exista un estudio de factibilidad tecnológica de cada alternativa de forma que satisfaga los requerimientos de la institución. 7. Verificar que para los proyectos de TI importantes para la institución exista un estudio costo beneficio de cada alternativa de forma que cubra los requerimientos de la institución.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
8. Verificar de la planeación de los proyectos de TI y comprobar la existencia de lo siguiente: 8.1 Verificar si existe un acta de inicio y autorización de la alta administración. 8.2 Verificar que estén definidos los miembros y responsables del equipo del Proyecto. 8.3 Verificar si poseen plan de aseguramiento de calidad de sistemas. 8.4 Verificar si posee un Plan de Pruebas (piloto, paralelo, modular, etc.) 8.5 Verificar si el plan considera contrataciones de personal adicional para el proyecto 8.6 Verificar si cuentan con un Plan de capacitación. 8.7 Verificar si cuentan con un plan de pruebas de estrés para las aplicaciones informáticas. 8.8 Verificar que exista un plan de Revisión Post Implementación 8.9 Verificar que la documentación de las aplicaciones informáticas se lleve actualizada. 8.10 Verificar que exista una programación financiera del proyecto. 9. Verificar que el área de TI tenga documentado la planeación de los proyectos finalizados, en proceso y los que estén por iniciar. 10. Verificar la plataforma tecnológica a utilizar para el desarrollo de los proyectos de TI, esto incluye base de datos, sistema operativo, software de desarrollo, etc. 11. Verificar que exista un comité de evaluación de proyectos con la responsabilidad de emitir actas que documenten los avances del proyecto y las decisiones tomadas en dicho comité. 12. Verificar que la Gerencia de tecnología tenga claramente definido las ventajas de la nueva tecnología a implantar y los riesgos asociados a cada una de ellas.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO8: ADMINISTRACIÓN DEL MANEJO DE INVERSIÓN. 1. Verificar la existencia de un presupuesto operativo anual para adquisición de tecnología. 2. Verificar que la compra de equipos y software estén de conformidad al presupuesto asignado para tal efecto. 3. Verificar que el presupuesto contemple cantidades realistas y coherentes con los precios de mercado de la tecnología de información y que cumplan con los planes estratégicos y operativos. 4. Verificar las licitaciones o matriz técnica de ofertas y analizar según proveedor y condiciones del producto. 5. Verificar que los cambios en el presupuesto anual y anterior estén de conformidad a las variaciones en los precios de mercado y necesidades de la institución. Cualquier variación considerable, pedir la justificación respectiva al personal que ha desarrollado dicho presupuesto. 6. Verificar que exista un control adecuado de los costos en que incurre el área de Tecnología de Información. 7. Verificar que existan procedimientos y políticas claras, definidas y documentadas respecto al monitoreo de costos. 8. Verificar que los excesos en comparación al presupuesto, sean controlados, justificados y se les de el seguimiento correspondiente, para cumplir con la proyección anual realizada 9. Verificar que los costos en que incurra la institución sean claramente justificados. 10. Verificar que toda salida de efectivo vaya acompaña de más de una firma, a fin de que quede reflejado quien realizó el desembolso, quien lo revisó y quien lo autorizó.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO9: RIESGO TÉCNOLOGICO 1. Verificar si existen normas o políticas para la Administración del Riesgo Tecnológico. 2. Verificar si existe un comité de evaluación de riesgo tecnológico. 3. Verificar si el comité tiene definido como identifica y mide el riesgo tecnológico. 4. Verificar si el aspecto de confidencialidad mantiene controles estrictos y si se han adoptado medidas de seguridad, sobre todo con las transferencias de datos que viajan a través de Internet, donde cabe la posibilidad que se coloquen "Sniffers" a la puerta de un servidor donde se realicen operaciones monetarias ó intercambios de documentos con información confidencial. 5. Verificar los procedimientos y mecanismos optados por TI para la identificación y autenticación de usuarios en la red, para garantizar la legitimidad de las operaciones que estos realizaron. 6. Verificar la existencia de procedimientos, prácticas y políticas de control interno, y si estos son adecuados. 7. Verificar si la institución ha incurrido en pérdidas derivadas de fraudes o errores; y establezca lo adecuado de las medidas adoptadas por la administración para minimizar este riesgo. 8. Verificar el nivel de competencia y capacidad de los funcionarios que hacen efectivo los procedimientos de control interno. 9. Verificar la idoneidad, experiencia y capacidad técnica del personal que realiza el trabajo de auditoría externa de sistemas.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar el nivel o grado de independencia de auditoría externa de sistemas tomando en consideración las recomendaciones que realiza a la Administración. 11. Verificar la efectividad de las actividades de auditoría externa de sistemas con relación a: objetivos, alcance, frecuencia, documentación apropiada, conclusiones, anexos, etc. 12. Verificar si el sistema de Información Gerencial provee al usuario información oportuna y de calidad, consistente, completa y relevante para la toma de decisiones, principalmente aquellas enfocadas a la administración de riesgos. 13. Verificar lo adecuado de la organización, lugar, recursos y la idoneidad del personal del área de sistemas de información, en función de la labor desempeñada, responsabilidad e independencia dentro de la organización. 14. Verificar la existencia y aplicación de medidas apropiadas que le den seguridad a la infraestructura y limiten el acceso a los recursos tecnológicos, así como a la información generada por dichos sistemas y su adecuado almacenamiento. 15. Verificar el cumplimiento en lo relacionado al uso de subcontratación o actividades de consultores externos, la existencia de políticas y procedimientos adecuados y alineados a la protección y no divulgación de la información. 16. Verificar si la institución cuenta con una adecuada planificación a corto y largo plazo para el cambio de infraestructura tecnológica y para los sistemas de información conforme a las tendencias del mercado y el mismo crecimiento de la institución. **17. Riesgo operacional o transaccional.** 17.1 Verificar qué mecanismos utilizan para medir la confiabilidad e integridad de los sistemas de información.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
17.2 Verificar la seguridad en las transacciones enviadas o recibidas. 17.3 Verificar si han recibido ataques internos o externos a los sistemas informáticos. 18. Verificar el cumplimiento de beneficios propuestos, tales como: 18.1 Rapidez y agilidad en las transacciones. 18.2 Tiempo de respuesta razonable. 18.3 Costos de transacción más bajos. 18.4 Accesos a nuevos mercados 18.5 Seguridad. 18.6 Menos gastos fijos y de operación. 18.7 Servicio sin restricción de tiempo. 18.8 Acceso desde cualquier parte. 18.9 Mejor imagen. 19. **Riesgo Dependencia Tecnológica**. 19.1 Verificar si en el contrato de adquisición de software no existe cláusula que obligue a la empresa a disponer exclusivamente del producto por tiempo definido. 19.2 Verificar que el software sea de arquitectura abierta, con el fin de poder migrar a una nueva plataforma. 19.3 Verificar los períodos de vigencia de uso de los módulos, para determinar el grado de obsolescencia. 19.4 Verificar la disposición de los proveedores al realizar el cambio de plataforma. 19.5 Verificar el estatus del proveedor del software y determinar si en la actualidad de representante o distribuidor. 19.6 Verificar cuando el servicio informático es subcontratado, existe disposición de acceso a los datos. 20. **Riesgo Legal.** 20.1 Verificar si existen litigios pendientes de ser resueltos, asociados a tecnología. 20.2 Verificar si el tratamiento que se da al riesgo legal en los nuevos productos a lanzar al mercado y la protección de la institución en la elaboración de contratos es adecuada.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
20.3 Verificar la frecuencia y el nivel de gravedad de los litigios a nivel tecnológico que se ha visto involucrada la institución, y evalúe su historial. 20.4 Verificar si el contrato sobre las pólizas de seguro, ha sido revisado por el asesor legal de la institución y las opiniones que ha vertido sobre el mismo. 20.5 Verificar que la institución cumpla con la normativa legal y reglamentaria, establecidas en las leyes de la República de El Salvador. **21. Riesgo de Reputación** 21.1 Verificar con la Administración la disposición de políticas, prácticas y procedimientos respecto del manejo de la imagen o reputación de la empresa. 21.2 Verificar si monitorean el comportamiento de funcionarios y empleados que se relacionen con las licitaciones y compras de equipo tecnológico. 21.3 Verificar como la Administración evalúa la percepción del público, respecto del servicio, estabilidad y calidad. 21.4 Verificar el volumen de reclamos del público, respecto a fraudes realizados por medio de sistemas informáticos, así como las medidas adoptadas para subsanar las deficiencias.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PO:10 ADQUISICIÓN Y SELECCIÓN DE TECNOLOGÍA 1. Verifique el cumplimiento de normas internas para la compra de tecnología. 2. Verifique el estudio inicial sobre la necesidad del requerimiento, según el monto de la inversión. 3. Verificar si el comité técnico evalúa cada inversión a realizar en tecnología. 4. Verificar cuál es el criterio de evaluación en adquisición de software y hardware. 5. Verificar si revisan los documentos fiscales correspondientes al hardware y software contratados, con la finalidad de comprobar los desembolsos. 6. Verificar si comparten con el personal responsable del área de informática las condiciones contractuales brindadas por el proveedor. 7. Verificar como se evalúa la nueva adquisición de hardware y software, conforme al condicionamiento del sistema actual. 8. Verificar si existe planificación en la migración de los datos con el proveedor y se definen responsabilidades internas dentro de la Organización. 9. Verificar que criterios técnicos usan para seleccionar al proveedor. 10. Verificar como se realiza la adquisición de equipo se realiza a través de licitación para los proveedores. 11. Verificar como analizan las fortalezas y debilidades de los proveedores versus características, por medio de una matriz técnica.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
12. Verifique si el estudio de viabilidad reúne las condiciones de la factibilidad técnica, operativa y financiera. 13. Verificar que procedimientos utilizan para la aplicación y desglose del porcentaje en cada desembolso. 14. Verificar la consideración en la adquisición de hardware o software la relevancia del proveedor de ser representante o distribuidor. 15. Verificar como evalúan la experiencia de otras organizaciones en cuanto al uso del producto. 16. Verifique en el universo de sus clientes la calidad del servicio proporcionado por el proveedor.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PLATAFORMA TECNOLÓGICA (PT) **PT1: IDENTIFICACIÓN DE APLICACIONES INFORMÁTICAS.** 1. Verificar si existe un inventario de software aplicativo en el que se detalle la versión, el proveedor, la vigencia de la licencia, etc. 2. Verificar el inventario de software contra las licencias, con el objetivo de evitar sanciones por la Ley de propiedad intelectual. 3. Verificar si el software es sensitivo cuando es utilizado en lugares remotos, considere el hacer una carga especial del software desde el lugar central. Este daría la seguridad de que no se hayan hecho cambios ilegales en los programas en lugar remoto. También verificar si se puede cargar así los programas cada vez que un proveedor de mantenimiento lo requiera. 4. Verificar que el software de seguridad controle las tablas sensitivas y que valide periódicamente contra acceso no autorizado el cambio de la configuración original. 5. Verificar que no se permita a los programadores de las aplicaciones modificar y ejecutar directamente programas en ambiente de producción. 6. Verificar que mecanismos se utilizan para prevenir probables intrusiones tipo “caballo de Troya”, es decir que el usuario carga al sistema un programa de software autorizado que contiene programa ó rutinas no autorizadas. 7. Verificar que existan controles sobre los recursos compartidos en los equipos informáticos como: discos duros, carpetas o archivos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT2: MANTENIMIENTO DE SOFTWARE DE APLICACIÓN. 1. Verificar si el diseño de las nuevas aplicaciones o de las modificaciones a los módulos puestos en producción, son revisados y aprobados por la Gerencia de TI. 2. Verificar e Identificar quienes son los responsables de aprobar cualquier proyecto de desarrollo, implementación o modificación. 3. Verificar si existen procedimientos definidos o estándares, para las etapas de desarrollo de un nuevo sistema o cambios a los ya existentes. 4. Verificar si cuentan con mecanismos para identificar los requerimientos de seguridad y control interno para cada proyecto de desarrollo o modificación de sistemas de información, previo a su desarrollo. 5. Verificar e identificar si se incluyen en el diseño de las nuevas aplicaciones o en las modificaciones de sistemas de información, controles de aplicación que garanticen que los datos de entrada y salida estén completos. 6. Verificar si consideran aspectos básicos de seguridad y control interno del módulo a ser desarrollado o modificado, y estos son evaluados junto con el diseño conceptual del mismo. 7. Identificar si existe una metodología estándar para el desarrollo de un plan de pruebas, en donde se incluyan pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga y estrés, para cada módulo. 8. Verificar si la formulación del procedimiento de prueba y los datos de prueba son revisados y aprobados por el jefe de programación.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
9. Verificar si se aplican adecuadas medidas de seguridad para prevenir divulgación de información sensitiva durante las pruebas. 10. Verificar que los resultados de las pruebas son revisados y aprobados por el usuario.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT3: CONTROLES DE PROGRAMAS Y APLICACIONES. 1. Verificar el conteo de la cantidad de "byte" de los programas fuentes actuales para hacer una comparación rápida entre la cantidad de byte de estos y los autorizados que se trasladaron a producción para alertar en caso de modificaciones. 2. Verificar que exista un archivo lóg o bitácora que permita identificar los errores de ejecución de aplicaciones, sistema operativo y BD. 3. Verificar si han considerado todos los dispositivos de seguridad que fueron recomendados por el fabricante o el programador. 4. Verificar que exista una persona responsable en el área de TI de revisar periódicamente los archivos lóg o bitácoras de los sistemas. 5. Verificar que la institución respete los límites de la capacidad de procesamiento recomendados por el proveedor como: memoria, espacio en disco, procesamiento CPU. Para garantizar el correcto funcionamiento de las aplicaciones informáticas. 6. Verificar que la institución cuente con un servidor de desarrollo que sea de uso de los programadores para el desarrollo y pruebas de las aplicaciones internas. 7. Verificar que los programadores no tengan acceso a la línea de comandos, en los servidores de producción y acceso a estos para consultas. 8. Verificar si existe una persona responsable dentro del área de tecnología en cargada de ejecutar programas de diagnóstico de la red institucional. 9. Verificar que exista un procedimiento de control de cambios de los programas y del traslado del ambiente de desarrollo a producción.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar que no exista más de un usuario además del administrador con el perfil de mantenimiento de parámetros de los módulos de las aplicaciones informáticas. 11. Comprobar que la custodia de la documentación del software de Aplicación, los software utilitario entre otros estén controlados por personal de tecnología.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT4: ADMINISTRACIÓN DE CAMBIOS DE APLICACIONES INFORMÁTICAS. 1. Verificar si existe un sistema para el control de requerimientos de usuarios que afecten la estructura de los sistemas de información. 2. Verificar el o los tipos de formularios utilizados para el control de cambios 3. Verificar si existen procedimientos definidos para determinar el estatus de cada solicitud para los cambios realizados. 4. Verificar el procedimiento para el tratamiento de solicitudes identificadas como urgentes. 5. Verificar la existencia de controles para la modificación de programas fuentes y el traslado a producción. 6. Verificar si se mantiene un registro de cambios en los programas, que indique la fecha en que se realizó, a fin de proveer el orden cronológico exacto del sistema. Asimismo identificar el responsable de realizar el cambio. 7. Verificar si se requiere de la aprobación y autorización por escrito de la Gerencia de TI, para todas las modificaciones antes de hacer cambios. 8. Verificar si los cambios al sistema operacional o programas aplicativos, sus pruebas y resultados, son revisados por el jefe de programación técnica o quien hace sus funciones. 9. Verificar si los usuarios que formularon el requerimiento lo revisan y dan su aprobación a dichos cambios.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar si existen disposiciones para probar los cambios de programas y revisar los resultados con personal de supervisión antes de que dichas revisiones sean trasladadas al ambiente de producción. 11. Verificar quienes son los encargados de efectuar los cambios y como se documentan. 12. Verificar que las pruebas se realizan en un área o servidor de desarrollo.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT5: ACREDITACIÓN DE SISTEMAS. 1. Verificar si como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información, existe un procedimiento para que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo. 2. Verificar si se planifica la migración de los datos con el proveedor y se definen responsabilidades. 3. Verificar que existan certificaciones independientes en que la conversión del sistema y datos se desarrolle de acuerdo al plan establecido. 4. Verificar si las pruebas a los nuevos sistemas o a las modificaciones a los sistemas, son llevadas a cabo por un grupo de prueba independiente, diferente al de los desarrolladores. 5. Verificar que las pruebas a los sistemas se desarrollen en un ambiente de prueba separado, el cual sea representativo del ambiente operacional futuro (por ejemplo: condiciones similares de seguridad, controles internos, cargas de trabajo, etc.) 6. Verificar si cuentan con procedimientos establecidos para asegurar que las pruebas piloto o en paralelo sean llevadas a cabo con planes pre establecidos. 7. Verificar si los criterios para la terminación del proceso de prueba son especificados con anterioridad. 8. Verificar si incluyen como parte del plan de instalación y acreditación de sistemas, pruebas de aceptación por parte de los usuarios finales de los sistemas nuevos o de las modificaciones a los sistemas de información.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
9. Verificar como certifican los usuarios finales la aceptación final del nuevo sistema o de las modificaciones a los sistemas. 10. Verificar el procedimiento utilizado para asegurar que la Gerencia usuaria acepta formalmente el nivel de seguridad para los sistemas. 11. Verificar el proceso utilizado para el traslado de nuevas aplicaciones o modificaciones al sistema a producción. 12. Verificar quién es el responsable de efectuar el traslado a producción.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT6: DOCUMENTACIÓN TECNICA 1. Verificar por medio de inventario los nombres de programas y descripción de ellos 2. Verificar por medio de Inventario los nombres de tablas o archivos con su respectiva descripción 3. Verificar la existencia y disponibilidad de diagramas de entidad relación. 4. Verificar la existencia de manuales de usuario de los aplicativos puestos en producción. 5. Verificar si los manuales de usuarios se encuentran autorizados y disponen de fecha de vigencia, con la finalidad de identificar su actualización 6. Verificar la existencia de diccionario de datos de las tablas o archivos que conforman los sistemas puestos en producción.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT7: CONTROL DE ENTRADAS Y SALIDAS **ENTRADAS (ORIGEN DE TRANSACCIONES)** 1. Verificar según sistema cuáles y cuántos son los aplicativos que se alimentan de forma automática y manual. 2. Verificar si la estructura de los formularios que se utilizan como base para la captura de información son adecuados y completos de acuerdo a lo requerido por el sistema. 3. Verificar la existencia de aplicativos que se alimentan por medio de dispositivos magnéticos de entidades externas, asimismo comprobar los mecanismos de control de calidad de los datos. 4. Verificar e identificar filtros de alertas o mensajes del sistema que permitan controlar la calidad de información que será ingresada. 5. Verificar según muestra de documentos fuente, aspectos como cifras de control firma de autorización y similares. 6. Verificar si existe un control a nivel de perfil de usuarios que ingresan datos para evitar ingreso de datos por usuarios no autorizados. 7. Verificar que existan restricciones controladas para el uso de diversos dispositivos magnéticos de entrada. 8. Verificar que cuando se diseñen formas, los campos de datos importantes tengan predefinido un formato de ingreso de datos, con el fin de minimizar errores. 9. Verificar que existan controles sobre los documentos de propiedad con números de series secuenciales y el ingreso de dichos números al sistema para crear la relación entre ambos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar que exista un registro de la fecha de proceso y la fecha de transacción para las transacciones de entrada. 11. Verificar si a los documentos ingresados, se les asigna una marca de control o sello con la finalidad de asegurase que estos no sean ingresados nuevamente. 12. Verificar qué mecanismos utilizan para identificar si existen documentos de entrada no ingresados al sistema. 13. Verificar el cumplimiento del artículo de 451 y 455 del Código de Comercio, que relaciona al período de resguardo de la información fuente u original. 14. Comprobar el control utilizado para demostrar que la información a ingresar se encuentra autorizada. 15. Identificar si la institución realiza un control de calidad sobre el estado de los documentos que van a ser digitalizados para ser almacenados como imagen. 16. Verificar qué procedimientos existen para el manejo de errores con el fin de proporcionar al personal usuario instrucciones para la corrección de errores en los documentos fuentes. 17. Revisar los tipos de errores y las razones de su ocurrencia con el fin de determinar si los problemas son ocasionados por el programa o por ingreso incorrecto de datos. 18. Verificar si se obtiene una copia del LOG que registra el sistema en relación a las entradas de datos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SALIDAS 1. Verificar si existe un inventario de reportes, que identifique: nombre del programa, nombre del módulo, unidad destino, frecuencia de emisión y medio de emisión. 2. Verificar el proceso de distribución de los reportes de manera que se envíen al personal autorizado. 3. Verificar el área donde se resguardan los reportes confidenciales de manera que el personal no autorizado no pueda tener acceso a ellos. 4. Comprobar que se eliminen de forma inmediata los archivos de salida, no finalizados cuando sean confidenciales. 5. Verificar que exista un responsable de efectuar un análisis general de los reportes con el objeto de determinar si hay reportes que puedan ser eliminados, fusionados, reagrupados, simplificados, o si se requiere nuevos reportes. 6. Evaluar quién ejerce la función de control de calidad en los reportes emitidos. 7. Verificar si los encabezados de cada reporte incluyen los siguientes aspectos: fecha de generación, nombre del programa, período cubierto de proceso, titulo descriptivo del contenido del reporte, usuario que generó, número de identificación del programa, número de página, etc. 8. Verificar que se etiquete cada reporte o grupo de reportes de manera que se indique en el nombre del usuario, destino y el área o departamento al que pertenece. 9. Verificar la existencia de códigos que identifiquen el nivel de confidencialidad del reporte.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar cuál es el procedimiento para la destrucción de reportes sobrantes o que no estén en uso. 11. Verificar que mecanismos de control utilizan para producir únicamente la cantidad requerida de reportes solicitados. 12. Evaluar el nivel de satisfacción de los usuarios respecto a la estructura de los reportes y a la confidencialidad de la información generada.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT8: ADMINISTRACIÓN DE BASE DE DATOS. 1. Verificar qué mecanismos o herramientas usa el Administrador de Base de Datos (DBA) para supervisar y administrar la Base de Datos. 2. Verificar el procedimiento utilizado para definir el nivel de acceso de los usuarios. 3. Verificar si únicamente el Administrador de Base de Datos tiene privilegios a nivel de administrador para hacer cambios a la base de datos. 4. Verificar los diferentes tipos de usuarios que tienen acceso a la Base de Datos, e identificar su clasificación por medio de la siguiente segmentación: 4.1 Usuarios que modifican la estructura 4.2 Usuarios que modifican los datos 4.3 Usuarios operativos 4.4 Usuarios técnicos 5. Verificar que el Administrador de Base de Datos disponga de procedimientos escritos para la restauración de la Base de Datos, en caso de una destrucción total o parcial. 6. Verificar que el usuario y clave del BDA se registre en un sobre lacrado y éste se resguarde en un lugar seguro. 7. Verificar que el Administrador de Base de Datos sea responsable de la integridad de la Base de Datos y desarrolle reglas de validación y acceso. 8. Verificar que el Administrador de Base de Datos documente cualquier cambio que se realice a la Base de Datos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
9. Verificar que el Administrador de Base de Datos administra el diccionario de datos. 10. Verificar que el Administrador de Base de Datos es el responsable de la seguridad global de la Base de Datos. 11. Verificar si el Administrador de Base de Datos tiene control para que no se realicen pruebas en la Base de Datos en producción, sino que se disponga de diferentes ambientes para este fin. 12. Verificar que los usuarios no tengan acceso directo a la Base de Datos, sino que el acceso sea a través del servidor de aplicaciones. 13. Verificar si existen pruebas que involucren atentados deliberados para destruir o modificar la Base de Datos, considérense atentados tanto internos como externos. Estos simulacros deben de ser desarrollados por el Administrador de Base de Datos. Las destrucciones descritas en los simulacros deben de ser llevados a cabo por personal autorizado o no autorizado que trate de cambiar la Base de Datos, modificar los programas de la Aplicación, sustraer copia de la Base de Datos o del diccionario de datos, etc. 14. Verificar que solo el usuario de administrador tenga el privilegio de acceso a las tablas de usuarios y contraseñas. 15. Verificar si el software de Base de Datos utilizado en la institución cuenta con tablas de registros de auditoría para revisar los eventos que tiene registrados. 16. Verificar en las tablas de registros de auditoría de la Base de Datos las acciones de intentos de conexión, acceso a los objetos y accesos a la base.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
17. Verificar las acciones que el Administrador de la Base de Datos realiza con las tablas de registros de auditoría de la base, para corregir posibles fallas o accesos no autorizados. 18. Verificar que el parámetro para permitir auditoría a la Base de Datos tenga el valor que equivale o permite auditoría. 19. Verificar que existan controles mínimos en la seguridad de las tablas: por ejemplo: 19.1 Clase de transacción: un usuario específico puede quedar limitado a ciertos tipos de transacciones. 19.2 Programas: los usuarios pueden estar restringidos al empleo de ciertos programas de proceso. 19.3 Grupos de archivos: se les puede permitir a los usuarios el acceso, la modificación, y el borrado únicamente de archivos específicos. 19.4 Archivos completos: puede ser dado el acceso a un conjunto completo de archivos. 19.5 Registros individuales: el acceso puede estar limitado a registros específicos. 19.6 Grupos de registros: a usuarios específicos se les puede permitir o restringir el uso de determinados grupos de registro. 19.7 Diversos controles de contraseña: los usuarios pueden quedar limitados al uso de solo ciertas porciones de la Base de Datos. 19.8 Diversos controles de terminales: varias terminales pueden quedar sujetas a un código de transacciones para restringir su acceso a ciertas porciones de la base de datos. 19.9 Controles del circuito: ciertos circuitos en la red de comunicación de datos pueden quedar limitados a ciertas porciones de la base de datos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT9: SEGURIDAD LÓGICA. 1. Verificar que el software de comunicaciones exige código de usuario y contraseña para su acceso. 2. Verificar si los usuarios no pueden acceder a ningún sistema, sin antes haberse autenticado correctamente en la red institucional. 3. Verificar si se inhabilita al usuario después de ingresar la contraseña después un número determinado de intentos fallidos. 4. Verificar que el sistema operativo obliga a cambiar la contraseña periódicamente. 5. Verificar que la contraseña no sea menor a 8 caracteres y que sea una combinación de números y letras, entre ellos mayúsculas y minúsculas. 6. Verificar que las contraseñas no son mostradas en pantalla cuando se ingresan. 7. Verificar si durante el procedimiento de identificación, los usuarios son informados de cuándo fue su última conexión para ayudar a identificar potenciales suplantaciones o accesos no autorizados. 8. Verificar que existe software para llevar estadísticas que incluyan tasas de errores y de retransmisión. 9. Verificar que los equipos puedan validar la identificación electrónica de las terminales que se agregan a la red.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT10: COMERCIO ELÉCTRONICO 1. Verificar que la organización disponga de documentación relacionada al e_commerce, tales como : 1.1 Planificación del proyecto al menos contendrá: objetivos y alcances, estudio de viabilidad, costo beneficio y plataforma tecnológica. 1.2 Copia de contratos de lo proveedores de servicio. 1.3 Copias de contratos del mantenimiento de equipo. 1.4 Descripción y esquema de la plataforma tecnológica. 1.5 Política de configuración. 1.6 Esquemas de red 1.7 Esquema de seguridad lógica. 1.8 Diagramas de entidad relación. 1.9 Diccionario de datos. 1.10 Inventario de aplicativos puestos en producción 1.11 Manual de Usuario de los aplicativos puestos en producción. 1.12 Pruebas de vulnerabilidad. 1.13 Estrategias del negocio y la necesidad de operaciones electrónicas. **2. Controles** 2.1 Verificar el volumen de información y los servicios utilizados 2.2 Verificar quienes tienen acceso a los diagramas de configuración del sistema. 2.3 Verificar los distintos reportes emitidos por el sistema. 2.4 Verificar el reporte de caídas del sistema, medir la frecuencia y magnitud de las mismas. 2.5 Verificar en las transacciones de pago las medidas de seguridad implementadas y que estas incluyan autenticación de usuarios, consistencia de datos y confidencialidad de las operaciones 2.6 Verificar quienes son los responsables de la seguridad de las operaciones electrónicas. 2.7 Hacer pruebas en el sitio para conocer de los productos y los servicios ofrecidos. 2.8 Verificar los mecanismos de privacidad asociado a la creación de contraseñas y usuarios del sistema.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
2.9 Verificar si el proceso para la administración de contraseñas de los sistemas de e_commerce, consideran aspectos como caracteres permitidos, cantidad mínima de caracteres, fechas de expiración, número de fallos permitidos y acción frente a las fallas, procesos para cambio de contraseñas entre otros. 2.10 Verificar si existe cumplimiento de los servicios ofrecidos en la parte legal y contractual, ofertada y publicada. 2.11 Verificar si la Organización tiene un proceso adecuado parar el control de las transacciones. 2.12 Verificar si existe un sistema de encripción adecuado para las operaciones realizadas en el sistema. 2.13 Verificar si existen mecanismos adecuados para proteger la reserva de los datos personales de sus clientes que utilizan el servicio. 2.14 Verificar si las firmas digitales son emitidas, manejadas y/o certificadas por un proveedor externo. 2.15 Verificar si existe control en las versiones y procedimientos de distribución de software, para las aplicaciones relacionadas con e_commerce 2.16 Verificar las técnicas utilizadas por la Organización para monitorear la seguridad de los sistemas de e_commerce. 2.17 Verificar si la Organización cuenta con un software para análisis de seguridad, si es utilizado y cual es su alcance. 2.18 Verificar si la administración requiere el uso de firmas digitales para autenticar a los usuarios en relación a las transacciones. 2.19 Verificar si disponen de herramientas para monitorear y detectar intromisiones a la red. 2.20 Verificar si la opinión de los usuarios que usan los servicios son consideradas en las proyecciones de crecimiento y la planeación de los recursos de la e_commerce. **3. Normativas** 3.1 Verificar si las políticas de seguridad incluyen adecuadamente el tema de encripción y los mecanismos que utilizan.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
3.2 Verificar si las políticas incluyen el uso de software para la detección de virus, y los mecanismos usados para la actualización.	
3.3 Verificar si las políticas de los cortafuegos (Firewalls) definen responsabilidad por su mantenimiento, dominios de acceso y reglas que permitan tráfico permitido y prohibido.	
3.4 Verificar si las políticas de seguridad incluyen lineamientos de control de acceso a la red y a los datos.	
3.5 Verificar la existencia de un proceso para evaluar periódicamente la composición de productos de e_commerce y las necesidades del mercado tecnológico.	
3.6 Verificar si el e_commerce es consistente con la misión del Organización y los planes estratégicos.	
4. Corta fuego (Firewall)	
4.1 Verificar si la Organización dispone de un proceso adecuado para identificar cualquier acceso remoto, diferente que el Firewall, y como la administración monitorea y controla ese acceso.	
4.2 Verificar la adecuación del proceso para restringir acceso a la documentación de la configuración del Firewall.	
4.3 Verificar el procedimiento utilizado por los responsables de la administración de los Firewall para prevenir el acceso no autorizado a la red interna.	
4.4 Verificar los procesos que la Organización utiliza para controlar el acceso no autorizado a la sala de los Firewall.	
4.5 Verificar los procedimientos usados para la certificación las pruebas y actualización políticas en los cortafuegos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
Prevención de virus. 5.1 Verificar el cumplimiento realizado por los usuarios para prevenir los virus informáticos. 5.2 Verificar si la Organización tiene un proceso adecuado para detectar y prevenir virus asociados a los sistemas de e_commerce. 5.3 Verificar si existe un proceso adecuado para actualizar el anti virus, y si la revisión de virus en la máquina se realiza periódicamente	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT11: CRIPTOGRAFIA Y BIOMETRIA **Criptografía** 1. Verificar los elementos protegidos bajo ambiente criptográfico. 2. Verificar que herramientas utilizan para proteger la información 3. Verificar si el cifrado es simétrico, es decir utilizar la misma clave para cifrar y descifrar un documento. 4. Verificar si el cifrado es asimétrico, es decir que es aquella en que el sistema de cifrado usa dos claves diferentes, una es la clave pública y que se puede enviar a cualquier persona y otra que se llama clave privada. 5. Verificar si el cifrado es híbrido, en donde el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. 6. Verificar si el cifrado se realiza bajo ambiente PGP (pretty good privacy), al menos debe disponer de: firma digital, encriptación del mensaje, comprensión y segmentación. 7. Verificar que para el cifrado existan dentro del servicio de red los Protocolos de comunicación tales como: TLS, SSL, SET, OpenPGP, DSS, SSH. 8. Verificar que tipo de algoritmo utilizan para el cifrado de datos, por ejemplo: AES, BLOWFISH, CAST-128. CAST-256, DES-X, ROT-13, RSA, Triple DES, Twofish, skipjack, etc. 9. Verificar la existencia de otros algoritmos tales como Sustitución Mono alfabética ó Poli alfabética , transposición, etc.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar de que procedimientos o herramientas disponen para la autentificación: 10.1 Mediante una firma (Firma Digital): la cual debe garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. 10.2 Mediante una contraseña: la cual debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta y correcta. 10.3 Mediante un dispositivo: se debe garantizar la presencia de un dispositivo válido en el sistema, por ejemplo una llave electrónica 11. Verificar si el certificado digital dispone de los siguientes elementos: 11.1 Nombre distintivo de la entidad, incluye la información de identificación (el nombre distintivo) y la llave pública. 11.2 Nombre distintivo de la Autoridad Certificadora. Identificación y firma de la Autoridad Certificadora (CA) que firmó el certificado. 11.3 Período de validez, tiempo durante el cual el certificado es válido. 11.4 Información adicional, puede contener información administrativa de la Autoridad Certificadora (CA) como un número de serie o versión 12. Verificar qué autoridad certificadora es la que ha sido contratada para el servicio, por ejemplo: VeriSign, Thawte Certificación, Xcert Sentir CA, Emtrust, Cybertrust, etc. **Biometría**. 1. Verificar si disponen de políticas para el uso de biometría. 2. Verificar quienes son los responsable de la administración del sistema biométrico. 3. Verificar que método es usado en la organización, por ejemplo: ojo-iris, ojo-retina, huellas dactilares, geometría de la mano, escritura, firma, voz.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
4. Verificar el hardware y software para el servicio y uso de biometría. 5. Verificar el procedimiento para crear un usuario o eliminarlo del sistema según el método biométrico usado. 6. Verificar el contrato con el proveedor e identificar fortalezas y debilidades 7. Verificar la plataforma tecnológica usada e identificar capacidades de almacenamiento y futura expansión.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
PT12: SEGURIDAD INFORMÁTICA 1. Verificar que existan políticas de seguridad, definidas y aprobadas por la Administración. 2. Verificar que las políticas de seguridad contengan, elementos como: confidencialidad, integridad y disponibilidad. 3. Verificar que las políticas contengan mecanismos para medir: riesgos y amenazas, análisis de riesgos, plan de seguridad, controles preventivos y correctivos, plan de contingencia, biometría, firma digitales, protección y defensas. 4. Identificar qué mecanismos utilizan para no revelar la información a personas no autorizadas, acceso a información confidencial y protección de datos. 5. Verificar como controlan las amenazas externas, como hackers o espías. 6. Verificar la existencia de procedimientos para controlar riesgos como por ejemplo: ausencia de planes de contingencia, ausencia de políticas de seguridad y estrategias, ausencia de procedimientos para modificación de aplicaciones, programadores con acceso irrestricto a los datos, seguridad débil en accesos a Internet, e-mail, Inadecuada segregación de funciones, falta de procedimientos de contingencia, débiles políticas para la creación de contraseñas, ausencia de bitácoras de seguridad y falta de oficiales de seguridad. 7. Verificar la existencia de procedimientos para controlar las amenazas, por ejemplo: Sniffing, Frame Spoofing, Crack, Hacking a un Website, Ingeniería Social, Caballos de Troya, Ataques de Denegación de servicios, Fake Mail.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
8. Verificar si están definidas las funciones de los cargos siguientes: el DBA (Data base administrator - administrador de base de datos), el NA (Administrador de red - Network administrator) y el SA (Administrador de sistema - System administrator). Dicha verificación es con la finalidad de no entrar en conflicto de funciones. 9. Verificar que tipo de sistemas de detección de intrusos (IDS) utilizan según las características siguientes: 9.1 HIDS (*HostIDS*): un IDS vigilando un único ordenador y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesado es mucho menor. 9.2 NIDS (*NetworkIDS*): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red. 9.3 *DIDS (DistributedIDS*): sistema basado en la arquitectura cliente servidor compuesto por una serie de NIDS (IDS de redes) que actúan como censores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN) 10. Verificar como administran los perfiles de los responsables de la seguridad, ó al menos que cumplan con las actividades siguientes: SecAdmin: Administrador de seguridad. Administra altas, bajas, y cambios de perfiles de usuarios. Otorga permisos de acceso a los recursos y puede auditar a los usuarios. System Administrator: Instalación de software de base, administración de recursos (capacidad, performance, etc.). Sin acceso irrestricto a los datos. Con utilización controlada de utilitarios sensitivos. Network Administrator: Atiende y monitorea la red. Instala y configura los componentes de software y hardware. Resuelve problemas de ambiente y conexiones.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:	
INSTITUCIÓN:	FECHA FIN:	
AUDITOR:	FIRMA:	
Áreas / Actividades		**Referencia**

DBA: Administra la base de datos. Genera las estructuras, los índices, el diccionario de datos, administra los espacios, etc.

Desarrollador: Puede modificar programas, compilar en librerías de test, y probar con datos de prueba. EL desarrollador puede tener línea de comandos restringidos.

Implementador: Debe pasar los programas de desarrollo a producción mediante un mecanismo que asegure la transparencia. Puede intervenir operaciones. El implementador puede tener línea de comandos restringidos.

Operador del sistema: Puede operar el sistema, encenderlo, apagarlo, descolgar usuarios por terminales, etc. El operador no debe tener línea de comandos.

Usuarios finales: Solo deben acceder a las aplicaciones mínimas que necesitan para desarrollar su tarea diaria.

11. Verificar que la seguridad informática y de datos, se aborda un proceso de seguridad recomendado a utilizar según las siguientes herramientas: un Firewall o combinación de ellos, Proxy es un sistema de detección de intrusos o IDS. sistemas de actualización automática de software, sistemas de control de la integridad de los servidores, paquetes, etc.

12. Verificar como se administra la información según los lineamientos establecidos en la Política de Seguridad de Información, aprobada por la Alta Dirección.

13. Verificar como establecen y mantienen los procedimientos que aseguren la integridad, confidencialidad, exactitud y disponibilidad de la información de la empresa, en niveles concordantes con la importancia que se merece.

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
14. Verificar los riesgos a que pueda estar expuesta la información, ya sea durante su almacenamiento, manipulación o comunicación, y recomendar los controles más adecuados según criterios de costo/beneficio, para eliminarlos o reducir sus efectos. 15. Verificar como monitorean y rastrean la actividad de los usuarios administrativos y operativos a fin de detectar y corregir desviaciones en el uso correcto de la información, o en el cumplimiento de las normas y procedimientos asociados a la seguridad de la información. 16. Verificar que controles lógicos y físicos se utilizan para asegurar que sólo el personal autorizado pueda acceder a la información, dentro de los niveles de atención. 17. Verificar que procedimientos operativos y programas computarizados idóneos, probados y autorizados, se pueda acceder, modificar, divulgar, destruir o mantener la Información. 18. Verificar el cumplimiento de las políticas de desarrollo de documentación mínima de los procedimientos operativos y aplicaciones, que permitan las operaciones de la empresa bajo una situación de contingencia. 19. Evaluar y seleccionar, en coordinación con la unidad de Sistemas tecnológicos, herramientas para apoyar las funciones de la unidad Seguridad de Informática. 20. Verificar el impacto que los cambios en la tecnología puedan ocasionar a la seguridad, y si estos cambios la afectaran, dirigir la transición hacia un nuevo entorno de garantía. 21. Verificar los procedimientos usados para evaluar las políticas en la destrucción de la información, especificando los medios a utilizar, procedimientos a aplicar, y la oportunidad en que se ejecutará.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SOPORTE (SO) **SO1: MANTENIMIENTO DE HARDWARE.** 1. Verificar que existan contratos de mantenimiento preventivo y correctivo para el equipo informático de la institución. 2. Verificar si el mantenimiento otorgado por el proveedor es conforme a lo establecido en el contrato. 3. Verificar la programación del mantenimiento preventivo y correctivo, con la finalidad de reducir la frecuencia y el impacto de fallas de rendimiento. 4. Verificar cuál es el proceso de notificación de las fallas del equipo informático y como se documenta dicho proceso. 5. Verificar si el mantenimiento cubre la totalidad del equipo de cómputo o si es algún equipo especifico. 6. Verificar el tiempo de respuesta de reparación o sustitución de partes por medio del proveedor de servicio. 7. Verificar si el proveedor tiene la capacidad de ofrecer la sustitución temporal del equipo principal como servidores en caso de retiro por reparación u otro tipo de mantenimiento. 8. Verificar si existen informes sobre el mantenimiento a nivel físico y de parámetros efectuados por el proveedor a los servidores principales de la institución.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SO2: CONTROLES DE REDES Y COMUNICACIONES. 1. Verificar que la Unidad de comunicaciones este integrada por el personal definido en el organigrama. 2. Verificar la existencia de un Inventario de direcciones IP asignada a los usuarios, con la información general asociada a cada IP. 3. Verificar la existencia de un inventario actualizado de equipo de comunicaciones: Módems, Hubs, Terminales, Routers, Firewalls, etc. 4. Verificar el inventario del software instalado en la red, por ejemplo: sistema operativo, lenguajes, programas, paqueterías, utilerías y demás software institucional. 5. Verificar el diagrama de red para identificar las interconexiones internas y externas. 6. Verificar si las claves para el uso de los equipos se resguardan en sobre sellado o lacrado para alguna eventualidad fortuita. 7. Verificar la existencia de servicios de Intranet, Extranet e Internet. 8. Verificar el tipo de Protocolo utilizado, por ejemplo: SNA, Netbios, IPX, TCP/IP 9. Verificar la existencia de procedimientos de autorización para conectar nuevo equipo en la red. 10. Verificar el procedimiento para el uso de cualquier conexión digital con el exterior, como línea conmutada o dedicada. 11. Verificar si el plan de contingencia considera el respaldo y recuperación de los sistemas de comunicaciones.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
12. Verificar si existe control y monitoreo de las conexiones a fin de deshabilitar aquellas que no estén en uso. 13. Verificar la existencia de software de monitoreo de las conexiones remotas, de forma que se documenten los incidentes o interrupción del servicio comunicación. 14. Verificar la existencia de una política que controle el uso del equipo de redes en producción y los equipos de prueba. 15. Verificar los tipos de prueba usadas para validar la operación del equipo de redes y comunicaciones. 16. Verificar si disponen de reportes de incidentes, contingencias y circunstancia que afecten el funcionamiento de la red, conforme a la bitácora. 17. Verificar como controlan el tamaño de los paquetes y flujo de la velocidad en la red. 18. Verificar cuales son los tipos de componente de obstáculos que dispone el Firewall, por ejemplo: Ruteador Filtra-paquetes, Gateway a nivel de Aplicación, Gateway a nivel de circuito. 19. Verificar como esta definida la política del perímetro de los Firewalls para el uso de Internet. 20. Verificar si están consideradas la bases para el diseño decisivo del Firewall en uso de Internet, asignadas por el administrador de red: Posturas sobre la política de Firewall, política interna propia de la organización, costo financiero y secciones de configuración 21. Verificar si han considerado por el responsable de seguridad en redes algunas características de diseño que son usadas para hacer mas seguro un servidor de defensa, al respecto se citan:	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades		Referencia
21.1	Verificar que la plataforma de Hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo, diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del Firewall.	
21.2	Verificar que únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.	
21.3	Verificar si la Autenticación adicional para que el usuario accese a los servicios Proxy, por medio del servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización. Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión	
21.4	Verificar que cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.	
21.5	Verificar que cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida	
21.6	Verificar que cada Proxy mantiene la información detallada y auditada de todos los registros del tráfico, cada conexión, y la duración de cada conexión. El registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso.	
21.7	Verificar que cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:	
INSTITUCIÓN:	FECHA FIN:	
AUDITOR:	FIRMA:	
Áreas / Actividades		**Referencia**
21.8 Verificar que cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si ocurriera un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aun, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa		
21.9 Verificar si el Proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial, desde que la Aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.		
21.10 Verificar que cada Proxy corre como un usuario no- privilegiado en un directorio privado y seguro del servidor de defensa		
22. Verificar la disponibilidad de licencias y permisos de instalación.		
23. Verificar que los equipos de comunicación dispongan de claves de acceso, así como la activación de lóg. o bitácoras de auditoría sobre los accesos realizados.		
24. Verificar si han considerado en análisis y diseño el modelo de comunicación OSI de la red, en cuento a las uso de las capas: físicas, enlace, red, transporte, sesión, presentación y aplicación.		
25. Verificar como se evalúa la confiabilidad en el funcionamiento de los medios de transmisión y del medio físico que utiliza para las comunicaciones.		
26. Verificar que técnicas de transmisión se usan para la comunicación de la red, tales como: síncrona, asíncrona, analógica, digital, serie o paralelo.		

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
27. Verificar el funcionamiento y la confiabilidad de los dispositivos para conectar las redes, tales como: Repetidores, Puentes, Enrutadores y Puertas de enlace. 28. Verificar que mecanismos de funcionamiento usan en las técnicas de transferencias: Simples, Semidúplex, Dúplex total. 29. Verificar que tipo de topologías utilizadas para el diseño y uso de la red, por ejemplo: Bus, Estrella, Anillo, Malla, Doble anillo. 30. Verificar el medio usado para la conexión de los dispositivos a los servidores principales. 31. Verificar el uso de los servidores dedicados, de soporte, no dedicados, de impresión y de comunicación. 32. Verificar el número y características de las estaciones de trabajo así como los tipos de nodo en la red. 33. Verificar el tipo de cable utilizado en la red, tales como: trenzado, coaxial, de base para un canal, banda ancha o fibra óptica. 34. Verificar que elementos tienen definidos para la expansión de la red, considerar: Repetidores (para recibir y trasmitir datos), puentes (capa de enlace OSI para el manejo de datos origen y destino), Enrutadores (relacionado a los Protocolos de comunicación), puertas de enlace (dispositivos para la conexión de computadores y mainframe).	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SO3: CONTROL DE ALMACENAMIENTO. 1. Verificar si la cintoteca se encuentra ubicada en el mismo edificio o en otro. 2. Verificar si los locales asignados a la cintoteca disponen de: Aire acondicionado, protección contra el fuego, cerradura de puerta especial (tarjeta electrónica, acceso biométrico, cerradura eléctrica, etc.) 3. Verificar e identificar las características del hardware usado para la creación de las copias. 4. Verificar e identificar el software usado para la creación de las copias de respaldo. 5. Verificar si la institución dispone de algún software para el control de cintas utilizadas. 6. Verificar que el inventario de la cintoteca contiene información mínima como: Número de serie, número o clave del usuario, número del archivo lógico, nombre del sistema que lo genera, fecha de expedición del archivo, número de volumen, etc. 7. Verificar con qué frecuencia se validan los inventarios de los archivos magnéticos. 8. Verificar que procedimientos utilizan para copiar: documentos, datos, programas, reportes, etc. y si éstos están documentados. 9. Verificar si en el proceso de copiado de la información utilizan procesos de encriptamiento y autenticación. 10. Verificar la periodicidad con la que realizan pruebas de restauración de los medios magnéticos con la finalidad de asegurar la recuperación.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
11. Verificar si disponen de procedimientos que permitan la reconstrucción de un archivo el cual fue inadvertidamente destruido. 12. Verificar si identifican en la viñeta del medio magnético la información de carácter confidencial. 13. Verificar si existe un control estricto de las copias de archivos de carácter confidencial. 14. Verificar si borran los archivos de los dispositivos de almacenamiento, cuando se desechan, por inservibles. 15. Verificar si existe certificación de la destrucción de dispositivos magnéticos. 16. Verificar que medidas de control utilizan en caso de extravío de algún dispositivo de almacenamiento. 17. Verificar si existe restricción de acceso al lugar donde se mantiene la custodia de los medios magnéticos. 18. Verificar el control para registrar los medios magnéticos que se prestan y la fecha en que serán devueltos. 19. Verificar el procedimiento utilizado para el reemplazo o actualización de medios magnéticos.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SO4: SEGURIDAD FÍSICA. 1. Verificar el cumplimiento de lo establecido en las normas de seguridad de acceso al centro de cómputo implementadas por TI. 2. Verificar que exista formulario de registro para el ingreso al centro de cómputo, para el personal externo al área. 3. Verificar que exista un sistema automático de extinción de fuego en el centro cómputo. 4. Verificar si los rociadores de agua, son del tipo de pre-acción cuya agua es suministrada con una cisterna, y que se activan a la primera alarma de incendio y se liberan por el mismo fuego, excepto la sala de cómputo. 5. Verificar la existencia de detectores de fuego y humo tanto en el área del techo y piso falso. 6. Verificar si en caso de una falsa alarma es posible de forma manual cortar la liberación automática de productos químicos extintores del fuego. 7. Verificar si estratégicamente existen extinguidores portátiles cerca del centro de cómputo, al nivel del suelo y marcados con una franja roja del suelo al techo. 8. Verificar que el sistema de alarma contra incendio automático tiene la capacidad de transmitir señales a un punto remoto que sea supervisado las 24 horas. El punto remoto puede ser una estación de guardia de la organización o la estación de bomberos local. 9. Verificar si los extintores instalados para fuego son de tipo automático ó manual.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar si el personal se encuentra capacitado para el uso y manejo de extintores.	
11. Verificar si existe supervisión sobre la periodicidad de las cargas de los extintores conforme a lo recomendado por el proveedor.	
12. Verificar si existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal pueda según el caso: cortar la acción, cortar la energía eléctrica, desalojar el edificio, etc.	
13. Verificar que el papel y otros suministros combustibles se almacene fuera del centro de cómputo, a excepción de aquellos que se van a utilizar inmediatamente.	
14. Verificar si existe un programa de capacitación para el personal, contra incendio y para la evacuación ordenada, en caso que se active la alarma de fuego.	
15. Verificar si se prohíbe fumar, comer y beber dentro del centro de cómputo.	
16. Verificar si existe vigilancia en el área de TI las 24 horas.	
17. Verificar si ha instruido al personal de seguridad sobre las medidas a tomar en caso de que alguien pretenda entrar sin autorización, al área de TI.	
18. Verificar si las visitas y demostraciones en el centro de cómputo, son controladas.	
19. Verificar si se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas.	
20. Verificar si existe vigilancia de la moral y comportamiento del personal de TI con el fin de mantener una buena imagen y evitar un posible fraude.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SO5: INFRAESTRUCTURA 1. Verificar si la administración dispone de planos del edificio, con la finalidad de visualizar su distribución para identificar riesgos para el equipo informático. 2. Verificar que la construcción del edificio, incluyendo las paredes, techo y pisos, son de materiales no inflamable, como medida de reducir la posibilidad de incendio. 3. Verificar que las paredes se extiendan desde la estructura del piso a la del techo del edificio y no desde pisos elevados a techos falsos. 4. Verificar que la sala de cómputo se encuentre separada físicamente de otros departamentos de la organización. 5. Verificar si el edificio del centro de cómputo se encuentre en un nivel adecuado con la finalidad de minimizar el riesgo de un acceso externo o daño por inundación. 6. Verificar la existencia de una bóveda o caja fuente con puerta de seguridad de cierre automático con resistencia al agua y fuego, para el resguardo de medios magnéticos. 7. Verificar que la construcción del techo está a prueba de agua de forma que no fluya a los pisos inferiores. 8. Verificar que el drenaje sea adecuado en pisos elevados y estos posean desnivel. 9. Verificar que las puertas de entrada y salida del área de TI dispongan de un mecanismo que permita abrirlas en caso de emergencia.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
10. Verificar que las cortinas, muebles, piso y techo falso son de materiales no combustibles. 11. Verificar cada cuanto tiempo se realiza limpieza bajo el piso falso. 12. Verificar la existencia de mecanismos de cierre manual o automático de los ductos de aire acondicionado y ductos de aire fresco para el centro de cómputo. Esto cortará el flujo de aire en el área de proceso en caso de incendio de manera que no se alimenten las llamas. 13. Verificar la existencia de un sistema de potencia ininterrumpirle de energía y/o un generador diesel. Debido a que estos sistemas pueden ofrecer una protección temporal que permita la continuidad del servicio en caso falla de la energía eléctrica, o bien pueden ofrecer un respaldo eléctrico a largo plazo. 14. Verificar la existencia de protección contra variaciones de voltaje a toda la potencia eléctrica que se suministra a la unidad central de proceso y al equipo de comunicación. 15. Verificar si existe protección de todos los circuitos de la computadora contra actos de vandalismo que se puede dar cuando alguien abre los tableros de los circuitos y corta la energía. Esto implica el proveer tableros con cerraduras para los controles del circuito y el situarlos en habitaciones cerradas. 16. Verificar que el panel de la distribución del sistema eléctrico esté en un área segura e inaccesible a personas no autorizadas. 17. Verificar que los tableros del circuito se encuentren marcados de manera que al brindar mantenimiento, permitan una referencia rápida y expedita. 18. Verificar la existencia de lámparas de emergencia en el centro de cómputo.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
19. Verificar que abajo del piso se encuentran las líneas eléctricas por la seguridad del personal. 20. Verificar el medio ambiente que la temperatura y humedad del centro de cómputo esté en rango de 18℃ a 22℃ 21. Verificar si el centro de cómputo dispone de aire acondicionado independiente del edificio central.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SUBCONTRATACIÓN (SC) **SC1: EVALUACIÓN DE CONTRATOS DE SERVICIOS** 1. Solicitar una copia de los contratos de servicios proporcionados por terceros. 2. Identificar y analizar las condiciones pactadas en cada cláusula de los contratos de prestación de servicios de TI. 3. Identificar si existe cláusula de acuerdos de seguridad sobre reserva y confidencialidad de la información proporcionada por la institución y lo que resulte como producto del contrato. 4. Verificar la fecha del contrato, vigencia del contrato, y que sea firmado por la Alta Administración de la institución. 5. Condiciones mínimas a considerar dentro del contrato: 5.1 Título o nombre del contrato 5.2 Objeto del contrato de servicio 5.3 Medidas de desempeño 5.4 Presentación de informes de trabajos realizados 5.5 Resolución de diferencias y jurisdicción. 5.6 Incumplimiento y rescisión 5.7 Propiedad y Acceso 5.8 Planificación en caso de contingencia 5.9 Derechos de auditoría 5.10 Subcontratación o dependencia de otros 5.11 Confidencialidad/seguridad/separación de propiedades 5.12 Monto de los servicios, objeto del contrato, forma de pago y tipo de moneda 5.13 Seguros / Garantías 5.14 Ubicación física de la documentación. 5.15 Revisiones periódicas a los acuerdos	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
6. Identificar las razones que llevaron a la suscripción del servicio: 6.1 Descentralizar operaciones 6.2 Liberar recursos para otros proyectos 6.3 Hardware o software obsoleto ó no actualizado. 6.4 Falta de Personal capacitado para efectuar funciones o procesos 6.5 Reducción de costos 6.6 Ampliación de operaciones. 6.7 Para ofrecer nuevos servicios a los clientes 6.8 Procesamiento general de redundancias y contingencias 6.9 Compromisos estratégicos 6.10 Cumplimiento legal o normativo 6.11 Cumplimiento de plazos críticos 6.12 Fusiones, adquisiciones e integración de servicios. 6.13 Minimizar riesgos 7. Verificar que la gerencia de TI haya establecido un proceso de monitoreo continuo sobre la prestación de servicios contratados, con el fin de asegurar el cumplimiento de las cláusulas del contrato. 8. Verificar que el contrato haga referencia a los anexos de especificaciones técnicas y plan de ejecución entre otros.	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SC2: EVALUACIÓN DEL PROVEEDOR. 1. Identificar si el proveedor es nacional o internacional, con el objetivo de obtener información sobre: tipo de representación, ubicación física, personal de enlace, teléfonos, etc. 2. Verificar si entre los criterios para elegir al proveedor del servicio se considera: 2.1 Experiencia en procesos/servicio. 2.2 Tamaño y situación financiera. 2.3 Confiabilidad e historial. 2.4 Conocimiento del mercado. 2.5 Soporte técnico. 2.6 Cultura corporativa 2.7 Referencias institucionales. 2.8 Cumplimiento de leyes y normas. 2.9 Costos / competencia 2.10 Tiempos de respuesta ante eventos programados e imprevistos 2.11 Soporte post- implementación. 2.12 Garantía sobre productos y servicios	

PROGRAMA DE AUDITORÍA DE SISTEMAS	FECHA INICIO:
INSTITUCIÓN:	FECHA FIN:
AUDITOR:	FIRMA:

Áreas / Actividades	Referencia
SC3: EXAMEN DE LOS SERVICIOS SUBCONTRATADOS. 1. Verificar que exista una persona responsable en el área de TI, que controla la calidad de los productos y/o servicios prestados por el proveedor. 2. Verificar si todas las relaciones del servicio con el proveedor están garantizadas con un contrato formal. 3. Verificar si el proveedor ha subcontratado parcial o total los servicios que proporciona la institución y qué controles tiene sobre estos. 4. Identificar el riesgo de dependencia de la institución hacia el proveedor de servicios y el impacto de éste en las operaciones diarias. 5. Identificar si existe un análisis de los principales riesgos en la subcontratación: 5.1 Documentación técnica. 5.2 Procesamiento de transacciones y operaciones 5.3 Energía eléctrica, comunicaciones y redes 5.4 Servicio al cliente 5.5 Planes para la continuidad/reanudación de las operaciones 5.6 Apoyo a sistemas y operaciones (consultas- soporte) 5.7 Planificación, ejecución y administración de proyectos 5.8 Seguridad informática y privacidad de la información de la empresa y de los clientes que implica riesgos legales, normativos y de reputación en las jurisdicciones del cliente-anfitrión. 5.9 Eventos externos (desastres naturales/disturbios, etc.) que restringen la movilidad del personal y el acceso a las instalaciones de procesamiento	

CONCLUSIONES

1. El manual tiene la flexibilidad de ser mejorado con la experiencia y conocimientos técnicos del auditor de sistemas, para adecuarlo a las necesidades de la Organización, según el giro y magnitud de la empresa en la cual se implementará.

2. La aplicación y adaptación total o parcial de los programas de auditoría según las áreas descritas en MASTI, están sujetas a la responsabilidad y la objetividad que defina los lineamientos de la Administración.

3. La globalización y los avances tecnológicos que suceden cada día, obligan a las Organizaciones a estar sujetas al cambio y no pueden dejar a un lado los riesgos que esta conlleva; Identificar, Reconocer, Cuantificar y Monitorear la existencia de ellos, con la finalidad de minimizar su impacto.

4. La Administración superior de cualquier Organización debe de considerar que si la mayoría de operaciones y servicios descansan en el computador, le obliga a incluir dentro de su presupuesto un rubro de inversión tecnológica.

5. Los objetivos que persigue la Auditoría de Sistemas consiste en salvaguardar los activos de información, mantener la integridad de los datos y alcanzar la efectividad, eficiencia y economía de los sistemas, estos principios estarán basados en el soporte que proporcionen las demás áreas de la Organización.

6. El alcance y ejecución de los programas de auditoría, deben estar definidos por las partes involucradas, con la finalidad de lograr en mejor forma los objetivos previstos.

7. La independencia del auditor de sistemas es fundamental, con respecto al desempeño de sus labores, debido a que es un factor de suma importancia para el desarrollo del examen y la aplicación de los programas de auditoría.

8. El esquema de trabajo que emplea el auditor de sistemas cambia de forma considerable, según la naturaleza de cada Empresa, las técnicas empleadas están sujetas al alcance que persiga la Administración.

RECOMENDACIONES.

1. El auditor de sistemas debe poseer un nivel académico o especialización en tecnología, asimismo la capacidad y experiencia son elementos importantes para el buen desarrollo de la auditoría de sistemas.

2. Las conclusiones evaluadas como producto final por parte del auditor de sistemas dentro de su informe, deberán contar con el conocimiento y respaldo del auditado para que puedan ser implementadas.

3. Al planificar una auditoría, el auditor de sistemas debe tener una comprensión suficiente del ambiente total que se revisa, debe incluir una idea general de las diversas prácticas comerciales y funciones relacionadas con el tema de la auditoría, así como los tipos de sistemas que se utilizan. El auditor de sistemas también debe comprender el ambiente normativo en el que opera el negocio.

4. El auditor de sistemas debe prestarle mucha atención a la documentación técnica de los sistemas puestos en producción, debido a que ello elimina hasta cierto punto la independencia del personal que lo administra.

5. Al aplicar los programas de auditoría descritos en MASTI, se debe de recolectar en las pruebas de evaluación, la evidencia que sustente las fortalezas y debilidades de los controles existentes, debido que ellos forman parte del informe y respaldan las observaciones señaladas por el auditor.

6. El documento propuesto se considera un material de soporte para profesionales afines en el área de auditoría de sistemas.

7. El auditor de sistemas puede apoyarse en las ISO-9000, de tal forma que le permita realizar la evaluación de los procedimientos con la finalidad de dictaminar y certificar la calidad de los mismos.

8. Para realizar auditorías al sector gubernamental, especialmente aplicando las Normas Técnicas de Control Interno emitidas por la Corte de Cuentas de la Republica, se recomienda usar los programas de auditoría de sistemas propuestos en la tesis nombrada “Manual de Auditoría de Sistemas para Instituciones Gubernamentales Autónomas”. No obstante, como elementos complementarios el auditor debe aplicar los programas de auditoría descritos en MASTI, para la evaluación del control interno del ambiente informático.

9. El auditor de sistemas puede valerse de herramientas que existen en el medio que le permitan realizar auditorías de forma automatizada con la data, así como software para controlar el trafico, calidad y confiabilidad de las redes de comunicaciones.

Anexo “A”

NOMBRE	DESCRIPCION
ALCANCE DE AUDITORIA	El término "alcance de una auditoría" se refiere a los procedimientos de auditoría considerados necesarios en las circunstancias para lograr el objetivo de la auditoría.
APLICACION	una pieza de software que ejecuta una determinada función. Por ejemplo, una aplicación de correo electrónico.
AUDITORIA INTERNA	Auditoría interna es una actividad de evaluación establecida dentro de una entidad como un servicio a la entidad. Sus funciones incluyen, entre otras cosas, examinar, evaluar y monitorear la adecuación y efectividad de los sistemas de control contables e internos.
AUTENTICACIÓN	Validación de la información de inicio de sesión de un usuario. Cuando un usuario inicia una sesión utilizando una cuenta en una computadora.
BASE DE DATOS	Es un conjunto integrado de datos junto con una serie de aplicaciones para su manejo accesibles simultáneamente por diferentes usuarios y programas.
BITÁCORA	Seguimiento de las actividades de los usuarios, mediante el registro de determinados tipos de sucesos en el registro de seguridad de un servidor o estación de trabajo.
CARTA COMPROMISO	Una carta compromiso documenta y confirma la aceptación del auditor del nombramiento, objetivo y alcance de la auditoría, el grado de las responsabilidades del auditor para el cliente y la forma de cualquier dictamen.
CERTEZA	Certeza o seguridad se refiere a la satisfacción del auditor respecto de la confiabilidad de una aseveración hecha por una de las partes para ser usada por otra de las partes.
CLIENTE	aplicación de software que permite a un usuario obtener un servidor localizado en la red.
CÓDIGO FUENTE	Programa en su forma original, tal y como fue escrito por el programador, el código fuente no es ejecutable directamente por el computador, debe convertirse en lenguaje de maquina mediante compiladores, ensambladores o interpretes.
CÓMPUTO	El cómputo consiste en revisar la exactitud aritmética de los documentos fuente y registros contables o de llevar a cabo cálculos independientes.
CONFIABILIDAD	Ser refiere a la provisión de información apropiada para la administración con el fin de operar la identidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
CONFIDENCIALIDAD	Se refiere a la protección de información sensible contra divulgación no autorizada.

CUMPLIMIENTO	Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios negocio impuestos externamente.
DATO	El termino que usamos para describir las señales con las cuales trabaja la computadora es dato; Aunque las palabras dato e información muchas veces son usada indistintamente, si existe una diferencia importante entre ellas. En un sentido estricto, los datos son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.
DICTAMEN	El dictamen del auditor contiene una clara expresión de opinión escrita sobre los estados financieros como un todo.
DISPONIBILIDAD	Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
DOCUMENTACIÓN	Documentación es el material (papeles de trabajo) preparado por y para, u obtenido o retenido por el auditor en conexión con el desempeño de la auditoría.
EFECTIVIDAD	Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
EFICIENCIA	Se refiere a la provisión de información a través de la utilización óptima (mas productiva y económica) de recursos.
ENRUTADOR	sistema que transfiere información entre dos redes que utilizan el mismo Protocolo pero pueden diferir en sus características físicas.
EVIDENCIA DE AUDITORIA	Evidencia de auditoría es la información obtenida por el auditor para llegar a las conclusiones sobre las que se basa la opinión de auditoría. La evidencia de auditoría comprenderá los documentos fuente y los registros de contabilidad subyacentes a los estados financieros y la información confirmatoria de otras fuentes.
EXPERTO	Un experto es una persona o firma que posee la habilidad, conocimiento y experiencia especiales en un campo particular distinto al de la contabilidad y auditoría.
FILE SERVER	servidor de archivos. Una computadora que almacena archivos en Internet, haciéndolos disponibles al acceso desde varias herramientas Internet.
FIREWALL	cortafuegos. Dispositivo de seguridad que ayuda a proteger una red privada de hackers o crackers de Internet. Es una máquina con dos interfases de red configurada para restringir que pueden ser usados y la dirección IP interna que puede ser mostrada al exterior de Internet.
GUIA	Lista de datos referentes a una materia.

HACKER	alguien que explora los sistemas computarizados generalmente en forma ilegal.
HARDWARE	Es la parte tangible del computador.
HOST	Anfitrión o computadora destinataria. Computadora que permite a los usuarios comunicarse con otras en la red.
INCUMPLIMIENTO	El término incumplimiento se usa para referirse a actos de omisión o comisión por parte de la entidad que está siendo auditada, ya sea en forma intencional o no intencional, y que son contrarios a las leyes y reglamentos vigentes.
INFORMACIÓN	Es lo que se obtiene del procesamiento de datos, es el resultado final.
INSTALACIONES	Recursos para alojar y dar soportes a los sistemas de información.
INTEGRIDAD	Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
LÓGICA	Es una secuencia de operaciones realizadas por el hardware o por el software.
MÓDEM	Modulador/DEModulador/o Modulador/DEModulador. Dispositivo que habitualmente interconecta una computadora con una línea telefónica para la transferencia de datos. Convierte señales binarias en señales analógicas.
MANUAL	Libro en que se recoge y resume lo fundamental de una asignatura o ciencia.
OBSERVACIÓN	La observación consiste en estar presente durante todo o parte de un proceso desempeñado por otros; por ejemplo, asistir a la toma de inventario físico capacitará al auditor para inspeccionar el inventario, para observar el cumplimiento de los procedimientos de la administración para contar cantidades y registrar dichos conteos, y para hacer conteos de comprobación.
OFF-LINE	No conectado a un sistema on-line.
ON-LINE	conexión directa entre dos computadoras a través de módems en tiempo real.
OUTSOURCING	Subcontratación.
PAPELES DE TRABAJO	Los papeles de trabajo pueden ser en forma de datos almacenados en papel, película, medios electrónicos u otros medios.
PERSONAL	Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.
POBLACIÓN	La población es todo el conjunto de datos sobre los cuales desea el auditor hacer el muestreo para alcanzar una conclusión.

PROCEDIMIENTOS / CONTROL	Procedimientos de control son aquellas políticas y procedimientos además del ambiente de control que la administración ha establecido para lograr los objetivos específicos de la entidad.
PROGRAMA (computador)	Es una colección de instrucciones que indican a la computadora que debe hacer. Un programa se denomina software, por lo tanto, programa, software e instrucción son sinónimos.
PROGRAMA DE AUDITORÌA	Un programa de auditoría expone la naturaleza, tiempos y grado de los procedimientos de auditoría planeados que se requieren para implementar el plan de auditoría global. El programa de auditoría sirve como un conjunto de instrucciones para los auxiliares involucrados en la auditoría y como un medio para controlar la ejecución apropiada del trabajo.
PROGRAMA FUENTE	Instrucción escrita por el programador en un lenguaje de programación para plantear al computador el proceso que debe ejecutar.
PROGRAMA OBJETO	Instrucciones en lenguaje maquina producida por el computador.
PROTOCOLO	instrucciones a partir de las cuales dos computadoras establecen su comunicación con la cual se transferirán datos. El Protocolo que utiliza Internet es TCP/IP.
REGISTRO	Es un grupo de campos relacionados que se usan para almacenar datos acerca de un tema (registro maestro) ó actividad (registro de transacción).
SEGURIDAD RAZONABLE	(seguridad razonable)- En un trabajo de auditoría, el auditor ofrece un alto, pero no absoluto, nivel de seguridad, expresado positivamente en el dictamen de auditoría como certeza razonable de que la información sujeta a auditoría está libre de declaraciones erróneas sustanciales.
SISTEMA CONTROL INTERNO	Un sistema de control interno consiste en todas las políticas y procedimientos (controles internos) adoptados por la administración de una entidad para auxiliar en el logro del objetivo de la administración de asegurar hasta donde sea practicable, la conducción ordenada y eficiente de su negocio, incluyendo adhesión a las políticas de la administración, la conservación de los activos, la prevención y detección de fraude y error, la exactitud e integridad de los registros contables, y la preparación oportuna de información financiera confiable. El sistema de control interno va más allá de estos asuntos que se relacionan directamente con las funciones del sistema contable.
SISTEMA DE INFORMACIÓN	Existe un entorno de Sistemas de Información por Computadora (SIC) cuando está involucrada una computadora de cualquier tipo o tamaño en el procesamiento por parte de la entidad de la información financiera de importancia para el auditor, ya sea que la computadora sea operada por la entidad o por terceras partes.

SOFTWARE	Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible de computador.
TECNOLOGÍA	La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
USUARIO	Cualquiera que requiere los servicios de los productos de un sistema de computación.

ANEXO "B"

RECURSOS FINANCIEROS

PRESUPUESTO PROYECTADO
(EN DOLARES AMERICANOS)

UNIDAD	***RECURSO***	***COSTO. UNITARIO***	***TOTAL***
RECURSOS HUMANOS			
1	*AUDITOR (640 horas a razón de $7.00/hora)*		*4,480.00*
1	*ASESOR*	*571.43*	*571.43*
	TOTAL RECURSOS HUMANOS		***$5,051.43***
RECURSOS TECNOLÓGICOS			
1	*DEPRECIACIÓN COMPUTADOR*	*250.00*	*250.00*
1	*DEPREC. IMPRESOR DE INYECCIÓN*	*40.00*	*40.00*
100	*HORAS INTERNET*	*1.25*	*125.00*
	OTROS – IMPREVISTOS (10%)	*41.50*	*41.50*
	TOTAL RECURSOS TECNOLÓGICOS		***$456.50***
RECURSOS MATERIALES			
8	*RESMAS DE PAPEL BOND T/CARTA*	*3.60*	*28.80*
4	*LAPICEROS*	*0.17*	*0.68*
2	*LAPICES*	*0.12*	*0.24*
4	*LIBRETAS DE APUNTES*	*1.00*	*4.00*
3	*CARTUCHOS DE TINTA*	*45.00*	*135.00*
1	*CAJA DE CD'S – RW*	*8.00*	*8.00*
1	*CAJA DE DISKETTES*	*4.00*	*4.00*
	COMBUSTIBLE	*125.00*	*125.00*
400hrs	*ENERGÍA ELÉCTRICA KW/Hr.*	*0.08515*	*34.06*
	OTROS – IMPREVISTOS (10%)	*35.57*	*35.57*
	TOTAL RECURSOS MATERIALES		***$391.29***
	TOTAL PRESUPUESTO		***$5,899.22***

Anexo "C"

Universidad Francisco Gavidia
Facultad de Ingeniería y Arquitectura

Fecha:_____ Tipo Empresa:_____ Código_____

Las presentes preguntas nos permiten conocer los problemas que atraviesan las organizaciones en el área de tecnología de información.

1. ¿Cuanto tiempo tiene de estar en el cargo?
2. ¿En su opinión como califica la comunicación interna dentro de la Organización?
3. ¿Cual es su opinión del servicio que prestan en área de tecnología de información hacia los usuarios?
4. ¿Cuales son los principales problemas que usted identifica?
5. ¿Cuales serían sus recomendaciones?

Anexo "D"

Universidad Francisco Gavidia
Facultad de Ingeniería y Arquitectura

Fecha:_____ Tipo Empresa:_____ Código_____

Sirva la presente para desearles éxitos en sus labores y aprovecho para solicitarle su colaboración al complementar la siguiente encuesta, la cual nos permitirá conocer la participación de auditoria de sistemas en la Tecnología de Información:

1. ¿Tienen evaluaciones de auditoria Externa (tecnología de información)?

   ☐ Si ☐ No Desconoce ☐

2. ¿Conoce los resultados y recomendaciones?

   ☐ Si ☐ No Desconoce ☐

3. ¿Existe Centro de Cómputo en la empresa?

   ☐ Si ☐ No

   Si la respuesta es NO muchas gracias, encuesta finalizada.

4. ¿Que nivel tiene el centro de cómputo dentro de la estructura organizacional?

   ☐ Gerencia ☐ Departamento ☐ Unidad ☐ Otro

5. ¿Cuántas personas forman el recurso humano informático?

   ☐ 1 – 3 ☐ 4 – 6 ☐ 7 – 10 ☐ 11 - 15 ☐ Más de 15

6. ¿En su opinión, en qué porcentaje hace uso de computadoras para desempeñar sus actividades laborales?

   ☐ 1 – 25% ☐ 26 -50% ☐ 51 – 75% ☐ 76 – 85% ☐ más de 85%

7. ¿Cuantos sistemas tiene la empresa en funcionamiento?

   ☐ 1 – 5 ☐ 6 – 10 ☐ 11 – 15 ☐ Más de 16 ☐

8. ¿Existe en la empresa personal interno que realice la Auditoria de Sistemas?

   ☐ Si ☐ No

   Si, la respuesta es NO pasar a la pregunta 14

Universidad Francisco Gavidia
Facultad de Ingeniería y Arquitectura

Fecha:_____ Tipo Empresa:_____ Código_____

9. ¿De quién depende jerárquicamente ó a quién reporta Auditoria de Sistemas?

☐ Junta Directiva ☐ Presidencia ☐ Informática ☐ Otros

10. ¿Se ha implementado en la empresa alguna metodología de Auditoria de Sistemas?

☐ Si ☐ No

11. ¿Poseen programas de auditorias de sistemas, para la evaluación de la tecnología?

☐ Completos ☐ Incompletos ☐ En proceso

12. ¿Qué opinión le merecen los programas actuales de auditoria?

☐ Buenos ☐ Regulares ☐ Malos ☐

13. ¿Como califica el contenido de estos programas de auditoria?

☐ No actualizados ☐ Alcance muy amplio ☐ Desordenados
☐ Alcance limitado ☐ No entendibles ☐ Ninguna opinión

14. ¿Disponen de software especializado para realizar auditoria de sistemas?

☐ Si ☐ No

Si la respuesta es NO, favor pase a la pregunta 16

15. ¿Qué opinión le merece el software de auditoria?

☐ Carece de Funciones especializadas ☐ Se necesita conocimientos estadísticos
☐ No es muy interactivo con el usuario ☐ Trabaja con extracciones de datos
☐ Es muy bueno

16. ¿Le Gustaría disponer de un manual de auditoria de sistemas que le permita evaluar la tecnología de información e identificar segmentos y objetivos definidos?

☐ Si ☐ No ☐ Sin Respuesta

MUCHAS GRACIAS POR SU COLABORACION.

Anexo "E"

Normas de Ética Profesional (ISACA)

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información.

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

NORMAS GENERALES PARA LOS SISTEMAS DE AUDITORÍA DE LA INFORMACIÓN

10 Título de auditoría

10.01 Responsabilidad, autoridad y rendimiento de cuentas.

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

20 Independencia

20.01 Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

20.02 Relación organizativa.

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

30 Ética y normas profesionales

30.01 Código de Ética Profesional

El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

30.02 Atención profesional correspondiente

En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

40 Idoneidad

40.01 Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

40.02 Educación profesional continua

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

50 Planificación

50.01 Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

60 Ejecución del trabajo de auditoría

60.01 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

60.02 Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

70 Informes

70.01 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de

auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

80 Actividades de seguimiento

80.01 Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Anexo “F”

****Auditoría de Sistemas ****

MEMORANDO No. 999/2007

Para :
De :
Fecha :
Asunto:

Por este medio hacemos de su conocimiento el avance de las observaciones identificadas, en la evaluación que estamos desarrollando, con datos de referencia al mes de diciembre/2006.

Las cuáles se detallan a continuación:

(*Describir las observaciones encontradas, en la medida de lo posible agregar ejemplos, así mismo poner plazo para que sean corregidas)*

Favor comunicar cuando las observaciones señaladas se encuentren corregidas, con la finalidad de que sean verificadas para dejarlas con el estado de superadas.

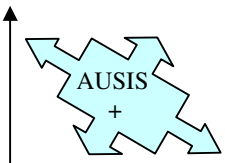
(cabe mencionar que este tipo de observaciones pueden transmitirse vía correo electrónico)

Atentamente,

*F:*_____.
Nombre y Firma

Auditoria de Sistemas

Anexo "G"



**Auditoría de Sistemas **

San Salvador, 15 de enero de 2007

Lic. (Nombre a quién se dirige)
Gerente General
Presente:

De acuerdo con las instrucciones giradas por la Gerencia General y Auditoría Interna de su empresa, me permito remitir a usted el informe de la auditoria de sistemas realizada al área de Tecnología, con especial énfasis en la evaluación de las Divisiones de: Planeación y Organización, Plataforma Tecnológica, Soporte y Subcontratación, misma que fue desarrollada en el período comprendido del 5 de noviembre al 30 de diciembre de 2006.

(Describir un párrafo sobre el alcance cubierto y relacionar el objetivo principal, así mismo describir antecedentes si existiera.)

Al respecto, le informamos que los hallazgos obtenidos se hicieron del conocimiento del Gerente de Tecnología.

(*enumerar las observaciones y separar por áreas*)

Describir las observaciones de mayor importancia a menor importancia seguidas de recomendación expuesta. La recomendación dependerá de cada auditor y lineamientos que tenga que cumplir)

De acuerdo con las pruebas ejecutadas, según los programas de auditoría, le solicitamos hacer las correcciones correspondientes y documentar cada observación con el fin de actualizar el estado actual de cada una de ellas; para lo cuál se les informamos que disponen de (número) días para subsanar lo señalado, debiendo comunicarnos de forma escrita las medidas correctivas a aplicar para su posterior verificación.

Atentamente,

F:_____.
Nombre y Firma

Auditoría de Sistemas

BIBLIOGRAFIA

INSTITUTO MEXICANO DE CONTADORES PÚBLICOS, A.C. "Normas Internacionales de Auditoría", Mexíco

JOHN J. WILLINGHAM, Auditoria Conceptos y Métodos, Editorial McGraw Hill, México.

JAMES A. SENN, Análisis y Diseño de Sistemas de Información, McGraw Hill, México.

HERNÁNDEZ SAMPIERI, Metodología de la Investigación, McGraw Hill, México.

ROGER S. PRESSMAN, Ingeniería del Software, McGraw Hill, México.

KENDALL & KENDALL, Análisis y Diseño de Sistemas, McGraw Hill, México

ARTIGA, Sandoval Carlos "Diseño de sistemas y procedimientos para la selección, evaluación y auditoría de los servicios informáticos", Trabajo de Graduación UCA, El Salvador

ROQUE HERNANDEZ, Marlene, "Diseño de manual para auditoria de sistemas aplicado a instituciones gubernamentales autónomas de El Salvador". Trabajo de Graduación, UFG, El Salvador.

SOLIS MONTES, Gustavo, "COBIT" Objetivos de Control ,CISA, ISACA

AMERICAN INSTITUTE OF Certified Accountants, "COSO"

BHALA, Raj "Pragmatic Strategy for the Scope of Sale"
Documento de Riesgos

SANDERS, Donald H.,¨ Informática presente y futuro ¨
Editorial McGraw Hill, México.

LOZANO, Letvin R., ¨ Diagramación y programación ¨
Editorial McGraw Hill, México.

NORTON, Peter., ¨ Introducción a la computación ¨
Editorial McGraw Hill, México.

LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. Edición virtual. España

FREEDMAN, Alan., ¨ Diccionario de computación ¨
Editorial McGraw Hill, Quinta edición, México.

TANIA, María Cuellar, “Aplicación de la auditoría de sistemas” Trabajo de Graduación, UCA, El Salvador

SUPERINTENDENCIA DE LA REPÚBLICA DOMINICANA, “Lineamientos Generales de Riesgos ”

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA, “Que es la Auditoria en Informática” Perú.

AUDITORIA SUPERIOR DEL ESTADO DE ZACATECAS, “Manual General de Auditoría”, México.

PRONUNCIAMIENTOS DEL CONSEJO TÉCNICO DE LA CONTADURÍA.,Eliana Moreno Montana, “Auditoria”, Colombia

Comitte of Sponsoring Organizations of the Treadway (COSO), “Control Interno de los nuevos instrumentos financieros una herramienta de información para considerar el COSO”

CARLOS MUÑOZ RAZO, “Auditoría en sistemas computacionales”, México

FITZGERALD JERRY, “Controles internos para sistemas de computación”

Sitios consultados en Internet:

www.Monografías.com
www.isaca.org
www.hispasec.com
www.lafacu.com
www.manuales.com
www.gnu.org
www.mundotutoriales.com
www.sugef.gob.cr
www.auditoriasdesistemas.com
www.solomanuales.org
www.nimsoft.com
www.es.wikipedia.org
www.iacr.org
www.rsasecurity.org
www.ieee.udistriatal.edu
www.ezone.net
www.seguridadenredes.org
www.segu-infor.org.ar
www.kriptopolis.org.
www.rsa.com
www.dara.es