

**AUDITORIA INFORMATICA APLICADA A LA INSTALACION FISICA Y
HARDWARE DEL AULA DE INFORMATICA DE LA INSTITUCION EDUCATIVA
SIMON BOLIVAR DEL MUNICIPIO DE SAMANIEGO NARIÑO.**

RUBY HERNANDEZ MESA

**UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016**

**AUDITORIA INFORMATICA APLICADA A LA INSTALACION FISICA Y
HARDWARE DEL AULA DE INFORMATICA DE LA INSTITUCION EDUCATIVA
SIMON BOLIVAR DEL MUNICIPIO DE SAMANIEGO NARIÑO.**

RUBY HERNANDEZ MESA

**Trabajo de grado presentado como requisito parcial para optar al título de
Ingeniera de Sistemas**

**Asesor
Msc. MANUEL BOLAÑOS GONZÁLEZ**

**UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016**

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

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

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre derecho de autor”.

Artículo 13, Acuerdo No. 005 de 2010 emanado del Honorable Consejo Académico.

NOTA DE ACEPTACIÓN

Jurado

Jurado

San Juan de Pasto, febrero 2016.

AGRADECIMIENTOS

En primer lugar a Dios, porque él me ha acompañado y guiado dándome la fortaleza que necesite para el día a día y nunca me ha desamparado, aunque por momentos me olvidara de él.

A mi padre, José Eliecer Hernández un padre amoroso que logro muchas cosas en su vida y que siempre me inculco que para tener una mejor calidad de vida el estudio era la mejor opción, que aunque ya no esté con nosotros siempre lo recordaremos con amor; a mi madre Rosa Elena Meza Rosas muy abnegada que siempre estuvo ahí para tenderme una mano cuando me sentí perdida con sus consejos y su amor me guio en el difícil camino que es la vida.

A mis hijos, Elkin, Stiven y Juan David quienes fueron mi fortaleza y en mis momentos de debilidad fueron aliento.

A mis hermanas, Yamile, Monica y Yaqueline, quienes han sido mi apoyo y me han tenido paciencia a lo largo de mi vida.

Al ingeniero Francisco Javier Solarte Solarte, por regalarnos un poco de su tiempo para brindarnos un conocimiento que me permitió desarrollar este proyecto.

Al ingeniero Manuel Bolaños, por su apoyo en la gestión de la realización y culminación de este proyecto.

Al señor Ramiro Toro, Rector de la Institución Educativa Simón Bolívar del municipio de Samaniego, quien estuvo presto a colaborar en todo lo que necesitara.

DEDICATORIA

A Dios, por haberme permitido lograr esta meta, permitiéndome superar las dificultades y gozarme de mis triunfos.

A mis padres, que me brindaron su apoyo incondicional y con su cariño y sabiduría hicieron que alcanzara este logro.

A mis hijos, Elkin, Stiven y Juan David quienes fueron mi motor que me impulso para conseguir esta meta y salir adelante.

A mis hermanas, que estuvieron ahí, y me dieron su confianza y su apoyo incondicional.

Gracias a todos que Dios los guarde en su infinita misericordia y los bendiga.

Amen.

RESUMEN

La auditoría informática es una herramienta que permite evaluar cómo se encuentra una empresa, cuáles son sus debilidades, amenazas, fortalezas y oportunidades, además de contribuir con el buen funcionamiento de la empresa con los planes de mejoramiento, también creando procesos y/o procedimientos que permita optimizarla.

La evaluación se hace a equipos de cómputo, equipos de comunicación en cuanto a su funcionalidad, su garantía está vigente y cada cuanto se hace el mantenimiento tanto a los equipos como a la red, al personal que lo usa y tiene acceso a ellos, si la infraestructura es la adecuada, es de fácil acceso, tiene una ruta de evacuación en caso de un desastre, cuenta con inventarios actualizados, que sistema de seguridad tiene el aula, la existencia o no de un manual de funciones, existe planos tanto de la red, como la infraestructura todo esto se evaluara con el siguiente trabajo.

Es importante mencionar que la auditoría se pueden realizar tantas veces el cliente lo requiera y de esta manera evaluar la eficiencia de cada una de las áreas, para beneficiar tanto a la empresa y a los usuarios que de una u otra forma requieren el servicio de la entidad.

Gracias al presente trabajo investigativo se logrará tener una mejor administración y control en el ámbito informático.

ABSTRACT

THE COMPUTER AUDIT IS A TOOL THAT ALLOWS US TO EVALUATE HOW YOU ARE DOING A BUSINESS, WHAT THEIR WEAKNESSES, THREATS, STRENGTHS AND OPPORTUNITIES, AND CONTRIBUTE TO THE SMOOTH FUNCTIONING OF THE SAME WITH THE IMPROVEMENT PLANS ARE ALSO CREATING PROCESSES AND / OR PROCEDURES ALLOWING OPTIMIZED.

THE COMPUTER AUDIT AT THE SCHOOL SIMÓN BOLÍVAR EVALUATES COMPUTER EQUIPMENT, COMMUNICATION EQUIPMENT IN TERMS OF ITS FUNCTIONALITY, WARRANTY IF APPLICABLE AND HOW OFTEN MAINTENANCE IS DONE BOTH TEAMS AND THE NETWORK, THE STAFF USES AND YOU HAVE ACCESS TO THEM; IF THE INFRASTRUCTURE IS ADEQUATE, IT IS EASILY ACCESSIBLE, HAS AN EVACUATION ROUTE IN CASE OF A DISASTER, HAS UPDATED INVENTORIES THAT SECURITY SYSTEM HAS THE CLASSROOM, THE EXISTENCE OF MANUAL FUNCTIONS, THERE PLANES BOTH NETWORK INFRASTRUCTURE AS ALL THIS WAS ASSESSED WITH THE NEXT PROJECT.

THE AUDIT CREATES IMPROVEMENT PLANS AND CONTINGENCY ARE VITAL FOR AN INSTITUTION THAT SHOULD BE AT THE FOREFRONT OF TECHNOLOGY BUT ALWAYS MAINTAINING ITS INTEGRITY, AND SECURITY OF YOUR TECHNOLOGY WELL. IT SHOULD BE NOTED THAT THE AUDIT NOT ONLY LET'S LOOK AT THE RISKS AND THREATS BUT THE STRENGTHS THAT THE COMPANY, WHICH CAN INFLUENCE THE DECISION-MAKING IS IMPORTANT TO MENTION THAT THE AUDIT CAN BE PERFORMED MANY TIMES THE CLIENT REQUIRES AND THUS EVALUATE THE EFFICIENCY OF EACH OF THE AREAS TO BENEFIT BOTH THE COMPANY AND USERS THAT REQUIRE ONE WAY OR ANOTHER SERVICE ENTITY.

CONTENIDO

Pág.

INTRODUCCIÓN	11
1. MARCO TEORICO.....	17
1.1. ANTECEDENTES	17
1.2. ASPECTOS GENERALES DE LA AUDITORIA.....	18
1.2.1. Enfoques de auditoria:.....	21
1.2.2. Auditoria informática	22
1.3. AUDITORIA INFORMÁTICA COMO OBJETO DE ESTUDIO	24
1.3.1 Objetivo fundamental de la auditoría informática.	25
1.3.2 Características de la auditoría informática.	26
1.3.3 Clasificación de la Auditoria informática.	27
1.3.4 Metodología de Auditoría Informática.	30
1.4 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA.....	36
1.5 ESTANDARES DE AUDITORIA.....	42
2 DESARROLLO DE LA AUDITORIA	66
2.3 ARCHIVO PERMANENTE.....	66
2.3.1 Institución Educativa Simón Bolívar	66
2.3.1.1 Misión.....	66
2.3.1.2 Visión.....	66
2.1.1.3 PERFIL DEL (A) ESTUDIANTE QUE QUEREMOS FORMAR	67
2.1.1.4 Perfil De Docente	68
2.1.1.5 Perfil Del(A) Bachiller	68
2.2 ARCHIVO CORRIENTE	68
2.2.1. Programa de Auditoria.....	69
2.3. DISEÑO DE LOS ELEMENTOS DE AUDITORÍA.	74
2.3.1. Cuadro de definición de fuentes de conocimiento.....	74
2.3.2. Análisis y evaluación riesgos preliminares.....	80

2.3.3.	HALLAZGOS	82
2.3.4.	INFORME EJECUTIVO	97
	CONCLUSIONES	100
	RECOMENDACIONES	102
	BIBLIOGRAFIA	103

INTRODUCCIÓN

En la actualidad muchos de los procesos que normalmente se hacían de forma manual, hoy en día todo gira alrededor de los sistemas y herramientas informáticas que permitan estar acorde con el avance que a diario existe en el mundo y más en las tecnologías de información que llevan consigo una gran responsabilidad por que estas se encargan de manejar grandes volúmenes de información, el cual hace que los procesos se automaticen para poder suplir las necesidades de la comunidad, generando más eficiencia, eficacia, efectividad y calidad de la información.

Basado en lo anterior, se presenta este trabajo para desarrollar una auditoría al aula de informática de la Institución Educativa Simón Bolívar, los sistemas son la fuente más importante para la obtención del conocimiento, ya que une los datos e información convirtiendo en algo útil para lograr satisfacer una necesidad o cumplir un objetivo, por esta razón el aula informática es considerada un bien, que necesita ser protegido y un mantenimiento continuo; por que la ausencia de ello conllevaría un retraso en la educación integral que el estudiante necesita.

La auditoría permite observar que el aula de informática este cumpliendo con las políticas de seguridad, la información que se requiera para poder dar clases está protegida y almacenada en un medio que sea seguro y fácil de administrar, tener los implementos necesarios para que se lleven de una manera eficiente los procedimientos que se requieran, la importancia dentro de una organización es que permite minimizar los errores que se puedan generar manualmente y a través de ellos solucionar o aminorar los riesgos que se presenten dentro del aula de informática para obtener buena calidad, además los costos, las distribuciones y el sistema productivo se manejan de una manera correcta y eficiente.

Los beneficios que traerá la auditoría al aula de informática de la Institución Educativa Simón Bolívar, radica en la revisión a los controles en cuanto al cumplimiento de los diferentes requerimientos de los usuarios del sistema, como también la seguridad del sistema operativo y acceso al aula de informática para comprobar su eficiencia y eficacia, recomendando la implementación de planes, herramientas, políticas, controles y mejoras para la protección de uno de los principales activos de la institución, garantizando que su funcionamiento sea optimo y que permita una gestión transparente por parte de sus usuarios.

ELEMENTOS GENERALES

TITULO

Auditoría Informática Aplicada a La Instalación Física y Hardware Del Aula De Informática De La Institución Educativa Simón Bolívar Del Municipio De Samaniego Nariño.

LÍNEA DE INVESTIGACIÓN

El trabajo está catalogado en esta línea ya que se desarrollara la auditoria informática en la Institución Educativa Simón Bolívar de Samaniego Nariño.

Línea de Sistemas Computacionales: Esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información.

La auditoría al aula informática de la Institución Educativa Simón Bolívar de Samaniego será enfocada a la funcionalidad y mantenimiento de los equipos, y seguridad de la misma.

MODALIDAD

Según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como acuerdo de Facultad 045 de octubre 10 de 2002 dado por el Consejo de Facultad, el trabajo corresponde a la línea de investigación de Sistemas Computacionales, ya que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de Auditoria de Sistemas.

DESCRIPCIÓN DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

En la actualidad las instituciones educativas se dotan de herramientas informáticas que les ayuden a educar a sus estudiantes de una manera integral, y estos

puedan obtener unos mejores resultados para poder competir por un cupo para su educación superior.

El aula de informática de la institución Educativa Simón Bolívar, se utiliza para la clase de informática y demás áreas que necesitan el uso de esta tecnología, por tal razón muchos de sus equipos se han dañado y ninguno de los que utilizan esta aula se han hecho responsables, ya que no se cuenta con un registro de entrada y salida de las personas que la utilizan; no cuenta con un área de mantenimiento fuera del salón de clase, ya que los equipos que se encuentran para reparación se aíslan a un costado, sin ninguna protección y restricción.

FORMULACIÓN DEL PROBLEMA

¿Cómo la auditoría evaluará los procedimientos que se llevan a cabo para el uso y mantenimiento de los equipos del aula informática de la Institución Educativa Simón Bolívar que garantice la seguridad, funcionamiento y usabilidad de los equipos permitiendo adelantar actividades de mejoramiento del aula?

SISTEMATIZACIÓN DEL PROBLEMA

- ❖ ¿Cómo la auditoría mejorará el funcionamiento del aula de informática de la Institución Educativa Simón Bolívar mediante un plan de mejoramiento?
- ❖ ¿Cómo la evaluación al aula de informática de la Institución Educativa Simón Bolívar permitirá obtener optimización en los procedimientos que maneja?
- ❖ ¿Qué actualizaciones se han realizado teniendo en cuenta el avance de la tecnología?
- ❖ ¿Cómo detectar los posibles riesgos o amenazas en el aula de informática de la Institución Educativa Simón Bolívar?
- ❖ ¿Cómo afecta la falta de controles en el aula el correcto funcionamiento de hardware?

LOCALIZACIÓN

El trabajo se llevará a cabo en el municipio de Samaniego sobre el aula informática de la Institución Educativa Simón Bolívar. La evaluación se hará específicamente en cuanto a funcionalidad y el mantenimiento de los equipos y la seguridad física del aula.

JUSTIFICACIÓN

Teniendo en cuenta que las tecnologías de la información avanzan a pasos agigantados y que todos los que no están junto con la evolución de los sistemas se van quedando obsoletos, y por ser la Institución Educativa Simón Bolívar, una entidad pública y prestadora de un servicio que no se puede quedar por fuera de este avance, se ha implementado de un aula de informática, la cual, tiene como objetivo educar a sus estudiantes en las diferentes herramientas tecnológicas que existen para un mejor desempeño tanto en la vida estudiantil como en sus actividades cotidianas.

La importancia de realizar una auditoría al aula de informática de la Institución Educativa Simón Bolívar radica en verificar que se cumpla sus procedimientos para poder brindar un correcto funcionamiento además de crear un plan de mejoras que ayude a que este bien tecnológico sea protegido.

Los beneficios que traerá la presente auditoria al aula de informática de la Institución Educativa Simón Bolívar, es que los controles en cuanto a la seguridad física y acceso a los equipos, sea más eficaz por cuanto se llevara un registro, que su reparación y mantenimiento, no se tarde tanto y llegue cuando realmente se lo necesite.

ALCANCE Y LIMITACIONES

El alcance de la auditoria informática implica la evaluación del aula de informática de la institución Educativa Simón Bolívar.

Los aspectos a evaluar específicamente en esta auditoria son:

- **HARDWARE:** revisar los equipos que están funcionando, inventarios, servidores, equipo de red, garantías y mantenimiento.
- **INFRAESTRUCTURA FISICA:** se revisara la seguridad del aula, ruta de evacuación.
- **PROCEDIMIENTOS:** se revisara que existan procedimientos y si los hay que sean agiles y estén documentados.

1. MARCO TEORICO

1.1. ANTECEDENTES

En los últimos años la tecnología ha dado grandes avances que ha hecho que la competencia sea cada día más fuerte, tanto a nivel comercial como laboral y por eso las empresas tanto privadas y públicas se han dotado de herramientas tecnológicas que las hagan estar acordes con la actualidad.

Es por eso sean creado una serie de herramientas que permita optimizar recursos, procesos y procedimientos.

La auditoría surge debido a que los equipos de cómputo y los sistemas de información se vienen encargando de muchos de los procesos que antes realizaban las personas, razón por la cual se hace necesario hacer una revisión constante del buen estado de estos recursos para su óptimo funcionamiento.

Mediante la auditoría lo que se hace es una evaluación de los recursos informáticos, que han venido evolucionando y estandarizándose, para facilitar su aplicación en cualquier organización. Actualmente hay una serie de procesos ya establecidos por medio de los cuales se puede llevar a cabo una auditoria informática de una forma eficiente y ordenada, generando resultados confiables y pertinentes para las instituciones.

La universidad de Nariño, se ha venido consolidando en el campo de la auditoria, ya que realiza convenios constantemente con entidades tanto públicas como privadas, los cuales permiten que estudiantes adquieran práctica y conocimientos para que los apliquen en proyectos de auditorías a dichos entes e instituciones.

Los siguientes trabajos sirven de referencia para el desarrollo del presente proyecto de aplicación y fueron realizados por estudiantes en instituciones a través de convenios, a continuación se enumera cada uno de los trabajos que servirán como guía para realizarlo.

- ❖ **Auditoría módulo de historia clínica electrónica del sistema de información en el Hospital Universitario Departamental de Nariño**, realizado por Jenny Burgos García y Carolina Domínguez, este trabajo consistió en la revisión de controles existentes en cuanto al cumplimiento de los diferentes requerimientos de los usuarios del módulo de historia

clínica y la seguridad lógica de del sistema operativo y acceso a la base de datos.

- ❖ **Auditoría informática a nivel de los sistemas e indicadores de funcionamiento del hardware y software en la empresa Dispropan S.A.S del Departamento de Nariño y Putumayo**, realizado por Jhoana Lorena Hernández Benavides, este trabajo consistió en evaluar el funcionamiento, actualización y mantenimiento del hardware, equipos móviles, red y el sistema de información.

1.2. ASPECTOS GENERALES DE LA AUDITORIA

De manera general se podría decir que la auditoria se define como “un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados cuyo fin consiste en determinar el grado de correspondencia de contenido informático, con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso”.

Con la auditoria se busca encontrar y evaluar las evidencias es realizado por una persona independiente y competente acerca de la información cuantificable de una entidad específica, con el propósito de determinar e informar sobre el grado de correspondencia entre la información cuantificable y criterios establecidos. De igual manera detecta todos los puntos de control en las diferentes dependencias que son críticas.

- ❖ Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados por el PAD
- ❖ Incrementar la satisfacción de los usuarios de los sistemas computarizados
- ❖ Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles
- ❖ Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- ❖ Seguridad de personal, datos, hardware, software e instalaciones
- ❖ Apoyo de función informática a las metas y objetivos de la organización

- ❖ Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático
- ❖ Minimizar existencias de riesgos en el uso de Tecnología de información
- ❖ Decisiones de inversión y gastos innecesarios
- ❖ Capacitación y educación sobre controles en los Sistemas de Información

Definición de auditoría¹: conceptualmente la auditoría es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Con frecuencia la palabra auditoría se ha empleado incorrectamente y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a utilizar la palabra "auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio: no sólo detecta errores, sino que es un examen técnico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

Así como existen normas y procedimientos específicos para la realización de auditorías contables, existen también normas y procedimientos para la realización de auditorías en informática como parte de una profesión; estas pueden estar basadas en las experiencias de otras profesiones pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y además la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

1 Piattini, Mario G y del peso, Emilio 2000. "Auditoría Informática: un enfoque práctico" computec RAMA. Madrid, España, Pag 4.

<http://ucapanama.org/wp-content/uploads/2011/12/Generalidades-en-la-Auditoria.pdf>

Auditor²: se refiere a la persona capacitada y experimentada que se designa por una autoridad competente o por una empresa de consultoría, para revisar, examinar y evaluar con coherencia los resultados de la gestión administrativa y financiera de una dependencia o entidad con el propósito de informar o dictaminar acerca de ellas, realizando las observaciones y recomendaciones pertinentes para mejorar su eficacia y eficiencia en su desempeño

Tipos de auditoría³: existen algunos tipos de Auditoría entre las que la Auditoría de Sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática.

Auditoría Externa: es el examen realizado para expresar un criterio profesional sobre el funcionamiento y eficiencia que tiene una organización en el desarrollo de una determinada gestión, este trabajo lo elabora personal independiente, ya sea que trabaje en forma lucrativa o no.

El objetivo de la auditoría externa es emitir una opinión sobre la razonabilidad, integridad y autenticidad de los estados, expedientes y documentos y toda aquella información producida por los sistemas de una organización.

La auditoría externa para cumplir con su objetivo debe de seguir los siguientes procedimientos específicos:

- ❖ Identificar riesgos (Negocio, Fraude y Procesos)
- ❖ Evaluar su susceptibilidad a distorsiones (errores) en la información.
- ❖ Diseñar procedimientos de auditoría que permitan evaluar el diseño, la implementación y efectividad de los controles implementados.
- ❖ Diseñar procedimientos de auditoría sustantivos de acuerdo con la evaluación de los riesgos.

Auditoría Interna: “La auditoría interna es una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones

²<http://es.wikipedia.org/wiki/Auditor>

³<http://www.mcgraw-hill.es/bcv/guide/capitulo/8448178971.pdf>

contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección”.⁴

La auditoría interna surge por la necesidad de mantener un control permanente y eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente se ocupa fundamentalmente del sistema de control interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger sus activos, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera.

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades proporcionándoles objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas.

1.2.1. Enfoques de auditoría:

Entre los principales enfoques de Auditoría se tiene los siguientes:

- ❖ Auditoría Financiera: Es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la situación financiera de la empresa, este proceso solo es posible llevarlo a cabo a través de un elemento llamado evidencia de auditoría, ya que el auditor hace su trabajo posterior a las operaciones de la empresa.

- ❖ Auditoría Administrativa: Revisa y evalúa si los métodos y procedimientos que se siguen en todas las fases del proceso administrativo aseguran el cumplimiento con políticas, planes, programas, leyes y reglamentaciones

⁴ Instituto de Auditores Internos de Estados Unidos.

que puedan tener un impacto significativo en operación de los reportes y asegurar que la organización los esté cumpliendo y respetando.

- ❖ Auditoría Operacional: se centra en la medición de la posición financiera, de los resultados de las operaciones y de los flujos de efectivos de una entidad, una auditoría operacional se centra en la eficacia, la eficiencia y la economía de las operaciones. El auditor operacional evalúa los controles operativos de la administración y de los sistemas sobre actividades tan diversas como las compras, procesamiento de datos, recepción, envío, servicios de oficina, publicidad, entre otros.

- ❖ Auditoría Gubernamental: Es la revisión y examen que llevan a cabo las entidades fiscalizadoras superiores a las operaciones de diferente naturaleza, que realizan las dependencias y entidades del gobierno central, estatal y municipal en el cumplimiento de sus atribuciones legales.

- ❖ Auditoría Integral: La auditoría integral es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la siguiente temática: la Información financiera, la estructura del control interno, el cumplimiento de las leyes pertinentes y la conducción ordenada en el logro de las metas y objetivos propuestos; con el propósito de informar sobre el grado de correspondencia entre la temática y los criterios o indicadores establecidos para su evaluación.

- ❖ Auditoría de Sistemas: Es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

1.2.2. Auditoria informática⁵

⁵Piattini, Mario G y del peso, Emilio 2000. "Auditoria Informática: un enfoque práctico" computec RAMA. Madrid, España, Pag 29.

Concepto de auditoría en informática⁶: La auditoría en informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, nada más se señalarán algunos aspectos básicos para su entendimiento.

Así, la auditoría en informática es:

1. Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento de las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleve a cabo de una manera oportuna y eficiente.
2. Las actividades ejecutadas por los profesionales del área de Informática y de auditoría encaminada a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.). Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual ha de contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y la optimización permanente de la tecnología de informática en el negocio.
3. El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que pasa por el área se manejan con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

De este modo la auditoria informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoria:

- ❖ Objetivos de protección de activos e integridad de datos.
- ❖ Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

1.3. AUDITORIA INFORMÁTICA COMO OBJETO DE ESTUDIO.

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Los factores que pueden influir en una organización a través del control y la auditoría en informática son:

- ❖ Necesidad de controlar el uso evolucionado de las computadoras.
- ❖ Controlar el uso de la computadora, que cada día se vuelve más importante y costosa.
- ❖ Altos costos que producen los errores en una organización.
- ❖ Abuso en las computadoras.
- ❖ Posibilidad de pérdida de capacidades de procesamiento de datos.
- ❖ Posibilidad de decisiones incorrectas.
- ❖ Valor del hardware, software y personal.
- ❖ Necesidad de mantener la privacidad individual.
- ❖ Posibilidad de pérdida de información o de mal uso de la misma.
- ❖ Necesidad de mantener la privacidad de la organización.

La información es un factor importante y cada día cobra más valor para una empresa u organización para la continuidad de las operaciones, ya que la imagen de su ambiente depende de la situación actual, su desarrollo y competitividad

dependen del ambiente pasado y futuro, ya que tomar una decisión incorrecta mediante datos erróneos proporcionados por los sistemas trae como consecuencia efectos significativos que afectan directamente a la organización.

1.3.1 Objetivo fundamental de la auditoría informática. La operatividad en una empresa es el punto más importante, es la encargada de vigilar el funcionamiento de mínimos consistentes de la organización y las maquinas a nivel global como parcial. La auditoría se debe realizar en el momento en que la maquinaria informática está en funcionamiento, con el fin de identificar falencias que obstruyan la operatividad de las mismas, con el objeto de corregir o buscar alternativas de solución a tiempo, sin tener que parar el trabajo.

La operatividad de los sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel.

Los controles técnicos generales son importantes en las instalaciones de empresas grandes, ya que se realizan para verificar la compatibilidad de funcionamiento simultáneo del sistema operativo y el software de base con todos los subsistemas existentes, como también la compatibilidad del hardware y del software instalado. En una empresa existen diferentes entornos de trabajo que conlleva a la contratación de productos de software básico, así como software especial para algunos departamentos, con el riesgo de abonar más de una vez el mismo producto o desaprovechar el software instalado, así mismo puede existir software desarrollado por personal de sistemas de la misma empresa que hagan mal uso y que no se aprovechen todos los recursos de este, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.

Los controles técnicos específicos, menos evidentes, son también necesarios para lograr la operatividad de los sistemas. Es decir por más pequeña que sea la aplicación que se deba ejecutar, esta debe funcionar al máximo, evitando así la inoperatividad, bien sea en hardware como en software. Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observación de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las normas generales de la instalación informática: se realiza una revisión inicial sencilla, verificando la aplicación de las normas pero también registrando las áreas que no cumplan o que no las apliquen, sin olvidar que esta normativa no está en contradicción con alguna norma no informática de la empresa.
2. Los procedimientos generales informáticos: se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por la persona responsable de este cargo. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los procedimientos de backup y recuperación correspondientes.
3. Los procedimientos específicos informáticos: igualmente, se revisara su existencia en las áreas fundamentales. Así, explotación no debería explotar una aplicación sin haber exigido a desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los procedimientos específicos no se opongan a los procedimientos generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la normativa y los procedimientos generales de la propia empresa, a los que la informática debe estar sometida.

1.3.2 Características de la auditoría informática.

La información de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma, como sus stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la auditoría de inversión informática.

Del mismo modo, los sistemas informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la auditoría de seguridad informática en general, o a la auditoría de seguridad de alguna de sus áreas, como pudieran ser desarrollo o técnica de sistemas.

Cuando se producen cambios estructurales en la informática, se reorganiza de alguna forma su función: se está en el campo de la auditoría de organización informática.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoría del área de desarrollo de proyectos de la informática de una empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

Teniendo en cuenta lo anterior y partiendo de las diferentes actividades de sistemas que cada empresa tiene dentro de su organización dentro de las áreas generales, se establecen las siguientes divisiones de auditoría informática: de

explotación, de sistemas, de comunicaciones y de desarrollo de proyectos. Estas son las áreas específicas de la auditoría Informática más importantes. Cada área específica puede ser auditada desde los siguientes criterios generales, que pueden modificarse según sea el tipo de empresa a auditar:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

1.3.3 Clasificación de la Auditoría informática.

Auditoría Informática de Explotación: explotación informática se encarga de obtener resultados informáticos, como son: listados impresos, ficheros soportados magnéticamente, órdenes automatizadas para lanzar o modificar procesos industriales, entre otras. Los datos es la materia prima que hay que transformar por medio del proceso informático (gobernado por programas), bajo el criterio de integridad y control de calidad y así lleguen finalmente al usuario. Para auditar explotación hay que auditar las sesiones que la componen y sus interrelaciones.

Auditoría Informática de Sistemas: encargada de analizar todo lo concerniente a Técnica de Sistemas en todas sus facetas, teniendo como resultado en la actualidad que todo lo que forme el entorno general de sistemas, como son las comunicaciones, líneas y Redes de las instalaciones informáticas, se auditen por separado. Dentro de la auditoría informática de sistemas se evalúa lo siguiente:

- ❖ **Sistemas operativos:** debe verificarse en primer lugar que los Sistemas estén actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas.
- ❖ **Software básico:** es fundamental para el auditor conocer los productos de software básico que han sido adquiridos aparte de la propia computadora.

Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agrede ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.

- ❖ **Tunning:** es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados.
- ❖ **Optimización de los sistemas y subsistemas:** las Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings pre-programados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.
- ❖ **Administración de Base de Datos:** el diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. El auditor de Base de Datos analizará los Sistemas de salvaguarda existentes, revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.
- ❖ **Investigación y Desarrollo:** como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del mismo campo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas. La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas.

Auditoría Informática de Comunicaciones y Redes: para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está

condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones: el Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones, que a su vez, engloba muchas áreas que tiene la empresa. Una Aplicación recorre las siguientes fases:

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

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costos, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Auditoría de la Seguridad informática: la computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes, virus, etc., que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos. La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica.

1.3.4 Metodología de Auditoría Informática.

Como auditor se debe recolectar toda la información general, que permita así mismo definir un juicio global objetivo siempre amparadas en pruebas o hechos demostrables. Dar como resultado un informe claro, conciso y a la vez preciso depende del análisis y experiencia del auditor, frente a diferentes entornos a evaluar, dependiendo de las debilidades y fortalezas encontradas en dicha empresa auditada. La recolección de información, el análisis, la aplicación de diferentes normas de acuerdo al tipo de auditoría, los hallazgos encontrados y pruebas que avalen estos resultados son indispensables en la realización de una auditoría. Para llegar al resultado hay que seguir una serie de pasos que permiten tener claridad y orden de la auditoría aplicar.

El método de trabajo del auditor pasa por las siguientes etapas:

1. Alcance y Objetivos de la Auditoría Informática.
2. Estudio inicial del entorno auditable.
3. Determinación de los recursos necesarios para realizar la auditoría.
4. Elaboración del plan y de los Programas de Trabajo.
5. Actividades propiamente dichas de la auditoría.
6. Confección y redacción del Informe Final.
7. Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

Alcance y Objetivos de la Auditoría Informática: El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar. A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas. Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

Estudio inicial del entorno auditable: Esta etapa es una de las más importantes en el desarrollo de la auditoría, ya que el auditor debe conocer todos los procesos desarrollados, relacionado con el área tomada como caso de estudio. Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

Organización: Para el auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto el auditor deberá fijarse en:

- ❖ Organigrama: el organigrama expresa la estructura oficial de la organización a auditar. Permite identificar las jerarquías, dependencias y direcciones entre las áreas existentes.
- ❖ Departamentos: se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.
- ❖ Relaciones jerárquicas y funcionales entre órganos de la organización: El auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.
- ❖ Flujos de información: además de las corrientes verticales intra - departamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra-departamentales.
- ❖ Número de Puestos de trabajo: El equipo auditor comprobará que los nombres de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas.
- ❖ Número de personas por puesto de trabajo: es un parámetro que los auditores informáticos deben tener en cuenta ya que la inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.
- ❖ Entorno operacional: el auditor informático debe tener una referencia del entorno en el que va a desenvolverse y se obtiene determinando lo siguiente:

- ❖ Situación geográfica de los Sistemas: Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa, continuando con la verificación de la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- ❖ Arquitectura y configuración de hardware y software: cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías, para esto es importante que los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.
- ❖ Inventario de hardware y software: el auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware figurarán las CPU'S, unidades de control local y remoto, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.
- ❖ Comunicación y Redes de Comunicación: Al realizar el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones, igualmente, poseerán información de las Redes Locales de la Empresa y todo lo que tenga que ver con la red de Comunicaciones.

Determinación de los recursos necesarios para realizar la auditoría: mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos humanos: la cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable. Es igualmente señalable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria. Recursos materiales: Los recursos materiales del auditor son de dos tipos:

- Recursos software como son, cantidad y complejidad de bases de datos y ficheros, que son programas propios de la auditoría, son muy potentes y flexibles.
- Recursos materiales hardware: los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado. Por lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, scanner, etc.

Elaboración del plan y de los programas de trabajo: una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo y así, se procede a la programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

- ❖ Si la revisión debe realizarse por áreas generales o áreas específicas.
- ❖ Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.
- ❖ En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- ❖ En el plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- ❖ En el plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- ❖ El plan establece disponibilidad futura de los recursos durante la revisión.
- ❖ El plan estructura las tareas a realizar por cada integrante del grupo.
- ❖ En el plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

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

Actividades propiamente dichas de la auditoría Informática: la auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad. Existen técnicas que hacen que el auditor las aplique de acuerdo a su juicio y al tipo de auditoría a ejecutar y son:

Técnicas de trabajo:

- ❖ Análisis de la información obtenida del auditado
- ❖ Análisis de la información propia cruzamiento de las informaciones anteriores
- ❖ Entrevistas
- ❖ Simulación
- ❖ Muestreos

- ❖ Inspección
- ❖ Confirmación
- ❖ Investigación
- ❖ Certificación
- ❖ Observación

Herramientas:

- ❖ Cuestionario general inicial
- ❖ Cuestionario checklist
- ❖ Estándares
- ❖ Monitores
- ❖ Simuladores (generadores de datos)
- ❖ Paquetes de auditoría (generadores de Programas)
- ❖ Matrices de riesgo

Confección y redacción del informe final: la función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Redacción de la carta de introducción o carta de presentación del informe final: la carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción. La carta de introducción poseerá los siguientes atributos:

- ❖ Tendrá como máximo 4 folios
- ❖ Incluirá fecha, naturaleza, objetivos y alcance
- ❖ Cuantificará la importancia de las áreas analizadas.
- ❖ Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- ❖ Presentará las debilidades en orden de importancia y gravedad.
- ❖ En la carta de Introducción no se escribirán nunca recomendaciones.

Estructura del informe final: el informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Siguiendo los siguientes pasos:

- ❖ Definición de objetivos y alcance de la auditoría:
- ❖ Enumeración de temas considerados:
- ❖ Cuerpo expositivo

Para cada tema, se seguirá el siguiente orden a saber:

- a) Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
- b) Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- c) Puntos débiles y amenazas.
- d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática. e) Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- ❖ El informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- ❖ El Informe debe consolidar los hechos que se describen en el mismo.
- ❖ El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:
 1. El hecho debe poder ser sometido a cambios.
 2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
 3. No deben existir alternativas viables que superen al cambio propuesto.
 4. La recomendación del auditor sobre el hecho, debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

Hecho encontrado.

- ❖ Ha de ser relevante para el auditor y para el cliente
- ❖ Ha de ser exacto, y además convincente.
- ❖ No deben existir hechos repetidos.

Consecuencias del hecho: las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

Repercusión del hecho: se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

Conclusión del hecho: no deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

Recomendación del auditor informático

- ❖ Deberá entenderse por sí sola, por simple lectura.
- ❖ Deberá estar suficientemente soportada en el propio texto.
- ❖ Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- ❖ La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

1.4 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA⁷

Cuestionarios: las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre-impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy

⁷ <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>

específicos para cada situación, y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos pre-impresos hubieran proporcionado.

Entrevistas

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

Checklist

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad

servirán para la cumplimentación sistemática de sus cuestionarios, de sus checklists.

Hay opiniones que descalifican el uso de las checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de checklist. Salvo excepciones, las checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma. Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable.

El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer. Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la checklist de modo que el auditado responda clara y concisamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. checklist de rango: Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo: Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

- 1: Muy deficiente.
- 2: Deficiente.
- 3: Mejorable.
- 4: Aceptable.
- 5: Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación de la checklist no debe realizarse en presencia del auditado. Ejm:

- ¿Existe personal específico de vigilancia externa al edificio?
Rta/ No, solamente un guarda por la noche que atiende además otra instalación adyacente.

<Puntuación: 1>

- Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los alrededores del Centro de Cálculo?
Rta/ Si, pero sube a las otras 4 plantas cuando se le necesita.

<Puntuación: 2>

- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
Rta/ Si, pero existen cajas apiladas en dicha puerta. Algunas veces las

quitan.

<Puntuación: 2>

- El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?
Rta/ No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.

<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: $(1 + 2 + 2 + 4) / 4 = 2,25$
Deficiente.

b. Checklist binaria: Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméricamente, equivalen a 1(unos) o 0(cero), respectivamente. Ejemplo :

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

- ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

- ¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

- ¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

- ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

- ¿Se conoce la norma anterior?

<Puntuación: 0>

- ¿Se aplica en todos los casos?

<Puntuación: 0>

Las checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor. Las checklists Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del < Si o No> frente a la mayor riqueza del intervalo. No existen checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

Trazas y/o Huellas

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos software muy potente y modular que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su

empleo. Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

Observación

La observación es una de las técnicas más utilizadas en la recolección de información para aplicación de una auditoria, ya que a través de diferentes técnicas y métodos de observación permite recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas. Existen diferentes tipos de observación

- ❖ Observación directa
- ❖ Observación indirecta
- ❖ Observación oculta
- ❖ Observación participativa
- ❖ Observación no participativa
- ❖ Introspección
- ❖ Estrospección
- ❖ Observación histórica, entre las cuales están:
 - Observación controlada
 - Observación natural

Inventarios

Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencias e investigar sus causas.

Los principales tipos de inventarios aplicables en el ambiente de sistemas computacionales son:

- ❖ Inventario de software
- ❖ Inventario de hardware

- ❖ Inventario de documentos
 - Inventario de documentos administrativos
- ❖ Manuales de la organización
- ❖ Manuales de procedimientos administrativos
- ❖ Manuales de perfil de puestos ·
 - Otros manuales administrativos
 - Inventario de documentos técnicos para el sistema
- ❖ Manuales e instructivos técnico del hardware, periféricos y componentes del sistema.
- ❖ Manuales e instructivos de mantenimiento físico del sistema (hardware), entre otros.

1.5 ESTANDARES DE AUDITORIA

Para la realización y ejecución de una auditoria se hace necesario aplicar normas o estándares bajo los cuales las empresas deben regirse, de allí la importancia identificar los estándares internacionales que en este caso son:⁸

Directrices Gerenciales de COBIT, desarrollado por la Information Systems Audit and Control Association (ISACA) Asociación de Auditoría y Control de los Sistemas de Información: Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y administre los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados. Uno de los objetivos de ISACA es promover estándares aplicables internacionalmente para cumplir con su visión. La estructura para los estándares de auditoría de SI brinda múltiples niveles de asesoría, como:

- ❖ Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el código de ética profesional de ISACA.
- ❖ La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- ❖ Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor, CISA) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede

⁸ www.adacsi.org.ar/files/es/content/146/Standards.doc

resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias, así:

1. The Management of the Control of data Information Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA): Este modelo está basado en el concepto de roles y establece responsabilidades relacionadas con seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y responsabilidad respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.
2. Administración de la inversión de tecnología de Inversión: un marco para la evaluación y mejora del proceso de madurez, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO): Este modelo identifica los procesos críticos, asegurando el éxito de las inversiones en tecnología de información y comunicación electrónicas. Además los organiza en cinco niveles de madurez, similar al modelo CMM.
3. Estándares de administración de calidad y aseguramiento de calidad ISO 9000, desarrollados por la Organización Internacional de Estándares (ISO): La colección ISO 9000 es un conjunto de estándares y directrices que apoyan a las organizaciones a implementar sistemas de calidad efectivos, para el tipo de trabajo que ellos realizan.
4. SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA: Este servicio pretende incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si un sistema de información es confiable, (si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).
5. Modelo de Evolución de Capacidades de software (CMM), desarrollado por el Instituto de Ingeniería de Software (SEI): Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización, con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

6. Administración de sistemas de información: Una herramienta de evaluación práctica, desarrollado por la Directiva de Recursos de Tecnología de Información (ITRB): Este es una herramienta de evaluación que permite a entidades gubernamentales, comprender la implementación estratégica de tecnología de información y comunicación electrónica que puede apoyar su misión e incrementar sus productos y servicios.

7. Guía para el cuerpo de conocimientos de administración de proyectos, desarrollado por el comité de estándares del instituto de administración de proyectos: Esta guía está enfocada en las mejores prácticas sobre administración de proyectos. Se refiere a aspectos sobre los diferentes elementos necesarios para una administración exitosa de proyectos de cualquier naturaleza. En forma precisa, este documento identifica y describe las prácticas generalmente aceptadas de administración de proyectos que pueden ser implementadas en las organizaciones.

8. Ingeniería de seguridad de sistemas – Modelo de madurez de capacidades (SSE – CMM), desarrollado por la agencia de seguridad nacional (NSA) con el apoyo de la Universidad de Carnegie Mellon: Este modelo describe las características esenciales de una arquitectura de seguridad organizacional para tecnología de información y comunicación electrónica, de acuerdo con las prácticas generalmente aceptadas observadas en las organizaciones.

9. Administración de seguridad de información: Aprendiendo de organizaciones líderes, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO): Este modelo considera ocho organizaciones privadas reconocidas como líderes respecto a seguridad en cómputo. Este trabajo hace posible la identificación de 16 prácticas necesarias para asegurar una adecuada administración de la seguridad de cómputo, las cuáles deben ser suficientes para incrementar significativamente el nivel de administración de seguridad en tecnología de información y comunicación electrónica.

El Modelo COBIT para Auditoría y Control de Sistemas de Información⁹

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. Las siglas COBIT significan Objetivos de Control para Tecnología de

⁹ <http://www.channelplanet.com/index.php?idcategoria=13932>

Información (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association). COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización. “La adecuada implementación de COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado. Cualquier tipo de empresa puede adoptar una metodología COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos IT y consecuentemente, sobre la posibilidad de evaluar el logro de los objetivos del negocio apalancado en procesos tecnológicos”, Señaló un informe de ETEK. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Criterios de información de COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciaros y de seguridad, se definieron los siguientes siete criterios de información:

- ❖ La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- ❖ La eficiencia consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

- ❖ La confidencialidad se refiere a la protección de información sensible contra revelación no autorizada.
- ❖ La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- ❖ La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

- ❖ La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a lo siguiente¹⁰:

- Administración y consejos ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad.

El diagrama de contenido de COBIT mostrado en la anterior figura presenta las audiencias principales, sus preguntas sobre gobierno TI y los productos que generalmente les aplican para proporcionar las respuestas. También hay productos derivados para propósitos específicos, para dominios tales como seguridad o empresas específicas.

Brevemente, los productos COBIT incluyen:

- ❖ **El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición:** Diseñado para ayudar a los ejecutivos a entender por qué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.
- ❖ **Directrices gerenciales / modelos de madurez:** Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad. □ **Marco de Referencia:** Explica cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.

¹⁰ <http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>

- ❖ **Objetivos de control:** Brindan objetivos a la dirección basados en las mejores prácticas genéricas para todos los procesos de TI
- ❖ **Guía de implementación de gobierno de TI:** Usando COBIT y Val TI 2ª Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI.
- ❖ **Prácticas de control de COBIT:** Guía para Conseguir los Objetivos de Control para el Éxito del Gobierno de TI 2ª Edición: Proporciona una guía de por qué vale la pena implementar controles y cómo implementarlos.
- ❖ **Guía de aseguramiento de TI:** Usando COBIT: Proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control. El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro “dominios” principales, a saber:
 - ❖ Planear y organizar (PO): Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
 - ❖ Adquirir e implementar (AI): Proporciona las soluciones y las pasa para convertirlas en servicios.
 - ❖ Entregar y dar Soporte (DS): Recibe las soluciones y las hace utilizables por los usuarios finales.
 - ❖ Monitorear y evaluar (ME): Monitorear todos los procesos para asegurar que se sigue la dirección provista.
- **Planificación y organización:**
 - PO1 Definir un plan estratégico de TI
 - PO2 Definir la arquitectura de la información
 - PO3 Determinar la dirección tecnológica
 - PO4 Definir los procesos, organización y relaciones de TI
 - PO5 Administrar la inversión en TI
 - PO6 Comunicar las aspiraciones y la dirección de la gerencia
 - PO7 Administrar recursos humanos de TI
 - PO8 Administrar la calidad
 - PO9 Evaluar y administrar los riesgos de TI
 - PO10 Administrar proyectos
- **Adquisición e implantación**
 - AI1 Identificar soluciones automatizadas
 - AI2 Adquirir y mantener software aplicativo
 - AI3 Adquirir y mantener infraestructura tecnológica
 - AI4 Facilitar la operación y el uso
 - AI5 Adquirir recursos de TI
 - AI6 Administrar cambios

AI7 Instalar y acreditar soluciones y cambios

➤ **Soporte y Servicios**

DS1 Definir y administrar los niveles de servicio

DS2 Administrar los servicios de terceros

DS3 Administrar el desempeño y la capacidad

DS4 Garantizar la continuidad del servicio

DS5 Garantizar la seguridad de los sistemas

DS6 Identificar y asignar costos

DS7 Educar y entrenar a los usuarios

DS8 Administrar la mesa de servicio y los incidentes

DS9 Administrar la configuración

DS10 Administrar los problemas

DS11 Administrar los datos

DS12 Administrar el ambiente físico

DS13 Administrar las operaciones

➤ **Monitoreo y evaluación**

ME1 Monitorear y evaluar el desempeño de TI

ME2 Monitorear y evaluar el control interno

ME3 Garantizar el cumplimiento regulatorio

ME4 Proporcionar gobierno de TI

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

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

Dominios de COBIT

Entendiéndose como dominio, la agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional, los procesos a su vez son conjuntos o series de actividades unidas con delimitación o cortes de control y las actividades son acciones requeridas para lograr un resultado medible.

COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aún más, se pueden combinar como se necesite por cada empresa.

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

Procesos

PO1 Definición de un plan estratégico

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros. Su realización se concreta a través de un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- ❖ La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
- ❖ El inventario de soluciones tecnológicas e infraestructura actual, se deberá a, evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
- ❖ Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.
- ❖ Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos.

PO2 Definición de la arquitectura de información

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

- ❖ La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
- ❖ El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización deberá ser continuamente actualizado.
- ❖ La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

PO3 Determinación de la dirección tecnológica

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

- ❖ La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- ❖ El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- ❖ Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- ❖ Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI

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

- ❖ El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
- ❖ Propiedad, custodia, la gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- ❖ Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente.
- ❖ Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.
- ❖ Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.
- ❖ La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- ❖ Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar una asignación de personal adecuada en el presente y en el futuro.
- ❖ El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

PO5 Manejo de la inversión

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

- ❖ Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.
- ❖ El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información
- ❖ La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

PO6 Comunicación de la dirección y aspiraciones de la gerencia

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

- ❖ Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido y promovido por la Alta Gerencia.
- ❖ Las directrices tecnológicas.
- ❖ El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
- ❖ El compromiso con la calidad, la gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
- ❖ Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

PO7 Administración de recursos humanos

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

- ❖ El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
- ❖ Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.
- ❖ La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- ❖ La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

PO8 Asegurar el cumplimiento con los requerimientos Externos

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

- ❖ Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continuo de los mismos.
- ❖ Leyes, regulaciones y contratos.
- ❖ Revisiones regulares en cuanto a cambios.
- ❖ Búsqueda de asistencia legal y modificaciones.
- ❖ Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- ❖ Privacidad
- ❖ Propiedad intelectual
- ❖ Flujo de datos externos y criptografía

PO9 Evaluación de riesgos

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

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

Actualización de evaluación de riesgos.

- ❖ Metodología de evaluación de riesgos.
- ❖ Medición de riesgos cualitativos y/o cuantitativos.
- ❖ Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.
- ❖ Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al

enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

PO10 Administración de proyectos

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

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

- ❖ El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- ❖ Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- ❖ Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- ❖ Presupuestos de costos y horas hombre.
- ❖ Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- ❖ Plan de administración de riesgos para eliminar o minimizar los riesgos.
- ❖ Planes de prueba, entrenamiento, revisión post-implementación.

PO11 Administración de calidad

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

- ❖ Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.
- ❖ Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorías,

inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.

- ❖ Metodologías del ciclo de vida de desarrollo de sistemas que rijan el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
- ❖ Documentación de pruebas de sistemas y programas.
- ❖ Revisiones y reportes de aseguramiento de calidad.

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

Procesos

AI1 Identificación De Soluciones Automatizadas

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

- ❖ Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
- ❖ Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
- ❖ Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
- ❖ Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
- ❖ Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensibles (ej. Identificación de usuarios contra divulgación o mal uso).
- ❖ Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
- ❖ Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología específica a ser proporcionada.

AI2 Adquisición y mantenimiento del software aplicativo

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

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

AI3 Adquisición y mantenimiento de la infraestructura tecnológica

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

- ❖ Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
- ❖ Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
- ❖ Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

AI4 Desarrollo y mantenimiento de procedimientos

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

- ❖ Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
- ❖ Manuales de Operaciones y controles, de manera que estén en permanente actualización.
- ❖ Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 Instalación y aceptación de los sistemas

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

- ❖ Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- ❖ Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- ❖ Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- ❖ Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
- ❖ Revisiones post implementación con el objeto de reportar si el sistema proporcione los beneficios esperados de la manera más económica.

AI6 Administración de los cambios

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

- ❖ Identificación de cambios tanto internos como por parte de proveedores
- ❖ Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- ❖ Evaluación del impacto que provocaran los cambios.
- ❖ Autorización de cambios
- ❖ Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

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

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

Procesos

Ds1 Definición de niveles de servicio

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

- ❖ Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
- ❖ Definición de las responsabilidades de los usuarios y de la función de servicios de información.
- ❖ Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
- ❖ Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de

desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

- ❖ Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.
- ❖ Garantías de integridad
- ❖ Convenios de confidencialidad □ Implementación de un programa de mejoramiento del servicio.

Ds2 Administración de servicios prestados por terceros

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.

Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- ❖ Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- ❖ Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
- ❖ Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- ❖ Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

Ds3 Administración de desempeño y capacidad

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

- ❖ Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
- ❖ Monitoreo y reporte de los recursos de tecnología de información.

- ❖ Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- ❖ Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño.
- ❖ Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

Ds4 Asegurar el Servicio Continuo

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- ❖ Planificación de Severidad
- ❖ Plan Documentado
- ❖ Procedimientos Alternativos
- ❖ Respaldo y Recuperación
- ❖ Pruebas y entrenamiento sistemático y singulares

Ds5 Garantizar la seguridad de sistemas

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- ❖ Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.
- ❖ Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario.
- ❖ Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución,

- certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
- ❖ Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
 - ❖ Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
 - ❖ Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización.

Ds6 Educación y entrenamiento de usuarios

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

- ❖ Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
- ❖ Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.
- ❖ Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

Ds7 Identificación y asignación de costos

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

- ❖ Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.
- ❖ Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades.
- ❖ Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía.

Ds8 Apoyo y asistencia a los clientes de TI

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

- ❖ Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda.
- ❖ Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas.
- ❖ Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

Ds9 Administración de la configuración

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

- ❖ Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición
- ❖ Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración.
- ❖ Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización.
- ❖ Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

Ds10 Administración de problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder. Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento

de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

Ds11 Administración de datos

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

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

Ds12 Administración de las instalaciones

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física. Ds13 Administración de la operación
Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

Dominio: Monitoreo y evaluación (ME)

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos

M1 Monitoreo del proceso

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos. Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

M2 Monitorear y evaluar el control interno

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

M3 Garantizar el cumplimiento con requerimientos

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

de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

M4 Proporcionar gobierno de TI

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoría. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría. La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoría, período de cobertura, naturaleza y trabajo de auditoría realizado, así como también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo. Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente. Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcancen y que los eventos no deseados se prevengan o se detecten, y corregirán". Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI". En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista: -Los recursos de las TI. -Los criterios empresariales que deben satisfacer la información. -Los procesos de TI. Para cada uno de estos 34 procesos, tiene un enlace a las metas de negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuáles son sus actividades clave y entregables principales, y quién es el responsable de ellas.

2 DESARROLLO DE LA AUDITORIA

2.3 ARCHIVO PERMANENTE

El archivo permanente contiene información importante que ayudara a comprender de la mejor manera el objeto de la auditoria.

2.3.1 Institución Educativa Simón Bolívar

2.3.1.1 Misión.¹¹

Contamos con una trayectoria histórica de más de 70 años de servicio a la sociedad samanieguense fundamentada a la calidad académica que ha dado frutos en diferentes contextos y cuyos egresados han dejado en alto el nombre de la institución.

Somos una comunidad educativa diversa con criterios claros de tipo social, pedagógicos y cultura que forma integralmente a personas, en un proceso constante de construcción de conocimientos, defensores y promotores de los derechos humanos, forjadores de ambientes sanos, de valores éticos y cívicos que de manera correlacionada, fundamentan un currículo coherente con los retos educativos, las políticas y expectativas del estado.

Trabajamos para formar a los futuros ciudadanos y ciudadanas con base a una educación activa y humanista, critica proyectada hacia la construcción de una nueva sociedad, considerando a nuestros educandos como sujetos activos de derechos, deberes y compromisos, de la cultura y de los beneficios que ofrecen las ciencias, el arte, el deporte y las tecnologías en permanente cambio.

2.3.1.2 Visión.¹²

A mediano plazo, nuestra institución será reconocida como una de las mejores del departamento de Nariño por su calidad educativa centrada en la formación integral del ser y el desarrollo de competencias, con un nivel de privilegio (superior o muy

¹¹ Manual de convivencia

¹² Manual de convivencia

superior) en las pruebas de estado, que aporte a la construcción de una nueva ciudadanía

2.1.1.3 PERFIL DEL (A) ESTUDIANTE QUE QUEREMOS FORMAR

El estudiante de la Institución Simón Bolívar se identificará durante su permanencia en la institución y en el transcurso de su vida personal, familiar, social y laboral, por las siguientes características.

- ❖ Una persona auténtica, íntegra, responsable, consciente de su libertad, que pone en práctica los valores éticos y morales.
- ❖ Un ser humano amante y practicante del civismo, la democracia, la solidaridad, la tolerancia y la convivencia en paz.
- ❖ Una persona con capacidad crítica, reflexiva y analítica, capaz de trascender y aportar al cambio positivo individual y social.
- ❖ Con capacidad de proyectarse responsablemente en las actividades familiares, sociales y laborales.
- ❖ Una persona preocupada por su continua formación como ser humano y en el campo del conocimiento.
- ❖ Un ser humano que ama la naturaleza, consciente de su protección y conservación, del uso racional de los recursos naturales, que promueve una cultura ecológica.
- ❖ Que pone en práctica la cordialidad, el amor, el respeto por la diferencia y la diversidad.
- ❖ Una persona que respeta y exige el respeto por los derechos humanos, la justicia, la equidad y la participación.
- ❖ Un ser humano consciente que debe mantener el equilibrio sano entre su mente y su cuerpo mediante la práctica del deporte, el fortalecimiento de su intelecto a través de la apropiación de lo conocido y la búsqueda de lo desconocido y lejos de todo vicio.
- ❖ Una persona que ame y defienda a su institución en cualquier escenario, que luche por ella y la represente dignamente, aportándole todo cuanto pueda por tratarse de un patrimonio que siempre estará al servicio de la comunidad.

2.1.1.4 Perfil De Docente

El perfil del docente de la institución Simón Bolívar es coherente con el perfil de sus estudiantes, teniendo en cuenta que la enseñanza guarda una estrecha relación con la práctica. El docente es al mismo tiempo un orientador y modelo a seguir y sus actos, además de ser pertinentes, deben estar fundamentados en los principios éticos, morales y profesionales; de tal manera que se identifiquen con la misión, visión y objetivos institucionales.

2.1.1.5 Perfil Del(A) Bachiller

La comunidad educativa de la institución Simón Bolívar reconoce a los y a las estudiantes como el eje central del quehacer formativo y centra todos sus esfuerzos para que al final del proceso, cuando ellos opten por el título de bachilleres, alcancen el siguiente perfil:

- ❖ Joven y señorita con conocimientos y competencias para continuar estudios superiores y/o desarrollar actividades laborales de manera responsable, ética y eficiente.
- ❖ Joven y señorita con capacidad crítica y de reflexión para entender la realidad de su entorno, proponer alternativas y contribuir con el cambio.
- ❖ Persona capaz de comprender la importancia y la necesidad de convivir en paz, de aplicar las buenas relaciones personales, de recurrir a la solución pacífica y concertada de los conflictos; de respetar la diferencia y diversidad, los derechos de los demás y cumplir con las responsabilidades que le son atribuibles.
- ❖ Con capacidad de reconocer, respetar, defender y apoyar en todo escenario la familia y la institución que le brinda su formación.
- ❖ Un ser humano en condiciones de dimensionar la importancia y poner en práctica las sanas costumbres, el rechazo de los malos hábitos, el respeto y el cuidado de los recursos naturales como fuente de vida.
- ❖ Persona que no solamente ha alcanzado nivel de conocimientos, sino que los pone al servicio de la sociedad.

2.2 ARCHIVO CORRIENTE

Para llevar a cabo el proceso de auditoría se hará una recopilación de documentos que tendrán que ver directamente con este desarrollo.

2.2.1. Programa de Auditoría.

Es importante señalar y detallar el trabajo a realizarse, los procedimientos a emplearse en la AUDITORIA INFORMATICA APLICADA AL AULA DE INFORMATICA DE LA INSTITUCION EDUCATIVA SIMON BOLIVAR DEL MUNICIPIO DE SAMANIEGO NARIÑO, así, esta auditoría se ejecutara mediante la aplicación de la metodología COBIT (Objetivos de Control para la Información y Tecnologías afines), dentro del cual existen 4 dominios, de los cuales se aplicaran los siguientes:

Objetivos de control para la Institución Educativa Simón Bolívar.

- ❖ **Planeación y organización:** Encargado de definir las estrategias y tácticas de las Tecnologías de la Información que permitan contribuir al logro y cumplimiento de los objetivos empresariales, a través del uso óptimo y conocimiento de los recursos de TI, apropiados para las necesidades de la empresa. En la ejecución de la auditoria a realizarse se aplican los siguientes procesos:

-Determinación de dirección tecnológica (PO3): Se evalúa la determinación de la dirección tecnológica para los Planes de Adquisición del Hardware, donde se evaluara las dependencias de valorización y planeación para que reflejen las necesi

dades identificadas en el plan de infraestructura tecnológica.

- PO3.1 Planeación de la Dirección Tecnológica: Analizar la tecnología existente en cuanto a la infraestructura de las comunicaciones y los servidores.
- PO3.2 Plan de Infraestructura Tecnológica: verificar que haya un plan de infraestructura tecnológica, evaluar planes de contingencia, evaluar procesos para la adquisición y la evolución de recursos tecnológicos.
- PO3.3 Monitoreo de Tendencias y Regulaciones Futuras: debe existir un proceso para monitorear las directrices del funcionamiento de la infraestructura tecnológica.

- PO3.4 Estándares Tecnológicos: evaluar si existen asesorías sobre el funcionamiento de la infraestructura, verificar si existen guías para la selección de la tecnología, medir el cumplimiento de estándares y directrices.

-Evaluación de riesgos(PO9): El objetivo es asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, mediante la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos.

- PO9.1 Marco de Trabajo de Administración de Riesgos: el área de sistemas deberá establecer un marco de referencia de evaluación sistemática de riesgos. Deberá contener una evaluación regular de los riesgos de la parte física de las comunicaciones y servidores e indicadores de cumplimiento.
 - PO9.2 Establecimiento del Contexto del Riesgo: establecer una metodología para la evaluación de riesgos, que garanticen resultados apropiados, bajo los criterios establecidos.
 - PO9.3 Identificación de Eventos: identificar riesgos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa), clasificar si son relevantes y en qué medida afectan los objetivos en este caso al área de sistemas y de la empresa.
 - PO9.4 Evaluación de Riesgos de TI: medir los riesgos, a través de la evaluación recurrente de la probabilidad e impacto de los riesgos identificados, usando métodos cuantitativos y cualitativos, que permitan obtener la magnitud del riesgo encontrado.
 - PO9.5 Respuesta a los Riesgos: definir un plan de acción contra riesgos, el proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos y así lograr mitigarlos.
 - PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos: priorizar y planear las actividades de control y respuesta a la solución de riesgos encontrados, teniendo en cuenta también la parte económica de la solución de esta prioridad. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.
- ❖ **Adquisición e implementación:** Para llevar a cabo la estrategia TI, se debe identificar las soluciones, desarrollarlas y adquirirlas, así como implementarlas e integrarlas en la empresa, esto para garantizar que las soluciones satisfaga los objetivos de la empresa. De este dominio se aplicaran las siguientes actividades:

-Adquisición y mantenimiento de la infraestructura tecnológica (AI3): El objetivo es proporcionar las plataformas apropiadas para soportar aplicaciones mediante la realización de una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema.

- AI3.1 Plan de Adquisición de Infraestructura Tecnológica: debe haber un plan que defina la adquisición, el mantenimiento de la infraestructura tecnológica, en este caso, en la parte física de las comunicaciones y de los servidores, un plan que satisfaga los requerimientos funcionales y técnicos de la empresa, se evaluara:

En cuanto a comunicaciones y a servidores, la capacidad, vida útil de los equipos tecnológicos, riesgos tecnológicos para la actualización de la tecnología al añadir capacidad técnica, proveedores de Red (Aprobados).

- AI3.2 Protección y Disponibilidad del Recurso de Infraestructura: para proteger los recursos tecnológicos, la empresa debe implementar medidas de control interno, seguridad y adaptabilidad durante la configuración, integración y mantenimiento de la infraestructura como es en este caso el hardware de los equipos de comunicación y de los servidores, que garanticen la disponibilidad e integridad de los recursos tecnológicos. Se debe monitorear y evaluar el uso y las responsabilidades de la utilización que se dé a estos componentes de infraestructura.
- AI3.3 Mantenimiento de la Infraestructura: la empresa debe desarrollar una estrategia de actualización y un plan de mantenimiento de la infraestructura, garantizar el control de los cambios de infraestructura tecnológica, incluir una revisión periódica contra las necesidades de la empresa, riesgos, identificar vulnerabilidades.
- AI3.4 Ambiente de Prueba de Factibilidad: Evaluar la efectividad y eficacia de la infraestructura, sobre todo en los procesos de adquisición, funcionalidad, configuración de hardware, pruebas de desempeño, estructura de Red.

-Adquirir recursos de TI (AI5) el objetivo es verificar y garantizar que la organización tenga todos los recursos de TI que se requieran de una manera oportuna y rentable.

- AI5.1 Control de Adquisición: evaluar el procedimiento general de adquisiciones y estándares de infraestructura tecnológica, como son instalaciones, hardware (Comunicaciones y servidores).
- AI5.2 Administración de Contratos con Proveedores: revisar los contratos con proveedores en cuanto la adquisición de infraestructura tecnológica, debe existir en la empresa un procedimiento establecido para modificar y concluir contratos para todos los proveedores.
- AI5.3 Selección de Proveedores: debe existir una lista de proveedores acreditados o un proceso de selección justa y viable de proveedores, que se ajuste a los requerimientos de la empresa.
- AI5.4 Adquisición de Recursos de TI: se debe proteger y cumplir los intereses de la empresa en todos los contratos de adquisición de infraestructura tecnológica, incluyendo los derechos y obligaciones de las partes en los términos contractuales.

❖ **Entrega de servicios y soporte:** Encargado de garantizar la entrega de los servicios requeridos por la empresa y se avalúan lo siguiente:

-Administración de las instalaciones (Ds12) Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

- DS12.1 Selección y Diseño del Centro de Datos: El área de sistemas debe definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia empresarial. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.
- DS12.3 Acceso Físico: La empresa debe definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.
- DS12.5 Administración de Instalaciones Físicas: se debe administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los

requerimientos técnicos y de la empresa, las especificaciones del proveedor y los lineamientos de seguridad y salud.

-Administración de la operación (Ds13) Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

- DS13.3 Monitoreo de la infraestructura de TI: Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.
- DS13.5 Mantenimiento preventivo del hardware: Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

Monitoreo y evaluación (ME): Monitorear y evaluar los procesos correspondientes al hardware de Comunicaciones y Servidores constantemente para asegurar el buen funcionamiento como también el desarrollo y cumplimiento de algunos Indicadores y que sigan las directrices implantadas por la empresa. Se aplicara lo siguiente:

- ✓ **Monitorear y evaluar el control interno (M2)** Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI. Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.
- ME2.1 Monitoreo del marco de trabajo de control Interno: deberá monitorear de forma continua, comparar y mejorar el ambiente de control de TI (infraestructura de la Red y de los equipos utilizados como

servidores) y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales.

- ME2.7 Acciones correctivas: Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

2.3. DISEÑO DE LOS ELEMENTOS DE AUDITORÍA.

Para el desarrollo de la Auditoria que permita evaluar la eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, servidores para la institución educativa Simón bolívar se utilizan los siguientes formatos de recolección de información.

Para dar comienzo a la auditoria, se realizaron diferentes entrevistas con el profesor de informática y el señor rector de la institución educativa Simón bolívar, información que sirve para el reconocimiento de los diferentes procesos, por tanto información clave para el desarrollo de este trabajo.

2.3.1. Cuadro de definición de fuentes de conocimiento.


Pruebas de análisis, y pruebas de auditoría: este cuadro es un instrumento que sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso dentro de los dominios del cobit, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar.

Los ítems relacionados a continuación son los que describirán los elementos de auditoría.

- ✓ **REF:** Identificación del cuadro de definición.
- ✓ **ENTIDAD AUDITADA:** En este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- ✓ **RESPONSABLES:** Nombre del auditor o auditores.
- ✓ **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.
- ✓ **MATERIAL DE SOPORTE:** En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.
- ✓ **DOMINIO:** Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.


- ✓ **PROCESO:** Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.
- ✓ **FUENTES DE CONOCIMIENTO:** Espacio que permite identificar las herramientas necesarias para obtener la información, puede ser a través de entrevistas, manuales, política, archivos físicos o magnéticos, reportes, contratos, etc.
- ✓ **REPOSITORIO DE PRUEBAS:** Se divide en dos tipos de pruebas:
 - **REPOSITORIO DE PRUEBAS DE ANALISIS:** espacio en el que describe el análisis de cada proceso y de la información obtenida.
 - **REPOSITORIO DE PRUEBAS DE EJECUCIÓN:** se describe las acciones a realizar para la ejecución de la auditoría, como las revisiones, verificaciones, pruebas y obtención de inconsistencias, etc

CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE ADITORIA			REF
ENTIDAD AUDITADA	INSITUCION EDUCATIVA SIMON BOLIVAR			
AREA AUDITADA	AULA DE INFORMATICA			
RESPONSABLE	RUBY HERNANDEZ MESA			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	MONITOREO Y EVALUACION	PROCESO	ME2. Monitorear y evaluar el control interno.	
DESCRIPCION DE ACTIVIDAD O PRUEBA				
FUENTES DE CONOCIMIENTO	REPOSITORIOS DE PRUEBAS APLICABLES DE ANALISIS		DE EJECUCION	

Cuestionario cuantitativo: permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar.


CUADRO CUESTIONARIO CUANTITATIVA

	CUESTIONARIO CUANTITATIVO			REF	
ENTIDAD AUDITADA	INSITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO				
RESPONSABLE	RUBY HERNANDEZ MESA				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	PLANEACION Y ORGANIZACIÓN (PO)	PROCESO	PO9 Determinar la Dirección Tecnológica		
PREGUNTA		SI	NO	NA	FUENTE
1.¿?					
2.¿?					
3.¿?					
TOTAL					
TOTAL CUESTIONARIO					

PORCENTAJE DE RIESGO

AUDITOR RESPONSABLE

Entrevistas preguntas abiertas y preguntas cerradas: técnica utilizada para la recolección de información amplia que permita aclarar dudas que dejan los cuestionarios. Los formatos utilizados para hacer las entrevistas están ajustados al personal del área de Sistemas, al personal técnico y en general a todo el personal involucrado en el personal del área de tecnologías de la Información y Comunicación. Se realizaron dos tipos de entrevistas: Entrevistas con preguntas Abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una. Entrevistas con preguntas cerradas: el entrevistado se limita a contestar Si o No, se recoge información útil para nuestra investigación, permitiendo en este formato adicionar la cantidad de algunos elementos y algunas observaciones.

		ENTREVISTA		REF	
ENTIDAD AUDITADA		INSITUCION EDUCATIVA SIMON BOLIVAR		PAGINA	
RESPONSABLE		RUBY HERNANDEZ MESA		1	DE 1
MATERIAL DE SOPORTE		COBIT			
DOMINIO		PROCESO			
ENTREVISTADO					
CARGO					

1.¿Qué hacen cuando se presenta un robo? ¿a quién acuden?

2.¿Qué hacen cuando se presenta un incendio o terremoto?

3.¿Se ha ideado un plan de contingencia para manejar estas situaciones?

4.¿El mantenimiento de los equipos lo hace personal especializado de la institución o externo?

5. ¿Qué procedimientos se hace cuando el hardware (equipos de cómputo, servidores o equipo de red) se daña?

6. ¿A qué lugar se llevan los equipos dañados?

7. ¿Cuánto tiempo se tardan en reparar los equipos?

8. ¿Cuales son los problema más frecuentes que se presentan en el aula de informática y como los resuelve?

9. ¿Cuándo se presentan daños por la energía a quien acuden?

10. ¿Conoce usted los planos del aula y redes?

ENTREVISTADO
FIRMA

AUDITOR RESPONSABLE
Ruby Hernández Mesa.

Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

Esta matriz fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

Matriz de probabilidad de impacto

Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

Probabilidad	Alto(3)	Riesgo Moderado (15)	Riesgo Importante (30)	Riesgo Inaceptable (60)
--------------	---------	----------------------	------------------------	-------------------------

	Medio(2)	Riesgo Tolerable (10)	Riesgo Moderado (20)	Riesgo Importante (40)
	Bajo(1)	Riesgo Aceptable (5)	Riesgo Tolerable (10)	Riesgo Moderado (20)
		Bajo(leve)(5)	Medio(moderado)(10)	Alto(catastrófico)(20)
	Impacto			

$$\% \text{ de Riesgo} = \frac{\text{Sumatoria de SI} * 100}{\text{Total Encuesta} - \text{Totales NA}}$$

$$\% \text{ Total de Riesgo} = 100 - \% \text{ de Riesgo}$$

Para determinar el nivel de riesgo total, se tuvo en cuenta la siguiente categorización:

- 1% - 30% = Riesgo Bajo
- 31% - 70% = Riesgo Medio
- 71% - 100% = Riesgo Alto

Riesgo bajo: Deficiencias bajas en grado de importancia mayor, fáciles de solucionar a largo plazo.

Riesgo medio: Se debe tomar medidas de solución o mejora en un determinado periodo de tiempo.

Riesgo alto: se debe establecer soluciones inmediatas para reducir el riesgo sin afectar los objetivos del caso de estudio.

Entonces, se calcula así:

$$\% \text{ de Riesgo Total} = 100 - \% \text{ de Riesgo}$$

2.3.2. Análisis y evaluación riesgos preliminares

		VALORACIÓN DE RIESGOS						REF
N°	RIESGOS/VALORACIÓN	PROBABILIDAD			IMPACTO			DOMINIO
		A	M	B	L	M	C	
R1	No se cuenta con un organigrama que especifique el área de informática			X	X			PO3
R2	No se cuenta con un manual de procedimientos		X			X		PO3
R3	No existe un plan de infraestructura tecnológica.		X			X		PO3
R4	No existe un plan de contingencia. No existe políticas para actuar en caso de desastre. No se han realizado simulacros. No hay ninguna estrategia para el manejo de TI		X			X		PO3
R5	No hay un plan de evaluación de riegos. No se ha hecho ningún estudio para determinar los riesgos. No existen unos procedimientos que nos diga que hacer en el momento del riesgo.	X					X	PO9
R6	No existen planes de acción.	X				X		PO9
R7	No existen estándares para la adquisición de infraestructura de TI.		X			X		AI3
R8	No existe un plan de mantenimiento.	X				X		AI3
R9	No existe un estándar para la escogencia de los proveedores.		X			X		Ai5
R10	No existe señalización adecuada.	X					X	DS12
R11	No existe un extintor de fuego en el aula de informática	X					X	DS12
R12	No cuenta con una iluminación adecuada	X					X	DS12

R13	No existen prohibiciones para fumar, consumir alimentos y bebidas. No tiene carteles que les recuerde estas prohibiciones.		X			X		DS12
R14	No existe una conexión eléctrica solo para el aula.	X					X	DS12
R15	No existen planos del aula ni de las redes.		X			X		DS12
R16	Los tomas no están debidamente marcados.		X			X		DS12
R17	No hay una bitácora de las fallas del hardware.		X			X		DS13
R18	No se posee una hoja de vida de los equipos.		X			X		DS13
R19	No se monitorea los mantenimientos			X		X		ME2
R20	No se monitorea que los usuarios cumplan con los requisitos mínimos para el uso de los equipos		X				X	ME2
R21	No se evalúa el funcionamiento del aula de informática		X			X		ME2

Probabilidad	Alto(3)		R6,R8	R5,R10,R11,R12,R14
	Medio(2)		R2,R3,R4,R7,R9,R13, R15,R16,R17,R18, R21	R20
	Bajo(1)	R1	R19	

	Bajo(leve)(5)	Medio(moderado)(10)	Alto(catastrófico)(20)
Impacto			

2.3.3. HALLAZGOS

Manual de navegación de hallazgos. En este manual se describe las inconsistencias encontradas.

Esta información será desglosada de la siguiente manera:

REF: Se refiere al ID del elemento.

ENTIDAD AUDITADA: En este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.


PROCESO: Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

HALLAZGO: Aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

CONSECUENCIAS Y RIESGOS: En este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

EVIDENCIAS: Aquí encontramos en nombre de la evidencia y el número del anexo donde ésta se encuentra.

RECOMENDACIONES: En este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a la entidad auditada.

	HALLAZGO		REF
RESPONSABLE	Ruby Hernández Mesa		
MATERIAL DE SOPORTE	COBIT		
DOMINIO		PROCESO	
HALLAZGO			

IMPACTO

RECOMENDACIÓN:

PROBABILIDAD – IMPACTO			
Probabilidad		Impacto	

HALLAZGO 1

	HALLAZGO			REF
				H-PO3
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO			
RESPONSABLE	Ruby Hernández Mesa			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	PLANEACION Y €	PROCESO	PO3.Determinar la dirección tecnológica.	
<p>HALLAZGO</p> <p>No tiene un plan de infraestructura tecnológica.</p> <p>No cuenta con un plan de contingencia.</p> <p>No se realizan simulacros</p>				

<p>CONSECUENCIA</p> <p>El plan de infraestructura tecnológica es importante tenerlo ya que permite tener una visión más completa de las metas que se quieren alcanzar a nivel de las TIC y de la empresa, el no hacerlo dificulta estas tareas.</p> <p>El plan de contingencia es de vital importancia tenerlo debidamente documentado porque permite saber cuáles son los procesos definidos para cada situación, y así poder garantizar el normal funcionamiento.</p> <p>Al no realizar los simulacros no se podría evaluar si los planes de acción definidos para ello funcionen y en caso de tener errores tomar los correctivos</p>

necesarios para que el plan de acción cumpla el objetivo para lo cual fue creado.

RECOMENDACIÓN

Construir un plan de infraestructura tecnológica el cual permitirá tener una competencia más acorde con los avances tecnológicos, donde se detalle un objetivo general que se quiere lograr e incluya las mejores opciones para poder tener una empresa más competitiva en el mercado cambiante, ya que si no se planea una buena adquisición tecnológica podría en poco tiempo quedar obsoleta.

Crear y documentar el plan de contingencia para que así puedan recurrir a los planes de acción previstos según sea la situación, se puedan llevar un orden en los procesos que se determinaron para poner en marcha los planes de acción en cuanto a la infraestructura tecnológica.

Realizar simulacros que permita evaluar la acción y reacción frente a las diferentes situaciones que se pueden presentar y dar una oportuna y certera solución de la situación.

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIO	Impacto	ALTO

HALLAZGO 2

	HALLAZGO			REF
				H-PO9
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO			
RESPONSABLE	Ruby Hernández Mesa			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	PLANEACION Y €	PROCESO	PO9 Evaluar y administrar los riesgos de TI	
<p>HALLAZGO</p> <p>No tiene un plan de evaluación de riesgos.</p> <p>Existen políticas y procedimientos para los riesgos pero no está debidamente documentados.</p>				

<p>CONSECUENCIA</p> <p>El plan de evaluación de riesgos es importante porque permite hacer un estudio detallado de los riesgos a los cuales está expuesta la institución educativa para poderlos evitar, reducir o mitigar, según su impacto.</p> <p>La no documentación de las políticas y procedimientos para los riesgos hace que la institución sea vulnerable y sean fácilmente omitidos.</p>

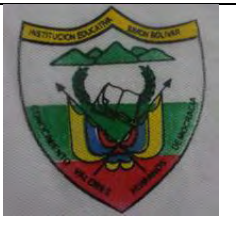
<p>RECOMENDACIÓN</p>

Hacer un estudio detallado de los riesgos para poder determinar su impacto el cual permite crear un plan de evaluación de riesgos, donde se categoricen según su impacto y se tomen las medidas más favorables al respecto.

Crear un documento donde estén contempladas todas las políticas y procedimientos que se tienen para evitar, reducir o mitigar los riesgos, el cual se debe socializar con toda la comunidad educativa (estudiantes, profesores, administrativos), para así aminorar los riesgos por falta de desconocimiento.

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIA	Impacto	ALTO

HALLAZGO 3

	HALLAZGO		REF
			H-AI3
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO		
RESPONSABLE	Ruby Hernández Mesa		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ADQUISICION IMPLEMENTACION	PROCESO	AI3 Adquisición y mantenimiento de la estructura tecnológica
HALLAZGO			

Se hace el mantenimiento pero no existe un plan de mantenimiento.

CONSECUENCIA

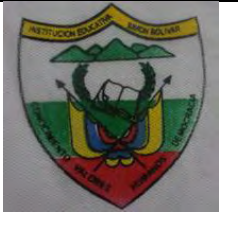
El no llevar un plan de mantenimiento hace que no se dé el mantenimiento preventivo sino correctivo, el cual implicaría pérdidas, más costos y tiempo.

RECOMENDACIÓN

En la institución educativa debe existir un plan de mantenimiento donde este calendarizado de manera que el mantenimiento preventivo cumpla su función y se lo ejecute periódicamente para obtener buenos resultados y se vean reflejados en el buen funcionamiento, aminorando así pérdidas, costos y tiempo.

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIA	Impacto	MEDIO

HALLAZGO 4

	<p>HALLAZGO</p>	<p>REF</p>
		<p>H-AI5</p>
<p>ENTIDAD AUDITADA</p>	<p>INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO</p>	
<p>RESPONSABLE</p>	<p>Ruby Hernández Mesa</p>	

MATERIAL DE SOPORTE	COBIT		
DOMINIO	ADQUISICION IMPLEMENTACION	E	PROCESO A13 Adquirir recursos TI.
HALLAZGO No existe un procedimiento estándar para la escogencia de los proveedores.			

CONSECUENCIA Al no existir un procedimiento estándar que regule este proceso se podría incurrir en fraude y conveniencia de alguna de las partes contratantes.
--

RECOMENDACIÓN En la institución educativa deben existir procesos o procedimientos que estén debidamente documentados que permitan hacer la adquisición de estos recursos de TI en una forma transparente y cumpliendo con las normas estipuladas para ello.

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIA	Impacto	MEDIO

HALLAZGO 5

	HALLAZGO			REF
				H-DS12
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO			
RESPONSABLE	Ruby Hernández Mesa			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	ENTREGA SERVICIO SOPORTE	DE Y	PROCESO	DS12 Administración de las instalaciones
<p>HALLAZGO</p> <p>No existe señalización adecuada de salida de emergencia y ruta de evacuación.</p> <p>No cuenta con medios de extinción de fuego en el aula de informática.</p>				

CONSECUENCIA

La no señalización de rutas de evacuación y salida de emergencia hace que los riesgos crezcan y en el momento de la emergencia no se las pueda encontrar.

No contar con un extintor de fuego dentro del aula hace que no se pueda evitar controlar la expansión del fuego causando pérdidas tanto materiales como humanas.

RECOMENDACIÓN

La institución educativa Simón Bolívar por ser una entidad pública, que presta un

servicio comunitario debe contar con la debida señalización de sus rutas de evacuación y salidas de emergencia, las cuales deben ser fáciles de observar en el momento de la emergencia.

Dotar al aula de informática de un extintor de fuego el cual debe estar en un lugar visible y de fácil acceso dentro del aula de informática.

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIA	Impacto	ALTO

HALLAZGO 6

	HALLAZGO		REF
			H-DS12
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO		
RESPONSABLE	Ruby Hernández Mesa		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGA SERVICIO SOPORTE	DE Y	PROCESO DS12 Administración de las instalaciones
HALLAZGO			
Existen prohibiciones de no fumar, consumir alimentos y bebidas pero no están documentadas, y no hay carteles dentro del aula que las recuerden..			

CONSECUENCIA

Al no acatar estas prohibiciones se pueden presentar diferentes situaciones como incendios, cortos circuito, etc. Que podrían ser evitadas

RECOMENDACIÓN

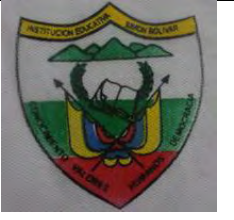
Documentar las prohibiciones para tomar las medidas correspondientes.

Hacer carteles que las den a conocer para se cumplan y así evitar circunstancias catastróficas y lamentables.

PROBABILIDAD – IMPACTO

Probabilidad	MEDIA	Impacto	ALTO
---------------------	-------	----------------	------

HALLAZGO 7

	HALLAZGO			REF
				H-DS12
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO			
RESPONSABLE	Ruby Hernández Mesa			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	ENTREGA SERVICIO	DE Y	PROCESO	DS12 Administración de

	SOPORTE		las instalaciones
<p>HALLAZGO</p> <p>La iluminación del aula no es adecuada.</p> <p>Tiene una planta eléctrica que es muy antigua y no está en funcionamiento.</p> <p>No se cuenta con los planos del aula y de las redes.</p> <p>Los cables no se encuentran dentro de los paneles</p>			

<p>CONSECUENCIA</p> <p>La poca iluminación del aula de informática puede ocasionar en los usuarios pérdida parcial o total de la visión.</p> <p>No contar con una planta eléctrica genera cese en las actividades académicas.</p> <p>No tener los planos del aula y las redes hace que las modificaciones o reparaciones se han mas dispendiosas y costosas.</p> <p>Los cables por fuera de los paneles son vulnerables, en el caso de las redes eléctricas son peligrosos.</p>			
--	--	--	--

<p>RECOMENDACIÓN</p> <p>Se debe gestionar ante la administración de la institución educativa lámparas o bombillas para dar una mejor iluminación al aula.</p> <p>Gestionar recursos para la adquisición de una nueva planta eléctrica, se podría dar la planta vieja en parte de pago, para así garantizar una continuidad en las clases que utilicen esta sala de informática.</p> <p>Se recomienda a la institución educativa levantar los planos del aula y las redes de datos, corriente normal y regulada para así tener claro cuáles son los ductos que les corresponden a cada red y no se cause daños innecesarios.</p>			
--	--	--	--

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIA	Impacto	MODERADO

HALLAZGO 8

	HALLAZGO			REF
				H-DS12
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO			
RESPONSABLE	Ruby Hernández Mesa			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	ENTREGA SERVICIO SOPORTE	DE Y	PROCESO	DS12 Administración de las instalaciones
HALLAZGO				
<p>Los tomas del aula de informática no están debidamente marcados.</p> <p>No existe una instalación eléctrica alterna.</p> <p>No se cuenta con un reglamento para estudiantes, profesores y personal.</p>				

CONSECUENCIA
Las tomas no marcadas pueden generar daños en los equipos, ya que la institución cuenta con dos cargas eléctricas de 110 y 220.

No tener una instalación alterna en caso de corto circuito su recuperación y funcionalidad tardaría.

La falta de reglamentos hace que los equipos estén más expuestos a daños y que los usuarios no tengan ninguna penalización por los daños causados.

RECOMENDACIÓN

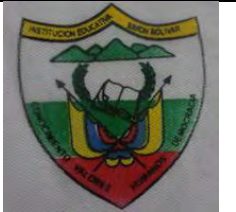
La institución educativa debe encargarse de marcar los tomas.

Debe proveerse de una instalación alterna que se pueda utilizar en caso de que la instalación principal falle.

Se debe implementar un reglamento para los usuarios del aula de informática, que contenga las prohibiciones y sus respectivas sanciones al desacato de ellas.

PROBABILIDAD – IMPACTO			
Probabilidad	MEDIO	Impacto	MODERADO

HALLAZGO 9

	HALLAZGO	REF
		H-DS13
ENTIDAD AUDITADA	INSTITUCION EDUCATIVA SIMON BOLIVAR SAMANIEGO	
RESPONSABLE	Ruby Hernández Mesa	
MATERIAL DE SOPORTE	COBIT	

DOMINIO	ENTREGA SERVICIO SOPORTE	DE Y	PROCESO	DS13 Administración de la operación
HALLAZGO				
Los equipos no tienen una hoja de vida.				

CONSECUENCIA
Al no llevar un registro de las fallas y reparaciones que se le han hecho al hardware en una hoja de vida del equipo hace que las prevenciones o correcciones futuras no se hagan adecuadamente.

RECOMENDACIÓN
Elaborar hojas de vida de los equipos de cómputo, servidores y equipos de red que permitan llevar un seguimiento para prevenir y corregir inconvenientes a futuro.

PROBABILIDAD – IMPACTO			
Probabilidad	BAJO	Impacto	MODERADO

2.3.4. INFORME EJECUTIVO

Pasto, 25 de febrero de 2016.

Señor:

RAMIRO TORO

Rector€ Institución Educativa Simón Bolívar.

Samaniego.

Ref. AUDITORIA INFORMATICA APLICADA A LA INSTALACION FISICA Y HARDWARE DEL AULA DE INFORMATICA DE LA INSTITUCION EDUCATIVA SIMON BOLIVAR DEL MUNICIPIO DE SAMANIEGO NARIÑO.

El presente informe de auditoría tuvo como objetivo principal evaluar la instalación física y hardware tales como equipos de cómputo, servidores y equipos de red en el aula de informática; los resultados que se obtuvieron fueron mediante la aplicación de técnicas y herramientas de auditoría, las cuales tuvieron como fuente principal de conocimiento la información suministrada por parte de las personas directamente relacionadas con el aula de informática.

Arrojando los siguientes resultados:

INSTALACION FISICA

En la evaluación de la instalación física se resalta que tiene suficiente espacio para trabajar, el material con que está construido es duradero y fácil de limpiar, la ubicación es estratégica porque no tiene necesidad de instalar ductor de aire acondicionado que mantenga la temperatura ideal que los equipos necesitan, además los protege del polvo que es uno de los factores que contribuye al mal funcionamiento de los equipos, también cuenta con cámaras de seguridad y alarma.

Sin embargo también se encontraron falencias como la falta de señalización de la salida de emergencia, ruta de evacuación, para carteles que prohíban fumar, el ingreso de alimentos y bebidas dentro del aula, un extintor de fuego, cables por fuera de los canales, tomas sin marcar y poca iluminación.

Se recomienda elaborar la respectiva señalización, implementar el aula con carteles de las prohibiciones, adquirir un extintor de fuego, adecuar el aula de tal manera que los cables estén dentro su canaletas correspondientes, los tomas marcados y más bombillos o lámparas para una mejor organización del aula.

HARDWARE

En la evaluación del hardware se encontró que cuenta con un inventario actualizado de los equipos, un control de las entradas y salidas de los usuarios, la instalación eléctrica no es independiente de la instalación general pero tiene break que permiten la suspensión eléctrica según el área que se requiera.

Se detectó las siguientes falencias no se lleva una hoja de vida de los equipos donde se registre las fallas que han presentado y los mantenimientos que se les ha hecho a lo largo de su vida útil, no cuentan con una planta eléctrica, UPS que garantice su funcionamiento en la ausencia de electricidad.

Se recomienda elaborar una hoja de vida de los equipos, servidores, equipos de red, donde se especifique fecha de la falla, fecha de mantenimiento, tiempo que duro la falla, la reparación y repuestos utilizados. Dotar de una planta eléctrica, UPS que contribuyan y gestionar la implementación de una red alterna en el caso de que la red principal falle para que se dé un buen funcionamiento de los equipos

PROCEDIMIENTOS

En cuanto a procedimientos se encontró que existe un control de las personas que ingresan al aula de informática ya que se lo hace mediante la asistencia, la adquisición de recursos TI e infraestructura tecnológica se hace mediante tres cotizaciones las cuales son evaluadas por el comité de bienestar quien escoge la mejor propuesta.

Las falencias que se encontraron fueron que no existe un plan de contingencia, un plan de riesgos, políticas y procedimientos acerca de la seguridad física y lógica de los equipos debidamente documentada, un plan de mejoramiento, políticas y procedimientos para la adquisición de hardware debidamente documentada, y simulacros.

Se recomienda elaborar un plan de contingencia donde se estipule los procesos y procedimientos a seguir para dar una solución adecuada a la situación que se presente; hacer un estudio a los riesgos que está expuesta el aula de informática para determinar su impacto y elaborar con esto un plan de riesgos donde se contemple todos los procesos y procedimientos a seguir para evitar, disminuir o mitigar el riesgo, se debe realizar simulacros permanentes para detectar las fallas que se puedan presentar y poderlas corregirlas a tiempo.

La adquisición de hardware se debe hacer mediante un proceso estándar que debe estar documentado para garantizar transparencia en la compra.

Este trabajo se pudo realizar gracias a la colaboración del señor rector Ramiro Toro y el profesor Rodrigo Imues quienes estuvieron prestos a darme toda la información que se requiso para el desarrollo del presente proyecto.

Atentamente,

Ruby Hernández Mesa

Auditor

CONCLUSIONES

La auditoría informática permitió que mediante herramientas de recolección de información y con el programa COBIT se detectó las fortalezas y debilidades que tiene la institución educativa Simón Bolívar.

Mediante los dominios y objetivos de control del programa COBIT se pudo establecer planes de contingencia, riesgos, mantenimiento y acción para obtener un funcionamiento óptimo de la institución educativa Simón Bolívar específicamente el aula de informática.

Uno de los mayores retos que se presentó fue elaborar los cuestionarios que pudieran abarcar toda la información que se requiriera para su posterior análisis y clasificación según su probabilidad e impacto.

El modelo COBIT es una herramienta que puede ser utilizada en cualquier empresa sea cual sea su razón social, además sus dominios y objetivos de control son aplicables en todos los procesos que tiene la empresa que es auditada.

RECOMENDACIONES

Crear políticas y procedimientos que contribuyan a la seguridad tanto física como lógica del aula de informática.

Crear procesos que estén debidamente documentados para así evitar toda clase de fraude o manipulación inadecuada en cuanto a adquisición de recursos tecnológicos.

Realizar planes de mejoramiento que permitan mantener el funcionamiento del aula de informática.

Adecuar el aula de informática bajo los estándares para así evitar algún riesgo que se pueda presentar, ya sea porque no cuenta con los carteles necesarios donde le recuerden las prohibiciones o por que algún toma no está debidamente marcado o los cable de la red eléctrica estén fuera de las canaletas dispuestas para ellos.

BIBLIOGRAFIA

Echenique García, José Antonio. Auditoría en Informática. 2 Edición. México: Mc Graw Hill, 2001.

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed, Alfaomega/RA-MA, México D.F, 2001.

Auditoria Informática, Wikipedia .

http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

Importancia de la auditoría informática en las organizaciones, Nubia Fernández Grajales.

http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica