UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES

TEMA:

ESTUDIO DE LA METODOLOGÍA COBIT 3ª EDICIÓN (OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y LAS TECNOLOGÍAS RELACIONADAS) – IT GOVERNANCE Y CONTROL OBJETIVES, APLICADOS A LA AUDITORÍA Y SEGURIDAD INFORMÁTICA.

APLICATIVO:

APLICACIÓN DE LA METODOLOGÍA COBIT 3ª EDICIÓN EN LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL GOBIERNO PROVINCIAL DE IMBABURA A TRAVÉS DEL DISEÑO E IMPLEMENTACIÓN DE LA GUÍA AUTOMATIZADA COBIT.

AUTORA: FERNANDA GEOCONDA ENDARA NÉJER
DIRECTOR: ING. JORGE CARAGUAY PROCEL
ASESORA: DRA. MARÍA DE LA PORTILLA VERA

IBARRA, FEBRERO DEL 2011

CERTIFICACIÓN

La elaboración de la tesis previa a la obtención del título de Ingeniera en Sistemas Computacionales con el tema: Estudio de la Metodología CObIT 3ª Edición (Objetivos de Control para la Información y las Tecnologías Relacionadas) – IT Governance y Control Objetives, aplicados a la Auditoria y Seguridad Informática, aplicativo: Aplicación de la Metodología CObIT 3ª Edición en la Dirección de Tecnologías de la Información y Comunicaciones del Gobierno Provincial de Imbabura a través del diseño e implementación de la Guía Automatizada CObIT, ha sido desarrollada y terminada en su totalidad por la Srta. Fernanda Geoconda Endara Néjer, con C.I.: 1002734406, bajo mi supervisión para lo cual firmo en constancia.

Atentamente,

_____

Ing. Msc. Jorge Caraguay
DIRECTOR DE TESIS

AGRADECIMIENTO

Al culminar este proyecto agradezco a Dios, Padre celestial te enaltece mi corazón porque eres nuestra Torre fuerte, amparo y refugio, gracias por tus bendiciones y la presencia de tu amor en cada uno de nuestros días.

A mis hermanos Stalin y Tania, quienes con sus valiosas ideas y apoyo incondicional fueron guía para llegar al cenit de mis aspiraciones.

Un agradecimiento especial al Ing. Jorge Caraguay y, a la Dra. María de la Portilla, por su asesoramiento técnico y orientación en el estudio y desarrollo de la presente tesis, su carisma y don de ser, hacen de ustedes personas excepcionales.

DEDICATORIA

El presente trabajo va dedicado a Lucía, quien con sacrificio, amor y tenacidad nos enseñó a luchar por alcanzar nuestras metas e ideales, sin ti madre esta investigación no habría sido posible.

"Madre eres mi fuerza que me da seguridad, mi roca y mi fortaleza, eres el escudo que me das la victoria para alcanzar el cenit y la gloria".

Salmo 18:17

ÍNDICE

CAPÍTULO I: LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

CAPÍTULO II: ESTÁNDARES Y NORMAS INTERNACIONALES DE AUDITORÍA

CAPÍTULO III: ESTÁNDARES Y LEGISLACIONES INTERNACIONALES PARA LA ADMISTRACIÓN DE LA SEGURIDAD Y CONTROL DE TI

CAPÍTULO IV: COBIT - OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS
(Control Objetives For Information And Related Technology)

CAPÍTULO V: APLICACIÓN DE LA METODOLOGÍA COBIT EN LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL GOBIERNO PROVINCIAL DE IMBABURA A TRAVÉS DE LA GUÍA AUTOMATIZADA COBIT

CAPÍTULO VI: DESARROLLO DEL APLICATIVO GUÍA AUTOMATIZADA DE CObIT

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

CAPÍTULO I: LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

CAPÍTULO IV: COBIT CONTROL OBJETIVES FOR INFORMATION AND RELATED TECHNOLOGY

(Objetivos de Control para la Información y Tecnologías Relacionadas)

CAPÍTULO VI: CAPÍTULO VI: DESARROLLO DEL APLICATIVO GUÍA AUTOMATIZADA DE CObIT.

ÍNDICE DE FIGURAS

CAPÍTULO I: LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

CAPÍTULO III: ESTÁNDARES Y LEGISLACIONES INTERNACIONALES PARA LA ADMISTRACIÓN DE LA SEGURIDAD Y CONTROL DE TI

CAPÍTULO IV: COBIT OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS CONTROL (Control Objetives For Information And Related Technology)

CAPÍTULO V: APLICACIÓN DE LA METODOLOGÍA COBIT EN LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL GOBIERNO PROVINCIAL DE IMBABURA A TRAVÉS DE LA GUÍA AUTOMATIZADA COBIT

CAPÍTULO VI: DESARROLLO DEL APLICATIVO GUÍA AUTOMATIZADA DE CObIT

RESUMEN EJECUTIVO

El entusiasmo popular por la creciente tecnología, ha hecho que el uso de la Información y Tecnología de Comunicaciones se vuelva intrínseco para el funcionamiento y bienestar de las organizaciones, y así como las iniciativas o nuevas prácticas comerciales maduran o se desarrollan, surgen con ellas los riesgos en las organizaciones que necesitan ser supervisados y administrados eficazmente.

La organización de hoy, debe tener definido su horizonte informático donde se tengan claros los riesgos inherentes y potenciales, así como las necesidades de esta respecto a la seguridad informática.

Es allí donde la Auditoría conduce la atención del carácter dinámico y a la naturaleza interrelacionada de las empresas, su gestión y su entorno, al análisis del riesgo, a los componentes técnicos y procedimentales de la administración de la Seguridad Informática, con elementos conceptuales y prácticos para que las empresas puedan orientar y aplicar directrices y alinearlas con el negocio.

De esta manera el auditor en seguridad informática asesora a la Gerencia recomendando procedimientos o protocolos para la prevención o corrección de procesos de seguridad, procurando a la luz de referentes internacionales, establecer las mejores alternativas en los temas críticos de la empresa donde la seguridad informática articule las necesidades operativas y las estratégicas de la organización.

SUMMARY

The popular enthusiasm for the growing technology, has made that the use of the Information and Technology of Communications becomes intrinsic for the operation and well-being of the organizations, and as well as the initiatives or new commercial practices mature or they are developed, the risks arise with them in the organizations that need to be supervised and administered efficiently.

Today's organization, should have defined their computer horizon where they are had clear the inherent and potential risks, as well as the necessities of this regarding the computer security.

It is there where the Audit drives the attention of the dynamic character and to the interrelated nature of the companies, it's administration and it's environment, to the analysis of the risk, to the technical and procedural components of the administration of the Information Security, with conceptual and practical elements so that the companies can guide and to apply guidelines and to align them with the business.

This way the auditor in information security advice to the Management recommending procedures or protocols for the prevention or correction of processes of security, offering by the light of relating international, to establish the best alternatives in the critical topics of the company where the information security articulates the operative necessities and the strategic of the organization.

CAPÍTULO I

LA AUDITORÍA
Y SEGURIDAD INFORMÁTICA

CONTENIDO

- INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA
- DEFINICIÓN DE AUDITORÍA INFORMÁTICA
- CLASES DE AUDITORÍA
- ÁREAS ESPECÍFICAS DE LA AUDITORÍA INFORMÁTICA
- HERRAMIENTAS Y TÉCNICAS DE AUDITORÍA INFORMÁTICA
- LA SEGURIDAD INFORMÁTICA
- ATAQUES A LA SEGURIDAD INFORMÁTICA
- MÉTODOS Y HERRAMIENTAS DE ATAQUE
- ANÁLISIS DE RIESGOS
- TÉCNICAS DE ASEGURAMIENTO
- GESTIÓN DE LA SEGURIDAD INFORMÁTICA
- LA SEGURIDAD UN PROBLEMA INTEGRAL
- METODOLOGÍAS Y NORMAS INTERNACIONALES EN LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

CAPÍTULO I

LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

1.7. INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA

Inicialmente, la auditoría se limitó a las verificaciones de los registros contables, dedicándose a observar si los mismos eran exactos, caracterizándose así, por centrar toda su atención en el área financiera y administrativa, de allí su importancia, que es reconocida desde los tiempos más remotos, teniéndose conocimientos de su existencia ya en las lejanas épocas de la civilización sumeria.

Sin embargo con el surgir de los tiempos, el campo de acción de la auditoría ha continuado extendiéndose en el ámbito organizacional, incorporándose a este trabajo un elemento esencial que es la Auditoría Informática, ya que en la actualidad, las tecnologías de la información están presentes en todas las áreas de las organizaciones, y que ésta, se encuentra en un 90% automatizada, haciendo que la Informática esté subsumida en la gestión integral de la empresa, en consecuencia entonces, la incursión de la auditoría en el ámbito informático, donde:

- El control de la función informática
- El análisis de la eficiencia de los Sistemas Informáticos que soporta,
- La verificación del cumplimiento de la normativa general de la empresa en este ámbito y,
- La revisión de la eficaz gestión de los recursos materiales y humanos informáticos. [LIB.001]

Son algunos de sus objetivos principales, proporcionándole a la organización de esta manera una base sólida para el desempeño diario de sus funciones.

Es por esto que en la actualidad, la Auditoría Informática es parte integral de las empresas, para ofrecer productos y servicios de alta calidad que se ajusten a las necesidades y preferencias del mercado, donde la información y la tecnología que la soporta, representan los activos más valiosos de la entidad, reconociendo así los beneficios potenciales que esta puede proporcionar para el éxito y la supervivencia de las mismas.

1.8. DEFINICIÓN DE AUDITORÍA INFORMÁTICA

Conceptualmente la Auditoría Informática ha sido definida bajo diversos criterios, y debido a su basto campo de aplicabilidad, es preciso hacer ciertas consideraciones, por ello citaremos a continuación varios puntos de vista que se hacen respecto a la definición de la Auditoría Informática.

Echenique define: *"Auditoría Informática es la revisión y 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 la adecuada toma de decisiones"*[1].

Acha conceptualiza a la Auditoría Informática de la siguiente forma: *"Se define como el conjunto de Procedimientos y Técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente"*[2]

[1] Echenique, José A. http://campus.uab.es/~2082564/indice2.htm
[2] Acha Iturmendi , J. José. "Auditoría Informática en la Empresa". Editorial Parainfo, 1994

En sus publicaciones Emilio Del Peso define: *"La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o alguna de sus áreas, los estándares y los procedimientos en vigor, su idoneidad y el cumplimiento de estos, los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y análisis de riesgos"*[3]

La ISACA (Information Systems Audit. and Control Association) la define de la siguiente manera: *"La auditoría de los sistemas de información abarca la revisión y evaluación de todos los aspectos (o cualquiera de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes"*[4]

En conclusión, la Auditoría Informática evalúa los sistemas informáticos a través de un conjunto de procedimientos y técnicas, con el fin de constatar si sus actividades son correctas, y si estas están de acuerdo a las normativas informáticas generales prefijadas en la organización; y también, evalúa a personas independientes y técnicamente competentes del entorno informático, sus funciones e idoneidad, la gestión de recursos, así como el cumplimiento de objetivos y políticas, abarcando de esta manera, todas o algunas de las áreas de la empresa.

Por tanto queda establecido, que la auditoría informática es un órgano de control de instituciones estatales y privadas, absolutamente independiente; no tiene carácter ejecutivo, contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones, así como también si es el caso, hace las respectivas sugerencias y planes de acción a tomarse.

[3] Del Peso, Emilio. "La Auditoría de los Sistemas de Información". http://www.iee.es/; Julio 2001.
[4] CNAACSI, Concejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información. "Normas Generales para la Auditoría de los Sistemas de Información ". http://www.isaca.org/; Mayo 2007.

1.9. CLASES DE AUDITORÍA

1.9.1. AUDITORÍA INFORMÁTICA EXTERNA

La Auditoría Informática Externa presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados, ya que es realizada por personas sin vínculos laborales afines a la empresa auditada, aplicando exámenes críticos, sistemáticos y detallados y técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como operan los sistemas de información, el control interno de los mismos y formular sugerencias para su mejoramiento.

El dictamen u opinión independiente tiene trascendencia a los terceros, pues da plena validez a la información generada por el sistema, ya que se produce bajo la figura de la Fe Pública, que obliga a los mismos a tener plena credibilidad en la información examinada.

La Auditoría Informática Externa o Independiente tiene por objeto averiguar la razonabilidad, integridad y autenticidad de toda la información producida por los sistemas de la organización, y se lleva a cabo cuando se desea publicar el producto del sistema de información examinado, con el fin de acompañar al mismo una opinión independiente que le dé autenticidad y permita a los usuarios de dicha información tomar decisiones confiando en las declaraciones del Auditor.

1.9.2. AUDITORÍA INFORMÁTICA INTERNA

La Auditoría Informática Interna, es el examen crítico, sistemático y detallado, realizado con recursos materiales y personas que pertenecen a la empresa auditada, utilizando técnicas determinadas con el objeto de emitir informes y

formular sugerencias para el mejoramiento de la misma. Los informes son de circulación interna y no tienen trascendencia a los terceros pues no se producen bajo la figura de la Fe Publica. La auditoría interna existe por expresa decisión de la empresa, o sea, que puede optar por su disolución en cualquier momento.

Los auditores internos tienen a su cargo la evaluación permanente del control de las operaciones y se preocupan en sugerir el mejoramiento de los métodos y procedimientos de control interno que redunden en una operación más eficiente y eficaz.

La imparcialidad e independencia absolutas no son posibles en este caso, puesto que no puede separarse completamente de la influencia de la alta administración, y aunque mantenga una actitud independiente como debe ser, esta puede ser cuestionada ante los ojos de los terceros.

Este tipo de auditoría interna es un servicio que reporta al más alto nivel de la dirección de la organización y tiene características de función asesora de control, la auditoría interna solo interviene en las operaciones y decisiones propias de su oficina, pero nunca en las operaciones y decisiones de la organización a la cual presta sus servicios, pues como se dijo es una función asesora.

La Auditoría Informática Interna cuenta con algunas ventajas adicionales muy importantes respecto de la Auditoría Informática Externa; la auditoría interna tiene la ventaja de que puede actuar periódicamente realizando revisiones globales, como parte de su plan anual y de su actividad normal, donde la informática trata de satisfacer lo más adecuadamente posible aquellas necesidades de la empresa, y esta necesita controlar su informática ya que su propia gestión esta sometida a los mismos procedimientos y estándares que el resto de aquella. [WWW.001]

1.10. ÁREAS ESPECÍFICAS DE LA AUDITORÍA INFORMÁTICA

Dentro de las áreas generales de la Auditoría Informática se establecen las siguientes divisiones: de Sistemas, de Comunicaciones, Desarrollo de Proyectos, y Seguridad, que comprenden las Áreas Específicas de la Auditoría Informática más importantes.

Cada Área Específica puede ser auditada desde los siguientes criterios generales:

- 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.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

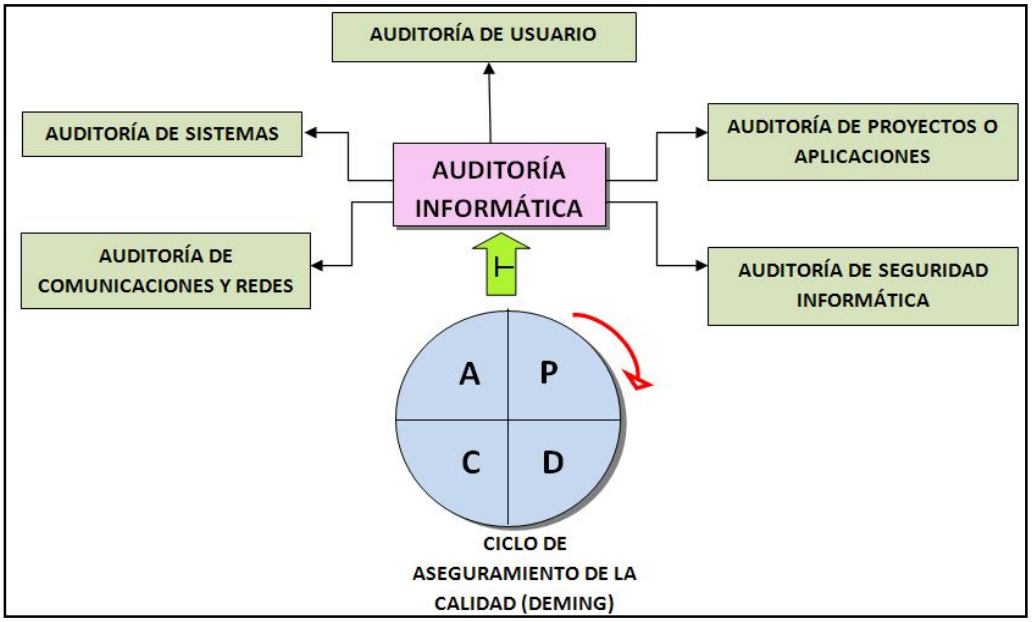


Fig. 1.1. La Auditoría Informática y el Ciclo del aseguramiento de la Calidad

1.10.1. AUDITORÍA INFORMÁTICA DE SISTEMAS

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Dentro de esta se contemplan:

- Sistemas Operativos
- Software Básico
- Optimización de los Sistemas y Subsistemas
- Administración de Base de Datos
- Investigación y Desarrollo

1.10.2. AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES

Para el informático y para el auditor informático, el entramado conceptual que constituyen las redes nodales, redes locales, concentradores, multiplexores, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor puede tropezar con dificultades técnicas del entorno en el análisis de situaciones y hechos alejados entre sí, debido a que las instalaciones están asociadas al establecimiento de los puestos de trabajo correspondientes. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales.

La Auditoría de Comunicaciones inquiere sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso, donde se provee la topología de la Red de Comunicaciones, actualizada. 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.

1.10.3. AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS O APLICACIONES

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Concisamente, una Aplicación recorre las siguientes fases:

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

Estas fases deben estar sometidas a un exigente control interno. Finalmente, la auditoría comprobará la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros. [WWW.002]

1.10.4. AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

En la actualidad el ordenador 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 haciendo un incorrecto uso de esta. También pueden ocurrir robos, fraudes o sabotajes 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.

El auditar los sistemas comienza desde el uso inadecuado del computador, así como 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.

1.10.5. AUDITORÍA INFORMÁTICA DE USUARIO

El departamento de Informática posee una actividad proyectada al usuario de la empresa, que representa auditoría informática de usuario; su objeto es conocer sobre los servicios que provee el departamento de Sistemas, así como la difusión de las aplicaciones de computadora y de los sistemas en operación, para determinar si los servicios proporcionados y planeados por la dirección de Informática cubren las necesidades de información de las dependencias

El control del funcionamiento del departamento de informática con el usuario, se realiza por medio de la Dirección. Su figura es importante, en tanto y en cuanto es capaz de interpretar las necesidades de la Compañía.

1.11. HERRAMIENTAS Y TÉCNICAS DE AUDITORÍA INFORMÁTICA

1.11.1. CUESTIONARIOS

Las auditorías informáticas se realizan obteniendo información y documentación de todo tipo. Los informes finales dependen de las capacidades del auditor para analizar las situaciones sean estas de debilidad o fortaleza de los

diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la posterior emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para ello, se comienza solicitando el cumplimiento de cuestionarios que se envían a las personas concretas que el auditor cree apropiadas. Estos cuestionarios no pueden ni deben ser repetidos, sino diferentes, muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Con y sobre esta base, se estudia y analiza la documentación recibida, de manera que el análisis determine la información que deberá elaborar el propio auditor. El cruzamiento de información es una de las bases fundamentales de la auditoría.

1.11.2. ENTREVISTAS

El auditor comienza las relaciones personales con el auditado por medio de entrevistas, en las que el auditor sigue un método preestablecido y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante realizadas por el auditor; en ellas, se recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

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, 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.

1.11.3. CHECKLIST

El auditor profesional, reelabora muchas veces sus cuestionarios en función de los escenarios auditados. 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, muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para el cumplimiento sistemático de sus Cuestionarios, de sus Checklists.

Con profesionalismo el auditor, pasará la información por un procesamiento interno a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes, hasta poseer preguntas muy estudiadas que han de formularse flexiblemente. El conjunto de estas preguntas recibe el nombre de Checklist.

Según la claridad de las preguntas, el auditado responderá desde posiciones muy distintas y con disposición muy variable a las preguntas que éste le formula, 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, sobre bases de autoridad, prestigio y ética.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas, claro esta que bajo apariencia distinta, donde el auditor formulará preguntas equivalentes, de este modo, se podrán descubrir con mayor facilidad los puntos contradictorios. 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. [WWW.003]

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de calificación o evaluación:

1.11.3.1.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.

AUDITORÍA SOBRE LA SEGURIDAD FÍSICA DE UNA INSTALACIÓN	
	P: ¿Existe personal específico de vigilancia externa al edificio? **R:** No, solamente un guardia por la noche que atiende a otra instalación adyacente. **Puntuación: 1**
VALORACION **1:** Muy deficiente **2:** Deficiente **3:** Mejorable	**P:** Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo? **R:** Si, pero sube a las otras 4 plantas cuando se le necesita. **Puntuación: 2** **P:** ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas? **R:** Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan. **Puntuación: 2**

Tabla 1.1. Ejemplo de un Checklist de Rango

1.11.3.2.CHECKLIST BINARIA

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente equivalen a: 1(uno) o 0(cero), respectivamente.

REVISIÓN DE MÉTODOS DE PRUEBAS DE PROGRAMAS
P: ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas? **Puntuación: 1**
P: ¿Conoce el personal de Desarrollo la existencia de la anterior normativa? **Puntuación: 1**
P: ¿Se aplica dicha norma en todos los casos? **Puntuación: 0**
P: ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

Tabla 1.2. Ejemplo de un Checklist Binario

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 ser auditadas. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

1.11.4. TRAZAS Y/O HUELLAS

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 potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

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.

En lo referente al análisis del Sistema, se 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. Los parámetros variables deben estar dentro de un intervalo marcado por el fabricante. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

1.11.5. SOFTWARE DE INTERROGACIÓN

Desde ya hace algunos años atrás se han utilizado productos Software llamados genéricamente *"paquetes de auditoría",* capaces de generar programas para auditores, que más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieron la obtención de consecuencias e hipótesis de la situación real de una determinada instalación.

En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del Software nativo propio de la instalación.

Así, del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de Software a desarrollar interfaces de transporte de datos entre computadores personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía y efectivamente, conectados como terminales al Host, almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. Por ello el auditor se ve obligado, dependiendo del alcance de la auditoría, a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos anteriormente descritos. [WWW.004]

1.12. LA SEGURIDAD INFORMÁTICA

La Seguridad Informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, que estos a su vez precisan de un nivel organizativo.

Sistema de Seguridad = TÉCNOLOGIA + ORGANIZACIÓN

Tabla 1.3. Niveles de Seguridad

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia, que nos indica que esta libre de peligro o daño. Ciertamente el elemento de riesgo esta siempre presente, independiente de las medidas que se tomen, por lo que en si, se habla de niveles de seguridad.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etcétera. La seguridad lógica se refiere a la seguridad de uso del Software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información

1.12.1. CRITERIOS PARA LA SEGURIDAD INFORMÁTICA

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (Hardware, Software y datos), y son estos los principales sujetos de protección de las técnicas de seguridad, por ello la seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información para que un sistema se pueda definir como seguro.

1.12.1.1.CONFIDENCIALIDAD

La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas" la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

1.12.1.2.INTEGRIDAD

La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de

transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

1.12.1.3.DISPONIBILIDAD

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental, situaciones fortuitas o de fuerza mayor.

No todos los riesgos que amenazan la información son de origen dañino. Es por ello que las medidas de seguridad no deben limitarse a la protección contra ataques e intrusiones de terceros, pues dentro de la misma organización y por parte de individuos de confianza existen riesgos contra la disponibilidad de la información ya sea por negligencia, descuido, ignorancia o cualquier otro tipo de mala práctica, la información puede ser alterada, sustituida o permanentemente borrada. Además están siempre presentes los riesgos de pérdida o alteración por virus o situaciones fortuitas de fuerza mayor, tales como incendios, inundaciones o catástrofes naturales. [WWW.005]

1.12.2. POLÍTICAS DE SEGURIDAD

Una política de seguridad generalmente se ocupa exclusivamente de asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio. La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.
- Sensibilizar los operadores con los problemas ligados con la seguridad de los sistemas informáticos. Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida.

1.12.3. ANÁLISIS DE RIESGOS

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales esta se almacene.

Estas técnicas las brindan la seguridad lógica, que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Los objetivos para conseguirlo son:

- Restringir el acceso: de personas de la organización y de las que no lo son a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.

- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o Software empleados.

1.12.4. TÉCNICAS DE ASEGURAMIENTO

Las técnicas de aseguramiento informático están estrechamente asociadas a las características que rigen el mercado de Tecnologías de la Información (TI), ya que, el Hardware, Software y los servicios especializados, son parte de la dinámica de la función de seguridad informática en las organizaciones. A continuación se citan algunas técnicas más utilizadas para disminuir los niveles de riesgo a los que puede o podría estar expuesta una organización.

- Codificar la información: Criptografía. Contraseñas difíciles de averiguar.
- Vigilancia de Red Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos.
- Tener instalado en la máquina únicamente el Software necesario, ya que con ello se reducen riesgos, de la misma manera, el tenerlo controlado asegura la calidad de la procedencia del mismo. Existe Software que es famoso por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades pero permitiendo una seguridad extra.
- Los puntos de entrada en la red son generalmente el correo, las páginas Web y la entrada de ficheros desde discos, o de computadores ajenos, como portátiles.
- Mantener al máximo el número de recursos de red en sólo en modo lectura impide que computadores infectados propaguen virus.
- Reducir los permisos de los usuarios al mínimo, controlar y monitorizar el acceso a Internet.

Fig. 1.2. Pilitos Live CD Windows XP SP2

1.12.5. GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Precisamente mantener la coordinación entre la tecnología, los procesos y el recurso humano, requiere establecer un marco de gestión integral que sintetice y aterrice las inversiones de seguridad informática para generar el valor esperado de la seguridad en el hacer mismo de la organización.

La inversión y la gestión de la seguridad son dos temas complementarios, los cuales sugieren una capacidad sistémica y sistemática para comprender por una parte, las relaciones que exige la seguridad en una organización y por otro, la detallada y delicada lista de actividades y acciones que son requeridas para operacionalizar el concepto intangible de la seguridad informática.

En este sentido formalizar un modelo de gestión de seguridad que considere las áreas de finanzas, mercadeo, junta directiva, es decir todas las áreas de la operación y control del negocio, como fuentes mismas de los insumos del área de seguridad y un área de seguridad concebida desde y para el negocio, podría

articular y dar sentido a las métricas cuantitativas y desarrollar en conjunto el concepto de valor agregado para el cliente basado en alto niveles tecnológicos de seguridad, confianza en la operaciones y estrategia personalizada de negocios.

Finalmente hablar sobre gestión de seguridad es comprender que la seguridad informática no es más que un permanente ciclo de tecnología, procesos y personas que establecen relaciones tangibles, en la asignación de recursos, para producir un bien intangible como lo es la seguridad informática.

1.12.6. ATAQUES A LA SEGURIDAD INFORMÁTICA

La importancia de conocer los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, es vital, ya que con ello podremos identificar las diferentes maneras de cómo nos pueden atacar

Los ataques pueden tener varios objetivos como: fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Pueden ser realizados por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

Con el desarrollo de la "*sociedad de la información*" y de las tecnologías computacionales, los piratas informáticos ya no son novedad, y a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan ilegalmente a ellas, con distintos fines. Por ello, los administradores de todos los sistemas, disponen de herramientas para controlar que los procesos, sean estos normales o sospechosos, queden registrados en archivos, que se revisan diariamente.

Hasta hoy esta nueva cibersociedad de "*piratas informáticos*", ha sido dividida en una decena de grandes áreas fundamentales, en las que se encuentran

la filosofía de cada uno de ellos. Todos los grupos aportan en gran medida, algo bueno en un mundo dominado por la tecnología, pero, no siempre sucede así, algunos de ellos toman estas iniciativas como partida de sus actos rebeldes.

1.12.6.1.HACKERS

Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es conocer los sistemas y el funcionamiento de ellos.

Normalmente son aquellos que dejan la "*marca*" de haber estado allí, en absoluto no modifican nada, y alertan de los fallos existentes de algún determinado sistema. Suele suceder y también es frecuente que son contratados por importantes empresas de seguridad.

Dentro ellos, se encuentra el Hacker Ético, aquel profesional de seguridad que aplica sus conocimientos de hacking con fines defensivos y legales.

Los modos de hacking ético son:

- Redes remotas: Simulación de un ataque desde Internet.
- Redes locales: Simulación de un ataque desde dentro (empleados, Hacker que ha obtenido privilegios en un sistema, otros)
- Ingeniería social: Probar la confianza de los empleados.
- Seguridad física – Accesos físicos (equipos, cintas de backup,...)

Sin duda los Hackers son el grupo es el más experto y el menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo

que implica el conocer la creación de virus o crack de un Software o sistema informático.

1.12.6.2.CRACKERS

Es el siguiente eslabón, Cracker es aquel Hacker con la capacidad de romper sistemas y Software, dedicándose única y exclusivamente a crackear sistemas, es por ello que en la actualidad es habitual ver como se muestran los cracks de la mayoría de Software de forma gratuita a través del Internet

Este grupo es el más rebelde de todos, ya que siempre encuentran la forma de violar la protección y seguridad de un sistema informático de forma similar a como lo haría un Hacker, sólo que a diferencia de este último, el Cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

1.12.6.3.LAMERS

Este grupo quizás es el más numeroso y de mayor incidencia en la red. Son individuos que tratan de hacer hacking pero que no tienen conocimiento alguno de programación o relacionado con la informática, únicamente nociones básicas, por ello lo vuelve un grupo muy peligroso, ya que pone en práctica todo el Software de hackeo que encuentra en el Internet.

1.12.6.4.COPYHACKERS

Son aquellos conocidos en el terreno del crackeo de Hardware, mayoritariamente en el sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Poseen conocimientos de tecnología y para elaborar o terminar

sus trabajos extraen información de los Hackers; su objetivo y principal motivación es únicamente económico.

1.12.6.5.BUCANEROS

Son individuos caracterizados por comerciar en el mercado negro los productos entregados por los Copyhachers. Los bucaneros tienen cabida fuera de la red, quienes son simplemente comerciantes de productos de cracking a nivel masivo.

1.12.6.6.PHREAKERS

Este grupo es muy conocido por tener profundos conocimientos sistemas de telefonía, tanto terrestres como móviles. En la actualidad los Phreakers también poseen amplios conocimientos en informática, debido a que las centrales de las compañías móviles necesitan de ella para el proceso de datos, además de ello, tienen acceso al uso, activación y códigos de tarjetas prepago, usadas habitualmente en la telefonía celular. [LIB. 002]

1.12.7. MÉTODOS Y HERRAMIENTAS DE ATAQUE

Los métodos de ataque descriptos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear un password, el intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de salir. [WWW.006]

1.12.7.1.INSIDER ABUSES

En los primeros años, los ataques involucraban poca sofisticación técnica, estos eran inducidos por los denominados insiders y outsiders. Los insiders, personas externas con acceso a sistemas dentro de la empresa, utilizaban sus permisos para alterar archivos o registros. Los outsiders, personas que atacan desde afuera de la ubicación física de la organización, ingresaban a la red simplemente averiguando el password válido.

Una técnica muy utilizada es la denominada *"Ingeniería Social"*. Básicamente consiste en convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password (contraseña) con alguna excusa convincente. Esto es común cuando en el Centro de Cómputo los Administradores son amigos o conocidos.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar agujeros en el diseño, configuración y operación de los sistemas, esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de empresas con altísimo grado de dependencia tecnológica como bancos, servicios automatizados, entre otros.

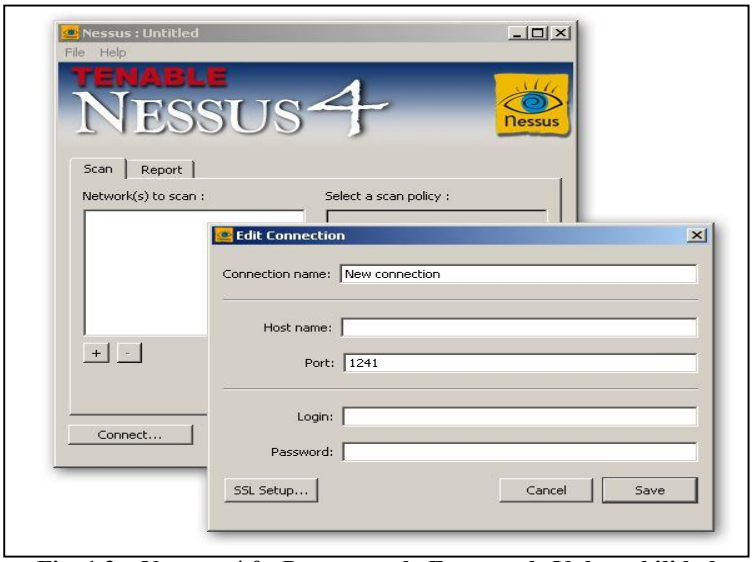


Fig. 1.3. Nessus v4.0, Programa de Escaneo de Vulnerabilidades

Con estos nuevos métodos de ataque, que han sido automatizados, en muchos casos sólo se necesita tener un conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos Boletines Hacker y sitios Web, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

1.12.7.2.MALWARE

Malware es la abreviatura de "Malicious software" (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento.

1.12.7.2.1. EAVESDROPPING Y PACKET SNIFFING

Muchas redes son vulnerables al Eavesdropping, que es la intercepción pasiva sin modificación del tráfico de red. En Internet esto es realizado por Packet Sniffers, que son programas que monitorean los paquetes de red que están direccionados al computador donde están instalados.

El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrante y saliente. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Fig. 1.4. Password Finder V2.0 XP /W2003

1.6.7.2.2. SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes y que además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o Software. Los casos mas resonantes de este tipo de ataques fueron: El robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

1.6.7.2.3. TAMPERING O DATA DIDDLING

El Tampering o Data Diddling es la modificación desautorizada a los datos, o al Software instalado en un sistema, incluyendo el borrado de archivos. Este tipo de ataques son particularmente serios, cuando el que lo realiza, ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier

comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

Como siempre, esto puede ser realizado por insiders u outsiders, generalmente con el propósito de fraude, o para dejar fuera de servicio un competidor. Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples sitios Web han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, ó el reemplazo de versiones de Software para descargar por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de Software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de ***Back Orifice*** y ***NetBus***.

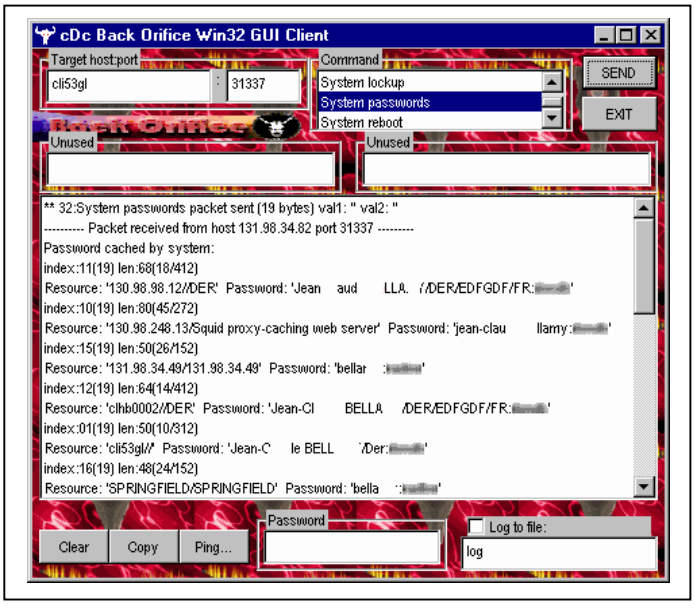


Fig. 1.5. Back Orifice v1.2. Sistema de administración remota

1.6.7.2.4. SPOOFING

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de Spoofing o Tampering. Una forma común de Spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, tal como puede ser el envío de e-mails falsos.

El intruso utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado ***Looping***, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al Spoofing. Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de Spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos.

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

1.6.7.2.5. JAMMING O FLOODING

Los ataques de este tipo desactivan o saturan los recursos del sistema. Por ejemplo, se puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ***ISP***[5]s han sufrido bajas temporales del servicio por ataques que explotan el protocolo ***TCP***[6]. El atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección ***IP***[7] del emisor, el mensaje contiene falsas direcciones IP (spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Cuantiosos host de Internet han sido dados de baja por el denominado *"ping de la muerte"*, una versión trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino. [WWW.006]

1.6.7.2.6. DIFUSIÓN DE VIRUS

En la actualidad y dado que los antiguos llamados Virus ahora comparten funciones con sus otras familias, son denominados directamente como un "Malware".

[5] ISP; Internet Service Protocol (Proveedor de Servicios de Internet)
[6] TCP, Transport Control Protocol (Protocolo de Control de Transmición)
[7] IP, Internet Protocol (Protocolo de Internet)

Si bien es un ataque de tipo Tampering, pero difiere de este porque puede ser ingresado al sistema por un dispositivo externo (dispositivos USB) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante.

Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una red LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

Existen distintos tipos de virus, aquellos que infectan archivos ejecutables y los sectores de discos, y aquellos que causan mas problemas como los macro virus, estos se encuentran ocultos en documentos o en hojas de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con su transmisión a través de cualquier red o Internet; además de ser multiplataforma, es decir, no están atados a un sistema operativo en particular.

Los virus son lo más común en la mayoría de las empresas; cientos de ellos son descubiertos mes a mes, pero así también, las técnicas para contrarrestarlos.

Dentro de este grupo podemos encontrar términos como: Trojan (Caballo de Troya), Gusano (Worm), Bombas lógicas, entre otros.

- **Caballos de Troya:** Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto. Por ejemplo: Formatear el disco duro, modificar un fichero, sacar un mensaje, entre otros.

- **Bombas lógicas:** Este suele ser el procedimiento de sabotaje mayormente comúnmente utilizado. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

- **Gusanos:** Son programas desarrollados para reproducirse por algún medio de comunicación como el correo electrónico (el más común), mensajeros o redes P2P. El objetivo de los mismos es llegar a la mayor cantidad de usuarios posible y lograr distribuir otros tipos de códigos maliciosos. Estos últimos serán los encargados de llevar a cabo el engaño, robo o estafa.

1.6.7.2.7. EXPLOTACIÓN DE ERRORES

Algunos sistemas están expuestos a agujeros de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades o *"puertas invisibles"*, han sido descubiertas en aplicaciones de Software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios en LAN o WANs.

Por ello es que hoy se hace indispensable contar con productos que conozcan de tales debilidades y que pueden diagnosticar un servidor, actualizando su base de datos de tests periódicamente, además y algo muy importante, normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática. [WWW.006]

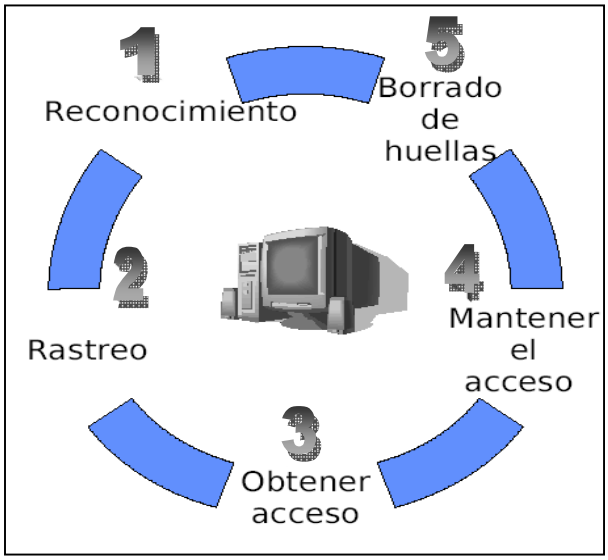


Fig. 1.6. Los pasos de un Hacker

1.6.8. LA SEGURIDAD UN PROBLEMA INTEGRAL

Los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a la de su punto más débil. Al asegurar nuestra casa no sacamos nada con ponerle una puerta blindada con sofisticada cerradura si dejamos las ventanas sin protección. De manera similar el uso de sofisticados algoritmos y métodos criptográficos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo.

Por otra parte, la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar. Es evidente que por mucha tecnología de seguridad que se implante en una organización, si no existe una clara disposición por parte de la Dirección General y una cultura a nivel de usuarios, no se conseguirán los objetivos perseguidos con la implantación de un sistema de seguridad. [WWW.007]

1.7. METODOLOGÍAS Y NORMAS INTERNACIONALES EN LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

El nacimiento de metodología en el mundo de la auditoría y el control informático se puede observar en los primeros años de los ochenta, naciendo a la par con la informática, la cual utiliza la metodología en disciplinas como la seguridad de los sistemas de información, misma que se define como la doctrina que trata de los riesgos informáticos, en donde la auditoría se involucra en este proceso de protección y preservación de la información y de sus medios de proceso.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática. Sin embargo, hay directivos que desconocen la existencia de normas de seguridad y calidad, que han sido diseñadas para la mejora o para la implementación de las

mismas, e intentan crear sus *"propias normas internas"*, las cuales pueden tener un superior margen de error y riesgo en comparación con normas ya existentes, justamente diseñadas a efectos de la administración, protección de datos y procesos de información. Ejemplos de estas normas son ISO[8] 27002, COBIT[9], COSO[10], Sarbanes Oxley, y otras que pueden surgir de acuerdo a la necesidad de aseguramiento de la empresa afectada.

La evolución del mundo hacia bloques económicos conlleva a que cada vez pierdan importancia las normas específicas de cada País y tome mayor auge la estandarización Internacional y las reglas que se fijen en ese contexto, de allí que las organizaciones que no estén dentro de este ámbito pierden grandes oportunidades de mejorar y tener menos posibilidades de desarrollo. Dentro de este contexto, los inversionistas internacionales exigen reglas estandarizadas que les faciliten la realización de sus negocios en este entorno, apoyados en el uso de la tecnología y en sistemas de información que les provean calidad y seguridad, mismas que servirán para la toma de decisiones. Por ello se viene difundiendo y adoptando cada vez más en la mayoría de los países del mundo, los denominados Estándares Internacionales.

Estas normas u estándares, son los referentes que establecen lineamientos generales de acción que deben ser afinados y contextualizados en la realidad de cada organización, desarrollando el concepto de métrica de seguridad, basado en la manera como se ejecutan y alcanzan objetivos y metas de seguridad informática, lo cual se materializa en los resultados deseados de la implementación de los programas de requeridos para tal fin.

[8] ISO, International Standards Organization (Organización Internacional de Estandarización)
[9] CObIT, Control Objetives for Information and Related Technology (Objetivos de Control para la Información y las Tecnologías Relacionadas)
[10] COSO, Committee Of Sponsoring Organization of the Treadway Commission (Organización para el Desarrollo de la Comunicación y la Sociedad)

CAPÍTULO II

ESTÁNDARES Y NORMAS INTERNACIONALES DE AUDITORÍA

CONTENIDO

- ESTÁNDARES PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN
- NORMAS INTERNACIONALES DE AUDITORÍA

CAPÍTULO II

ESTÁNDARES Y NORMAS INTERNACIONALES DE AUDITORÍA

2.1. ESTÁNDARES PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que se aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión.

Las Estándares definen requisitos obligatorios para la auditoría, con directrices que proporcionan asesoramiento en la aplicación y cumplimiento de los mismos. A continuación señalaremos algunos.

2.1.1. INDEPENDENCIA PROFESIONAL

En todas las cuestiones relacionadas con la auditoría, el auditor de Sistemas de Información deberá ser independiente de la organización y del área auditada, asumiendo una actitud de imparcialidad, lo cual le permitirá actuar objetivamente y con justicia.

El auditor debe evitar situaciones que podrían perjudicar su independencia, puesto que su trabajo y reporte realizados deben ejemplificar la integridad y objetividad.

2.1.2. ÉTICA Y NORMAS PROFESIONALES

El auditor deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información, ejerciendo especial atención correspondiente al cumplimiento de normas aplicables de auditoría.

Según el Código de Ética de ISACA los Auditores de Sistemas Certificados deberán:

a) Apoyar el establecimiento y cumplimiento apropiado de estándares, procedimientos y controles en los sistemas de información.
b) Cumplir con los Estándares de Auditoría de Sistemas de Información adoptados por la Asociación de Auditoría y Control de Sistemas de Información.
c) Dar servicio a sus empleadores, accionistas, clientes y público en general en forma diligente, leal y honesta y no formar parte de actividades impropias o ilegales.
d) Mantener la confidencialidad de la información obtenida en el curso de sus tareas. Dicha información no debe ser usada en beneficio propio ni ser entregada a terceros.
e) Realizar sus tareas en forma objetiva e independiente, y rechazar la realización de actividades que amenacen o parezcan amenazar su independencia.
f) Mantener competencia en los campos relacionados a la auditoría de sistemas de información a través de la participación en actividades de desarrollo profesional.
g) Obtener suficiente material y documentación de sus observaciones que le permita respaldar sus recomendaciones y conclusiones.
h) Informar a las partes que correspondieren los resultados del trabajo de auditoría realizado.
i) Dar apoyo a la educación y el conocimiento de clientes, gerentes y público en general sobre la auditoría de sistemas de información.

j) Mantener altos estándares de conducta y personalidad tanto en las actividades profesionales como personales. [WWW.008]

2.1.3. IDONEIDAD

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y conocimientos necesarios para realizar el trabajo del auditor, manteniendo sus aptitudes a través de la educación profesional correspondiente de forma permanente.

La conducción de un trabajo de auditoría no implica que el profesional sea infalible, solo que enfoque con diligencia los asuntos que requieren un juicio profesional.

2.1.4. PLANIFICACIÓN

Es vital planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de auditoría y para cumplir con las normas aplicables de auditoría profesional.

Por ello el debido cuidado profesional debe extenderse en cada aspecto de la auditoría, incluyendo: la evaluación del riesgo, formulación de objetivos y alcance de auditoría, así como la selección de pruebas y evaluación de los resultados de estas.

2.1.5. EJECUCIÓN DEL TRABAJO DE AUDITORÍA

El personal de auditoría debe contar con la supervisión apropiada para proporcionar la garantía de cumplir con los objetivos de auditoría establecidos.

Durante el transcurso de una auditoría, el auditor colecciona información, conocida también como evidencia, misma que deberá ser suficiente, confiable, relevante y útil, quedando a juicio del auditor determinar la naturaleza de esta. Los hallazgos y conclusiones de auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia, de allí la importancia de documentarla y organizarla apropiadamente.

Son varios los tipos de evidencia que el auditor puede utilizar, entre ellas:

- Evidencia física: Observación de actividades, bienes y funciones de sistemas, inventarios.
- Evidencia documentaria: Registros de transacciones, listados de programas, logos de control, entre otros.

La evidencia también puede consistir en las políticas y procedimientos, flujogramas de Sistemas y declaraciones escritas u orales.

Los procedimientos usados para recolectar la evidencia pueden variar, mismos que pueden incluir: averiguaciones, observaciones, inspección, confirmación o reejecución, entre otros.

El uso de valoración de riesgos es imprescindible durante la planeación de auditoría, puesto que facilitara la toma de decisiones durante el desarrollo de esta, ya que sumados a la documentación respectiva y la evidencia de auditoría obtenida, soportarán de mejor manera las conclusiones del auditor.

2.1.6. INFORMES

En el momento de completar el trabajo de auditoría, el auditor de sistemas deberá proporcionar un informe, de formato apropiado a los destinatarios en cuestión. El informe de auditoría deberá enunciar su alcance, los objetivos, el

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

2.1.7. ACTIVIDADES DE SEGUIMIENTO

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

2.2. NORMAS INTERNACIONALES DE AUDITORÍA

El IAASB[11] comprometido con el objetivo de desarrollar un conjunto de Normas Internacionales generalmente aceptadas en todo el mundo, difunde y publica pronunciamientos que rigen los trabajos de auditoría, revisiones y trabajos de aseguramiento, conducidos de acuerdo a cánones internacionales, que contienen los principios básicos y esenciales así como lineamientos, facilitando la convergencia de normas nacionales e internacionales y estableciendo de manera independiente y bajo su propia autoridad, normas de elevada calidad sobre auditoría.

Es así que la IAASB sigue un riguroso procedimiento al desarrollar sus declaraciones, obteniendo apoyo de su Grupo Consultivo (CAG), de los emisores nacionales de normas de auditoría, de los organismos que integran IFAC[12] y sus miembros. En este sentido, y en línea con lo antes mencionado en las Normas Internacionales de Auditoría aprobadas por IFAC, se ha considerado el exponer a

[11] IAASB, Concejo de Normas Internacionales de Auditoría y Aseguramiento
[12] IFAC, International Federation of Accountants, (Federación Internacional de Contadores Públicos).

continuación las normas que se han revisado para el desarrollo del presente proyecto, de las que se han tomado criterios de actuación que debe seguir el auditor en relación a: distinción de fraude y error, responsabilidades respectivas de los encargados del gobierno corporativo, administración y entendimiento de la entidad y su entorno, selección y obtención de evidencia de auditoría, entre otros.

2.2.1. NORMA INTERNACIONAL DE AUDITORÍA 240: RESPONSABILIDAD DEL AUDITOR DE CONSIDERAR FRAUDE EN UNA AUDITORÍA DE ESTADOS FINANCIEROS.

El propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar lineamientos sobre la responsabilidad del auditor de considerar el fraude en una auditoría y en cómo deben aplicarse las normas, describe los tipos de fraude relevantes para el auditor, así como las responsabilidades respectivas de los encargados del gobierno corporativo y de la administración de la entidad sobre la prevención y detección de fraude, describe las limitaciones inherentes de una auditoría en el contexto de fraude, y fija las responsabilidades del auditor para detectar representaciones erróneas de importancia relativa debidas a fraude.

2.2.1.1.Características del Fraude

El término "error" se refiere a una representación errónea no intencional de la información en estados financieros incluyendo:

- Equivocación en la compilación de datos o procesamiento de datos con los que se preparan los estados financieros.
- Omisión de cantidades
- Estimación contable incorrecta que se origina al pasar por alto o malinterpretar los hechos.

- Equivocación en la aplicación de los principios de contabilidad relativos a valuación, reconocimiento, clasificación, presentación o revelación.

El término "fraude" se refiere a un acto intencional por parte de una o más personas de la administración, los encargados del gobierno corporativo, empleados o terceros, implicando el uso de engaño para obtener una ventaja injusta o ilegal. El fraude que involucra a uno o más miembros de la administración o de los encargados del gobierno corporativo se conoce como "fraude administrativo"; el fraude que involucra sólo a empleados de la entidad se conoce como "fraude de empleados".

La malversación de activos implica el robo de activos de una entidad que a menudo, es perpetrada por empleados en cantidades relativamente pequeñas y de poca importancia Sin embargo puede también involucrar a la administración, donde generalmente hay más posibilidad de simular u ocultar las malversaciones en formas difíciles de detectar. Las malversaciones de activos pueden lograrse en una variedad de formas como: falsificación de recibos, robos de activos físicos o de propiedad intelectual, pago por bienes y servicios no recibidos y uso de los activos para uso personal.

El fraude implica un incentivo o presión para cometerlo, una oportunidad percibida para hacerlo y alguna racionalización del acto. La información fraudulenta puede ser cometida deliberadamente porque la administración está bajo presión, para lograr el cumplimiento de metas y objetivos esperados, así como puede existir la oportunidad para malversación de activos debido al cargo de desempeño dentro de la entidad y al conocimiento que posee sobre las debilidades específicas que puedan existir en el control interno.

2.2.1.2. Responsabilidades de los encargados del Gobierno Corporativo y de la Administración.

Es importante que la administración, con los encargados del gobierno corporativo, ponga un fuerte énfasis en la prevención del fraude, fomentando una cultura de honradez y comportamiento ético, lo que implica: el crear un ambiente positivo, contratar, entrenar y promover a los empleados apropiados, confirmación de responsabilidades, entre otros; así como también el establecer y mantener un control interno para dar seguridad razonable respecto a la confiabilidad de la información, efectividad y eficiencia de las operaciones, que ayuden a la consecución de los objetivos de la entidad, esto lo cual significaría reducir las oportunidades de que un fraude ocurra.

2.2.1.3. Limitaciones inherentes de una auditoría en el contexto de fraude

El riesgo para el auditor de no detectar un fraude, es más alto que no detectar una representación errónea, ya que este puede implicar trampas sofisticadas cuidadosamente organizadas para ocultarlo; siendo más difícil de detectar cuando van acompañados de colusión, puesto que la evidencia presentada al auditor pretenda ser persuasiva cuando de hecho es falsa.

Frecuentemente la administración está en una posición de manipular directa o indirectamente información, y dada su posición de autoridad dentro de la entidad, la administración tiene la capacidad de ordenar a los empleados o solicitar su ayuda para llevar a cabo un fraude, con o sin su consentimiento. [LIB.003]

2.2.1.4. Responsabilidades del auditor de detectar representación errónea de importancia relativa debida al fraude

Un auditor no puede obtener seguridad absoluta de que las representaciones erróneas de importancia relativa se detectarán debido a factores como el uso del

juicio, uso de pruebas, las limitaciones inherentes del control interno y el hecho de que mucha de la evidencia disponible al auditor es persuasiva, más que conclusiva. Sin embargo en la obtención de seguridad razonable, el auditor mantiene una actitud de escepticismo profesional en toda la auditoría, considerando la probabilidad de que la administración sobrepase los controles, así también el hecho de reconocer que los procedimientos de auditoría que son efectivos para detectar error puedan no ser apropiados.

El mantener el escepticismo profesional respecto a la información y evidencia de auditoría obtenida es primordial, pese a la experiencia que el auditor pueda tener con la entidad sobre la honradez e integridad de la Administración y de los encargados del Gobierno Corporativo, ya que pudieron haber cambios circunstanciales en la misma, por ello no debe dejar de averiguar y desempeñar otros procedimientos de auditoría respecto a que la evidencia de auditoría obtenida pueda o no ser auténtica. No obstante la experiencia que tenga el auditor con la entidad contribuye aun mejor entendimiento del entorno de la misma.

2.2.1.5.Procedimientos de Evaluación de Riesgos

Para obtener un entendimiento de la entidad y su entorno, incluyendo su control interno, el auditor desempeña los siguientes procedimientos:

- Hacer averiguaciones con la administración y con otros dentro de la entidad, según sea apropiado, para obtener entendimiento de cómo los encargados del Gobierno Corporativo ejercen vigilancia sobre los procesos de la administración para identificar y responder a los riesgos de fraude.
- Considerar si están presentes uno o más factores de riesgos de fraude.
- Considerar relaciones inusuales o inesperadas que se hayan identificado al realizar procedimientos analíticos.
- Considerar otra información que pudiera ser útil para identificar los riesgos de representación errónea de importancia relativa debido al fraude.

"Al evaluar las respuestas de las averiguaciones, el auditor mantiene una actitud de escepticismo profesional, por lo tanto, el auditor usa su juicio profesional al decidir cuando es necesario corroborar las respuestas a las averiguaciones con otra información."[13]

El hecho de que el fraude generalmente se oculta, puede hacer más difícil su detección. Sin embargo, al obtener un entendimiento de la entidad y de su entorno, el auditor puede identificar eventos o condiciones que indiquen un incentivo o presión para cometer fraude o que presenten una oportunidad para cometerlo.

2.2.1.6.Evaluación de la Evidencia de Auditoría

El auditor con base en los procedimientos de auditoría desempeñados y la evidencia de auditoría obtenida, evalúa si las valoraciones de los riesgos siguen siendo apropiadas. Esta evaluación es primordialmente un asunto cualitativo que se basa en el juicio del auditor.

2.2.1.7.Comunicaciones con la Administración y los encargados del Gobierno Corporativo

Al identificar el auditor un fraude o ha obtenido información mediante la evidencia que indica que puede existir un fraude, el auditor deberá comunicar estos asuntos tan pronto como sea factible al nivel apropiado de la administración, que podrá ser de manera oral o escrita. La determinación de cual nivel de administración es apropiado, es cuestión de juicio profesional.

[13] Normas Internacionales de Auditoría, Edición 2008

2.2.2. NORMA INTERNACIONAL DE AUDITORÍA 315: ENTENDIMIENTO DE LA ENTIDAD Y SU ENTORNO Y EVALUACIÓN DE LOS RIESGOS DE REPRESENTACIÓN ERRONEA DE IMPORTANCIA RELATIVA.

En esta Norma Internacional de Auditoría (NIA) se establecen normas y guías para obtener un entendimiento de la entidad y su entorno, incluyendo su control interno, así como para evaluar los riesgos de representación errónea de importancia relativa en una auditoría.

Es trascendental que el auditor obtenga un suficiente entendimiento de la entidad y su entorno así como de su control interno, tanto para diseñar y desempeñar procedimientos adicionales de auditoría, como para identificar y evaluar los riesgos de representación errónea.

2.2.2.1. Procedimientos de Evaluación del Riesgo y Fuentes de Información sobre la Entidad y su Entorno, incluyendo su Control Interno.

Obtener un entendimiento de la entidad y su entorno incluyendo su control interno, es un proceso continuo, dinámico, de compilación, actualización y análisis de información en toda la auditoría, ya que algo de la información obtenida al desempeñar ciertos procedimientos, puede usarse por el auditor como evidencia de auditoría.

Para la evaluación del riesgo, entendimiento de la entidad y su control interno el auditor podrá realizar:

- Investigaciones con la administración y otros dentro de la entidad;
- Procedimientos analíticos; y
- Observación e inspección.

Aunque mucha de la información obtenida por el auditor en las investigaciones puede recibirse de la administración y de los responsables de la información, las investigaciones con otros dentro de la entidad puede ser muy útil para el auditor al dar una diferente perspectiva para identificar riesgos.

La observación e inspección pueden apoyar las investigaciones al dar información sobre la entidad y su entorno. Estos procedimientos incluyen lo siguiente:

- Observación de actividades y operaciones de la entidad.
- Inspección de documentos (plan estratégico, manuales, entre otros).
- Lecturas de informes preparados por la administración.
- Visitas a las instalaciones de la entidad. [LIB.003]

2.2.2.2. Entendimiento de la Entidad y su Entorno, incluyendo su Control Interno.

Obtener un entendimiento de la entidad y su entorno es un aspecto esencial del desempeño de una auditoría, ya que el entendimiento establece un marco de referencia dentro del cual el auditor planea la auditoría y ejerce juicio profesional acerca de evaluar los riesgos, donde:

- Identifica áreas en las que puede ser necesario consideraciones especiales de auditoría.
- Desarrolla expectativas para su uso cuando realice procedimientos analíticos.
- Diseña y realiza procedimientos adicionales de auditoría para reducir el riesgo a un nivel aceptable.
- Evalúa lo suficiente y apropiado de la evidencia de auditoría.

El entendimiento consiste:

- Factores de industria y regulaciones.
- Naturaleza de la entidad.
- Objetivos, estrategias y riesgos del negocio.
- Medición y revisión del desempeño.
- Control interno.

2.2.2.3. Evaluación de los Riesgos de Representación Errónea de Importancia Relativa.

El auditor identifica los riesgos a lo largo del proceso de entendimiento de la entidad y su entorno, utilizando la información obtenida, ya que al evaluar el ambiente de control, los controles y su implementación, el auditor podrá determinar cuales de los riesgos identificados son, a juicio suyo, riesgos que requieran una consideración especial de auditoría.

Si el auditor identifica riesgos que la entidad no haya controlado, o cuyo control relevante es inadecuado, o si a su juicio hay debilidades de importancia en el proceso de evaluación del riesgo, se comunicará pertinentemente al gobierno corporativo o a la administración.

2.2.2.4. Documentación.

El auditor deberá documentar:

- Discusiones entre el equipo de trabajo respecto a la susceptibilidad a error o fraude y las decisiones importantes que se alcancen.
- Elementos claves del entendimiento que se obtiene respecto de cada uno de los aspectos de la entidad y su entorno, incluyendo los componentes del control interno, y las fuentes de información.
- Los riesgos identificados y evaluados
- Los riesgos identificados y los controles relacionados.

"La manera en que se documenten esos asuntos debe determinarla el auditor usando su juicio profesional. La forma y extensión de esta documentación está influida por la naturaleza, tamaño y complejidad de la entidad y su control interno, así también la disponibilidad de la información de entidad, la metodología y tecnología específicas usadas en el curso de la auditoría."[14]

2.2.3. NORMA INTERNACIONAL DE AUDITORÍA 330: PROCEDIMIENTOS DEL AUDITOR EN RESPUESTA A LOS RIESGOS EVALUADOS.

El objetivo de esta norma es proporcionar guías para determinar respuestas globales, diseñar y desempeñar procedimientos adicionales para responder a los riesgos evaluados.

2.2.3.1.Respuestas Globales.

El auditor deberá determinar respuestas globales para atender a los riesgos evaluados, estas pueden incluir la necesidad de dar mayor supervisión, tener mayor escepticismo al compilar y evaluar la evidencia de auditoría, entre otros; sin embargo, es importante destacar que el entendimiento del entorno de control de la entidad afecta a la evaluación de los riesgos, ya que este al ser efectivo permite al auditor tener más confianza en el control interno y confiabilidad en la evidencia de auditoría obtenida.

La evaluación, proporciona una base para considerar si se deben diseñar y desempeñar procedimientos adicionales de auditoría, tomando en consideración: la naturaleza, oportunidad y extensión de los mismos.

[14] Normas Internacionales de Auditoría, Edición 2008

2.2.3.2.Evaluación de lo Suficiente y Apropiado de Evidencia de Auditoría.

Al desarrollar una opinión, el auditor considera toda la evidencia relevante, así como lo suficiente y apropiado de esta para soportar las conclusiones de auditoría.

El juicio del auditor en cuanto a lo adecuado en evidencia está influido por factores como:

- Efectividad de los controles para atender a riesgos.
- Fuente y confiabilidad de la información disponible.
- Persuasividad de la evidencia de auditoría.
- Entendimiento de la entidad y su entorno, incluyendo su control interno.

2.2.3.3.Perspectiva del Sector Publico

Al llevar a cabo auditorías de entidades del sector público, el auditor toma en cuenta el marco de referencia legal y cualesquier otra regulación, ordenanza o directiva ministerial relevante que afecte a la auditoría y sus requisitos.

2.2.4. NORMA INTERNACIONAL DE AUDITORÍA 500: EVIDENCIA DE AUDITORÍA.

La Norma Internacional de Auditoría 500, provee de guías sobre lo que constituye la evidencia de auditoría, la cantidad y calidad que se debe obtener.

2.2.4.1.Evidencia de Auditoría

Evidencia es toda la información que usa el auditor para llegar a las conclusiones en las que basa la opinión de auditoría, sin embargo no es

imprescindible que el auditor examine toda la información disponible, ya que se puede llegar a conclusiones con el uso de enfoques de muestreo y otros medios.

La calidad y cantidad de la evidencia se basan en la relevancia y confiabilidad, por ello el auditor debe ejercer escepticismo profesional al evaluar estos dos aspectos, esta última afecta notablemente a la evidencia, ya que la fuente y las circunstancias en las cuales se la ha obtenido es determinante, por tanto el auditor deberá obtener suficiente evidencia que sea apropiada para poder llegar a conclusiones razonables en las cuales basar su opinión de auditoría.

La información que se utiliza como evidencia de auditoría puede ser: registros, minutas de reuniones, informes, manuales, confirmaciones de terceros, documentos filmados, digitalizados, entre otros; así como también información obtenida por el auditor de procedimientos de auditoría como: investigación, observación e inspección. [LIB.003]

2.2.4.2.Procedimientos de Auditoría para obtener evidencia

Como se ha mencionado, el auditor obtiene evidencia para llegar a conclusiones razonables en las cuales basar su opinión de auditoría, ya sea a través de uno o más tipos de procedimientos que se describen a continuación:

- **Inspección de registros o documentos:** Consiste en examinar registros o documentos ya sean internos o externos, en forma impresa, electrónica, o en otros medios. La inspección proporciona evidencia de grados variables de confiabilidad dependiendo de su fuente.
- **Inspección de activos tangibles:** Radica en el examen físico de los activos, esto proporciona evidencia de auditoría confiable respecto a su existencia.
- **Observación:** Como su nombre lo indica, es el observar un proceso o procedimiento desempeñado por otros.

- **Investigación:** Consiste en buscar información de personas bien informadas tanto en la entidad como fuera de ella. Las investigaciones pueden ser formales por escrito u orales informales.
- **Confirmación:** La confirmación es un tipo específico de investigación, es obtener información de una condición directamente de un tercero.
- **Volver a Calcular:** Reside en verificar la exactitud matemática de los documentos o registros.

Estos entre otros procedimientos, son fundamentales para el auditor al momento de obtener evidencia sustentable para el informe de auditoría.

CAPÍTULO III

ESTÁNDARES Y LEGISLACIONES

INTERNACIONALES PARA LA ADMISTRACIÓN DE LA SEGURIDAD Y CONTROL DE TI

CONTENIDO

- INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA
- INTRODUCCIÓN
- IMPORTANCIA
- TIPOS DE METODOLOGÍAS Y NORMAS
- INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)
- CAPABILITY MATURITY MODEL (CMM)
- APPLICATION SERVICES LIBRARY (ASL)
- PROJECT MANAGEMEN INSTITUTE (PMI)
- AUSTRALIAN STANDARD FOR CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY - AS 8015
- SIX SIGMA
- COMMITE OF SPONSORING ORGANIZATION OF TREADWAY COMMISSION (COSO)
- BRITISH STANDARDS INSITITUTION (BSI)
- INTERNATIONAL STANDARDS ORGANIZATION (ISO)

CAPÍTULO III

ESTÁNDARES Y LEGISLACIONES INTERNACIONALES PARA LA ADMINISTRACIÓN DE LA SEGURIDAD Y CONTROL DE TI

3.1. INTRODUCCIÓN

Actualmente el uso de los medios electrónicos informáticos como: Internet, Redes de Comunicaciones y Computadores es algo que se ha masificado a nivel mundial en diferentes áreas como: Gobierno, Educación e Investigación, Salud, Comercio e Industria, así mismo, el interés en los temas de riesgo se ha extendido entre inversores, directores, gerentes y organismos reguladores, tanto a nivel público como privado en todo el mundo; y las expectativas a nivel internacional en todos los sectores, se centran en la aplicación de estándares y marcos de referencia que permitan a las organizaciones apoyar las tareas de administración con herramientas efectivas y eficaces para obtener los beneficios esperados con la consecución de los objetivos del negocio.

Es por ello, que los sistemas de calidad basados en reglamentos y procedimientos estandarizados según normas internacionales de aceptación mundial, representan desde hace algunos años, la mejor opción para las empresas de todo tipo y tamaños que se desenvuelven en diferentes industrias y organizaciones, ya que están comprometidas a involucrar procedimientos adecuados y eficientes que reflejen un alto grado de calidad y mejora continua, que a diferencia de muchos programas de este tipo, la implantación de estándares, no caduca, sino que se renuevan en forma dinámica logrando mantener niveles máximos de calidad en forma permanente, sin embargo, ello no significa la eliminación total de fallas en los procesos internos, pero ofrece métodos y procedimientos eficaces y sistematizados, logrando que las organizaciones

mejoren significativamente su gestión, permitiéndoles ofrecer productos y servicios de alta calidad, y sobre todo alcanzar el éxito.

3.2. IMPORTANCIA

La importancia radica en función del dinamismo y competitividad que caracterizan al mercado actual, para esto las empresas de hoy deben estar lo suficientemente preparadas en forma interna para responder a los retos actuales.

Hasta hace poco tiempo, el riesgo operativo en las organizaciones era visto como un concepto no muy difundido, que en la mayoría de los casos implicaba pérdidas o resultados no esperados. Sin embargo, hoy en día la Alta Gerencia ha reconocido que la importancia de implementar un programa completo para la seguridad de la información a través de una metodología o estándar, con base en las necesidades de la empresa, es una parte integral en su gestión, que manejada adecuadamente permite agregar valor muy significativo a la organización.

Es así que una apropiada administración permite definir cuál es el perfil de riesgo de la organización, identificando y evaluando, en todos los niveles de su actividad, las amenazas que constituyen un riesgo real para la misma, así como el impacto negativo que ésta pueda provocar en caso de materializarse.

Indudablemente el área de Tecnología de Información (TI) es una parte muy importante de las organizaciones que hace el logro de las metas del negocio. Una administración global de los riesgos inherentes a cada uno de sus recursos, brindará por lo tanto trascendentales beneficios para toda la organización, además de lograr mejorar significativamente la gestión de la propia gerencia de TI. En este sentido, existen estándares internacionalmente aceptados, así como un marco de referencia, cuya implementación proporciona una adecuada administración del riesgo derivado del uso de la tecnología de información.

3.3. TIPOS DE METODOLOGÍAS Y NORMAS

Las metodologías y normas existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que las amenazas que se materialicen en hechos sea lo mas baja posible o al menos quede reducida de una forma razonable en costo-beneficio.

Todas las metodologías y normas desarrolladas y utilizadas en la auditoría y el control informático, se puede agrupar en dos grandes familias:

3.3.1. CUANTITATIVAS

Basadas en un modelo matemático numérico que ayuda a la realización del trabajo. Están diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

3.3.2. CUALITATIVAS

Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base al experiencia acumulada. Puede excluir riesgos significantes desconocidos. Basadas en métodos estadísticos y lógica borrosa, que requiere menos recursos humanos y tiempo que las metodologías cuantitativas [LIB.004].

La calidad sin duda continuará siendo un arma competitiva para las compañías, ya que al certificarse bajo las normas y estándares internacionales se enfocan en el mejoramiento de calidad de servicios y el uso de innovación tecnológica.

3.4. INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)[15]

La Information Technology Infrastructure Library (ITIL), es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de Tecnologías de la Información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI[16]. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI. La filosofía ITIL esta basada en la administración de servicios desde el punto de vista del negocio, y ha crecido en popularidad en la medida en la que estos dependen de la tecnología y buscan la mejor forma de aprovechar sus recursos humanos y tecnológicos.

Lo que actualmente se conoce como ITIL, fue desarrollada a finales de 1980 por iniciativa del gobierno del Reino Unido, específicamente por la Oficina Gubernativa de Comercio Británica (Office of Goverment Comerce, OGC), se tituló Government Information Technology Infrastructure Method (Método de Infraestructura de la Tecnología de Información del Gobierno, GITM), durante varios años terminó expandiéndose en un sinnúmero de libros en un proyecto inicialmente dirigido por Peter Skinner y John Stewart.

IBM[17] hizo aportaciones claves para el conjunto original de libros de ITIL, mismos que surgieron de los denominados Yellow Books (A Management System for the Information Business, Un Sistema de Gestión para el Negocio de la Información).

Inicialmente la Biblioteca de Infraestructura de TI (ITIL) dentro de su primera versión publicó 10 libros centrales cubriendo las dos principales áreas de Soporte

[15] Information Technology Infrastructure Library (ITIL), Biblioteca de Infraestructura de Tecnologías de Información
[16] TI, Technology Information (Tecnologías de la Información)
[17] IBM, International Business Machines Corporation (Corporación Internacional de Máquinas para Negocio)

del Servicio y Prestación del Servicio, sin embargo tras la publicación inicial de estos, su número creció rápidamente hasta 31 libros. Para hacer a ITIL más accesible y menos costosa, uno de los objetivos del proyecto de actualización ITIL versión 2 fue agrupar los libros según unos conjuntos lógicos destinados a tratar los procesos de administración que cada uno cubre. De esta forma, diversos aspectos de los sistemas de Tecnologías de la Información y Comunicaciones, de las aplicaciones y del servicio se presentan en conjuntos temáticos. Actualmente existe la nueva versión 3 de ITIL que fue publicada en mayo de 2007.

Bajo versión 3 de ITIL, que sustituye a las anteriores, hay cinco volúmenes, estos son: Estrategia De Servicio de ITIL, Diseño Del Servicio de ITIL, Transición Del Servicio de ITIL, Operación Del Servicio de ITIL, y Mejora Continua del servicio de ITIL.

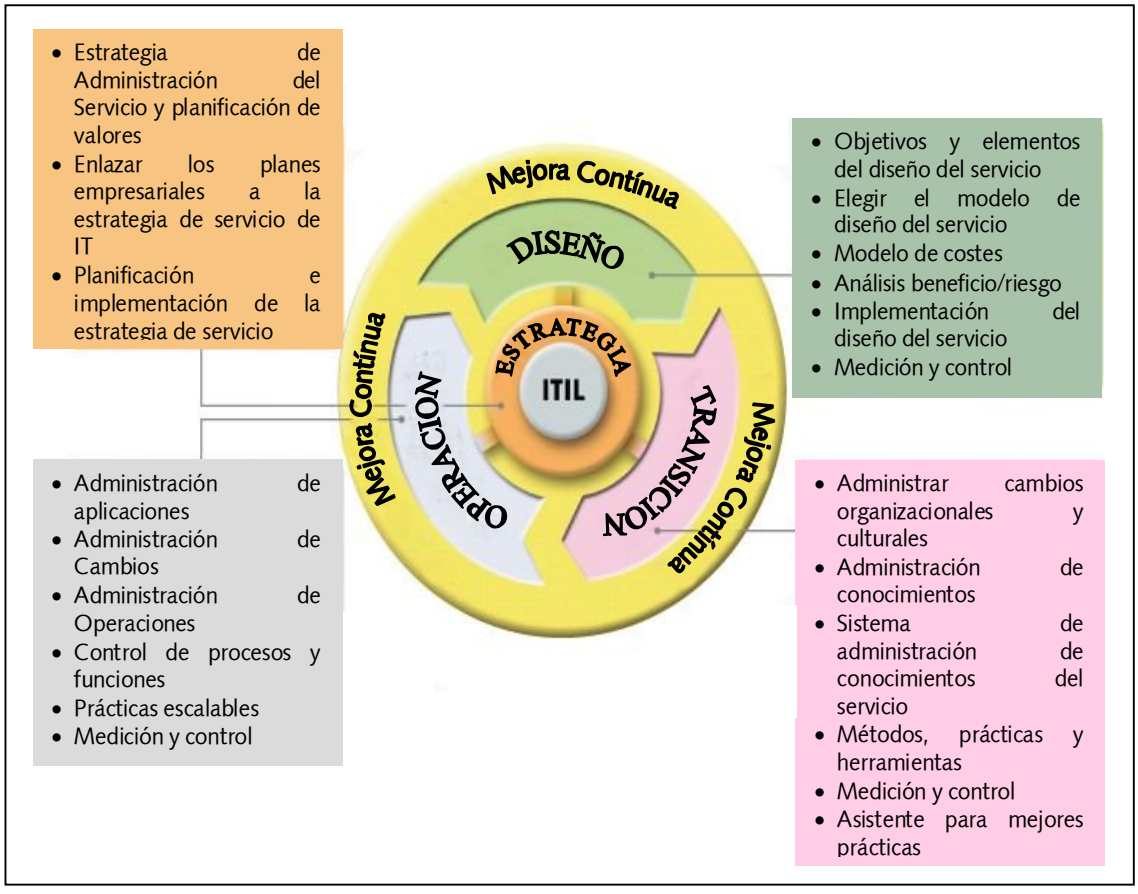


Fig. 3.1. Componentes de ITIL

La Gestión de Servicio ITIL está actualmente integrada en el estándar ISO 20000, estándar internacional para la gerencia del servicio. Fue publicada en 2005, y es ya el conductor principal para la calidad de ITSM (Information Technology Service Management)[18].

La ISO 20000 abarca dos porciones: una especificación de ITSM para la gerencia del servicio y un código de ITSM de la práctica para la gerencia del servicio.

Sin embargo cabe mencionar que no es posible certificar una organización o sistema de gestión en base a ITIL, pero una organización que haya implementado las guías de ITIL sobre Gestión de los Servicios de TI puede lograr certificarse bajo la ISO/IEC 20000. [WWW.009]

3.5. CAPABILITY MATURITY MODEL (CMM)[19]

Capability Maturity Model (CMM), mas que un método es una herramienta para definir y gestionar los procesos a realizarse en una organización, brindando una guía en la selección de estrategias para mejorar los procesos de ingeniería y administración, la calidad del software y la seguridad de la información.

Fue desarrollado inicialmente para los procesos relativos al software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute).

En noviembre de 1986 el SEI, a requerimiento del Gobierno Federal de los Estados Unidos de América, desarrolló una primera definición de un modelo de madurez de procesos en el desarrollo de software, que se publicó en septiembre de 1987.

[18] ITSM, Information Technology Service Management (Administración de Servicios de Tecnologías de la Información)
[19] Capability Maturity Model (CMM), Modelo de Capacidad y Madurez

Este modelo establece un conjunto de prácticas o procesos clave agrupados en Áreas Clave de Proceso (KPA)[20], para los cuales define un conjunto de buenas prácticas que habrán de ser:

- Definidas en un procedimiento documentado.
- Provistas (la organización) de los medios y formación necesarios.
- Ejecutadas de un modo sistemático, universal y uniforme (institucionalizadas).
- Medidas.
- Verificadas.

Consolidando de esta manera claramente sus objetivos: el de determinar el nivel de madurez del Proceso de Desarrollo y el de servir de guía en el Proceso de Desarrollo permitiendo la Mejora Continua de la organización.

Posteriormente al trabajo original del CMM o (SW-CMM) (CMM for Software), este evolucionó, publicándose un nuevo modelo en diciembre de 2000, denominándose CMMI, con el objetivo de realizar algunas mejoras el cual incluye cuatro disciplinas, en función de la amplitud de los procesos que cubre:

- CMMI-SW : Software
- CMMI-SE/SW : Ingeniería de sistemas
- CMMI-SE/SW/IPPD :Desarrollo integrado de procesos y productos
- CMMI-SE/SW/IPPD/SS : Gestión de proveedores

A su vez se presenta en dos posibles representaciones: Por niveles y Continua. En el primer caso permite evaluar el nivel de madurez de una organización en todas las áreas de proceso, mientras que el segundo permite evaluar el nivel en cada área independientemente. [LIB.005]

[20] KPA, Key Process Area (Áreas Clave de Proceso)

3.5.1. CMMI-SSE

El System Security Engineering Capability Maturity Model o Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas es un modelo derivado del CMMI, que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas.

Ha sido desarrollado por la International Systems Security Engineering Association (ISSEA), la Agencia Nacional de Seguridad (NSA) y por compañías dedicadas a las tecnologías de la información, seguridad de sistemas y defensa. La versión más actual (v3.0) fue publicada en junio de 2003.

Su característica principal es que define 22 áreas para cada una de las cuales se puede alcanzar un nivel en función del cumplimiento de unas "*características comunes*", de las cuales 11 áreas son de procesos de ingeniería y otras 11 dedicadas a la gestión de proyectos y organización, poniendo un mayor énfasis en el uso continuo de métricas.

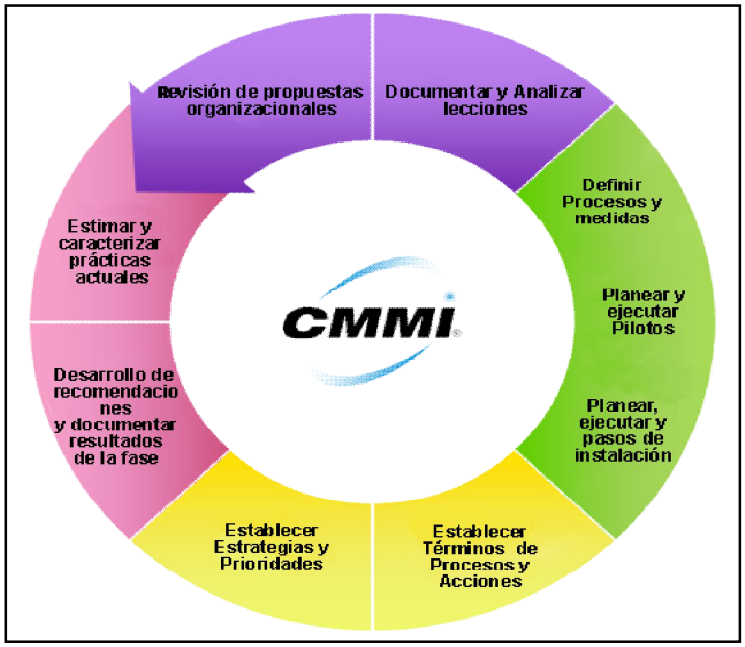


Fig. 3.2. Procesos CMMI

Básicamente es una herramienta para que las organizaciones evalúen las prácticas de ingeniería de seguridad y definan mejoras a las mismas, mediante mecanismos estándar, para que los clientes puedan evaluar la capacidad de los proveedores de ingeniería de seguridad, proporcionando a la organización un mecanismo de evaluación y certificación.

Sin embargo frecuentemente se critica al modelo CMMI por no ser más específico en la definición de los procesos, ya que para guiar a las organizaciones a definir y mejorar sus procesos indica qué actividades se han de realizar, pero nada sobre cómo hacerlo, tanto en lo referente a la ingeniería, herramientas o técnicas de gestión y seguridad. Del mismo modo, aunque exhorta a la necesidad del uso de métricas, no da ninguna guía concreta del tipo de métricas aceptables para una correcta práctica profesional.

3.6. APPLICATION SERVICES LIBRARY (ASL)[21]

ASL es una metodología utilizada en la industria de la Tecnología de la Información que describe las normas para los procesos internos de la administración de la Aplicación (Sistemas de Información y Aplicaciones).

Este estándar se originó en Holanda y se desarrollo debido a la incapacidad de estructurar la forma de trabajar dentro de los departamentos de la administración de los Sistemas de Información tan solo usando la estructura de ITIL. ITIL fue acogido por los departamentos de infraestructura de IT para estructurar sus operaciones, sin embargo este decaía en el soporte para la administración de diseño y desarrollo de aplicación.

Para ello fue creado ASL como resumen de todas las publicaciones y varios modelos para la gestión de la administración, que es un nuevo modelo y una

[21] Application Services Library (ASL), Librería de Servicios de Aplicaciones

librería que contiene un ***Framework*** con las mejores prácticas, que viene a resumir varios de los modelos más aceptados (ITIL, CMMI, entre otros).

El objetivo de este modelo, basado en el estudio de los otros, es el de ser capaz de describir la gestión de aplicaciones en profundidad, así como su amplitud, de manera que se pueda apreciar los entornos de actividad y los aspectos que requieren la atención de la dirección. El modelo soporta tres puntos de vista en la gestión: Estratégico, Táctico, y Técnico u Operacional.

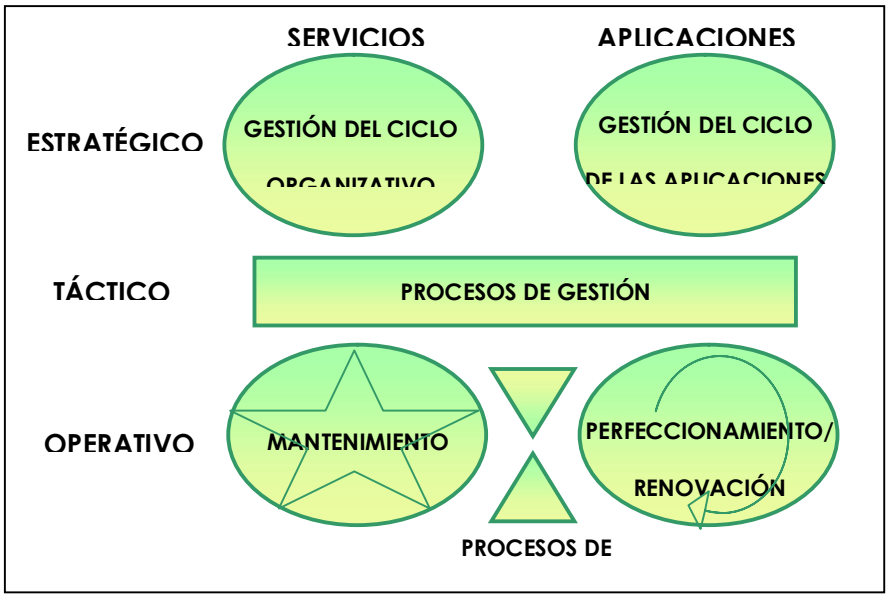


Fig. 3.3. Modelo ASL

3.6.1. NIVEL OPERATIVO

El nivel operativo contempla dos grupos de procesos:

- **Mantenimiento de aplicaciones:** Los procesos que aseguran la disponibilidad óptima de las aplicaciones actuales que soportan los procesos de negocio con un mínimo de recursos e interrupción en la operación.

- **Perfeccionamiento/Renovación de Aplicaciones:** Los procesos que adaptan las aplicaciones a nuevos requerimientos en respuesta a cambios de la organización y el entorno. Se realizan los ajustes necesarios en el software, el modelo de datos y la documentación.

3.6.2. NIVEL TÁCTICO

El nivel táctico comprende todos los procesos de gestión. Estos procesos proporcionan a la dirección la posibilidad de gestión de los mismos. Tanto el nivel estratégico como el operativo suministran la gestión de procesos, de esta forma se aseguran realidad futura.

3.6.3. NIVEL ESTRATÉGICO

El nivel estratégico también distingue dos tipos de procesos, basados en la subdivisión desde el "punto de vista del servicio" y "punto de vista de aplicación", ya que hoy en día se debe contemplar la flexibilidad en los proveedores de servicios, debido a la posibilidad de cambiar de modelo y de elegir a diferentes proveedores de servicio.

Los grupos de procesos en el nivel estratégico son:

- **Gestión del Ciclo de Organización (OCM)[22]:** los procesos enfocados al desarrollo de una futura visión de la organización de servicio de IT, trasladando la visión a una política de renovación**.**
- **Gestión del Ciclo de Aplicaciones (ACM)[23]:** los procesos que sirven para formar una estrategia a largo plazo para las aplicaciones, alineada a las previsiones de cambios organizativos a largo plazo. [WWW. 010]

3.7. PROJECT MANAGEMEN INSTITUTE (PMI)[24]

[22] OCM, Organization Cycle Management (Gestión del Ciclo de Organización)
[23] ACM, Applications Cycle Management (Gestión del Ciclo de Aplicaciones)

El Project Management Institute (PMI)**,** con más de 215.000 miembros en 150 países, es la asociación de gestión de proyectos más reconocida a nivel internacional. Dedicado al desarrollo y fomento de la gestión de proyectos, PMI ha estado comprometido con el mejoramiento de la disciplina de la Gerencia de Proyectos y a la creación de estándares en el área.

El PMI fue fundado en 1969 por cinco voluntarios en Estados Unidos. Durante los años 1970 se fundó el primer capítulo, llevándose a cabo el primer seminario fuera del país.

Durante los años 1980 se efectuó la primera evaluación para la certificación como Profesional en Gestión de Proyectos PMP (Professional Project Manager), siendo esta en la actualidad la mas reconocida en todo el mundo, posteriormente a la certificación se estableció un código de ética para la profesión. En los años 1990 fue publicada la primera edición de la Guía del PMBOK (A Guide to the Project Management Body of Knowledge), texto base para la enseñanza de Gestión de Proyectos y para la creación de los estándares profesionales que se fundamentan en el.

La Guía del PMBOK, contiene una descripción general de los fundamentos de la Gestión de Proyectos reconocidos como buenas prácticas. Actualmente en su tercera edición, es el único estándar ANSI (Instituto de Estándar Nacional Americano) para la gestión de proyectos[25]. Todos los programas educativos y certificaciones brindadas por el PMI están estrechamente relacionados con el PMBOK.

[24] Project Managemen Institute (PMI), Instituto para la Gestión de Proyectos
[25] ANSI, American National of Standard Institute (Instituto de Estándar Nacional Americano)

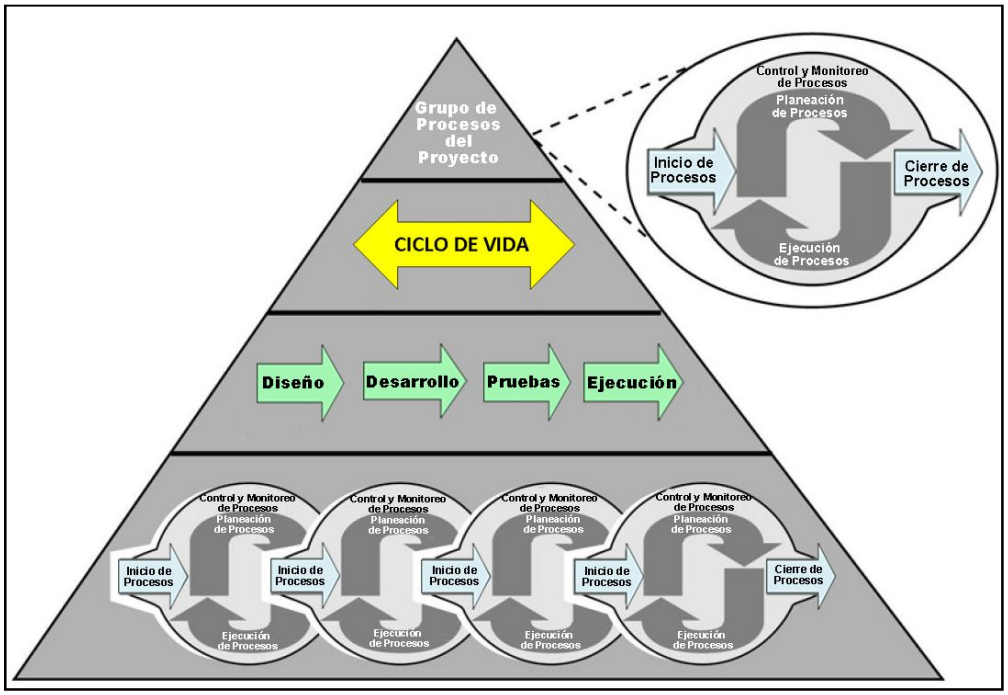


Fig. 3.4. Triángulo PMI, Procesos del Proyecto Administrativo.

3.7.1. CERTIFICACIONES CAPM Y PMP

El Project Management Institute ofrece dos niveles de certificación:

- Asociado en Gestión de Proyectos Certificado CAPM (Certified Assistant in Project Management), acreditado a quienes demuestran una base común de conocimientos y términos en el campo de la gestión de proyectos. Para ello se requiere 1500 horas de trabajo en un equipo de proyecto o 23 horas de educación formal en gestión de proyectos para conseguir esta certificación.

- Profesional en Gestión de Proyectos PMP (Professional Project Manager), acreditado a quienes han experimentado una educación específica y requerimientos de experiencia bajo los códigos de conducta profesional. Además, aprobar el examen designado para determinar y medir objetivamente sus conocimientos en gestión de proyectos. Un PMP debe

satisfacer requerimientos de certificación continuos, de lo contrario perderá la certificación.

En el 2006, el PMI reportó más de 220,000 miembros y cerca de 200,000 PMPs en 175 países. Más de 40,000 certificaciones PMP expiran anualmente, ya que un PMP debe documentar experiencia en proyectos en curso y educación cada tres años.

El PMP Certification es la certificación más distinguida y valorada a nivel mundial en esta área, los profesionales son reconocidos como miembros del grupo de practicantes certificados internacionalmente más exitoso de la profesión de la Dirección de Proyectos [WWW.011]

3.8. AUSTRALIAN STANDARD FOR CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) - AS 8015[26]

Las aplicaciones útiles, modelos comerciales exitosos, leyes y normas sociales muchas veces sólo surgen claras algún tiempo después de que una nueva tecnología surge. Los nuevos riesgos surgen a menudo al igual que las iniciativas en las Tecnologías de la Información y Comunicaciones se desarrollan y las prácticas comerciales maduran.

AS8015 Norma australiana para la Gobernación Corporativa de la Tecnología de la Información y Comunicaciones desarrollada en el 2005, se bosquejó en el contexto de pérdidas corporativas significantes en Australia, notablemente el fracaso de ONE.TEL. En amplia escala el ***Outsourcing*** también había demostrado que los intereses de los vendedores no siempre estaban alineados con los de la organización.

[26] Australian Standard for Corporate Governance of Information and Communication Technology - AS 8015, Norma Australiana para la Gobernación Corporativa de Tecnología de la Información y Comunicación

Por ello el AS, un informe breve y conciso, presenta una guía para el Gobierno y el uso de las Tecnología de la Información y Comunicaciones eficazmente.

La norma AS 8015 proporciona un Framewok que fluye a través de los Directores, personal al cual se delegan las responsabilidades y manejo los funciones de la organización, tales como los Gerentes Senior, especialistas técnicos, vendedores y proveedores de servicio, permitiéndoles comprender de mejor manera sus obligaciones para el desarrollo eficaz del trabajo, aumentar al máximo los beneficios y minimizar los riesgos de la organización que provienen de las TI.

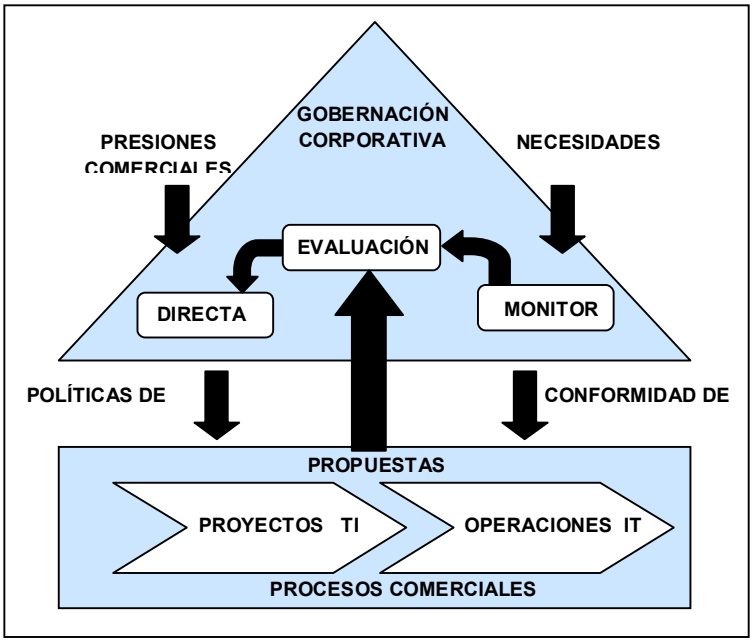


Fig. 3.5. Framework del Modelo AS 8015

La serie 8000 de normas de la Gobernación Corporativas provee una guía para aquellos que deseen mejorar en los siguientes aspectos:

- Los Principios de la Gobernación
- Control para el fraude y Corrupción
- Códigos de Conducta Organizacional
- Responsabilidad Social Corporativa
- Protección de Programas Whistle Blower

La mundialmente reconocida norma AS4360 de Riesgo y Dirección también se revisó en 2004. Esto junto con la adopción de BS15000 (ahora ISO 20000) como AS8018 Administración de Servicios de IT, proporcionó el contexto para el bosquejo y publicación subsiguiente de AS8015, que provee una guía de la Ggobernación Corporativa de Información y la Tecnología de la Comunicación para las organizaciones, anteriormente mencionada.

Actualmente las publicaciones realizadas por el Comité de Normas de Australia AS8015 y AS8018, forman parte de ISO20000.

3.9. SIX SIGMA[27]

SIX SIGMA es una metodología de gestión de la calidad, centrada en el control de procesos cuyo objetivo es lograr disminuir el número de defectos en la entrega de un producto o servicio al cliente, comprendiendo todo un sistema donde se da importancia al establecimiento de metas acordes con los requisitos del cliente, la medición estadística de los resultados, la reingeniería, el trabajo en equipo y la mejora continua.

La metodología SIX SIGMA fue creada por Motorola en el año 1982, posteriormente se consolidó de la mano de General Electric y en la actualidad es utilizada en todo el mundo por todas aquellas empresas que compiten para ocupar niveles de liderazgo en su sector.

Esta metodología se basa en la curva de la distribución normal (para conocer el nivel de variación de cualquier actividad), que consiste en elaborar una serie de pasos para el control de calidad y optimización de procesos industriales.

La estructura para el desarrollo de SIX SIGMA está basada en la creación de equipos de trabajo liderados por los llamados Cinturones Verdes o Negros, según la importancia económica del proyecto, estos equipos a su vez están representados

[27] Six Sigma, Seis Sigma (σ)

en el equipo de dirección de la empresa por los llamados Champions, con el fin de dar apoyo y soporte a las actividades que el equipo de trabajo desarrolle.

El proceso Six Sigma se caracteriza por 5 etapas bien definidas:

- Definir el problema o el defecto
- Medir y recopilar datos
- Analizar datos
- Mejorar
- Controlar

Procesos que son definidos en las metodologías: DMAIC (Definir, Medir, Analizar, Mejorar y Controlar) y DMADV (Definir, Medir, Analizar, Diseñar y Verificar).

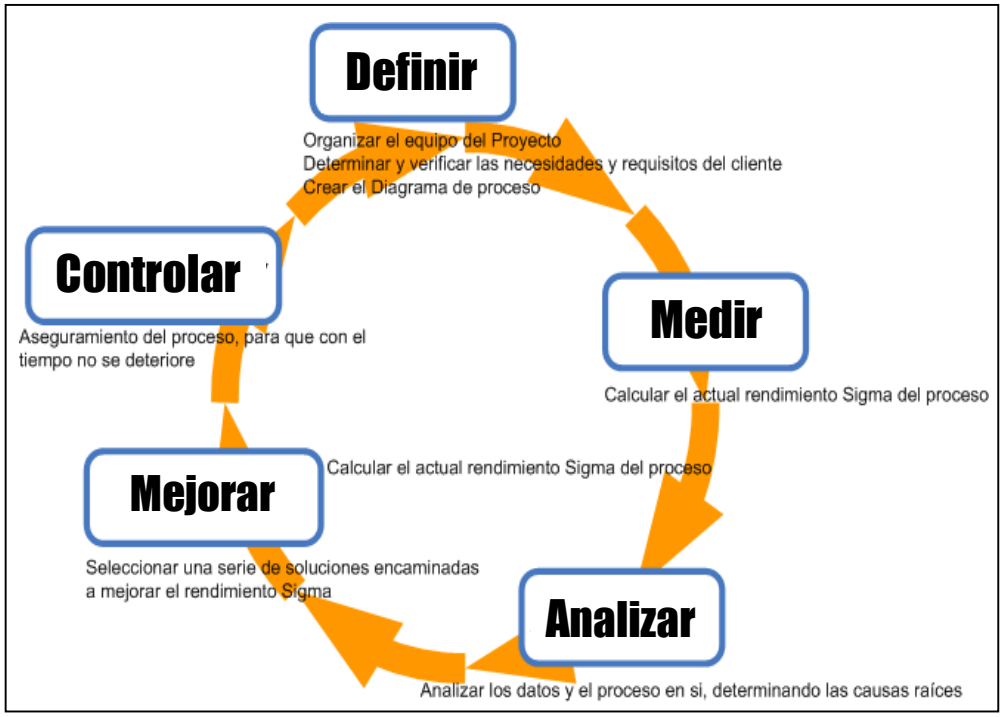


Fig. 3.6. Mejora Continua (D.M.A.I.C.)

3.9.1. DEFINIR (D)

En la fase de definición se identifican los posibles proyectos SIX SIGMA, que deben ser evaluados por la dirección para evitar la infrautilización de recursos. Una vez seleccionado el proyecto se prepara su misión y se selecciona el equipo más adecuado para el proyecto, asignándole la prioridad necesaria.

3.9.2. MEDIR (M)

La fase de medición consiste en la caracterización del proceso identificando los requisitos clave de los clientes, las características clave del producto (o variables del resultado) y los parámetros (variables de entrada) que afectan al funcionamiento del proceso y a las características o variables clave. A partir de esta caracterización se define el sistema de medida y se mide la capacidad del proceso.

3.9.3. ANALIZAR (A)

En esta fase, el equipo analiza los datos de resultados actuales e históricos. Se desarrollan y comprueban hipótesis sobre posibles relaciones causa-efecto utilizando las herramientas estadísticas pertinentes. De esta forma el equipo confirma los determinantes del proceso, es decir las variables clave de entrada o "pocos vitales" que afectan a las variables de respuesta del proceso.

3.9.4. MEJORAR (I)[28]

En la fase de mejora el equipo trata de determinar la relación causa-efecto (relación matemática entre las variables de entrada y la variable de respuesta que interese) para predecir, mejorar y optimizar el funcionamiento del proceso. Por

[28] Mejorar, Improve (I)

último se determina el rango operacional de los parámetros o variables de entrada del proceso.

3.9.5. CONSOLIDAR (C)

La fase de control, consiste en diseñar y documentar los controles necesarios para asegurar que lo conseguido mediante el proyecto Seis Sigma se mantenga una vez que se hayan implantado los cambios. Cuando se han logrado los objetivos y la misión se dé por finalizada, el equipo informa a la dirección y se disuelve.

La aplicación del SIX SIGMA, ha generado un avance en los sistemas de calidad y por lo tanto en los productos, a través del uso disciplinado de datos, análisis estadístico y práctica intensiva de administración, mejora y re-diseño de procesos, para mejorar la rentabilidad de las organizaciones, donde la mejora en calidad y eficiencia son subproductos inmediatos de SIX SIGMA. [WWW.0.12]

3.10. SARBANES OXLEY (SOX)

La Ley Sarbanes-Oxley Act. (SOX), fue establecida por el Congreso de los Estados Unidos de América, como respuesta al gran número de escándalos financieros y contables relacionados con algunas de las más importantes compañías en este país como: Enron, Tyco International, WorldCom y Peregrine Systems, sucitados a finales del 2001, producto de quiebras, fraudes y otros manejos administrativos no apropiados. Estos escándalos repercutieron negativamente sobre la confianza depositada por parte de los accionistas y el Estado, con efectos negativos sobre la eficiencia de los mercados de capitales. Asustados por las repercusiones económicas que la prolongación de esta situación hubiese podido causar, las autoridades americanas decidieron que la mejor solución era endurecer los controles impuestos a las empresas. Es importante

notar que esta ley, en sus inicios alcanzó únicamente a aquellas compañías inscritas en el Security Exchange Comision (SEC) de EEUU.

Es así que en Julio 30 del 2002, la Ley impulsada por el senador demócrata Paul Spyros Sarbanes y el congresista Michael G. Oxley, fue aprobada por el gobierno de Estados Unidos, como mecanismo para endurecer los controles de las empresas y devolver la seguridad en los mercados de valores sobre la información financiera.

El texto legal abarca temas como el buen gobierno corporativo, la responsabilidad de los administradores, la transparencia, y otras importantes limitaciones al trabajo de los auditores, que van más allá de de la auditoría financiera.

3.10.1. REGLAMENTACIONES

La Ley SOX incluye un aumento en el hermetismo de la divulgación financiera, procesos mejorados para denunciantes internos y la sección más destacada que concierne a la responsabilidad de directores generales y financieros. SOX ordena que estos directores certifiquen todas las declaraciones financieras e impone penas individuales a estas personas. Los requisitos de la ley Sarbanes Oxley exigen sólidos cambios tecnológicos y de cultura en los procedimientos y rutinas de los recursos humanos.

Esta Ley contiene 11 títulos y numerosas secciones, en los cuales regula diferentes aspectos empresariales. En síntesis las regulaciones observadas por la ley respecto a la gerencia de las compañías son las siguientes:

- Requerimiento de comités de auditoría independientes que deben incluir, al menos, un experto financiero que tenga la capacidad de interpretar y detectar situaciones anómalas.

- Sanciones (multas y prisión) por la presentación de estados financieros fraudulentos.
- Códigos de ética para funcionarios "senior", basándose en la premisa que el comportamiento ético debe transmitirse desde la cúpula directiva hacia las bases.
- Revelar en tiempo real cambios que afecten de forma importante al negocio y que, por tanto, deban ser conocidos por el público inversor
- Responsabilidad personal definida del director general y director financiero sobre la "exactitud" en los estados financieros y adecuados controles internos sobre la información financiera. [WWW.013]

Además, dentro de las regulaciones se establecen las multas y penas para los responsables legales, mismas que van desde 1 a 5 millones de dólares, o de 10 a 20 años de cárcel, y en algunos casos las dos situaciones. Esta sección de código penal en la Ley es toda una novedad, ya que específica la pena para el tipo de infracción en cuestión, y endurece las penas anteriormente existentes para este tipo de delitos.

3.10.2. SECCIÓN 404

El artículo 404 de la Ley Sarbanes-Oxley o IT CONTROL OBJETIVES FOR SARBANES-OXLEY, impone la necesidad de controles internos realizados mediante las técnicas que ofrecen las tecnologías de la información sobre la información y las declaraciones financieras. Los departamentos competentes en tecnologías de la información, los equipos de auditores internos y externos y los cuadros directivos deberán desarrollar una relación activa para asegurar que tales controles sean implementados en todas las áreas exigidas. Las organizaciones, deben certificar la información que revelen garantizando que los controles internos aseguren la integridad de los datos que se incluyan.

Además de ello, el auditor de la compañía debe estar de acuerdo con la Dirección respecto a la cantidad necesaria de controles internos diseñados para proteger la integridad y confidencialidad de la información. El objetivo de esta legislación es el de poder transmitir de forma segura la información entre las organizaciones. Esto incluye algunas medidas estrictas de privacidad y seguridad entre las que figuran el acceso restringido a la información y el uso de codificación.

El marco de control interno sugerido, para cumplir con los lineamientos establecidos por la Ley SOX para la prevención de fraudes en las Tecnologías de la Información (TI) y Control Interno fue diseñado por COSO.

Las normas referidas a las Tecnologías de la Información son:

- Implementar un programa completo de Controles de Tecnologías de la Información para todos los sistemas que incluyan informes financieros.
- Comprobar que los sistemas cumplen los indicadores de referencia adecuados para garantizar la integridad y validez de la información financiera.
- Dirigir y ajustar correctamente todos los Controles Internos de Tecnologías de la Información mediante evaluaciones de riesgo adecuadas, análisis y verificación del cumplimiento de las normas.
- Proteger la seguridad o integridad de la información contra cualquier amenaza o riesgo previsible.

Cabe mencionar que también se incluye al personal que esté inmerso en el estudio de los Sistemas de Gestión de Seguridad de la Información, Risk Management, Control Plans, entre otros.

3.11. COMMITEE OF SPONSORING ORGANIZATION OF THE TREADWAY COMMISSION (COSO)[29]

La necesidad de integrar metodologías y conceptos en todos los niveles de las diversas áreas administrativas y operativas con el fin de ser competitivos y responder a las nuevas exigencias empresariales, dio surgimiento a un nuevo concepto de control interno denominado informe COSO.

El Committee of Sponsoring Organization of Treadway Commission (COSO) fue originalmente instaurado en el año 1985 con la finalidad de estudiar los factores que permitían la emisión fraudulenta de reportes financieros.

COSO plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo de la TREADWAY COMMISSION y NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING. Este grupo estaba constituido por representantes de las siguientes organizaciones:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executive Institute (FEI)
- Institute of Internal Auditors (IIA)
- Institute of Management Accountants (IMA)

El objetivo fundamental era el definir un nuevo marco conceptual del control interno, capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre este tema, logrando así que, al nivel de las organizaciones públicas o privadas, de la auditoría interna o externa, o de los niveles académicos o legislativos, se cuente con un marco conceptual común, una visión integradora que satisfaga las demandas generalizadas de todos los sectores involucrados.

[29] Committee of Sponsoring Organization of the Treadway Comisión (COSO), Organización para el Desarrollo de la Comunicación y la Sociedad

En 1990, el Comité junto con la asesoría de PricewaterhouseCoopers, realizó un estudio extensivo sobre controles internos, cuyo resultado fue el marco de control interno COSO, que consta de componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión, que pueden ser implementados en todas las compañías de acuerdo a las características administrativas, operacionales y de tamaño.

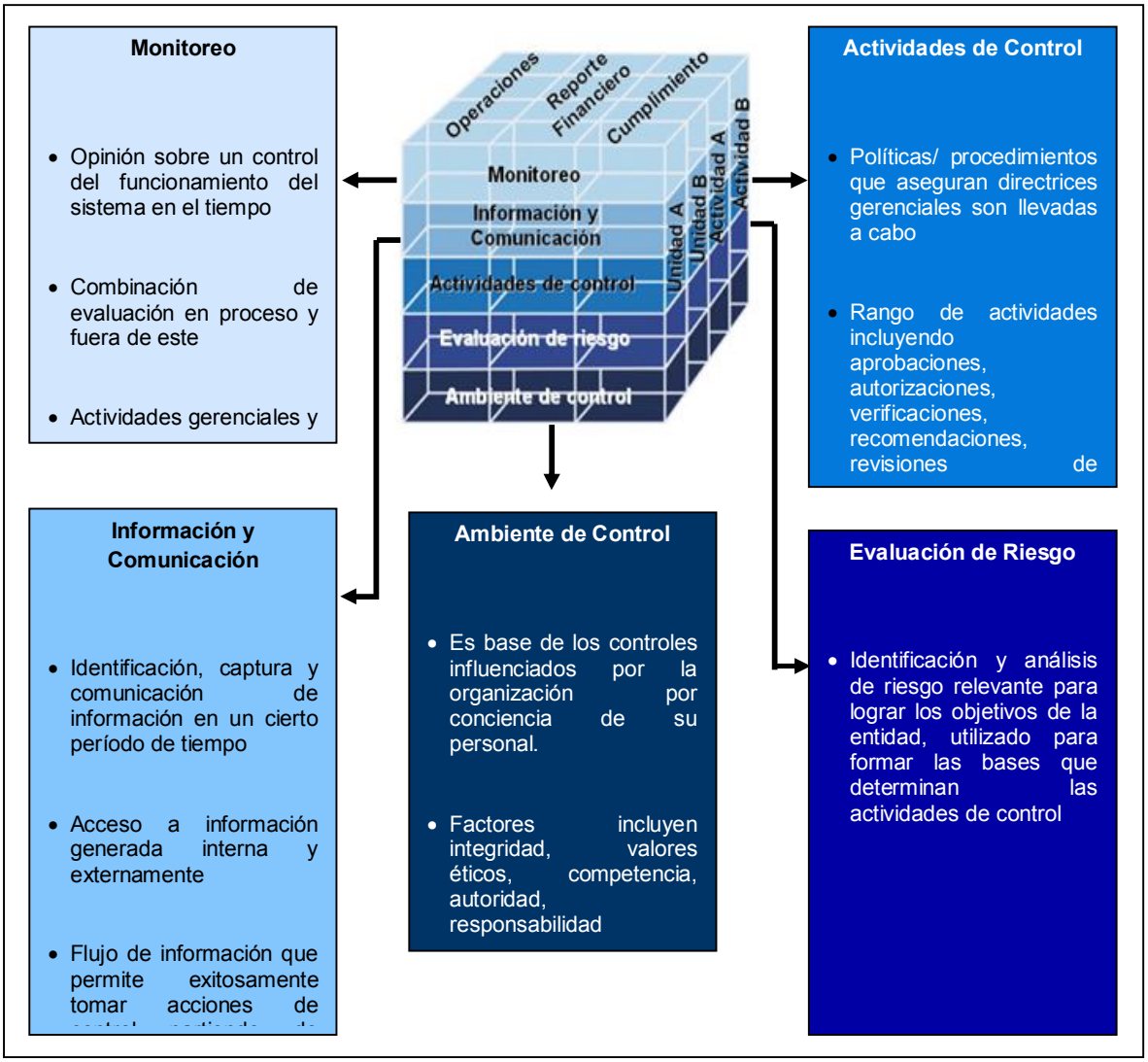


Fig. 3.7. Los cinco (5) componentes de Control Interno según COSO

3.11.1. COMPONENTES COSO

COSO posee cinco (5) componentes de control los cuales, al ser integrados en cada una de las unidades de negocio de la organización, ayudan a lograr los objetivos de control en los siguientes aspectos: eficiencia y efectividad de las operaciones para alcanzar los objetivos del negocio, preparación de cuentas financieras confiables y el cumplimiento de leyes y regulaciones.

A continuación se indican las características de control de los cinco (5) componentes COSO:

3.11.1.1.AMBIENTE DE CONTROL

Entre los factores, interno o externos, que pudiesen incidir en un ambiente de control, se encuentran los siguientes: integridad y valores morales del personal, compromiso para contratar y mantener personal de calidad, capacidad en la identificación de riesgos operacionales, adiestramiento especializado sobre la aplicación de controles internos y los roles desempeñados por la Junta y el Comité de Auditoría.

3.11.1.2.EVALUACIÓN DE RIESGO

Incluye procedimientos para identificar cambios externos que puedan afectar el negocio, herramientas y metodologías para la identificación, evaluación y medición de los riesgos operacionales y evaluación periódica de los riegos operacionales en las diversas áreas de la organización. En este sentido, se establecen los siguientes objetivos de la evaluación del riesgo: existencia, totalidad, derechos y obligaciones, evaluación, presentación, divulgación y segregación de funciones.

3.11.1.3.ACTIVIDADES DE CONTROL

Se refieren a las acciones tomadas para implementar políticas y estándares dentro de las organizaciones. La Ley SOX requiere la evaluación de las actividades de control para cada actividad relevante del negocio. Las actividades de control incluyen administración de los riesgos operacionales en los procesos de negocio, control de acceso a los sistemas de información y recursos informáticos, así como la existencia de controles para mitigar errores operacionales. Adicionalmente, exige una evaluación de los controles generales de cómputo, asociados al área de Tecnologías de la Información (TI).

3.11.1.4.INFORMACIÓN Y COMUNICACIÓN

Incluye el despliegue de información suficiente para la toma de decisiones, información adecuada y oportuna de los sistemas de información, comunicación apropiada entre los Departamentos para la coordinación de actividades conjuntas, así como la disponibilidad de medios para comunicar irregularidades y resultados a la Alta Gerencia de la Compañía.

3.11.1.5.MONITOREO

Un sistema de control necesita ser monitoreado para asegurar que el mismo continúa operando efectivamente. Esto incluye actividades de supervisión, así como la labor desempeñada por Auditoría Interna. El seguimiento incluye el monitoreo permanente entre los indicadores de riesgos operacionales y situaciones críticas, seguimiento periódico a la efectividad de los controles implantados, así como la disponibilidad de herramientas para el monitoreo de los riesgos operacionales y su impacto. [WWW.014]

3.12. BRITISH STANDARDS INSTITUTION (BSI)[30]

El British Standards Institution ha sido el encargado de ejecutar varias actividades y sin lugar a dudas, la parte central de estas es la creación y actualización de normas; su trabajo ha dado pauta a la conformación de entidades internacionales tales como ISO, que favorecen el desarrollo de la normalización en el mundo, con miras a facilitar entre las naciones los intercambios comerciales y de realizar el entendimiento en los planes técnico y económico en las organizaciones.

El origen de las organizaciones encargadas de crear normas para la industria tiene su inicio en Gran Bretaña. El Comité de Normas de Ingeniería establecido en 1901 fue el primer organismo que emitió reglamentos definidos para que se desarrollaran procesos de ingeniería en las industrias manufactureras. Luego se le cambió el nombre en 1918 por British Engineering Standards Association (Asociación Británica de Normas para Ingeniería), organismo que recibió la Carta Real Constitucional en 1929; posteriormente, en 1931 se enmienda la carta constitucional, para cambiar a su nombre actual British Standards Institution (Instituto Británico de Normas) con el objeto de reflejar su expansión fuera de los dominios de la ingeniería.

Con ello se amplificó el desarrollo del trabajo en normas a ser aplicables en diferentes sectores como la industria, la ingeniería, construcción, energía, medio ambiente entre otras.

3.12.1. BS 7779

En mayo del 1987 la Fundación del Centro de Seguridad de Informática Comercial dependiente del Departamento de Comercio e Industria del Reino Unido (CCSC/DTI), establecieron criterios de evaluación internacionalmente

[30]British Standards Institution (BSI), Instituto Británico de Normas

reconocidos, con el objetivo de cubrir dos áreas fundamentales: la primera establecida para la certificación y evaluación en relación con productos de seguridad en las tecnologías de la información, dando lugar a ITSEC (Information Technology Security); y la segunda consistente en un Código de Práctica para Usuarios, como una guía de ayuda, este trabajo con un esquema de asociación fue publicado en 1989.

Más tarde fue mejorado por el Centro de Nacional de Computación y posteriormente por un consorcio de usuarios en representación de la Industria Británica, con el objetivo de que fuera comprensible y práctico. El resultado se publicó en 1993 como Código de Prácticas para la Gestión de la Seguridad de la Información, también conocido como PD003.

Este código se publica a su vez en 1995 como Estándar Británico BS7799, teniendo una rápida aceptación. En 1998 se publica la parte dos de la norma relacionada con el código de Buenas Prácticas, denominándose BS7799-2, cuyo contenido permite implantar un SGSI (Sistema de Gestión de Seguridad de la Información) en base al ciclo PDCA[31](Plan, Do, Check, Act); luego de un periodo de revisión conjunta, se publican los resultados en 1999 con la nomenclatura de BS7799-1 parte uno y BS7799-2 parte dos.

El BS7799 esta organizado en 10 secciones:

- Políticas de Seguridad
- Organización de Activos y Recursos
- Clasificación y Control de Activos
- Seguridad del Personal
- Seguridad Ambiental y Física
- Comunicaciones y Administración de Operaciones
- Control de Acceso
- Sistemas de Desarrollo y Mantenimiento

[31] PDCA, Plan - Do - Check - Act (Planificar, Hacer, Verificar, Actuar)

- Administración de Continuidad del Negocio
- Acatamiento

Pese a los códigos emitidos y a otros diferentes desarrollados en otros países por organismos normativos nacionales, no existía mayoritariamente la tendencia de certificar dichos procesos, o sistemas de gestión a nivel internacional, por ello, ISO vino a redefinir la certificación con la finalidad principal de promover el desarrollo de estándares internacionales y actividades relacionadas de conformidad a estatutos, para facilitar el intercambio de bienes y servicios en todo el mundo. [WWW.015]

3.13. INTERNATIONAL STANDARDS ORGANIZATION (ISO)[32]

La International Standards Organization, es una organización internacional no gubernamental, compuesta por representantes de los organismos de normalización (ONs) nacionales, que establece normas internacionales industriales y comerciales. Dichas normas se conocen como normas ISO y su finalidad es la coordinación de las normas nacionales, en consonancia con el Acta Final de la Organización Mundial del Comercio, con el propósito de facilitar la comercialización, facilitar el intercambio de información y contribuir con unos estándares comunes para el desarrollo y transferencia de tecnologías.

ISO e IEC[33] (International Electrotechnical Commission) conforman un especializado sistema para los estándares mundiales que tiene sus orígenes en Londres en octubre de 1946 después de la segunda guerra mundial.

Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los borradores de estas normas adoptadas por la unión de este comité

[32] International Standards Organization (ISO), Organización Internacional de Estandarización
[33] IEC, International Electrotechnical Comisión (Comisión Electrotécnica Internacional)

técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una norma internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

3.13.1. ISO/IEC 27002

Hasta inicios del año 1999 no existía una norma ISO relacionada con las Tecnologías de la Información, ya que al momento se certificaba en normas inglesas (BSI) o españolas (UNE).

Es así que tras la publicación del Estándar Británico BS7799, la parte uno BS7799-1(Guía de Buenas Prácticas) es propuesta en octubre de 1999 como norma ISO, que tras breves modificaciones y siguiendo la vía de aprobación rápida "*Fast Track"*, en diciembre del 2000 la BS7799-1 se publicó como Estándar Internacional ISO/IEC17799, convirtiéndose desde entonces en la nueva norma de referencia. Luego del periodo natural de revisión fijado por ISO en cinco (5) años esta norma ha sido revisada y nuevamente publicada en junio del 2005 como ISO/IEC 17799:2005.

Sin embargo el pasado 1 de julio del 2007, ISO publicó el llamado *"Technical Corrigendum"* (ISO/IEC 17799:2005/Cor.1:2007-07-01 - Information technology - Security techniques - Code of Practice for Information Security Management), es decir, se aprobó el cambio de denominación de la ISO/IEC 17799 por ISO/IEC 27002:2005 ya que su contenido publicado en junio del 2005 no ha sido modificado.

Con este paso la norma ISO/IEC 17799 ahora ISO/IEC 27002 se incorpora a la familia ISO 27000.

ISO/IEC 27002 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. Por ello el objetivo

de la norma ISO/IEC 27002 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad, sin embargo se trata de una norma no certificable, pero que recoge la relación de controles a aplicar para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI).

La norma no cambia el contenido y su texto sigue incluyendo 33 objetivos de control y 133 controles agrupados en los siguientes 11 dominios de control que cubren por completo la Gestión de la Seguridad de la Información, estos son:

- Política de Seguridad.
- Organización de la Seguridad de la Información.
- Control y Clasificación de los recursos de información (Gestión de Activos).
- Seguridad del Personal.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Acceso.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- **Gestión de Incidentes de Seguridad de la Información [**].**
- Gestión de Continuidad del Negocio.
- Cumplimiento (Conformidad con la Legislación).

Sin embargo, ISO/IEC 27002 no ordena los procedimientos específicos, ni tampoco define cómo implementar los controles necesarios. Como tal, las empresas que desean adoptar los estándares ISO/IEC 27002 u obtener las certificaciones BS 7799 se encuentran frente a estos problemas:

- Evaluar, planificar y diseñar programas para los cumplimientos de ISO 27002 / BS7799

[**] Las modificaciones realizadas a BS7799 dieron como resultado un nuevo control que se anexó a ISO/IEC 17799 publicada en junio del 2005, ahora nominada ISO/IEC 27002

- Implementar y coordinar a las personas, a los procesos y a la tecnología requerida para cumplir con los estándares
- Administrar y mantener de manera continua los controles de seguridad y los procedimientos establecidos, junto con la supervisión, corrección y ajustes necesarios cuando no se cumplen los estándares. [WWW.016]

3.13.2. ISO/IEC 27001

En el año de 1999 surgió la idea de posibilitar que la parte dos de BS7799 se convirtiera también en ISO, sin embargo en esta se contemplaba la ausencia de indicaciones para utilizar, mantener y mejorar el Sistema de Gestión de la Seguridad de la Información (SGSI).

Luego en el 2002 la BS7799-2 alcanza la madurez y adopta el modelo PDCA (Plan, Do, Check, Act) que se encuentra en ISO9001 e ISO14001, además de reflejar los principios establecidos en la guía de OCDE para el adecuado gobierno de la información y redes. En el 2005 el BS7799-2 se revisa para adecuarse a normas ISO de sistemas de gestión y entra en proceso de aprobación rápida que culmina con la publicación del Estándar Internacional como ISO27001 el 15 de octubre de ese año.

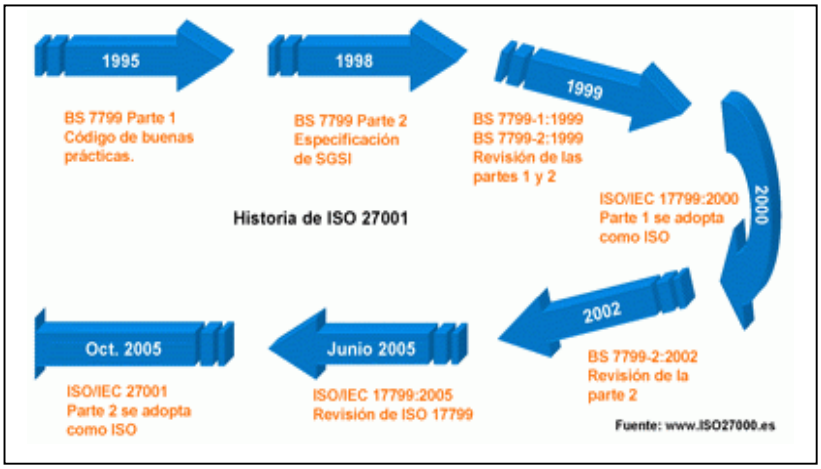


Fig. 3.8. Evolución de ISO/IEC 27001

ISO/IEC 27001 fue diseñado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI, la adopción del SGSI debe ser una decisión estratégica de la organización, ya que está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa.

El anexo A de esta norma propone una detallada tabla de los controles, los cuales quedan agrupados y numerados de la siguiente forma:

- A.5 Política de Seguridad
- A.6 Organización de la Información de Seguridad
- A.7 Administración de Recursos
- A.8 Seguridad de los Recursos Humanos
- A.9 Seguridad Física y del Entorno
- A.10 Administración de las Comunicaciones y Operaciones
- A.11 Control de Accesos
- A.12 Adquisición de Sistemas de Información, Desarrollo y Mantenimiento
- A.13 Administración de los Incidentes de Seguridad
- A.14 Administración de la Continuidad de Negocio
- A15 Cumplimiento (Legales, de Estándares, Técnicas y Auditorías)

El anexo B, que es informativo, a su vez proporciona una breve guía de los principios de OECD (Guía de Administración de Riesgos de Sistemas de Información y Redes) y su correspondencia con el modelo PDCA. Además del Anexo C, también informativo, resume la correspondencia entre esta norma y los estándares ISO 9001:2000 y el ISO 14001:2004

Este estándar internacional adopta el modelo PDCA (Plan, Do, Check, Act), el cual es aplicado a toda la estructura de procesos de SGSI (Sistema de Gestión de la Seguridad de la Información) y significa lo siguiente:

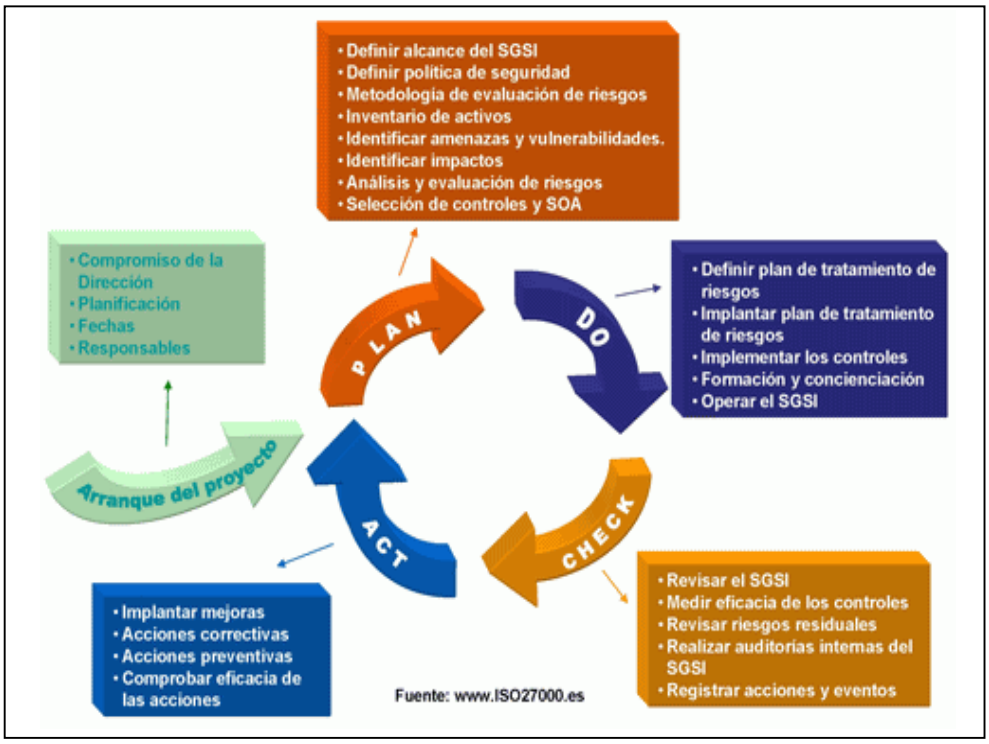


Fig. 3.9. Estructura de ISO/IEC 27001

3.13.2.1.PLAN (Establecer el SGSI)

La planificación comprende:

- Definición del alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI.
- Establecimiento de políticas de seguridad: Esta deben incluir el marco general y los objetivos de seguridad de la información de la organización, tomándose en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, alineada con la gestión de riesgo general, además de establecer criterios de evaluación de riesgos aprobados por la Dirección.
- Definir enfoque de evaluación de riesgos: Definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.

- Inventario de activos, de todos aquellos activos de información que tienen algún valor para la organización y que estén dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades que afecten a los activos del inventario.
- Identificar impactos: Todos los impactos que podrían suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: Evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: Formas en las cuales el riesgo puede ser reducido, eliminado, aceptado o transferido.
- Selección de controles: Seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: Los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
- Confeccionar una Declaración de Aplicabilidad: SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. [WWW.016]

3.13.2.2.DO (Implementar y Operar el SGSI)

Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

- Definir plan de tratamiento de riesgos: Que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos**:** Con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: Todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: De todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: Normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

3.13.2.3.CHECK (Monitorizar y Revisar el SGSI)

Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- Ejecutar procedimientos y controles de monitorización y revisión: Para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, además de determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Revisar regularmente la eficacia del SGSI: En función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

- Medir la eficacia de los controles: Para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente la evaluación de riesgos: Los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.
- Realizar regularmente auditorías internas: Para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- Revisar regularmente el SGSI por parte de la Dirección: Con ello se determinará si el alcance definido sigue siendo el adecuado, además de identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- Actualizar planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI que sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

3.13.2.4.ACT (Mantener y Mejorar el SGSI):

Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del SGSI.

- Implantar mejoras, poniendo en marcha todas aquellas que se hayan propuesto en la fase anterior.
- Acciones correctivas para solucionar no conformidades detectadas.
- Acciones preventivas para prevenir potenciales y no conformidades.

- Comunicar las acciones y mejoras con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos, la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

La organización deberá mejorar continuamente la eficiencia del SGSI a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración, para eliminar las causas que no estén en conformidad con los requerimientos del SGSI con la finalidad de evitar la recurrencia de los mismos.

ISO/IEC 27001 es la norma principal de requisitos del sistema de gestión de seguridad de la información con los adecuados objetivos de control y controles que desarrolla para el desarrollo de un SGSI; sin embargo a pesar de no ser obligatoria la implementación de todos los controles, la empresa deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Actualmente la ISO-27001:2005 es un estándar aceptado internacionalmente para la administración de la seguridad de la información aplicable a todo tipo de organizaciones, tanto por su tamaño como por su actividad. [WWW.016]

3.14. GOBERNABILIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

En la actualidad la evolución en el concepto de la Administración de las Tecnologías de la Información ha pasado de considerar las TI desde el punto de vista puramente tecnológico a considerarlas como habilitadoras del negocio, focalizando de forma primordial las necesidades y requerimientos de la empresa mediante la integración de las TI, con el logro de los objetivos de la empresa como parte fundamental de la estrategia organizacional.

Es debido a esta relación de dependencia entre TI y los con requerimientos de la empresa, que la Gobernabilidad de TI se ha tornado en un eje clave en el ámbito organizacional.

Por ello surge CObIT, como una herramienta efectiva basada en estándares técnicos internacionales de: Tecnologías de la Información, Control interno y Auditoría, y Negocios, que provee un marco para el control y la gobernabilidad de TI mediante una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de estratégicos empresariales y añadir valor mientras se balancean los riesgos versus el retorno sobre TI y sus procesos. (Fig. 3.10)

La orientación al negocio es el tema principal de CObIT, ya que proporciona un Gobierno de TI que une los procesos de TI, los recursos de TI y la información con las estrategias y los objetivos de la empresa, además de integrar e institucionalizar buenas (o mejores) prácticas de planeación y organización, adquisición e implementación, entrega de servicios - soporte y monitoreo del desempeño de TI, para asegurar que la información de la empresa y las tecnologías relacionadas soportan los objetivos del negocio; conduciendo a la organización a tomar total ventaja de su información logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva.

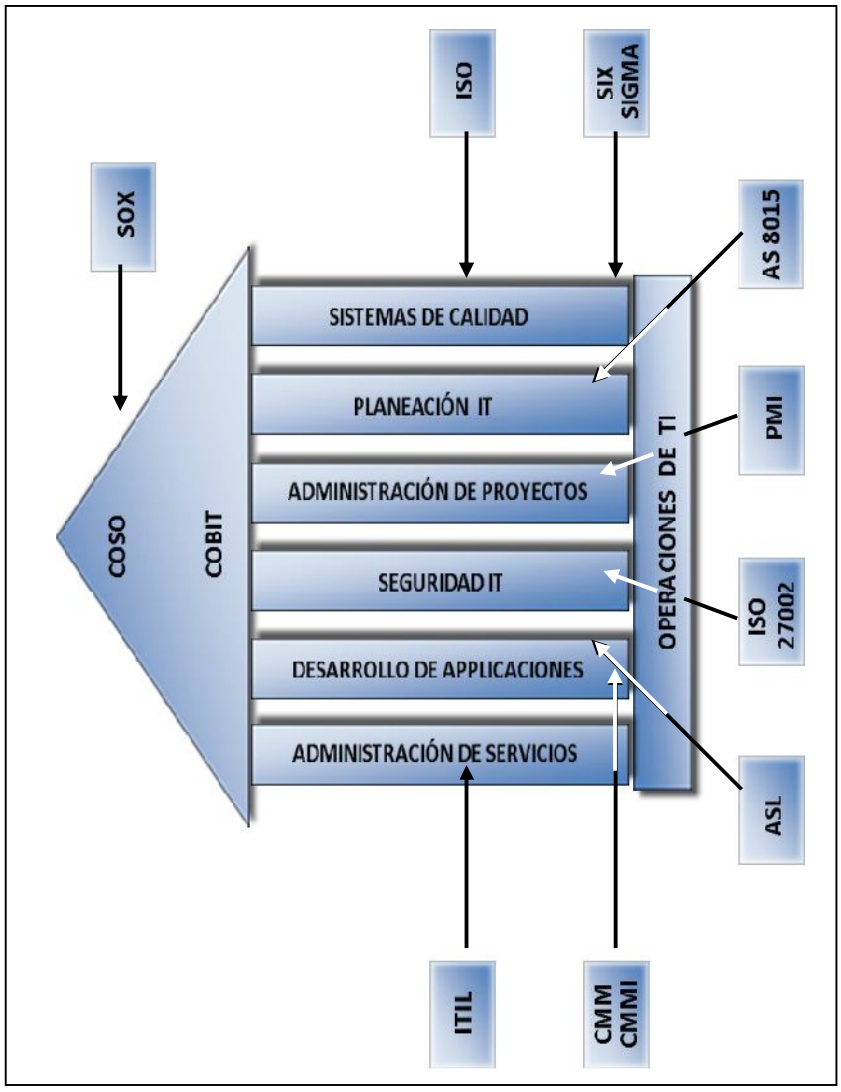


Fig. 3.10. Gobierno de TI

Cap3

CAPÍTULO IV

COBIT - OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (Control Objetives For Information And Related Technology)

CONTENIDO

CAPÍTULO IV

COBIT

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS CONTROL

(Control Objetives For Information And Related Technology)

4.1. INTRODUCCIÓN

En nuestro competitivo y rápidamente cambiante ambiente actual, las tecnologías de la información y las comunicaciones se han convertido en el eje promotor de cambios sociales, económicos y culturales, propiciando de modo significativo la interacción e intercambio entre las personas y organizaciones, llegando a ser un instrumento y elemento crítico para la gestión de las empresas, así como para el éxito y la supervivencia de las mismas.

Sin embargo, esto también ha provocado la aparición de nuevos riesgos y amenazas con respecto a la información y a los activos de TI, por tanto, es necesario considerar las particularidades de dichas tecnologías para construir nuevos enfoques de Auditoría y Seguridad de los Sistemas de Información.

Es así que surge en los últimos años la Metodología CObIT, un estándar de aplicación mundial, como una herramienta innovadora para el Gobierno de las Tecnologías de la Información, fundamentada en objetivos de control de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento, que han sido desarrollados para

su aplicación en sistemas de información en toda la empresa para las buenas prácticas de seguridad y control en Tecnología de Información (TI).

4.2. GENERALIDADES

CObIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en TI, siendo una herramienta innovadora para la Gobernabilidad de las Tecnologías de la Información, ya que ayuda a satisfacer las múltiples necesidades de la Administración acortando la brecha existente entre las exigencias de control, cuestiones técnicas y riesgos de negocio, con el desarrollo de una política clara en una estructura manejable y lógica, integrando y conciliando normas y reglamentaciones internacionales existentes como:

- Estándares Técnicos: ISO, EDIFACT[34], entre otros.
- Códigos de conducta emitidos por el Concejo Europeo, OECD[35], ISACA, etc.
- Criterios de Calificación para sistemas y procesos de TI: ITSEC[36], ISO9000, SPICE, TickIT, Common Criteria, etc.
- Estándares Profesionales para control interno y auditoría: reporte COSO, IFAC[37], IIA, ISACA, GAO, PCIE, CICA, AICPA, entre otras.
- Prácticas y requerimientos de la Industria de foros industriales (ESF[38], I4) y plataformas patrocinadas por el gobierno (IBAG, NIST, DTI); y
- Nuevos requerimientos específicos de la industria de la banca, Comercio Electrónico y manufactura de Tecnología de la Información.

[34] EDIFACT, Electronic Data Interchange for Administration Commerce and Trade (Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria)
[35] OECD, Organization for Economic Cooperation and Development. Guidelines for the Security of Information, Paris, 1992.
[36] ITSEC, Information Technology Security Evaluation Criteria (Criterios de Evaluación de Seguridad de Tecnología de Información).

[37] IFAC, International Guidelines for Managing Security of Information and Communications: International Federation of Accountants, New York, NY, 1997. (Federación Internacional de Contadores Públicos).
[38] ESF, European Security Forum (Foro Europeo de Seguridad).

- Incluye Objetivos de control emitidos por la ISACA (EDPAA)

Independientemente de la realidad tecnológica, CObIT como se ha mencionado determina, un conjunto de mejores prácticas para la seguridad, calidad, eficacia y eficiencia que son necesarias para alinear TI con el negocio, proporcionando a gerentes, interventores, y usuarios TI una guía clara y entendible para coadyuvar a maximizar las ventajas sacadas por el empleo de tecnología de información, desarrollo de la gobernación apropiada de TI y el control en una empresa.

4.3. HISTORIA Y ANTECEDENTES DE CObIT

La metodología CObIT fue inicialmente lanzada por la Information Systems Audit and Control Foundation (ISACF), publicándose su primera edición en 1996. Posteriormente a esta publicación se sumaría la tutela de ISACA[39] (Information Systems Audit and Control Association), quienes ante la necesidad de disponer de un método para gestionar, controlar y "gobernar" la complejidad y responsabilidades de los Sistemas Información, desarrollaron un modelo fundamentado en las más sólidas técnicas de gestión empresarial y en los estándares internacionales de seguridad y control.

ISACA comenzó en 1967, cuando especialistas en áreas de control y auditoría de los sistemas de información, observaron que estos se tornaban cada vez más críticos para las operaciones de las organizaciones, es así que en 1969, el grupo se formalizó incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos), mas tarde conocido como ISACA.

En 1998 ISACA y sus Fundaciones asociadas forman el IT Governance Institute (Instituto de Gobierno de TI), una organización de educación para llevar

[39] ISACA, Information Systems Audit and Control Association (Asociación de Auditoría y Control de los Sistemas de Información)

a cabo proyectos de investigación de gran escala, para expandir los conocimientos y el valor del campo de gobernación y control de TI. De esta manera el IT Governance Institute formó parte fundamental en la edición de CObIT para avanzar en el entendimiento y la adopción de principios de gobierno de TI, adquiriendo un rol de liderazgo en el desarrollo de la publicación.

CObIT se basó originalmente en los Objetivos de Control de la ISACF y ha sido mejorado con los actuales y emergentes estándares internacionales. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información de toda la empresa, siendo estos **"***generalmente aplicables y aceptados***",** término utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). [WWW.017]

4.4. MISIÓN DE CObIT

"Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas, auditores y usuarios."[40]

Actualmente las organizaciones han considerado como parte substancial de su éxito y liderazgo a la administración efectiva de la información y de las Tecnologías de Información Relacionadas, lo cual ha incrementando la expectativa de la Gerencia respecto a la entrega de servicios de TI, sin embargo, la Administración también comprende que hay numerosos cambios en TI y en su ambiente operacional, lo que enfatiza la necesidad de un mejor manejo relacionado con los riesgos de TI. Esta criticidad emerge de:

[40] Information Systems Audit and Control Association (ISACA) - IT Governance Institute. "Governance Guides and Audit for Information and Related Technology" – Executive Summary, 3era Edición.

- La creciente dependencia en información y en los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información.
- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Por ende, la Administración requiere niveles de servicio que presenten incrementos en: calidad, funcionalidad, facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega; y que se realice a un costo más bajo**,** donde la administración del riesgo relacionado con TI se encuentra formando un aspecto clave en el gobierno o dirección empresarial.

Es así que, el objetivo principal del proyecto CObIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta es el desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa.

4.5. MARCO REFERENCIAL DE CObIT (FRAMEWORK)

Hasta hace poco el riesgo operativo en las organizaciones era visto como un concepto no muy difundido, que en la mayoría de los casos implicaba pérdidas o resultados no esperados. Sin embargo, hoy en día la Alta Gerencia ha reconocido que la administración del riesgo operativo es una parte integral en su gestión, que manejada adecuadamente permite agregar valor significativo a la organización.

Entre las responsabilidades de la Administración está el decidir cual es la inversión razonable en seguridad y en control en TI, lograr un balance adecuado entre riesgos e inversiones en control en un ambiente de TI que es frecuentemente impredecible, está también el decidir el nivel de riesgo que está dispuesta a aceptar, sin duda, la globalización ha hecho que las organizaciones se reestructuren con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en Tecnologías de la Información para mejorar su posición competitiva.

Por ello, ha sido cada vez más evidente la necesidad de un Marco Referencial para la seguridad y el control de tecnología de información (TI). Las organizaciones exitosas requieren una apreciación y un entendimiento básico de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles adecuados.

Independientemente de la realidad tecnológica de cada caso concreto, CObIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, calidad, eficacia y eficiencia en Tecnologías de la Información (TI) que son necesarias para entregar valor al negocio, gestionar recursos y cumplimiento de metas de la organización.

La manera en que CObIT provee este marco para el control y la gobernabilidad de TI se exponen a continuación como sus principales características.

4.5.1. EL GOBIERNO DE TI

Gobernanza de TI es la alineación de las Tecnologías de la Información con las estrategias del negocio. Transmite las metas y estrategias a todos los departamentos de la empresa, apoyando a la organización, supervisando y

proveyendo el mejor uso de la tecnología y de sus estructuras organizacionales para alcanzarlas.

En la actualidad la necesidad de integrar el negocio con las Tecnologías de la Información con éxito, es crítico, puesto que una buena Gobernación de las Tecnologías de la Información juega un papel muy importante en la creciente necesidad de una buena alineación TI y las estrategias comerciales, ya que a través de ella se consigue optimizar el valor de la información acorde a los objetivos de la empresa, capitalizándolos con tecnologías que verdaderamente nos permiten obtener competitividad y mantenernos ante el ambiente global que actualmente experimentamos.

Sin embargo pese al desarrollo y publicación de modelos de control generales de negocios como COSO en los EUA, *Cadbury* en el Reino Unido, *CoCo* en Canadá y *King* en Sudáfrica, y por otro lado la existencia de un número importante de modelos de control más enfocados al nivel de tecnología de información, tal como son: el *Security Code of Conduct* del DTI (*Departamento de Industria y Comercio*, Reino Unido) y el *Security Handbook* de NIST (*National Institute of Standards and Technology*, EUA), estos modelos de control con orientación específica no proporcionan un modelo de control completo y utilizable sobre tecnología de información como soporte para los procesos del negocio. [LIB.008].

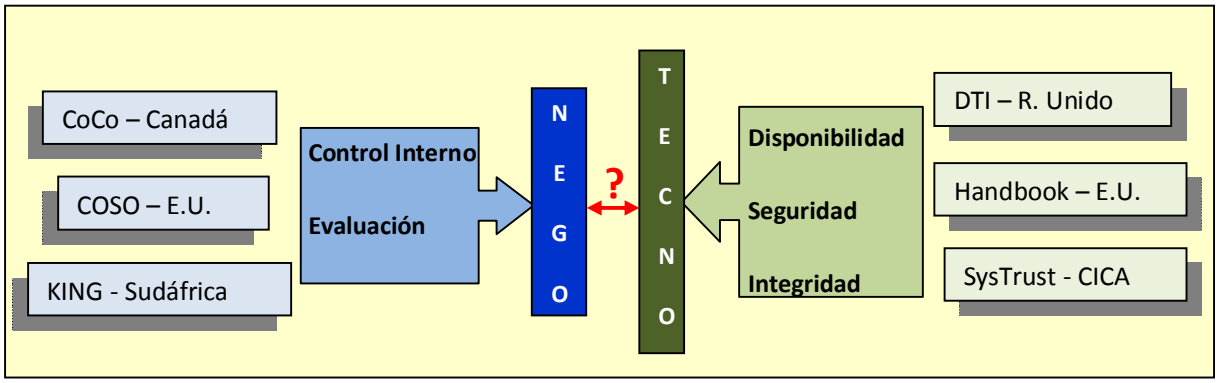


Fig. 4.1. Modelos de Control de Negocios y Tecnologías de la Información

La automatización de las funciones organizacionales, marca la incorporación de mecanismos de control más poderosos, tanto para las basadas en hardware como las basadas en software. Además, las características estructurales fundamentales de estos controles están evolucionando al mismo paso que las tecnologías, por tanto, para lograr el éxito en esta economía de información, el Gobierno de la empresa y el Gobierno de TI no pueden ser considerados separadamente y en distintas disciplinas, ya que el Gobierno de TI es parte integral del éxito de la Gerencia de la Empresa al asegurar mejoras medibles, eficientes y efectivas de los procesos relacionados de la empresa. (Fig. 4.2)

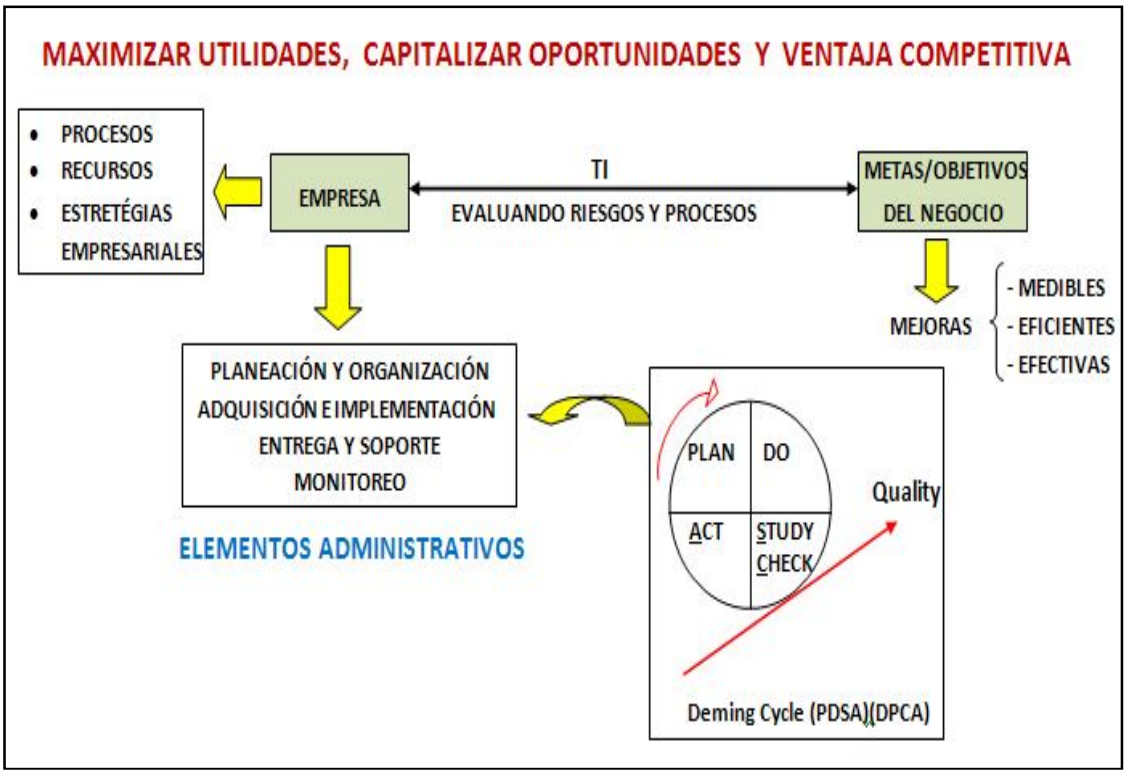


Fig. 4.2. Marco de Control y Gobernabilidad en la empresa

El propósito de CObIT es cubrir este vacío proporcionando una base que esté estrechamente ligada a los objetivos de negocio, al mismo tiempo que se enfoca a la tecnología de información. (Fig. 4.3)

Es importante considerar que dentro del marco de Gobierno de TI de CObIT, forma parte esencial el ciclo PDCA (Ciclo Deming), modelo para el mejoramiento continuo de la calidad, mismo que es adoptado por la ISO/IEC 27001 aplicado a toda la estructura de procesos de SGSI (Sistema de Gestión de la Seguridad de la Información).

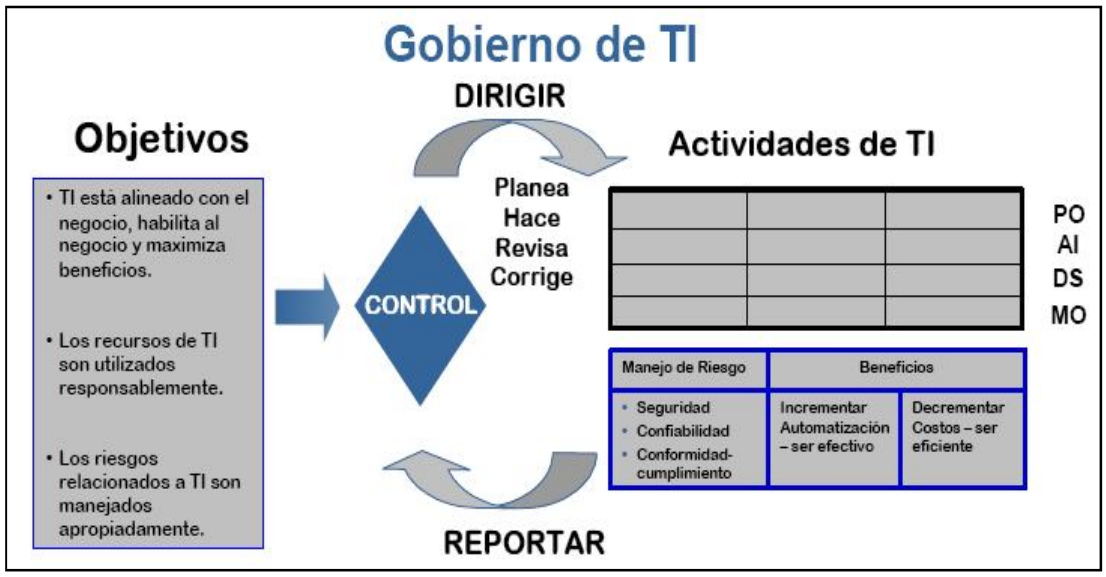


Fig. 4.3. Gobierno de TI de CobiT

4.5.2. DEFINICIONES GENERALES

CObIT proporciona las definiciones de "Control" y "Objetivos de Control", que han sido adaptadas del reporte COSO (Committee of Sponsoring Organisations of the Treadway Comisión) Internal Control-Integrated Framework), 1992 y de SAC (Systems Auditability and Control Report, The Institute of Internal Auditors Research Foundation, 1991 y 1994).

4.5.2.1.CONTROL

Se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del

negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos

4.5.2.2.OBJETIVOS DE CONTROL

Es una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

4.5.3. PRINCIPIOS DEL MARCO REFERENCIAL

El concepto fundamental del Marco Referencial de CObIT se refiere a que el enfoque del control en Tecnologías de la Información, se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

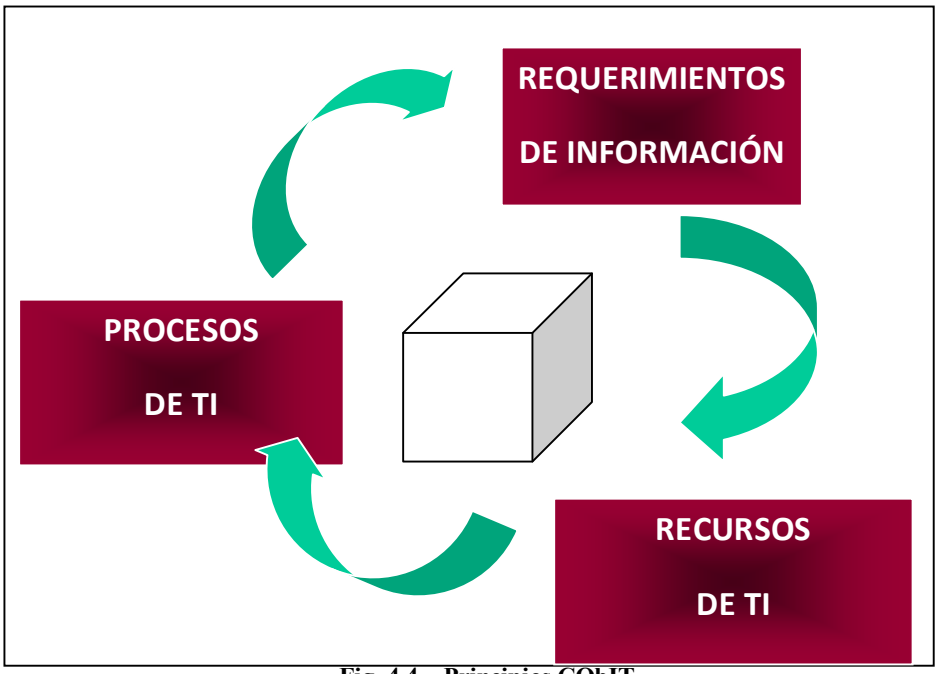


Fig. 4.4. Principios CObIT

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que CObIT hace referencia como "Requerimientos de negocio para la información". Al establecer la lista de requerimientos, CObIT combina los principios contenidos en los modelos referenciales existentes y conocidos, tal como se muestra a continuación:

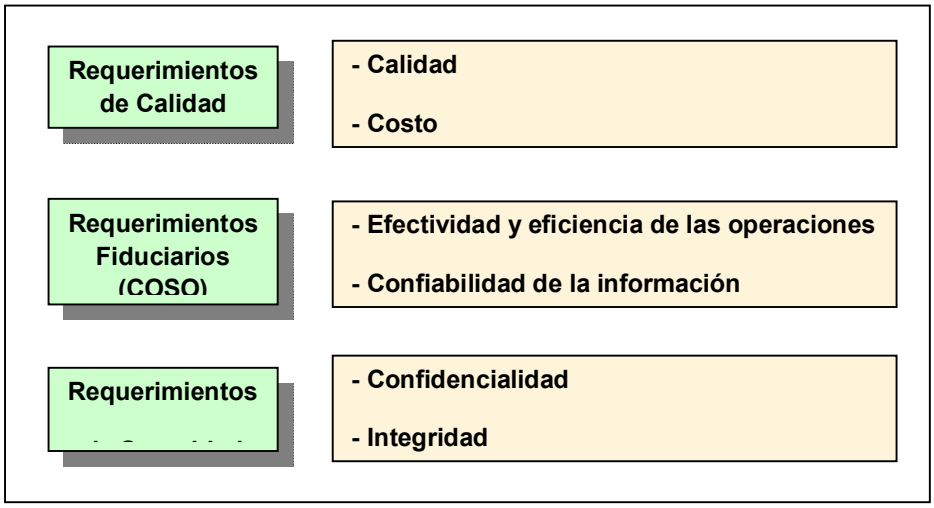


Fig. 4.5. Principios del Marco Referencial de CObIT

Dentro del análisis realizado a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se han extraído siete categorías distintas. A continuación se muestran las definiciones utilizadas por CObIT:

- **Efectividad:** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- **Eficiencia:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- **Confidencialidad:** Se refiere a la protección de información sensible contra divulgación no autorizada**.**
- **Integridad:** Suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

- **Disponibilidad:** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- **Cumplimiento:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- **Confiabilidad de la Información:** Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento. [LIB.008]

Los recursos de TI identificados en CObIT pueden explicarse y/o definirse como se muestra a continuación:

- **Datos:** Son objetos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
- **Sistemas de Aplicación:** Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados**.**
- **Tecnología:** La tecnología cubre hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- **Instalaciones:** Recursos para alojar y dar soporte a los sistemas de información.
- **Personal:** Habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

4.5.4. ESTRUCTURA DEL MARCO REFRENCIAL CObIT

El Marco de Referencia de CObIT consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación, que han

sido basadas en tres niveles de actividades de TI al considerar la administración de sus recursos. Estos son:

- **Actividades:** Las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.
- **Procesos:** Son conjuntos de actividades o tareas con delimitación o cortes de control.
- **Dominios:** Es la agrupación natural de procesos denominado frecuentemente como dominios que corresponden a la responsabilidad organizacional.

Por lo tanto, el Marco de Referencia conceptual puede ser enfocado desde tres puntos estratégicos: Criterios de información, Recursos de TI y Procesos de TI. Estos tres puntos estratégicos son descritos en el Cubo CObIT que se muestra a continuación:

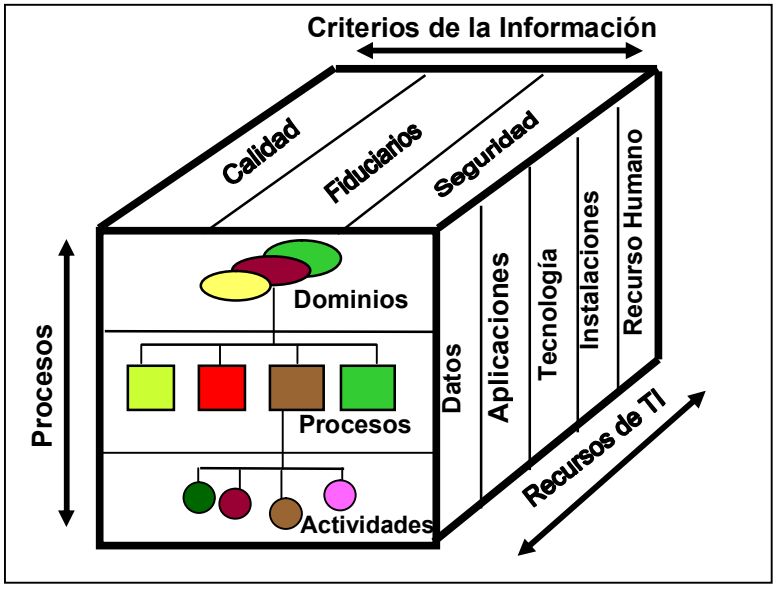


Fig. 4.6. Cubo CObIT

Con lo anteriormente señalado como Marco de Referencia, cuatro grandes dominios son identificados: Planeación y Organización, Adquisición e

Implementación, Entrega de servicios y Soporte y Monitoreo, a los cuales se aplican un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de TI.

Las definiciones para los dominios mencionados son las siguientes:

4.5.4.1. PLANEACIÓN Y ORGANIZACIÓN (PLANNING AND ORGANIZATION)

Este dominio cubre las estrategias y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberá establecerse una organización y una infraestructura tecnológica apropiadas.

4.5.4.2. ADQUISICIÓN E IMPLEMENTACIÓN (ACQUISITION AND IMPLEMENTATION)

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, para asegurar que el ciclo de vida es contínuo para esos sistemas.

4.5.4.3. ENTREGA Y SOPORTE (DELIVERY AND SUPPORT)

En este dominio se hace referencia a la entrega o distribución de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la continuidad de las operaciones así

como aspectos sobre entrenamiento. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos el cual es ejecutado por los sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

4.5.4.4.MONITOREO (MONITORING)

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Este dominio también advierte a la Administración sobre la necesidad de asegurar procesos de control independientes, los cuales son provistos por auditorías internas y externas u obtenidas de fuentes alternativas.

Es importante tener en cuenta que los procesos de TI pueden ser aplicados en diferentes niveles de la organización, unos al nivel de la empresa, otros al nivel de la función de TI, otros al nivel del propietario de los procesos del negocio, etc.

También se establece que todas las medidas de control no necesariamente satisfarán los diferentes requerimientos del negocio para la información en el mismo grado, por lo cual se determinan los siguientes:

- **Primario:** Es el grado en el cual se definen objetivos de control que impactan directamente los criterios de información considerados.
- **Secundario:** Es el grado en el cual se definen objetivos de control que solo satisfacen una extensión pequeña o satisfacen indirectamente al criterio de información considerado.
- **En blanco:** Los requerimientos son satisfechos de una forma mas apropiada por otro criterio en este proceso y/o en otro proceso.

El Marco de Referencia de CObIT, esta dirigido a objetivos de control de alto nivel para cada uno de los 34 procesos de TI del Marco Referencial, enfocándose en las necesidades del negocio, con el fin de proveer la información que la organización necesita para lograr sus objetivos. [LIB.008]

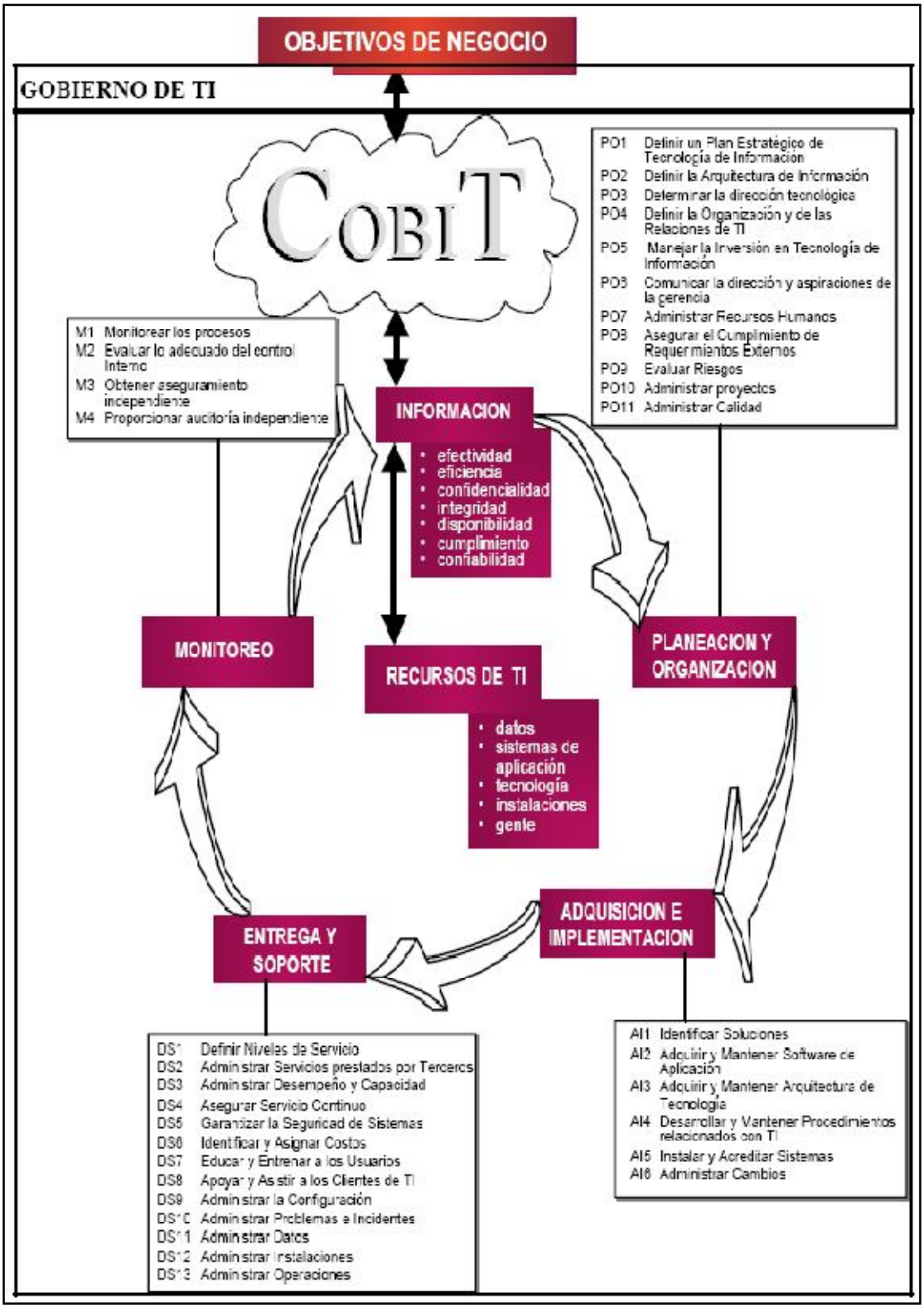


Fig. 4.7. Procesos de TI de CObIT definidos en los cuatro dominios

4.6. OBJETIVOS DE CONTROL CObIT

Los Objetivos de Control están dirigidos a la Administración y al staff de TI, a las funciones de control y auditoría, y lo más importante, a los propietarios de los procesos del negocio. Con los Objetivos de Control se aseguran la efectividad, eficiencia y economía de la utilización de los recursos de TI.

Los Objetivos de Control se alinean para cubrir todo el Marco referencial con objetivos de control detallados. Mientras que el Marco de Referencia de CObIT enfoca controles a alto nivel para cada proceso, los Objetivos de Control se enfocan sobre objetivos de control detallados y específicos asociados a cada proceso de TI. Por cada uno de los 34 procesos de TI del Marco Referencial, hay desde tres hasta 30 objetivos de control detallados, para un total de 318.

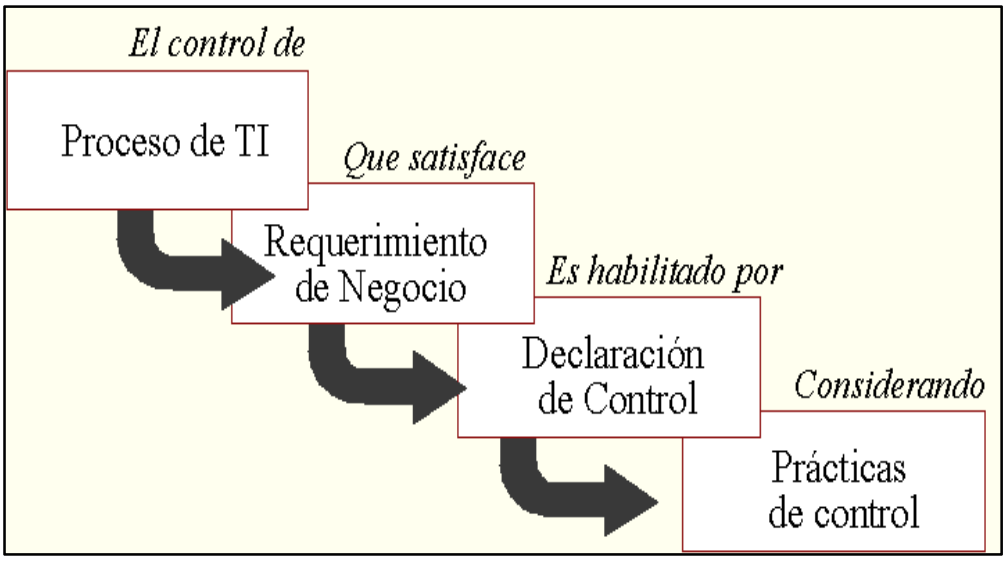


Fig. 4.8. Proceso de los Objetivos de Control

Estos Objetivos han sido organizados por proceso/actividad, facilitando enfoques combinados o globales, tales como instalación/implementación de un proceso, responsabilidades gerenciales y utilización de recursos de TI por un proceso. Además contienen sentencias de los resultados deseados o propósitos a ser alcanzados mediante la implementación de procedimientos de control

específicos en una actividad de TI, proveyendo de esta manera políticas claras y buenas prácticas para los controles de TI a través de la industria.

A continuación presentamos las relaciones existentes de los Objetivos de control, es decir detallaremos los controles existentes por cada proceso definido en los cuatro dominios del Marco referencial: Planeación y Organización, Adquisición e Implementación, Entrega y Soporte y Monitoreo. [LIB.010]

4.6.1. OBJETIVOS DE CONTROL PARA LOS PROCESOS DE PLANEACIÓN Y ORGANIZACIÓN (PO)[41]

PO 1 Definición de un Plan Estratégico de Tecnología de Información

1.1. Tecnología de Información como parte del Plan de la Organización a corto y largo plazo
1.2. Plan a largo plazo de Tecnología de Información
1.3. Plan a largo plazo de Tecnología de Información - Enfoque y Estructura
1.4. Cambios al Plan a largo plazo de Tecnología de Información
1.5. Planeación a corto plazo para la función de Servicios de Información.
1.6. Comunicación de los planes de TI
1.7. Evaluación y Monitoreo de los planes de TI.
1.8. Valoración de los sistemas existentes.

PO 2 Definición de la Arquitectura de Información

2.1. Modelo de la Arquitectura de Información
2.2. Diccionario de Datos y Reglas de sintaxis de datos corporativos
2.3. Esquema de Clasificación de Datos
2.4. Niveles de Seguridad.

[41] PO, Planning and Organization (Planeación y Organización)

PO 3 Determinación de la Dirección Tecnológica

1.1. Planeación de la Infraestructura Tecnológica

1.2. Monitoreo de Tendencias y Regulaciones Futuras

1.3. Contingencias en la Infraestructura Tecnológica

1.4. Planes de Adquisición de Hardware y Software

1.5. Estándares de Tecnología

PO 4 Definición de la Organización y de las Relaciones de TI

4.1. Planeación de TI o Comité de planeación/ dirección de la función de servicios de información

4.2. Ubicación de los servicios de información en la organización

4.3. Revisión de Logros Organizacionales

4.4. Funciones y Responsabilidades

4.5. Responsabilidad del aseguramiento de calidad

4.6. Responsabilidad por la seguridad lógica y física

4.7. Propiedad y Custodia

4.8. Propiedad de Datos y Sistemas

4.9. Supervisión

4.10. Segregación de Funciones

4.11. Asignación de Personal para Tecnología de Información

4.12. Descripción de Puestos para el Personal de la Función de TI

4.13. Personal clave de TI

4.14. Procedimientos y políticas para el personal contratado

4.15. Relaciones

PO 5 Manejo de la Inversión en Tecnología de Información

5.1. Presupuesto Operativo Anual para la Función de Servicio de información

5.2. Monitoreo de Costo – Beneficio

5.3. Justificación de Costo – Beneficio

PO 6 Comunicación de los Objetivos y Aspiraciones de la Gerencia

6.1. Ambiente positivo de control de la información

6.2. Responsabilidad de la Gerencia en cuanto a Políticas

6.3. Comunicación de las Políticas de la Organización

6.4. Recursos para la implementación de Políticas

6.5. Mantenimiento de Políticas

6.6. Cumplimiento de Políticas, Procedimientos y Estándares

6.7. Compromiso con la Calidad

6.8. Política sobre el Marco Referencial para la Seguridad y el Control Interno

6.9. Derechos de propiedad intelectual

6.10. Políticas Específicas

6.11. Comunicación de Conciencia de Seguridad en TI

PO 7 Administración de Recursos Humanos

7.1. Reclutamiento y Promoción de Personal

7.2. Calificación del Personal

7.3. Roles y Responsabilidades

7.4. Entrenamiento del personal

7.5. Entrenamiento Cruzado o Respaldo de Personal

7.6. Procedimientos para la Acreditación del Personal

7.7. Evaluación de Desempeño de los Empleados

7.8. Cambios de Puesto y Terminación de contrato de trabajo

PO 8 Aseguramiento del Cumplimiento con Requerimientos Externos

8.1. Revisión de Requerimientos Externos

8.2. Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos

8.3. Cumplimiento de los Estándares de Seguridad y Ergonomía

8.4. Privacidad, Propiedad Intelectual y Flujo de Datos

8.5. Comercio Electrónico

8.6. Cumplimiento con Contratos de Seguros

PO 9 Análisis de Riesgos

9.1. Análisis de Riesgos del Negocio
9.2. Enfoque de Análisis de Riesgos
9.3. Identificación de Riesgos
9.4. Medición de Riesgos
9.5. Plan de Acción para mitigar los Riesgos
9.6. Aceptación de Riesgos
9.7. Selección de Protección.
9.8. Compromiso de Análisis de Riesgos

PO 10 Administración de Proyectos

10.1. Marco Referencial para la Administración de Proyectos
10.2. Participación del Departamento Usuario en la Iniciación de Proyectos
10.3. Miembros y Responsabilidades del Equipo del Proyecto
10.4. Definición del Proyecto
10.5. Aprobación del Proyecto
10.6. Plan maestro del proyecto
10.7. Plan Maestro del Proyecto
10.8. Plan de Aseguramiento de Calidad de Sistemas
10.9. Planeación de Métodos de Aseguramiento
10.10. Administración Formal de Riesgos de Proyectos
10.11. Plan de Prueba
10.12. Plan de Entrenamiento
10.13. Plan de Revisión Post Implementación

PO 11 Administración de Calidad

11.1. Plan General de Calidad
11.2. Enfoque de Aseguramiento de Calidad
11.3. Planeación del Aseguramiento de Calidad

11.4. Revisión de Aseguramiento de Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información
11.5. Metodología del Ciclo de Vida de Desarrollo de Sistemas
11.6. Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual
11.7. Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas
11.8. Coordinación y Comunicación
11.9. Marco Referencial para la Adquisición y Mantenimiento de la Infraestructura de Tecnología
11.10. Relaciones con Terceras Partes en su rol de Implementadores
11.11. Estándares para la Documentación de Programas
11.12. Estándares para Pruebas de Programas
11.13. Estándares para Pruebas de Sistemas
11.14. Pruebas Piloto/En Paralelo
11.15. Documentación de las Pruebas del Sistema
11.16. Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo
11.17. Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información
11.18. Métricas de Calidad
11.19. Reportes de Revisiones de Aseguramiento de la Calidad.

4.6.2. OBJETIVOS DE CONTROL PARA LOS PROCESOS DE ADQUISICIÓN E IMPLEMENTACIÓN (AI)[42]

AI 1 Identificación de Soluciones

1.1. Definición de Requerimientos de Información
1.2. Formulación de Acciones Alternativas

[42] AI, Adquisition and Implementation (Adquisición e Implementación)

1.3. Formulación de Estrategias de Adquisición.
1.4. Requerimientos de Servicios de Terceros
1.5. Estudio de Factibilidad Tecnológica
1.6. Estudio de Factibilidad Económica
1.7. Arquitectura de Información
1.8. Reporte de Análisis de Riesgos
1.9. Controles de Seguridad costo-efectivo
1.10. Diseño de Pistas de Auditoría
1.11. Ergonomía
1.12. Selección de Software del Sistema
1.13. Control de Abastecimiento
1.14. Adquisición de Productos de Software
1.15. Mantenimiento de Software de Terceras Partes
1.16. Contratos para la Programación de Aplicaciones
1.17. Aceptación de Instalaciones
1.18. Aceptación de Tecnología

AI 2 Adquisición y Mantenimiento de Software de Aplicación

2.1. Métodos de Diseño
2.2. Cambios Significativos a Sistemas Actuales
2.3. Aprobación del Diseño
2.4. Definición y Documentación de Requerimientos de Archivos
2.5. Especificaciones de Programas
2.6. Diseño para la Recopilación de Datos Fuente
2.7. Definición y Documentación de Requerimientos de Entrada de Datos
2.8. Definición de Interfases
2.9. Interfases Usuario-Máquina
2.10. Definición y Documentación de Requerimientos de Procesamiento
2.11. Definición y Documentación de Requerimientos de Salida de Datos
2.12. Controlabilidad
2.13. Disponibilidad como Factor Clave de Diseño

2.14. Consideración de Integridad de TI en programas de software de aplicaciones
2.15. Pruebas al Software de Aplicación
2.16. Materiales de Consulta y Soporte para Usuario
2.17. Reevaluación del Diseño del Sistema

AI 3 Adquisición y Mantenimiento de la Arquitectura de Tecnología

3.1. Evaluación de Nuevo Hardware y Software
3.2. Mantenimiento Preventivo para Hardware
3.3. Seguridad del Software del Sistema
3.4. Instalación del Software del Sistema
3.5. Mantenimiento del Software del Sistema
3.6. Controles para Cambios del Software del Sistema
3.7. Uso y Monitoreo de Utilidades/Utilitarios del Sistema

AI 4 Procedimientos de Desarrollo y Mantenimiento de TI

4.1. Requerimientos Operacionales y Niveles de Servicio
4.2. Manual de Procedimientos para Usuario
4.3. Manual de Operación
4.4. Material de Entrenamiento

AI 5 Instalación y Acreditación de Sistemas

5.1. Entrenamiento
5.2. Medición del Desempeño del Software de Aplicación
5.3. Plan de Implementación
5.4. Conversión del Sistema
5.5. Conversión de datos
5.6. Planes y estrategias de pruebas
5.7. Pruebas a cambios
5.8. Criterios y Desempeño de Pruebas en Paralelo/Piloto
5.9. Prueba de Aceptación Final
5.10. Pruebas y Acreditación de la Seguridad

5.11. Prueba Operacional

5.12. Promoción a Producción

5.13. Evaluación de la Satisfacción de los Requerimientos del Usuario

5.14. Revisión Gerencial Post – Implementación

AI 6 Administración de Cambios

6.1. Inicio y Control de Solicitudes de Cambio

6.2. Análisis de Impacto

6.3. Control de Cambios

6.4. Cambios de Emergencia

6.5. Documentación y Procedimientos

6.6. Mantenimiento Autorizado

6.7. Política de Liberación de Software

6.8. Distribución de Software. [LIB. 010]

4.6.3. OBJETIVOS DE CONTROL PARA LOS PROCESOS DE ENTREGA DE SERVICIOS Y SOPORTE (DS)[43]

DS 1 Definición de Niveles de Servicio

1.1. Marco de Referencia para acuerdos de Nivel de Servicio

1.2. Aspectos sobre los Acuerdos de Nivel de Servicio

1.3. Procedimientos de Desempeño

1.4. Monitoreo y Reporte

1.5. Revisión de Contratos y Acuerdos de Nivel de Servicio

1.6. Elementos sujetos a Cargo

1.7. Programa de Mejoramiento del Servicio

DS 2 Administración de Servicios prestados por Terceros

2.1. Interfases con Proveedores

2.2. Relaciones con los Dueños

[43] DS, Delivery and Support (Entrega y Soporte)

2.3. Contratos con Terceros
2.4. Calificaciones de terceros
2.5. Contratos con Outsourcing
2.6. Continuidad del Servicios
2.7. Relaciones de Seguridad
2.8. Monitoreo

DS 3 Administración de Desempeño y Capacidad

3.1. Requerimientos de Disponibilidad y Desempeño
3.2. Plan de Disponibilidad
3.3. Monitoreo y Reporte
3.4. Herramientas de Modelado
3.5. Administración de Desempeño Proactivo
3.6. Pronóstico de Carga de Trabajo
3.7. Administración de Capacidad de Recursos
3.8. Disponibilidad de Recursos
3.9. Calendarización / Programación de recursos

DS 4 Aseguramiento de Servicio Continuo

4.1. Marco de Referencia de Continuidad de Tecnología de Información
4.2. Estrategia y Filosofía del Plan de Continuidad de Tecnología de Información
4.3. Contenido del Plan de Continuidad de Tecnología de Información
4.4. Minimización de requerimientos de Continuidad de Tecnología de Información
4.5. Mantenimiento del Plan de Continuidad de Tecnología de Información
4.6. Pruebas del Plan de Continuidad de Tecnología de Información
4.7. Entrenamiento sobre el Plan de Continuidad de Tecnología de Información
4.8. Distribución del Plan de Continuidad de Tecnología de Información

4.9. Procedimientos de Respaldo de Procesamiento para Departamentos Usuarios
4.10. Recursos críticos de Tecnología de Información
4.11. Centro de Cómputo y Hardware de respaldo
4.12. Almacenamiento de copias de respaldo fuera del sitio
4.13. Procedimientos de Refinamiento del Plan de Continuidad de TI[44]

DS 5 Garantizar la Seguridad de Sistemas

5.1. Administrar Medidas de Seguridad
5.2. Identificación, Autenticación y Acceso
5.3. Seguridad de Acceso a Datos en Línea
5.4. Administración de Cuentas de Usuario
5.5. Revisión Gerencial de Cuentas de Usuario
5.6. Control de Usuarios sobre Cuentas de Usuario
5.7. Vigilancia de Seguridad
5.8. Clasificación de Datos
5.9. Administración Centralizada de Identificación y Derechos de Acceso
5.10. Reportes de Violación y de Actividades de Seguridad
5.11. Manejo de Incidentes
5.12. Re-acreditación
5.13. Confianza en las Contrapartes
5.14. Autorización de Transacciones
5.15. No Rechazo
5.16. Sendero Seguro
5.17. Protección de las funciones de seguridad
5.18. Administración de las Llaves Criptográficas
5.19. Prevención, Detección y Corrección de Software "Malicioso"
5.20. Arquitecturas de Firewalls y conexión a redes públicas
5.21. Protección de Valores Electrónicos

[44] Refinamiento del Plan de Continuidad de TI (wrap up): procedimiento seguido para evaluar y actualizar el Plan

DS 6 Identificación y Asignación de Costos

6.1. Elementos Sujetos a Cargo

6.2. Procedimientos de Costeo

6.3. Procedimientos de Cargo y Facturación a Usuarios

DS 7 Educación y Entrenamiento de Usuarios

7.1. Identificación de Necesidades de Entrenamiento

7.2. Organización de Entrenamiento

7.3. Entrenamiento sobre Principios y Conciencia de Seguridad

DS 8 Apoyo y Asistencia a los Clientes de Tecnología de Información

8.1. Help Desk

8.2. Registro de consultas del Cliente

8.3. Escalamiento de consultas del Cliente

8.4. Monitoreo de Atención a Clientes

8.5. Análisis y Reporte de Tendencias

DS 9 Administración de la Configuración

9.1. Registro de la Configuración

9.2. Base de la Configuración

9.3. Registro de status

9.4. Control de la Configuración

9.5. Software no Autorizado

9.6. Almacenamiento de Software

9.7. Procedimientos para la Administración de la Configuración

9.8. Contabilidad y registro del Software

DS 10 Administración de Problemas e Incidentes

10.1. Sistema de Administración de Problemas

10.2. Escalamiento de Problemas

10.3. Seguimiento de Problemas y Pistas de Auditoría

10.4. Autorizaciones para acceso temporal y de emergencia.

10.5. Prioridades en Procesos de Emergencia. [LIB.010]

DS 11 Administración de Datos

11.1. Procedimientos de Preparación de Datos

11.2. Procedimientos de Autorización de Documentos Fuente

11.3. Recopilación de Datos de Documentos Fuente

11.4. Manejo de Errores de Documentos Fuente

11.5. Retención de Documentos Fuente

11.6. Procedimientos para la Autorización de Entrada de Datos

11.7. Chequeos de Exactitud, Suficiencia y Autorización

11.8. Manejo de Errores en la Entrada de Datos

11.9. Integridad de Procesamiento de Datos

11.10. Validación y Edición de Procesamiento de Datos

11.11. Manejo de Errores en el Procesamiento de Datos

11.12. Manejo y Retención de Datos de Salida

11.13. Distribución de Datos de Salida

11.14. Balanceo y Conciliación de Datos de Salida

11.15. Revisión de Salida de Datos y Manejo de Errores

11.16. Provisiones de Seguridad para Reportes de Salida

11.17. Protección de Información Sensitiva durante transmisión y transporte

11.18. Protección de Información Sensitiva a ser Desechada

11.19. Administración de Almacenamiento

11.20. Períodos de Retención y Términos de Almacenamiento

11.21. Sistema de Administración de la Librería de Medios

11.22. Responsabilidades de la Administración de la Librería de Medios

11.23. Respaldo y Restauración

11.24. Funciones de Respaldo

11.25. Almacenamiento de Respaldo

11.26. Archivo

11.27. Protección de Mensajes Sensitivos

11.28. Autenticación e Integridad

11.29. Integridad de Transacciones Electrónicas

11.30. Integridad Continua de Datos Almacenados

DS 12 Administración de Instalaciones

12.1. Seguridad Física

12.2. Discreción (bajo perfil) de las Instalaciones de Tecnología de Información

12.3. Escolta de Visitantes

12.4. Salud y Seguridad del Personal

12.5. Protección contra Factores Ambientales

12.6. Suministro Ininterrumpido de Energía

DS 13 Administración de Operaciones

13.1. Manual de Instrucciones y procedimientos de Operaciones de procesamiento

13.2. Documentación del Proceso de Inicio y de Otras Operaciones

13.3. Calendarización/programación de Trabajos

13.4. Ejecución de los Trabajos estándar programados

13.5. Continuidad de Procesamiento

13.6. Bitácoras de Operación

13.7. Protección de Formas Especiales y dispositivos de salida

13.8. Operaciones Remotas. [LIB. 010]

4.6.4. OBJETIVOS DE CONTROL PARA LOS PROCESOS DE MONITOREO (M)

M 1 Monitoreo del Proceso

1.1. Recolección de Datos de Monitoreo

1.2. Análisis del Desempeño

1.3. Evaluación de la Satisfacción de Clientes

1.4. Reportes Gerenciales

M 2 Evaluar lo adecuado del Control Interno

2.1. Monitoreo de Control Interno

2.2. Operación oportuna del Control Interno

2.3. Reporte sobre el Nivel de Control Interno

2.4. Seguridad en las operaciones y aseguramiento del Control Interno

M 3 Obtención de Aseguramiento Independiente

3.1. Certificación / Acreditación Independiente de Control Interno y Seguridad de los servicios de TI

3.2. Certificación / Acreditación Independiente de Control Interno y Seguridad de proveedores externos de servicios

3.3. Evaluación Independiente de la Efectividad de los Servicios de TI

3.4. Evaluación Independiente de la Efectividad de proveedores externos de servicios

3.5. Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales

3.6. Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales con proveedores externos de servicios

3.7. Competencia de la Función de Aseguramiento Independiente

3.8. Participación Proactiva de Auditoría

M 4 Proveer Auditoría Independiente

4.1. Estatutos de Auditoría

4.2. Independencia

4.3. Ética y Estándares Profesionales

4.4. Competencia

4.5. Planeación

4.6. Desempeño del Trabajo de Auditoría

4.7. Reporte

4.8. Actividades de Seguimiento [LIB.010]

4.6.5. TABLA RESUMEN DE LOS OBJETIVOS DE CONTROL

Los procesos de TI definidos son evaluados por los Objetivos de Control anteriormente detallados a través de los criterios de la información y recursos de TI. Los criterios de la información se agrupan en una matriz, la cual contiene los requerimientos del negocio a ser alcanzados como se muestra a continuación:

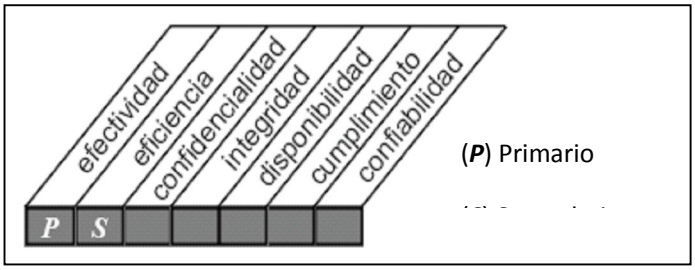


Fig. 4.9. Matriz de Criterios de la Información

De similar manera se agrupan los recursos de TI en la siguiente matriz:

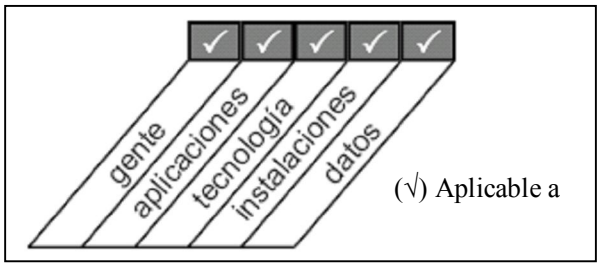


Fig. 4.10. Matriz de Recursos de TI

Los criterios de información son evaluados de acuerdo al grado que estos representan (Primario, Secundario o en blanco) que se han definido en el Marco Referencial de CObIT, así como también se muestra el dominio al que se hace referencia.

La Tabla 4.1. proporciona una indicación, por proceso y dominio de TI, de cuáles criterios de información son impactados por los objetivos de control de alto nivel, así como una indicación de cuáles recursos de TI son aplicables.

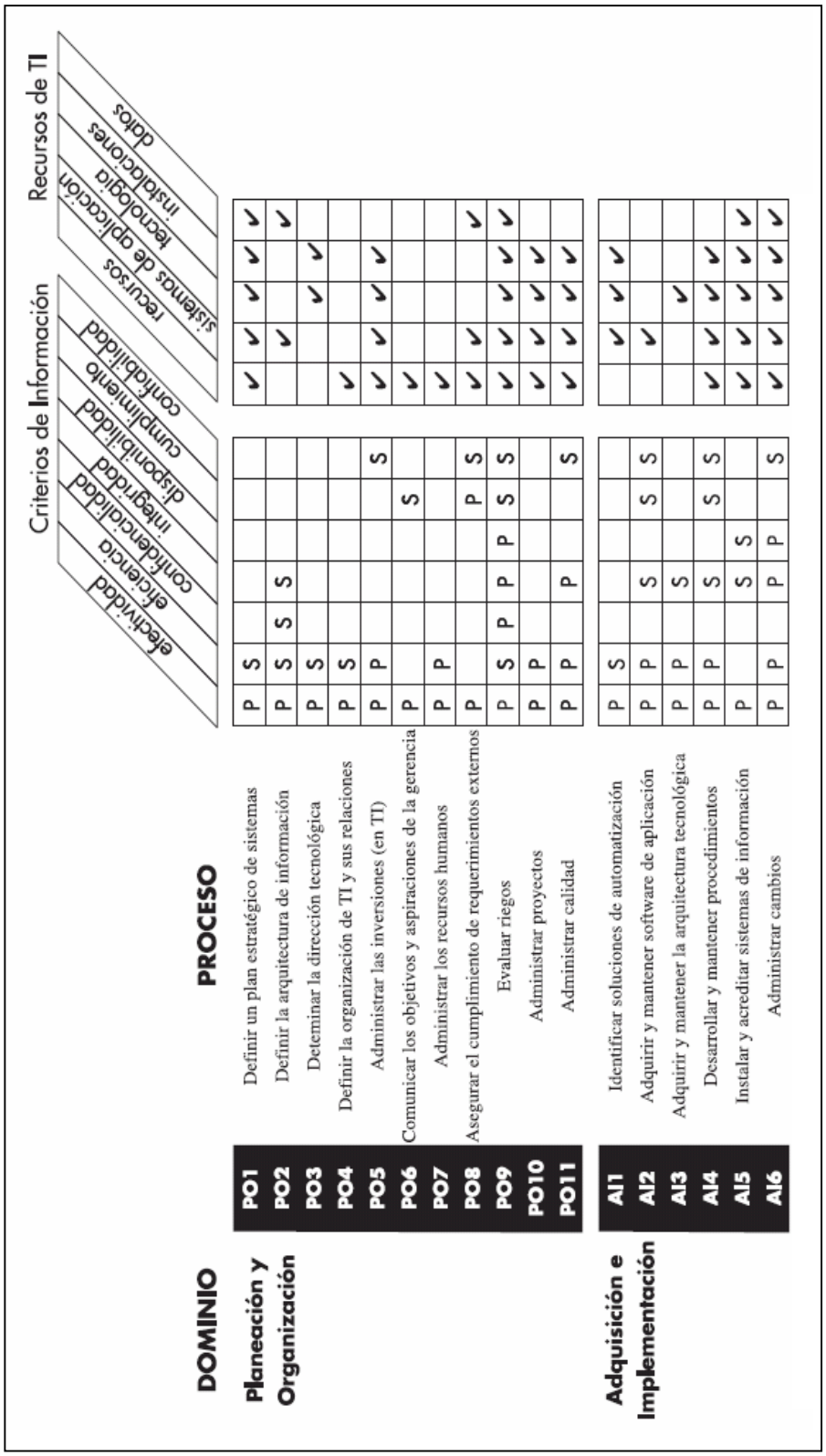


Tabla 4.11 Tabla resumen de los Objetivos de Control

4.7. DIRECTRICES DE AUDITORÍA

Las Directrices de Auditoría ofrecen una herramienta complementaria para la fácil aplicación del Marco Referencial y los Objetivos de Contro*l* CObIT dentro de las actividades de auditoría y evaluación. El propósito de las Directrices de Auditoría es contar con una estructura sencilla para auditar y evaluar controles, con base en prácticas de auditoría generalmente aceptadas y compatibles con el esquema global CObIT.

Los objetivos y prácticas individuales varían considerablemente de organización a organización, por ello, las Directrices de Auditoría tienen una estructura genérica y de alto nivel.

CObIT ofrece políticas claras y prácticas eficaces en materia de seguridad y para los controles de información y la tecnología asociada. Es así que las Directrices de Auditoría firmemente basadas en los Objetivos de Control, proporcionan guías para preparar planes de auditoría que se integran al Marco Referencial de CObIT y a los Objetivos de Control detallados, de esta manera toma la opinión del auditor a partir de la conclusión de auditoría, remplazándola con criterios normativos (41 estándares y mejores prácticas tomadas de normas privadas y públicas aceptadas a nivel mundial).

No obstante, hay cuatro cosas que las Directrices no son:

1. Las Directrices de Auditoría no pretenden ser una herramienta para crear el plan global de auditoría que considera una amplia gama de factores, incluyendo debilidades anteriores, riesgo de la organización, incidentes conocidos, nuevos acontecimientos, y selección de estrategias. Aun cuando el Marco Referencial y los Objetivos de Control ofrecen algunas orientaciones, los alcances de las Directrices no incluyen una guía precisa para actividades específicas.

2. Las Directrices de Auditoría no están diseñadas como instrumento para enseñar las bases de la auditoría, aun cuando incorporen los elementos normalmente aceptados de la auditoría general y de TI.

3. Las Directrices de Auditoría no pretenden explicar en detalle la forma en que pueden utilizarse las herramientas computarizadas para apoyar y automatizar los procesos de auditoría a TI, en materia de planeación, evaluación, análisis y documentación (que están incluidas, pero no se limitan a ellas, en las Técnicas de Auditoría Asistidas por Computador).

   Existe un enorme potencial para usar la tecnología de información dirigida a aumentar la eficiencia y efectividad de las auditorías, pero una orientación en este sentido, no está dentro de los alcances de las Directrices.

4. Las Directrices de Auditoría no son exhaustivas ni definitivas, pero se desarrollarán conjuntamente con CObIT y sus Objetivos de Control detallados.

Las Directrices de Auditoría de CObIT permiten al auditor comparar los procesos específicos de TI con los Objetivos de Control de CObIT recomendados para ayudar a los directivos a identificar en qué casos los controles son suficientes, o para asesorarlos respecto a los procesos que requieren ser mejorados.

4.7.1. ESTRUCTURA GENERAL DE LAS DIRECTRICES DE AUDITORÍA

En base a los objetivos de la auditoría, el modelo más común para evaluar controles, es el modelo de auditoría.

La estructura generalmente aceptada del proceso de auditoría es:

- Identificación y documentación
- Evaluación
- Pruebas de cumplimiento
- Pruebas sustantivas

Las Directrices de Auditoría de CObIT, presentan los requerimientos genéricos para auditar procesos de TI y brindar el primer nivel de las directrices de auditoría, generalmente aplicables a todos los procesos. Está primordialmente orientado hacia la comprensión del proceso y la determinación de la propiedad y deberá ser el fundamento y el marco referencial para todas las directrices detalladas de auditoría.

El proceso de TI, por lo tanto, se audita mediante:

- **La obtención** de un entendimiento de los riesgos relacionados con los requerimientos del negocio y de las medidas relevantes de control
- **La evaluación** de la conveniencia de los controles establecidos
- **La valoración** del cumplimiento probando si los controles establecidos están funcionando como se espera, de manera consistente y continua
- **La comprobación** que existe el riesgo de que los objetivos de control no se estén cumpliendo mediante el uso de técnicas analíticas y/o consultando fuentes alternativas. [LIB.011]. (Tabla 4.2)

Por tanto el enfoque general de auditoría está dado en tres niveles. En el nivel más alto, este enfoque general de auditoría está apoyado por:

El Marco Referencial de CObIT, particularmente el resumen con la clasificación de los procesos de TI, los criterios de información aplicables y los recursos de TI

- Los requerimientos para el proceso de auditoría
- Los requerimientos genéricos para la auditoría de procesos de TI
- Los principios generales de control

OBTENCIÓN DE UN ENTENDIMIENTO
Los pasos de auditoría que se deben realizar para documentar las actividades que generan inconvenientes a los objetivos de control, así como también identificar las medidas/procedimientos de control establecidas. Entrevistar al personal administrativo y de staff apropiado para lograr la comprensión de: • Los requerimientos del negocio y los riesgos asociados • La estructura organizacional • Los roles y responsabilidades • Políticas y procedimientos • Leyes y regulaciones • Las medidas de control establecidas • La actividad de reporte a la administración (estatus, desempeño, acciones) Documentar el proceso relacionado con los recursos de TI que se ven especialmente afectados por el proceso bajo revisión. Confirmar el entendimiento del proceso bajo revisión, los Indicadores Clave de Desempeño (KPI) del proceso, las implicaciones de control, por ejemplo, mediante una revisión paso a paso del proceso.
EVALUACIÓN DE LOS CONTROLES
Los pasos de auditoría a ejecutar en la evaluación de la eficacia de las medidas de control establecidas o el grado en el que se logra el objetivo de control. Básicamente, decidir qué se va a probar, si se va a probar y cómo se va a probar. Evaluar la conveniencia de las medidas de control para el proceso bajo revisión mediante la consideración de los criterios identificados y las prácticas estándares de la industria, los Factores Críticos de Éxito (CSF) de las medidas de control y la aplicación del juicio profesional de auditor. • Existen procesos documentados • Existen resultados apropiados • La responsabilidad y el registro de las operaciones son claros y efectivos • Existen controles compensatorios, en donde es necesario Concluir el grado en que se cumple el objetivo de control.
VALORACION DEL CUMPLIMIENTO
Los pasos de auditoría a realizar para asegurar que las medidas de control establecidas estén funcionando como es debido, de manera consistente y continua, y concluir sobre la conveniencia del ambiente de control. Obtener evidencia directa o indirecta de puntos/períodos seleccionados para asegurarse que se ha cumplido con los procedimientos durante el período de revisión, utilizando evidencia tanto directa como indirecta. Realizar una revisión limitada de la suficiencia de los resultados del proceso. Determinar el nivel de pruebas sustantivas y trabajo adicional necesarios para asegurar que el proceso de TI es adecuado.
JUSTIFICAR/COMPROBAR EL RIESGO
Los pasos de auditoría a realizar para justificar el riesgo de que no se cumpla el objetivo de control mediante el uso de técnicas analíticas y/o consultas a fuentes alternativas. El objetivo es respaldar la opinión e "impresionar" a la administración para que tome acción. Los auditores tienen que ser creativos para encontrar y presentar esta información que con frecuencia es sensitiva y confidencial Documentar las debilidades de control y las amenazas y vulnerabilidades resultantes. Identificar y documentar el impacto real y potencial; por ejemplo, mediante el análisis de causa-efecto.

Tabla 4.2 Directriz General de Auditoría

El segundo nivel está compuesto por las Directrices detalladas de auditoría para cada uno de los procesos de TI que sigue la estructura general de Obtención, Evaluación, Valoración y Comprobación.

En el tercer y último nivel, el auditor puede complementar las Directrices de Auditoría para cubrir las condiciones locales, conduciendo la fase de planeación de auditoría con puntos de atención de auditoría que influyen sobre los objetivos detallados de control mediante:

- Criterios específicos del sector
- Estándares de la industria
- Elementos específicos de la plataforma
- Técnicas detalladas de control empleadas. (Tabla. 4.3)

Cabe notar que para este nivel es importante el hecho de que los objetivos de control no son necesariamente aplicables en todos los casos y en cualquier lugar.

Todos estos elementos se ofrecen para apoyar la planeación y la realización de las auditorías de TI, y para una mejor aplicación integrada de las directrices/lineamientos detallados de auditoría

ESTRUCTURA DETALLADA PARA LA APLICACIÓN DE LAS DIRECTRICES DE AUDITORÍA	
Nivel 1 Enfoque general de auditoría de TI	• Marco Referencial de CObIT • Requerimientos del Proceso de Auditoría • Observaciones de Control • Directriz General de Auditoría
Nivel 2 Directrices del proceso de auditoría	• Directrices de Auditoría detalladas
Nivel 3 Puntos de atención de auditoría para complementar los objetivos detallados de control	• Condiciones Locales → Criterios específicos del sector → Estándares de la industria → Elementos específicos de la plataforma → Técnicas detalladas de control utilizadas

Tabla 4.3. Estructura de Directrices de Auditoría

4.7.2. REQUERIMIENTOS DEL PROCESO DE AUDITORÍA

Una vez definido qué vamos a auditar y sobre qué vamos a proporcionar aseguramiento, tenemos que determinar el enfoque o estrategia más apropiada para llevar a cabo el trabajo de auditoría. Primero se debe determinar el alcance correcto de nuestra auditoría. Para lograrlo, necesitamos investigar, analizar y definir:

- Los procesos del negocio involucrados;
- Las plataformas y los sistemas de información que están apoyando el proceso del negocio, así como la interconectividad con otras plataformas o sistemas;
- Los roles y responsabilidades de TI definidas, incluyendo las correspondientes al outsourcing interno y/o externo; y
- Los riesgos del negocio y las decisiones estratégicas asociadas.

El siguiente paso es identificar los requerimientos de información que tienen una relevancia particular con respecto a los procesos del negocio. Luego necesitaremos identificar los riesgos inherentes de TI, así como el nivel general de control que puede asociarse con el proceso del negocio. Para lograrlo, identificamos:

- Los cambios recientes en el ambiente del negocio que tienen impacto sobre TI;
- Los cambios recientes al ambiente de TI, nuevos desarrollos, etc.;
- Los incidentes recientes relevantes para los controles y el ambiente del negocio;
- Los controles de monitoreo de TI aplicados por la administración;
- Los reportes recientes de auditoría y/o certificación; y
- Los resultados recientes de auto evaluaciones.

Con ello obtendremos la información necesaria para seleccionar adecuadamente los procesos relevantes de CObIT, así como también los recursos que aplican a los mismos. Sin embargo, esto pudiera requerir que ciertos procesos de CObIT necesiten auditarse varias veces, cada vez para una plataforma o sistema distinto.

REQUERIMIENTOS DEL PROCESO DE AUDITORÍA	
Definir el alcance de la auditoría	• procesos del negocio involucrados • plataformas, sistemas y su interconectividad, que apoyan el procesos • roles, responsabilidades y estructura organizacional
Identificar los requerimientos de información relevantes para el proceso del negocio	• importancia para el proceso del negocio
Identificar los riesgos inherentes de TI y el nivel general de control	• cambios recientes e incidentes en el ambiente del negocio y de la tecnología • resultados de auditorías, autoevaluaciones, y certificación • controles de monitoreo aplicados por la administración
Seleccionar procesos y plataformas a auditar	• procesos • recursos
Fijar una estrategia de auditoría	• Controles versus riesgos • Pasos y tareas • Puntos de decisión

Tabla 4.4. Requerimientos del Proceso de Auditoría

4.7.3. OBSERVACIONES DEL PROCESO DE CONTROL

Los principios generales de control también pueden proporcionar una guía adicional sobre cómo complementar las Directrices de Auditoría. Estos principios están primordialmente enfocados sobre el proceso y las responsabilidades del control, los estándares de control y los flujos de la información de control.

El proceso de control consiste de cuatro pasos. Primero, se especifica un estándar de desempeño deseado para un proceso. Segundo, existe un medio de saber qué esta sucediendo en el proceso, por ejemplo, el proceso proporciona

información de control a una unidad de control. Tercero, la unidad de control compara la información con el estándar. Cuarto, si lo que realmente está sucediendo no cumple con el estándar, la unidad de control dirige aquella acción correctiva a tomar, en forma de información para el proceso. A partir de este modelo, las siguientes observaciones de control pueden resultar relevantes para la auditoría:

1. Para que este modelo funcione, la responsabilidad por el proceso del negocio (o en este caso, de TI) debe ser claro y la responsabilidad no debe ser ambigua. Si no es así, la información de control no fluirá y no podrá tomarse acción correctiva.
2. Los estándares pueden ser de una amplia variedad, desde planes y estrategias de alto nivel hasta indicadores clave de desempeño (KPI - Key Performance Indicators) y factores críticos de éxito (CSF – Critical Success Factors). Los estándares claramente documentados, mantenidos y comunicados son necesarios para un buen proceso de control. La responsabilidad clara por la custodia de dichos estándares también es un requerimiento para un buen control.

3. El proceso de control tiene los mismos requerimientos: bien documentado en cuanto a cómo funciona y con responsabilidades claras. Un aspecto importante es la clara definición de lo que constituye una desviación, esto es, cuáles son los límites de desviación.

4. La oportunidad, integridad y conveniencia de la información *de* control, así como también otra información, son básicas para el buen funcionamiento de un sistema de control y es algo que el auditor debe tratar.

5. Tanto la información de control como la información de acción correctiva tendrán que cumplir los requerimientos de *evidencia*, con el fin de establecer la responsabilidad después del evento.

Por tanto con los controles se podrá determinar lo qué se está logrando, evaluar el desempeño y si es necesario aplicar medidas correctivas para que el desempeño esté de acuerdo con lo planeado.

En resumen, las Directrices de Auditoría siempre pueden complementarse tomando en cuenta el Lineamiento Genérico y el proceso bajo revisión, y obteniendo tareas de auditoría adicionales para lograr el objetivo de auditoría, tomando en consideración los requerimientos del proceso de auditoría de TI, el Marco Referencial de CObIT y los Objetivos de Control de Alto Nivel, y las Consideraciones de Control.

En resumen, este desarrollo se ha concentrado en la definición tanto de los lineamientos orientados hacia la acción como en los lineamientos genéricos para la administración, requeridos para mantener el control sobre la información de la empresa y sobre los procesos relacionados y la tecnología. [LIB.012]

4.8. CObIT UNA HERRAMIENTA PARA LA AUDITORÍA Y SEGURIDAD INFORMÁTICA

Sin duda los cambios en la tecnología influyen en qué auditar y en cómo auditar, por lo que inevitablemente, la auditoría ha cambiado de manera drástica en los últimos años con el gran impacto que han generado las técnicas informáticas en la forma de procesarla.

Empero, y haciendo eco a estas tendencias, la Metodología CObIT ha superado las brechas existentes entre los negocios y las Tecnologías de la Información en la organización, haciendo de su modelo 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 contribuyan al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

CAPÍTULO V

APLICACIÓN DE LA METODOLOGÍA COBIT EN LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL GOBIERNO PROVINCIAL DE IMBABURA

CONTENIDO

- DEFINICIÓN DE LA MÉTODOLOGÍA
- PROGRAMA DE AUDITORÍA INFORMÁTICA

CAPÍTULO V

APLICACIÓN DE LA METODOLOGÍA CObIT EN LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL GOBIERNO PROVINCIAL DE IMBABURA A TRAVÉS DE LA GUÍA AUTOMATIZADA CObIT

5.1. INTRODUCCIÓN

La Metodología CObIT, en sus Directrices de Auditoría, nos presentan los requerimientos genéricos para auditar procesos de TI, siendo estas generalmente aplicables a todos los procesos existentes y pudiendo complementarse con tareas adicionales para lograr el objetivo de auditoría.

Por tanto, para la aplicación de la Guía Automatizada de CObIT en la Dirección de TIC's[45] del Gobierno Provincial de Imbabura, se tomó en cuenta su enfoque a la Auditoría y Seguridad Informática. Por consiguiente el enmarcar la Metodología CObIT dentro del esquema de la auditoría informática fue primordial para la consecución de los objetivos propuestos en el desarrollo del presente proyecto.

5.2. DEFINICIÓN DE LA METODOLOGÍA

Para aplicación de la Metodología CObIT (Objetivos de Control para la Información y las Tecnologías Relacionadas), fue necesario un estudio exhaustivo que nos permitiera determinar adecuadas guías, requerimientos y niveles de

[45] TIC's, Tecnologías de la Información y Comunicaciones.

administración de seguridad y control en la definición de un modelo para la implementación de la misma.

Dentro de este estudio, se llevó a cabo la tarea de instaurar un Framework[46] de IT Governance[47] y Objetivos de Control CObIT, para obtener los beneficios esperados con las herramientas que las tecnologías de la información nos proveen.

Posteriormente a ello, se diseñó una guía automatizada del modelo de implementación de CObIT para la Dirección de Informática del Gobierno Provincial de Imbabura, y con ello evaluar el Gobierno de TI y Los Objetivos de Control CObIT en sus cuatro dominios de manera eficaz y efectiva.

5.3. PROGRAMA DE AUDITORÍA INFORMÁTICA

Previo a una planificación de auditoría informática, debemos obtener una comprensión del control interno suficiente. Esta comprensión debe incluir conocimiento sobre el diseño de controles pertinentes y si estos han sido puestos en operación por la entidad, con ello se podrán identificar tipos de errores potenciales, factores de riesgo y diseñar pruebas sustantivas.

5.3.1. ALCANCE DE LA AUDITORÍA

El alcance de la auditoría expresa los límites de la misma, denotando las funciones, materias y organizaciones a auditar, para efectos de facilitar el desarrollo del proceso de auditoría.

El desarrollo del Plan General de Auditoría en la Dirección de Tecnologías de La Información y Comunicaciones del Gobierno Provincial De Imbabura, se

[46] Framework (Marco Referencial), Procesos y actividades en una estructura manejable y lógica.
[47] IT Governance (Gobierno de TI), es un término que representa el sistema de control o administración que establece la alta gerencia para asegurar el logro de los objetivos de una Organización

realizó a través de la aplicación del IT Governance (Gobierno de las Tecnologías de la Información) y Control Objetives (Objetivos de Control) de la Metodología CObIT.

El trabajo comprende un diagnóstico de la Dirección de Informática en cuanto a su gestión dentro de la entidad, por ello, en desarrollo del proceso auditor, se evaluó el área de Informática y, anexo a esta, a los usuarios de las Tecnologías de la Información en sus diferentes dependencias: Financiero, Comunicación, Tesorería, Bodega, entre otros.

La revisión está limitada a los controles vigentes en la metodología antes mencionada, aplicándose los pertinentes a gobiernos seccionales. [LIB. 013]

5.3.2. OBJETIVOS DE LA AUDITORÍA

Los objetivos serán los que rijan el programa de auditoría y a los que toda tarea emprendida debe llegar.

5.3.2.1.OBJETIVO GENERAL

Aplicar la Evaluación del Gobierno de Tecnologías de la Información y Objetivos de Control CObIT en la Dirección de Tecnologías de la Información y Comunicaciones del Gobierno Provincial De Imbabura.

5.3.2.2.OBJETIVO ESPECÍFICO

Determinar a través de la aplicación de la Guía Automatizada CObIT, el nivel de seguridad y control; y con ello establecer correctivos e implementar políticas necesarias.

5.3.3. ESTUDIO PRELIMINAR

El estudio preliminar consiste en examinar las funciones y actividades generales de la institución y así como de la entidad a auditar.

Se realizó un estudio inicial de la Dirección de Informática del Gobierno Provincial de Imbabura, en el cual se examinaron sus funciones y actividades generales, así como su relación con de las demás dependencias de la corporación.

Se procedió al análisis y conocimiento de:

- Normativa legal
- Organigrama institucional
- Organigrama del departamento.
- Relaciones jerárquicas y funcionales entre dependencias de la organización con la Dirección de Informática.
- Plan estratégico Informático.
- Entorno Operacional: Arquitectura y configuración de Hardware y Software, Aplicaciones, Bases de datos, Inventarios, entre otros.

Este estudio preliminar nos permitió obtener un entendimiento de la entidad y su entorno incluyendo el control interno, como aspecto esencial del desempeño de la auditoría, ya que se establece un marco de referencia y se ejerce juicio profesional.

5.3.3.1.EL GOBIERNO PROVINCIAL DE IMBABURA

Luego de haber transcurrido 177 años de la Constitucionalidad y vida del Estado independiente y soberano del Ecuador, los Gobiernos Provinciales, desde su posicionamiento en la representación y administración del Estado a nivel de gobierno subnacional intermedio, existen por más de 93 años; esto es: 2 años desde 1843 a 1845 como Concejos Provinciales; 8 años entre 1861 y 1869 en calidad de Municipalidades Provinciales; 6 años en el período comprendido entre

1878 y 1884, como Cámaras Provinciales; y, 77 años, en el período que va desde 1929 hasta la presente fecha, como Gobiernos Provinciales; todos cumpliendo la misión estatal a nivel provincial, atendiendo prioritariamente a los sectores menos favorecidos de la sociedad ecuatoriana.

5.3.3.2.CONFORMACIÓN

De acuerdo a lo previsto en los artículos 233 de la Constitución Política de la República y, 2 de la Ley de Régimen Provincial, está conformado por un cuerpo ejecutivo y un estamento de Legislación y de Fiscalización:

5.3.3.2.1. EL EJECUTIVO

Es ejercido por el Prefecto Provincial, quien es el máximo personero del Gobierno Provincial, elegido por votación popular, desempeña sus funciones durante cuatro años; su accionar se operativiza a través de las unidades y jefaturas administrativas de la entidad. Sus atribuciones y deberes constan en la Constitución y en la Ley; la función la ejerce con el concurso de Áreas, Unidades, Direcciones Administrativas.

5.3.3.2.2. EL ESTAMENTO LEGISLATIVO Y DE FISCALIZACIÓN

El Estamento Legislativo y de Fiscalización o Cuerpo Colegiado, es ejercido por el Consejo Provincial o “Cámara Provincial", integrado por el Prefecto, quien lo preside con el número de consejeros elegidos en base a la población de cada provincia, que en Imbabura llegan a ser en numero de cuatro (4).

5.3.3.3.COMPETENCIAS Y ATRIBUCIONES

El Gobierno Provincial es la entidad del poder público, regida por una Ley Orgánica que ejerce el gobierno, la administración y representación política del

Estado en la jurisdicción provincial goza de plena autonomía para su organización y funcionamiento, y que no puede ejercer sino las competencias y atribuciones consignadas en la Constitución Política de la República y en la Ley.

En consideración a lo anteriormente expuesto, notaremos algunas de las más principales:

- Dictamen de ordenanzas provinciales para la buena organización administrativa y económica de los servicios provinciales, creando, modificando o suprimiendo tasas y contribuciones especiales de mejoras. [LIB. 014]
- Participar del Sistema Nacional de Salud, atendiendo y vigilando el estado sanitario de la provincia y propendiendo su mejoramiento, a través de acciones conjuntas con los organismos estatales, municipales y juntas parroquiales.
- Participar del Sistema Nacional Descentralizado de Protección Integral para los niños y la adolescencia; formular políticas provinciales y destinar recursos para programas y servicios orientados a niños y adolescentes, así como también, el promover la asistencia económica de servicios que garanticen la estabilidad física y mental de las personas de la tercera edad, los jubilados y otros grupos vulnerables en el área rural de la provincia.
- Promover y estimular la cultura, la creación, la formación artística y la investigación científica en el área rural de la provincia, ejerciendo todo cuanto esté a su alcance para el desarrollo de la educación, fomentando la ciencia y tecnología en el área de la provincia.
- El Gobierno Provincial es la entidad estatal responsable de llevar a cabo en la jurisdicción provincial todas las competencias y atribuciones que en materia de obras y servicios públicos
- Proteger el medio ambiente, velando que este derecho no sea afectado y garantizando la preservación de la naturaleza en toda la jurisdicción provincial.

- Promover y ejecutar obras de alcance provincial en vialidad, medio ambiente, riego y manejo de las cuencas y microcuencas hidrográficas de la jurisdicción.
- Ejercer el desarrollo prioritario, integral y sostenido de las actividades agrícolas, pecuaria, acuícola, pesquera y agro industrial; y estimular los proyectos de forestación y reforestación de la jurisdicción.

Los recursos para su funcionamiento provendrán de:

- Las rentas generadas por Ordenanzas propias (tributos provinciales consistentes en: tasas y contribuciones especiales de mejoras).
- Los que perciben con cargo a los Fondo de Desarrollo Seccional y de Desarrollo Provincial; y, aquellos provenientes de Leyes Especiales, que son selectivas para ciertas provincias; y,
- La asignación resultante de la distribución del 15% que se asignan a los consejos provinciales dentro del Presupuesto General del Estado, se rigen por los siguientes criterios: número de habitantes de la provincia; necesidades básicas insatisfechas en la población provincial; logros en el mejoramiento de los niveles de vida; y, eficiencia administrativa del gobierno provincial.

Estos recursos se incrementarán anualmente en la misma proporción que se incremente globalmente el Presupuesto General del Estado, siendo prohibida toda asignación discrecional o extrapresupuestaria al Gobierno Provincial, salvo casos de catástrofe.

5.3.3.4.ESTRUCTURA ORGANIZACIONAL

El Gobierno Provincial de Imbabura en sus funciones encaminadas a velar por progreso de la comunidad imbabureña, gestiona proyectos de salud, educación, cultura, entre otros, que se cristalizan a través de las diferentes dependencias con las que cuenta la Corporación, siendo estas:

- Asesoría Jurídica
- Turismo
- Cultura
- Comunicaciones
- Ambiente y Fomento Productivo
- Estudios
- Financiero
- Fiscalización
- Informática
- Planificación
- RRHH y SSAA
- Secretaría General
- Vialidad. [WWW. 018]

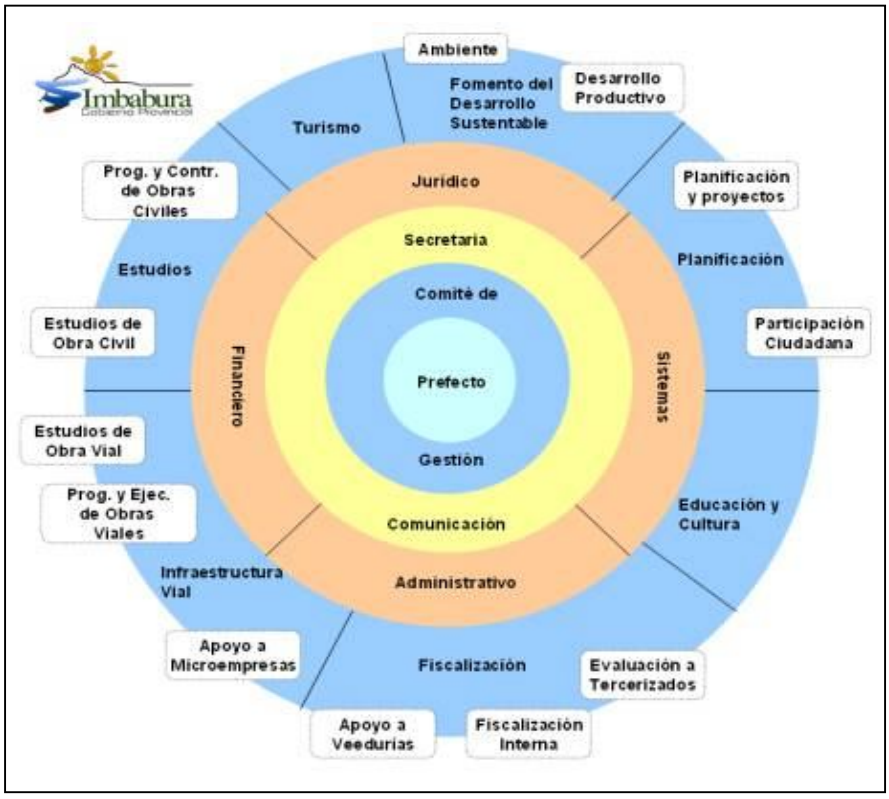


Fig. 5.1. Estructura Organizacional del Gobierno Provincial de Imbabura

5.3.3.5.LA DIRECCIÓN DE INFORMATICA (SISTEMAS)

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa, ya que sin lugar a dudas es la base fundamental para el éxito de cualquier organización, pués en ella se sustentan todos los procesos administrativos, financieros y operacionales.

La Dirección de Informática del Gobierno Provincial de Imbabura no es la excepción, ya que por hoy ha proporcionado una completa innovación tecnológica acorde a las necesidades de la Corporación.

5.3.3.5.1. MISIÓN

Administrar la Tecnología Informática del Gobierno Provincial de Imbabura, a través de su personal profesional y técnicamente preparado, brindando a nuestros usuarios soporte y servicios de calidad, que permitan una operación eficiente, optimización de recursos y un mejoramiento contínuo en los procesos del Gobierno Provincial de Imbabura.

5.3.3.5.2. VISIÓN

La Dirección de Informática será la base tecnológica que fomente los procesos administrativos, financieros y operacionales del Gobierno Provincial de Imabaura, en forma automatizada y con tecnología de punta, al servicio de la Provincia de Imbabura.

5.3.3.5.3. OBJETIVOS

- Usar Tecnología Informática para el desarrollo de las actividades, administrativas y financieras del Gobierno Provincial de Imbabura.

- Planificar la requisición de los recursos computacionales del Gobierno Provincial de Imbabura, estratégica y prospectivamente, que propicie una administración de la tecnología informática con criterios de eficiencia, eficacia y economía.

- Normar el uso de hardware, software y comunicaciones, estableciendo regulaciones y procedimientos que garanticen la correcta utilización de los recursos informáticos.

5.3.3.5.4. ESTRUCTURA ORGANIZACIONAL

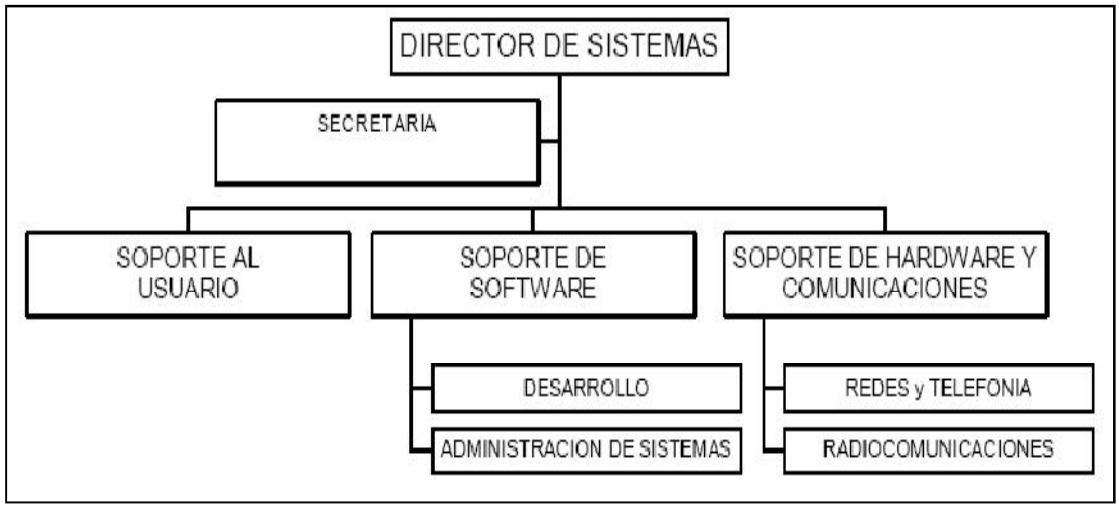


Fig. 5.2. Estructura Organizacional de La Dirección de Sistemas

5.3.3.5.5. ESTRUCTURA FUNCIONAL

5.3.3.5.5.1. DIRECTOR DE SISTEMAS

a) <u>De Administración</u>:

- Realizar, actualizar y ejecutar el Plan Informático del Gobierno Provincial de Imbabura en concordancia con el Plan Estratégico.

- Administrar la Tecnología Informática y Sistemas de Información del Gobierno Provincial de Imbabura.
- Asesorar a las Autoridades y Directores del Gobierno Provincial de Imbabura en el area de su competencia.
- Coordinar las interrelaciones de funciones y procesos del Gobierno Provincial de Imbabura con cada una de las Unidades Administrativas, para la automatización y el desarrollo del Sistemas de Información, con visión integradora.
- Gestionar y establecer las especificaciones técnicas para la adquisición de equipos, partes y piezas computacionales, así como también del Software.
- Conformar el Comité Estratégico Informático para delinear los Proyectos Informáticos.
- Las demas funciones que le asigne el Prefecto Provincial en el ámbito de su competimiento. [LIB.015]

b) De Normatividad:

- Establecer normas de uso y seguridad de hardware, software y networking.
- Dictar normas y procedimientos de estandarización sobre el Análisis, Diseño e Implementación de los Sistemas de Información.
- Vigilar que se cumplan las normas legales de licencia de uso de software para evitar la exposición innecesaria de la institución.
- Reglamentar la instalación y uso del software.
- Reglamentar la administración y manejo de la red de comunicaciones, tanto en la intranet, como en la extranet.

c) De Capacitación:

- Presentar anualmente el Plan de Capacitación Informática para los funcionarios de la Dirección de Informática y para los usuarios del software básico y de aplicaciones del Gobierno Provincial de Imbabura.

- Promover seminarios, conferencias y presentaciones sobre tecnología de punta y actualidad informática.

5.3.3.5.5.2. ÁREA DE SOPORTE AL USUARIO

- Receptar, registrar en el FSTU (Formulario de Soporte Técnico al Usuario) y atender en primera instancia las solicitudes de soporte técnico de los usuarios.
- Entrenar a usuarios sobre procedimientos de encendido, apagado y recuperación por caídas de voltaje o pérdida de comunicaciones.
- Entrenar a los usuarios sobre procedimientos de solución de problemas básicos.
- Actualizar el Inventario del Parque Tecnológico del Gobierno Provincial de Imbabura.
- Actualizar el Inventario de Software del Gobierno Provincial de Imbabura.
- Receptar y llevar el archivo de Documentación Informática Normal y Técnica de la Dirección de Informática.
- Ejecutar el mantenimiento preventivo de hardware y software.

5.3.3.5.5.3. ÁREA DE SOFTWARE

a) <u>Del Software Básico</u>:

- Instalar software básico, esto es sistemas operativos, procesadores de palabra, hojas de cálculo, graficadores, antivirus, entre otros.
- Configurar Sistemas operativos de usuarios y de servidores**.**

b) De la Base de Datos

- Administrar la base de datos: planificar, organizar, integrar, dirigir y controlar.
- Atender los requerimientos de los sistemas de información para la determinación de los perfiles de usuario y creación de nuevas aplicaciones informáticas.
- Mantener el Diccionario de Datos y la Estructura de los sistemas de bases de datos.
- Asegurar la consistencia, integridad y disponibilidad de las bases de datos.
- Efectuar los respaldos de la información almacenada en la base de datos, de acuerdo a las políticas de la Dirección.
- Investigar las nuevas tendencias tecnológicas.

c) De las Aplicaciones o Sistemas de Información:

- Atender y dar soporte especializado a los problemas y nuevos requerimientos de los sistemas de información del Gobierno Provimcial de Imbabura.
- Integrar Grupos de Gestión con usuarios de las Unidades Administrativas para el análisis y definición de los procedimientos susceptibles de automatización y durante el proceso de implementación de los sistemas de información.
- Determinar los perfiles de usuario para redes y bases de datos.
- Estandarizar la tecnología usada en el desarrollo e implementación de las aplicaciones.
- Documentar las aplicaciones desarrolladas, con sus respectivos manuales.
- Asegurar el soporte técnico y la apropiación de los sistemas desarrollados por terceros, con la tecnología usada.
- Efectuar los respaldos de las aplicaciones de acuerdo a las políticas de la Dirección.

5.3.3.5.5.4. SOPORTE DE HARWARE Y COMUNICACIONES

- Instalar, configurar y administrar y monitorear las redes alambricas e inalámbricas del Gobierno Provincial de Imabura.
- Asegurar el funcionamiento y disponibilidad de la red.
- Obtener estadísticas de usuarios sobre uso de los recursos en la red.
- Ejecutar el mantenimiento preventivo y correctivo del hardware de comunicaciones.
- Actualizar el inventario de equipos de comunicación.
- Administrar y configurar paquetes de redes, correo y seguridades.
- Transferir, explorar y sugerir mecanismos de apropiación de nuevas tecnologías.

5.3.3.5.6. POLÍTICAS DE LA DIRECCIÓN DE INFORMÁTICA

a) De la Tecnología Informática:

2. Todas las nuevas adquisiciones de equipos, partes o piezas computacionales, se realizarán con el asesoramiento y criterio técnico de la Dirección de Informática.

Esta política promueve la estandarización del uso de recursos tecnológicos, enmarcados dentro de la Planificación Informática.

3. Los nuevos computadores que se adquieran deben incluir licencias del software que se van a usar: sistemas operativos, procesadores de palabras, hojas electrónicas, graficadores, bases de datos, entre otros. Solo aquellos paquetes que son de tipo free o shareware, podrán ser instalados.

La política anterior crea conciencia en todos los usuarios, que no se puede instalar software ilegal o pirata, puesto que es un atentado a los derechos

de autor y que está tipificado como delito, según la nueva Ley de la Propiedad Intelectual, lo que nos conllevaría a afrontar serios problemas que van desde fuertes multas económicas, hasta la incautación de los computadores y de la información generada.

4. Se prohibe la utilización de la tecnología informática, recursos y suministros del Gobierno Provincial de Imbabura en beneficio personal o de terceras personas, con las siguientes salvedades:

- Por autorización escrita o sumilla del Prefecto, Consejeros o Directores.
- Por autorización del Director de Sistemas.
- Por estudios universitarios de los empleados y trabajadores, previa suscripción de una acta transaccional o convenio.
- Por pasantías y prácticas de bachillerato o pre-profesionales. [LIB.015]

b) <u>De los Recursos Humanos</u>:

1. Para los futuros integrantes de la Dirección de Sistemas del Gobierno Provincial de Imbabura, es requisito aprobar los Test Tecnológicos en la materia de su competencia.

2. Como requisito para el ingreso de un nuevo empleado al Gobierno Provincial de Imbabura y que vaya a desempeñar funciones administrativas y financieras, deberá rendir el Test Básico de Suficiencia Tecnológica, en las instalaciones de la Dirección de Informática del Gobierno Provicncial de Imbabura.

Esto permite evaluar el grado de conocimiento computacional del nuevo prospecto, para determinar el nivel de soporte, entrenamiento y capacitación que se le debe dar.

3. Toda capacitación recibida por los integrantes de la Dirección de Sistemas, deberá tener un efecto retroalimentador (feedback), a través de la entrega del material didáctico y / o apuntes, así como también con la capacitación al personal.

c) <u>De la Infraestructura Física</u>:

1. Se prohibe el acceso a las instalaciones de la Dirección de Sistemas, con las siguientes salvedades:

- Por autorización escrita o sumilla del Prefecto.
- Por autorización del Director de Sistemas.
- Por capacitación y asesoramiento a usuarios directos.
- Por visitas dirigidas, practicantes y pasantes.

2. Se prohibe comer, beber y fumar en las instalaciones de la Dirección de Sistemas, en especial en el Area de Soporte de Hardware y Comunicaciones.

3. La Limpieza de moviliario y Area Física se realizará durante horas laborables y en presencia de al menos un integrante de la Dirección de Sistemas.

d) <u>Del Soporte Técnico al Usuario</u>:

1. La Dirección de Sistemas brindará soporte técnico informático, en el ámbito de su competencia, a todas las Direcciones y Unidades Administrativas del Gobierno Provincial de Imbabura. Se brindará soporte a Terceros en los siguientes casos:

- Por autorización escrita o sumilla del Prefecto.
- Por autorización del Director de Sistemas.
- Por capacitación y asesoramiento a usuarios relacionados con el Gobierno Provicnial de Imbabura.
- Por Convenios, Conferencias o Seminarios.

Se ejecutará lo anterior, siempre y cuando no se atente contra los intereses del Gobierno Provincial de Imbabura, ni se viole las Leyes de la Propiedad Intelectual.

2. EL Soporte Técnico Informático se registrará en el Formulario de Soporte Técnico al Usuario. Lo anterior permite un mejor control interno de los recursos humanos y tecnológicos de la Dirección, así como también llevar estadísticas de evaluación de desempeño de los profesionales. Según el siguiente procedimiento:
Procedimiento:

i. El personal de la Dirección de Sistemas registrará con copia de papel carbón, todo soporte técnico al usuario que conste en el campo del Formulario – tipo de soporte – , que implique salir de las instalaciones de la Dirección de Informática o del Gobierno Provincial de Imbabura, detallando el requerimiento en el campo –Detalle del requerimiento –.
ii. De no exisitir en el Formulario el – tipo de soporte –, se especificará en el campo –Detalle del requerimiento –.
iii. Se llenará toda la información adicionalmente requerida en el Formulario en los campos –Datos– y – Condición -. Adicionalmente usted sumillará a un lado del campo –Autorizado por–.
iv. La copia será entregada al Director de Informática.
v. El original será sumillado con rubrica y sello del usuario atendido, una vez finalizado el soporte, para los casos 6 y 7 de este procedimiento, se sumillará antes de entregar los equipos, y luego el formulario original deberá ser entregado al Director de Sistemas para contrastar y archivar.

vi. Para el caso de Préstamo de Equipos, se indicará la fecha de –Inicio– y la fecha –Fin–, especificando el número de horas o días, y las condiciones en las que se entrega el equipo

vii. Para el caso del Infocus, se indicará el tiempo del reloj del Infocus en los campos –Inicio– y –Fin–, especificando el número de horas, y las condiciones en las que se entrega el equipo

viii. Se podrá registrar a la vez, más de un tipo de soporte, siempre y cuando sea para un mismo caso.

e) <u>De las Donaciones de Recursos Tecnológicos</u>:

2. Para aquellas entidades que solicitan donación de equipos computacionales se procederá a entregar equipos del parque informático actual, de las categorías C(Semiobsoletas) y D(Obsoletas), con el fin de renovar y evitar que el Gobierno Provincial de Imbabura se quede con computadores obsoletos. Solo en casos especiales podrán donarse equipos nuevos o de las categorías A(Buenas) y B(Regulares). Son casos especiales:

- Autorización del Prefecto.
- Para Aplicaciones Críticas.

5.3.3.6. ENFOQUE A LA TECNOLOGÍA INFORMÁTICA DEL GOBIERNO PROVINCIAL

Los principales elementos que conforman la tecnología informática lo constituyen: el Hardware, Software, Network y el Humanware, mismos que gestionados e integrados óptimamente forman la base sólida de las Tecnologías de la Información de una empresa.

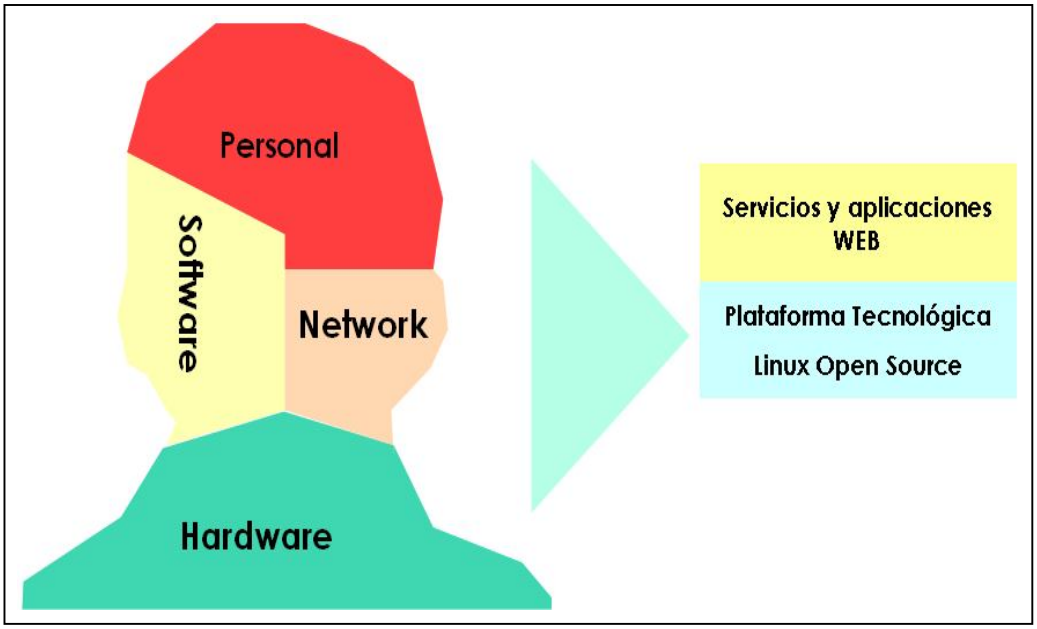


Fig. 5.3. Tecnología Informática en el Gobierno Provincial de Imbabura

Tras estudios y análisis realizados en la entidad, a continuación proporcionaremos información aproximada de los componentes que conforman la tecnología del Gobierno Provincial de Imbabura.

5.3.3.6.1. HARDWARE

El Gobierno Provincial de Imbabura cuenta con los equipos tecnológicos adecuados, tanto en lo referente a Servidores como a PC's, estos últimos se encuentran distribuidos en cada una de sus dependencias en un número de 105 computadores en total.

De manera general determinamos lo siguiente:

- Servidores: Server Elastix: VozIp, Server StickGate: Servidor Proxi, Server HP Proliant: Servidor de Aplicaciones y web de turismo.

En cuanto a ordenadores:

- Procesador: En su gran mayoría Core2 Duo con el 38%, seguido de Pentium IV con el 34%, Pentium D 14%, Core2 Quad 5%, Intel Celeron PIV 3%, Pentium III 3% y otros 3% (Fig. 5.5).
- Velocidad de Procesador: La velocidad varía de 1.30 Ghz a 3.40 Ghz.
- Memoria RAM: De manera similar los valores fluctúan entre 140 Mb a 1024 Mb
- Disco Duro: Mínimo tamaño en disco 30 Gb a un máximo de 500 Gb.
- Impresoras: Láser, Inyección a Tinta y Matriciales (Fig. 5.6).

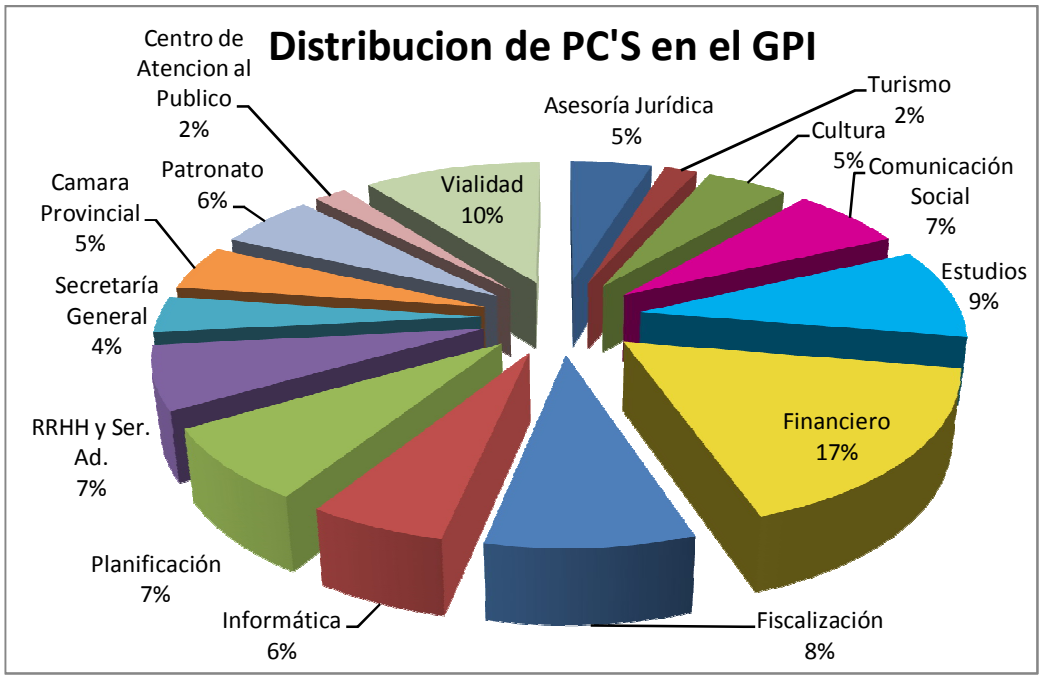


Fig. 5.4. Distribución de computadores en el Gobierno Provincial de Imbabura

La dirección de Informática ha promovido el uso de impresoras láser por las matriciales de manera efectiva, sin embargo algunas de estas han permanecido en la entidad debido a su utilidad en actividades de las dependencias de Recaudación y Tesorería. [LIB.015]

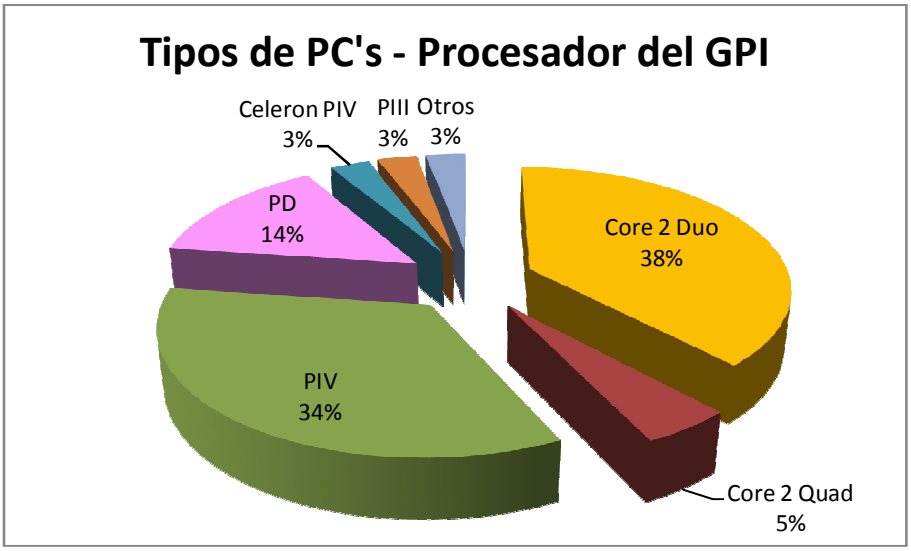


Fig. 5.5. Tipos de computadores existentes en el Gobierno Provincial de Imbabura

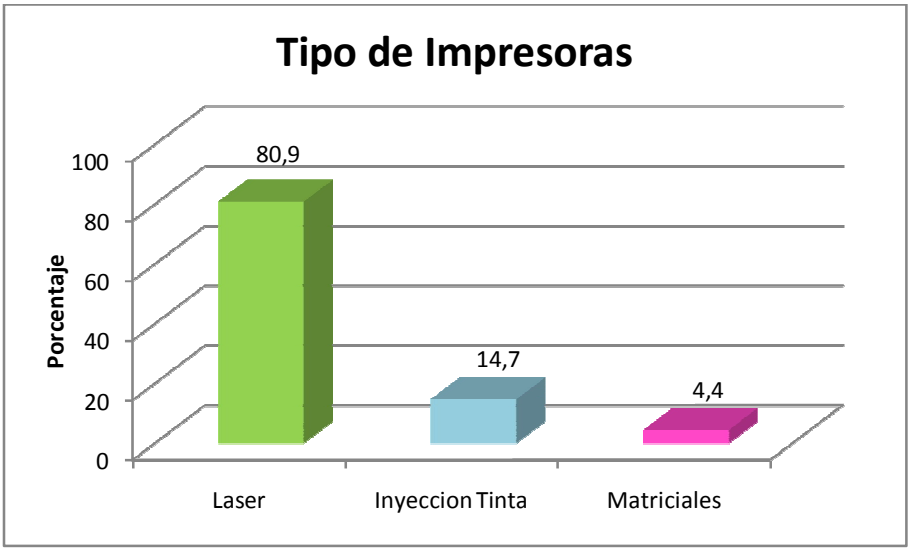


Fig. 5.6. Tipos de Impresoras

5.3.3.6.2. SOFTWARE

Los Sistemas de Información que comprenden desde el Software básico, hasta los Servicios y Aplicaciones Web en el Gobierno Provincial, están basados en una sólida plataforma tecnológica, que brinda a la entidad y usuarios todas las ventajas que las TI pueden proporcionar.

Sistemas Operativos y Software de Escritorio

- Windows Vista, Windows XP, Windows 98, Kernel (Macintosh), Linux, Mandriva, CentOS (Servidores).(Fig.5.7)
- Microsoft Office 2007: 51%, Microsoft Office 2003: 46%, Otros (Open Office): 3%.
- Adobe System Photoshop e Ilustrator, ArcGIS Developer Kit, Autodesk AcStdApply Module y Autodesk Land Desktop, Adobe CS2.
- Visual FoxPro, Visual Studio.
- Otras aplicaciones: Winzip, Panda Platinium, y AVG Antivirus, Ahead Nero.

Todo el software de Sistemas Operativos y Escritorio cuenta con las respectivas licencias.

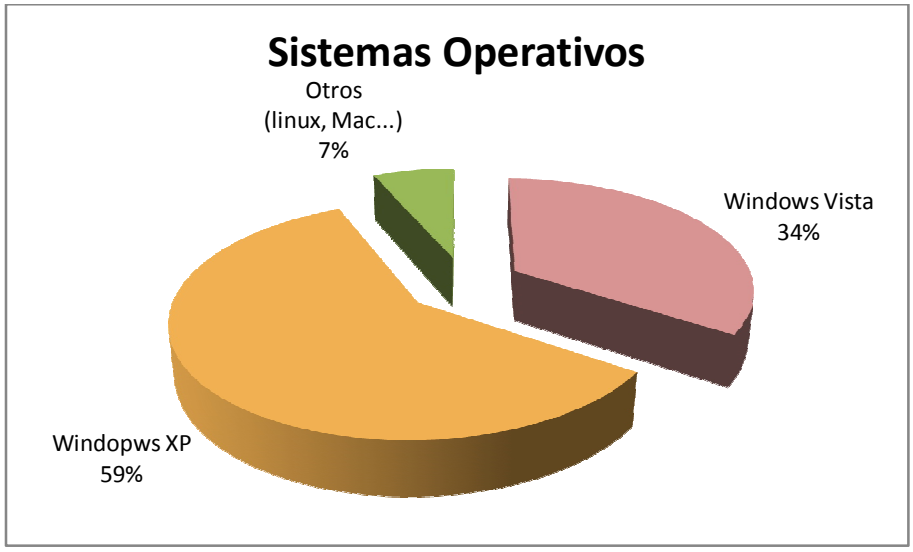


Fig. 5.7. Sistemas Operativos en Pc's del Gobierno Provincial de Imbabura

Servicios y Aplicaciones Web

- Intranet: Insaturada en año 2003, facilita el intercambio transparente de todos los recursos informáticos.

- SCOAD (Sistema de Costos y Administración Directa): En el se registran todos los costos de Proyectos y de las Obras que se realizan por Administración Directa.
- Contratos: Este módulo se refiere a los registros de contratos realizados con pólizas (garantías por servicios).
- Sistema de Roles y Asociación: En el se registran los roles de pago mensuales, así como los préstamos realizados por los trabajadores de la entidad y sus respectivos descuentos.
- Documentación: Como su nombre lo indica hace referencia a la documentación de todos los trámites para la gestión de obras que se realizan en el Gobierno Provincial.
- Administración: Módulo de administración de las aplicaciones de Intranet.
- Transparencia: Referente a la Ley de Transparencia y Libre Acceso a la Información Pública Gubernamental tiene como objeto establecer una relación entre el gobierno y su pueblo basándose en la rendición de cuentas, y en cumplimiento a la mencionada Ley , publica la información señalada en el Artículo 7.
- E-government Fase I: Contiene las aplicaciones de gobierno es decir conocimiento en los procesos internos de gobierno y en la entrega de los productos y servicios del Estado a la ciudadanía. Este módulo se encuentra en fase de desarrollo.
- Email: Correo Corporativo del Gobierno Provincial de Imbabura, alrededor de 80 usuarios.
- Pagina oficial del Gobierno Provincial de Imbabura www.imbabura.gov.ec.
- Pagina Web de Turismo de Imbabura en ingles y español www.imbaburaturismo.gov.ec, muestra una guía completa de los lugares turísticos existentes en los cantones de la provincia.
- Foro de la Educación www.imbabura.gov.ec/foro, movimiento ciudadano que constituye una herramienta social para impulsar la implementación y operativización del Plan de Desarrollo Estratégico Provincial , en el eje de

la educación; así como también posibilitar el diálogo, los aportes, los cuestionamientos y las propuestas de mejoramiento educativo.

- Portal de Transparencia, sitio de acceso a la información de Obras Contratadas y Obras por Administración Directa. (Fig.5.8)

Sistema Financiero Contable

- GUBWIN es un sistema tercerizado que contiene: Plan de cuentas, ingresos y egresos del Gobierno Provincial de Imbabura, así como también asientos y reportes para entidades de control. Actualmente se realiza la migración del sistema GUBWIN a e-government fase 1.

En relación a los datos obtenidos, como resultado observamos que la Corporación cuenta con Software: Legal 90%, Free 2%, Ilegal 8%.

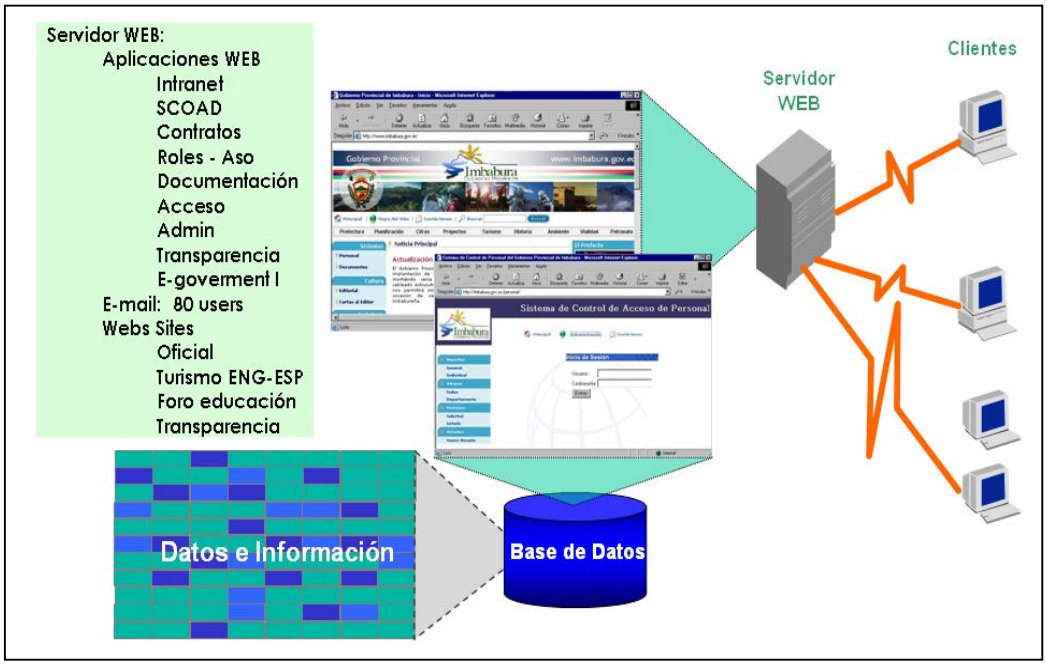


Fig. 5.8. Servicios y Aplicaciones Web del Gobierno Provincial de Imbabura

Por tanto podemos apreciar que esta completa integración de sistemas bajo la tecnología de Open Source (Linux Red Hat 9, SentOS 4.1 y Fedora), contempla

todos los procesos que en la Corporación existen, sean estos administrativos, financieros u operativos. [LIB.0015]

5.3.3.6.3. NETWORK

La network que posee el Gobierno Provincial es una red de área local Ethernet, sus características generales son:

- Cableado UTP[48] Cat 6 (nivel de prestaciones eléctricas, LAN Ethernet mayor de 100 MHz) en cada una de las dependencias.
- Posee 124 puntos de Voz y Datos con 100 extensiones.
- Conectividad ISP CC de 512 Kbps.
- Servidor Megadatos: Internet.
- Servidor StickGate: Servidor de Red (web y correo)
- Servidor Proliant: Servidor de Aplicaciones
- Servidor Elastix: Servidor de VoIP

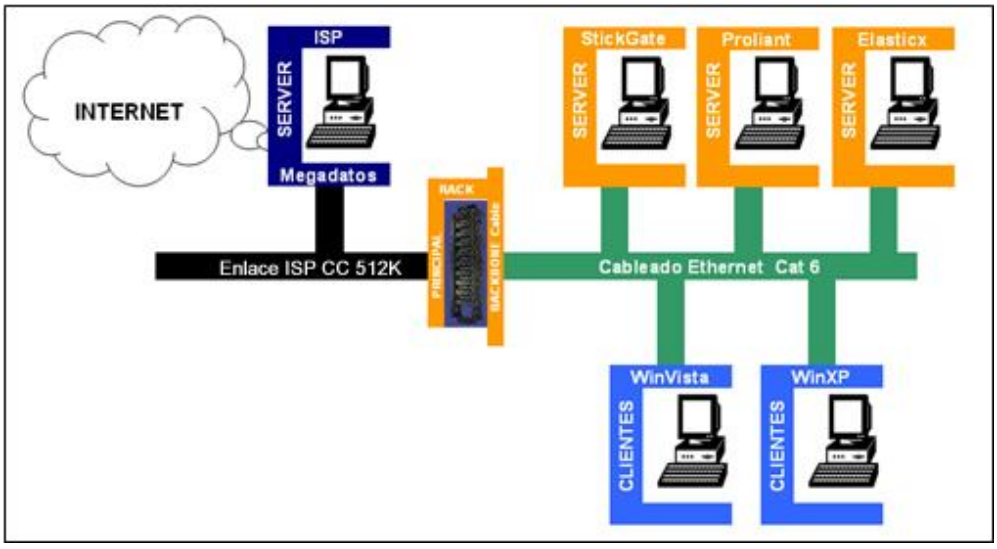


Fig. 5.9. Esquema general de Network del Gobierno Provincial de Imbabura

[48] UTP, Unshielded twisted Pair (Par Trenzado)

Fig. 5.10. Servidores: Elastix, StickGate y Proliant respectivamente

Fig. 5.11. Rack Principal

Es así que la innovación tecnológica con la que hoy cuenta el Gobierno Provincial de Imbabura, refleja una óptima gestión realizada por la Dirección de Informática en la actualización de la tecnología informática y comunicaciones, prestando y proveyendo a todas las dependencias de la Corporación, servicios de: intranet, Web oficial, Sistema de Costos, Internet, entre otros, mismos que están a la par del avance tecnológico y a los diferentes requerimientos de la Corporación.

Sin embargo la Dirección de Informática en su interés de aportar a la Corporación una completa innovación tecnológica, no ha profundizado los temas de normativas, seguridad y control de TI.

5.3.4. EVALUACIÓN DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

En esta fase procederemos a la evaluación de responsabilidades y controles internos de la Dirección de Informática en la entidad, con ello podremos determinar el nivel de Gobernabilidad de TI[49] existente, que lo realizaremos a través de la Guía Automatizada de CObIT.

Dentro de la Evaluación al Gobierno de TI, se encuentran definidos 5 módulos de evaluación, uno a aplicarse a los Usuarios de las Tecnologías de la Información (TI), y cuatro restantes específicamente para el Departamento de Informática.

Cabe mencionar que dichos cuestionarios fueron elaborados en base a las guías y criterios de la Metodología CObIT, lineamientos para test de ISACA y otras instituciones líderes en temas relacionados con la Gobernabilidad de TI y sus procesos y auditoría informática.

[49] IT Governance, Gobierno o Gobernabilidad de las Tecnologías de la Información.

5.3.4.1. EVALUACIÓN DE USUARIOS DE TI

La primera instancia a evaluar fueron los usuarios de las tecnologías de la información de la entidad, contando entre ellos a usuarios de Sistemas Aplicativos tal como son el Sistema de Costos y Administración Directa.

Como se mencionó anteriormente, la Evaluación del Gobierno de TI tiene determinado un módulo denominado UsuarioTI, que contiene 30 preguntas, distribuidas en 4 encuestas:

- Nivel de Conocimientos
- Procedimientos
- Seguridad
- Servicios

El usuario una vez que ha ingresado a la aplicación con su nombre de sesión y clave respectiva, contesta las preguntas designadas en el test, mostrándose al finalizar la calificación obtenida.

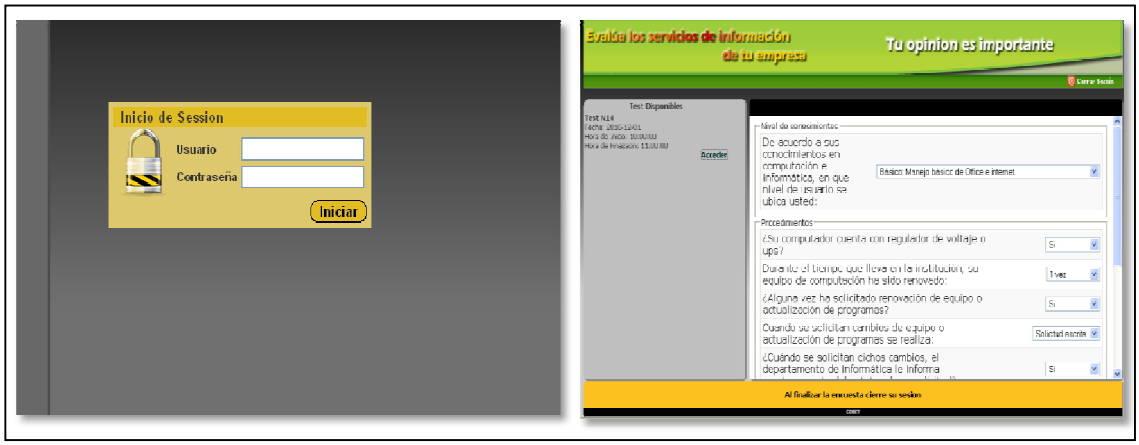


Fig. 5.12. Guía Automatizada CObIT – Evaluación de Usuarios de TI.

Dichas encuestas serán aplicadas al personal que labora en las diferentes dependencias de la institución, para con ello determinar diversos aspectos relacionados con el desempeño del Departamento de Informática y los servicios que presta.

5.3.4.2. EVALUACIÓN DE LA DIRECCIÓN DE INFORMÁTICA

Parte fundamental de la Evaluación del Gobierno de TI es la valoración a la Dirección de Informática, para ello se determinaron cuestionarios relacionados con el orgánico funcional de ésta y las actividades que desempeña.

Para esta evaluación, la Guía Automatizada CObIT posee cuatro Módulos, los cuales a su vez contienen las encuestas a ser aplicadas de la siguiente forma:

a. Módulo Gestión y Dirección de TI: Dirigida al Director / Gerente de Informática, contiene 132 preguntas distribuidas en 7 encuestas:
    - Organización de TI
    - Arquitectura de TI
    - Procesamiento de Datos
    - Planes de Contingencia
    - Inventarios
    - Personal y Procedimientos
    - Seguridad

b. Módulo de Software y Desarrollo: Destinada al personal inmerso en el desarrollo y administración de Software y Bases de Datos, posee 144 preguntas comprendidas en 7 encuestas:
    - Organización de TI
    - Arquitectura de TI
    - Procesamiento de Datos
    - Planes de Contingencia
    - Inventarios
    - Personal y Procedimientos
    - Seguridad

c. Módulo Hardware y Comunicaciones: Orientada al personal encargado de la Infraestructura de TI referente al Hardware y Comunicaciones, contiene 132 preguntas distribuidas en 6 encuestas:

- Organización de TI
- Infraestructura Locativa y Operacional
- Planes de Contingencia
- Inventarios
- Personal y Procedimientos
- Seguridad

d. Módulo Help Desk: Como su nombre lo específica está dirigida al personal que brinda Soporte Técnico al Usuario en la entidad, tiene 139 preguntas distribuidas en 7 encuestas:

- Organización de TI
- Hardware
- Software
- Planes de Contingencia
- Inventarios
- Personal y Procedimientos
- Seguridad

De similar forma, el usuario ingresará a la aplicación que, luego de contestar las preguntas se mostrará la calificación obtenida.

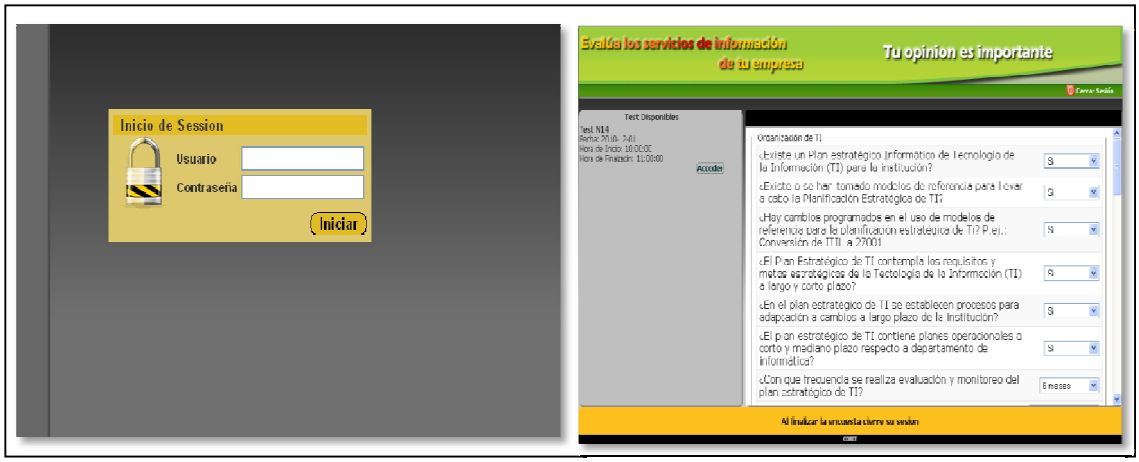


Fig. 5.13. Guía Automatizada CObIT – Evaluación al Departamento de Informática.

La Evaluación del Gobierno de TI, nos permitieron valorar el control interno de la Dirección de Informática, y determinar el nivel de cumplimiento. Además que pueden ser utilizadas como evidencia, ya generan pistas de auditoría para posterior uso en la elaboración del informe final y sustentación del juicio profesional de auditoría.

5.3.5. EVALUACIÓN DE CONTROLES COBIT

La segunda parte de valoración se refiere a la aplicación de los Objetivos de Control de la Metodología CObIT, y la evaluación de estos en la Dirección de Informática en sus diferentes dominios: Planeación y Organización, Adquisición e Implementación, Entrega y Soporte y Monitoreo, que constan el la Guía Automatizada. Cabe mencionar que estos conservan los lineamientos y principios proporcionados por la normativa.

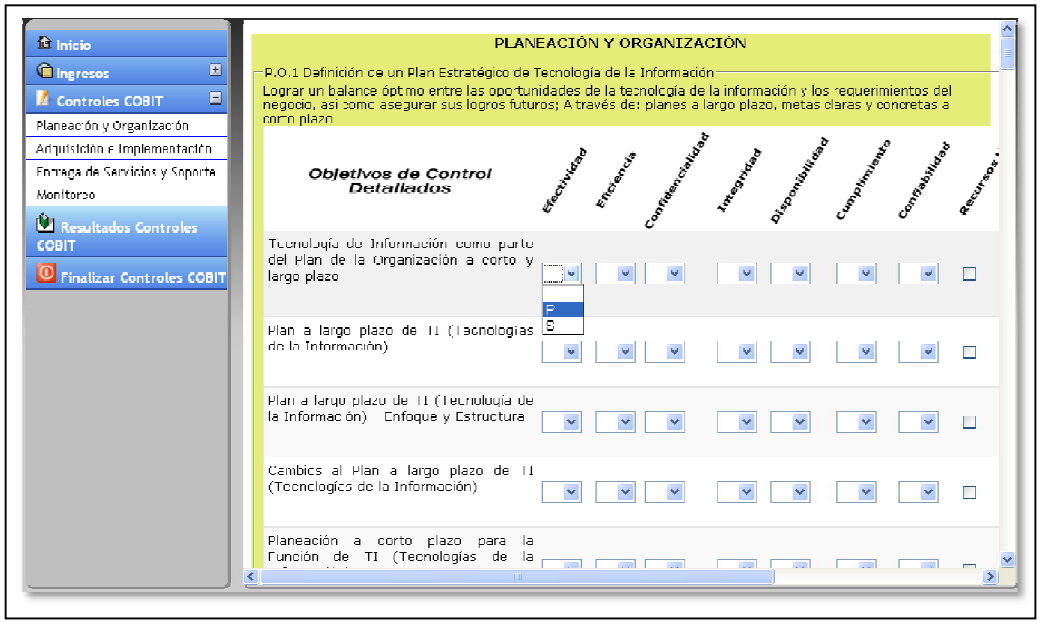


Fig. 5.14. Guía Automatizada CObIT – Controles CObIT.

La Guía Automatizada nos presenta los resultados obtenidos de forma gráfica, numérica, y cualitativa como se muestra.

PLANEACIÓN Y ORGANIZACIÓN

CRITERIOS DE TI	PUNTAJE	RESULTADO
Efectividad	25.00	Inferior a lo estimado en: 75 pts.
Eficiencia	25.00	Inferior a lo estimado en: 33 pts.
Confidencialidad	25.00	Superior a lo estimado en: 15 pts.
Integridad	25.00	Inferior a lo estimado en: 4 pts.
Disponibilidad	25.00	Superior a lo estimado en: 17 pts.
Cumplimiento	25.00	Superior a lo estimado en: 9 pts.
Confiabilidad	25.00	Superior a lo estimado en: 7 pts.
TOTAL	175	

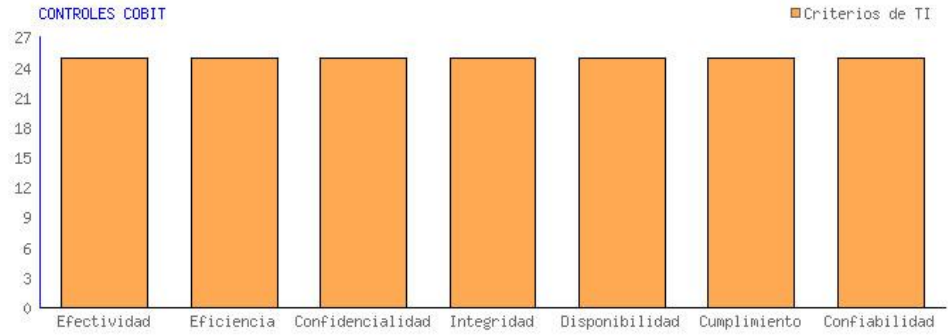


Fig. 5.15. Guía Automatizada CObIT – Resultados Controles CObIT.

Con ello podremos determinar el nivel de control de TI existente y sustentar de mejor manera las conclusiones en la elaboración del informe final de auditoría.

5.3.6. PRESENTACIÓN DE RESULTADOS

La presentación de resultados se lo realiza en el informe que se entrega a la Dirección de Informática, la forma y contenido del cuerpo del informe debe ser debidamente estructurado y ordenado. Previa elaboración del informe final, se realizó la redacción del informe en borrador.

En el informe CObIT, se revelan todos los hallazgos importantes de la auditoría, estos son respaldados por los papeles de trabajo. Los comentarios, conclusiones y recomendaciones se realizaron en base a que cumplen la condición de hallazgo de auditoría: condición, criterio, causa y efecto.

- **Comentario**: Narrativa de los hallazgos o aspectos trascendentales encontrados durante la auditoría. Los atributos del hallazgo deberán ser redactados claramente para facilitar: la identificación de cada uno de ellos, las conclusiones y recomendaciones.

  Los comentarios se realizan en base a cuatro criterios: Condición (Lo que es), Criterio (Lo que debe ser), Causa (Por que sucedió), y Efecto (Diferencia entre lo que es y lo que debe ser).

- **Conclusiones**: Juicios del auditor basados en los hallazgos, y realidades encontradas en la entidad.

- **Recomendaciones**: Las acciones correctivas que deben realizarse en base a los hallazgos y conclusiones formuladas.

La aplicación de la Guía Automatizada de la Metodología CObIT, permitirá evaluar el ambiente de Control Interno de la Dirección de Informática del Gobierno Provincial, determinar que tan eficaces son, y verificar si se da cumplimiento a dichos controles, estableciendo un uso eficiente de los recursos TI, garantizando mayor seguridad y control sobre el rendimiento de las mismas.

Por lo anterior, es necesario la aplicación de una de las Metodologías internacionales como lo es CObIT, para una adecuada administración y control de las Tecnologías de la Información, de tal manera garanticen una continuidad del servicio, en beneficio de la comunidad Imbabureña en general.

CAPÍTULO VI

DESARROLLO DEL APLICATIVO GUÍA AUTOMATIZADA DE COBIT

CONTENIDO

CAPÍTULO VI

DESARROLLO DEL APLICATIVO GUÍA AUTOMATIZADA CObIT.

6.1. PLANIFICACIÓN DEL SISTEMA

El desarrollo de una nueva aplicación conlleva en si mismo el compromiso de generar herramientas efectivas y eficaces que coadyuven a solucionar determinada problemática, en este caso, el desarrollo de una herramienta que contribuya a la Gestión de las Tecnologías de la Información para de esta manera asegurar el cumplimiento de los objetivos institucionales.

Por ello la necesidad una planificación, cuyo objetivo es establecer lineamientos de trabajo como referencia para el desarrollo de los cada uno de los componentes de la Guía Automatizada CObIT, tomando como base a los requerimientos que implica dicha normativa así como la integración de esta con los procesos de la institución.

Es así que para el desarrollo de esta aplicación, la hemos enmarcado dentro de las fases de proyectos web.

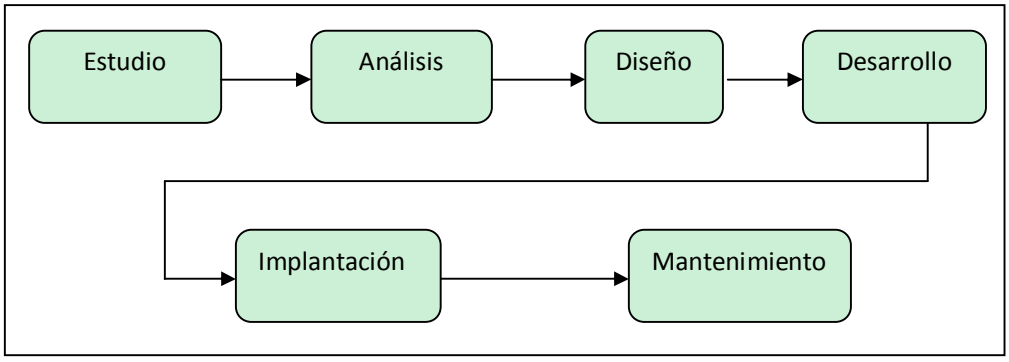


Fig. 6.1. Fases del Proyecto Web.

6.2. ESTUDIO DE VIALIDAD

El estudio de vialidad tiene como finalidad establecer las necesidades que se cubrirán con el desarrollo de la Guía Automatizada CObIT, el cual realizando un análisis tecnológico general se tomarán en cuenta todos los aspectos técnicos y operativos, cuyo resultado nos permitirá determinar cuan viable es la aplicación, las posibles soluciones y seleccionar la más adecuada, así también podremos determinar la medida en que se cumplirán los objetivos generales y específicos del proyecto.

Como resultado tendremos una perspectiva más clara en cuanto a: el impacto en la institución, la inversión a realizarse y los riesgos asociados.

6.2.1. ALCANCE DEL SISTEMA

Al no poseer la Dirección de Informática del Gobierno Provincial de Imbabura un estándar de seguridad y control basado en normas internacionales, se expone a un sinnúmero de riesgos tanto tecnológicos como administrativos. La aplicación automatizada de la Metodología CObIT permitirá utilizar la normativa adecuada para una administración efectiva de la TI, lo cual ayudará a satisfacer las múltiples necesidades de la Administración, y controles necesarios en aspectos técnicos.

Sin embargo debido a la complejidad que implica el desarrollo de toda la Metodología, el desarrollo de la Guía Automatizada de la misma abarca 2 grades módulos que son: El Gobierno de TI y los Controles CObIT.

6.2.1.1. MÓDULO DE GOBIERNO DE TI

Este módulo consiste en evaluar los procesos de TI en la Dirección de Informática, y a su vez la relación de esta con la institución, podremos determinar el nivel de control, servicios proporcionados a la entidad, entre otros.

Las funciones de este módulo son:

- **Panel de Control:** Donde el administrador del sistema podrá acceder con facilidad opciones como:
    a. Administrar usuarios.- Asignar nuevo, eliminar, editar.
    b. Auditoría.- Registro de todos cambios registrados en el sistema.
    c. Tutorial.- Manual de usuario de la Guía Automatizada.
    d. Objetivos de Control.- Archivo pdf de ayuda sobre la Metodología CObIT.
    e. Informe de Auditoría.- El respectivo informe con los resultados finales.
- **Ingresos:** Como su nombre lo especifica, se podrán realizar ingresos respecto a:
    a. Encuesta.- Test con sus respectivas preguntas y respuestas.
    b. Módulos.- A quienes o que estancias se dirigirán las encuestas.
    c. Test: Grupo de encuestas asignadas a un solo test. En esta sección también se añadirán usuarios participantes al test, así como fecha y hora.
    d. Resultados Test: Visualización por departamento de los resultados obtenidos en el Test.
    e. Departamento: Ingreso, modificación eliminación de departamentos.

6.2.1.2. MÓDULO CONTROLES CObIT

En esta sección, se aplicarán los Objetivos de Control de la Metodología CObIT, que al igual que en anterior módulo, se presentarán los resultados de forma inmediata.

Las funciones de este módulo son:

- **Controles CObIT:** Evaluación de dichos controles en sus cuatro dominios: Planeación y Organización, Adquisición e Implementación, Entrega y Soporte, y Monitoreo.
- **Finalizar Controles CObIT:** Opción con la cual el auditor o administrador da por terminada la evaluación aplicada de controles.
- **Resultados Controles CObIT:** Una vez finalizada la evaluación de los controles, se genera automáticamente los resultados obtenidos.

6.2.2. ESTUDIO DE LA SITUACIÓN ACTUAL

En la actualidad el éxito de las empresas está basado en ofrecer productos y servicios de alta calidad que se ajusten a las necesidades y preferencias del mercado, donde la información y la tecnología que la soporta, representan los activos más valiosos de la empresa, reconociendo así los beneficios potenciales que esta puede proporcionar.

En el Ecuador pese a que la mayoría de las empresas conocen la existencia de normas de calidad y seguridad internacionales, son muy escasas las que han tomado la pauta respecto a este referente, constituyendo este grupo los sectores comercial y financiero a nivel nacional.

El Gobierno Provincial de Imbabura a través de la Dirección de Informática, ha proporcionado desde sus inicios una óptima gestión en actualización de la tecnología informática y comunicaciones, prestando y proveyendo a todas las dependencias de la Corporación, servicios de: intranet, Web oficial, Sistema de Costos, Internet, entre otros, mismos que están a la par del avance tecnológico y a los diferentes requerimientos de la empresa, sin embargo a pesar a ello, la falta de una adecuada administración de las Tecnologías de la Información y en sí, la no

inobservancia de una normativa de seguridad y control en relación a las diferentes innovaciones tecnológicas realizadas en la entidad, conlleva a que posteriormente se originen numerosos conflictos; por ello es necesario la emplear de una de las Metodologías internacionales como lo es CObIT, que a través de la aplicación de la Guía Automatizada de la misma, nos permita determinar riesgos potenciales, para tomar acciones correctivas o contramedidas, que eviten ser mas vulnerables, y de esta manera garantizar la continuidad del servicio, en beneficio de la comunidad Imbabureña en general.

6.2.3. SELECCIÓN DE ALTERNATIVA DE SOLUCIÓN

Considerando los costes de instalación y mantenimiento, además de la descripción general del sistema, se han considerado los siguientes factores para la elección de la solución que es Windows XP SP3 + aplicaciones libres:

- **Requisitos planteados:** La alternativa seleccionada cubren en mayor o menor medida los requisitos básicos a nivel funcional y técnico. En cuanto a los aspectos económicos y legales, Windows XP SP3 + aplicaciones libres es la ganadora.
- **Análisis costo/beneficio:** Este análisis ha dado como resultado que, la solución Windows XP SP3 + aplicaciones libres o propias es la más barata.
- **Riesgos:** Los posibles problemas que pudieren generarse serán de más fácil solución los relacionados con el sistema operativo Windows XP SP3 + aplicaciones libres o propias.

6.3. ANÁLISIS DEL SISTEMA

En esta etapa se realizará un análisis detallado y sistemático de los módulos a desarrollarse, los requisitos a cumplir y los usuarios a satisfacer.

El propósito del sistema es implementar un modelo de la Guía Automatizada de CObIT para la Dirección de Informática, para ello se desarrollará dos módulos con los que se espera instaurar a futuro un efectivo Gobierno de las TIC en el Gobierno Provincial de Imbabura.

Cabe mencionar que esta será una herramienta innovadora, única en su género pudiéndose aplicar a cualquier entidad pública en el momento que creyere necesario.

El análisis del sistema se realizara para cada uno de los módulos los respectivos y sus procesos detallados por cada actividad, elaborándose los modelos de casos de uso respectivos.

6.3.1. DEFINICIÓN DEL SISTEMA

En esta fase describiremos el sistema, y se establecerá qué usuarios serán representativos en el uso del mismo.

- La información presentada en el sistema deberá ser presentada de forma atractiva, en concordancia con la imagen de la institución.
- El contenido de la aplicación deberá ser administrado mediante una herramienta web que permita crear, actualizar y borrar contenido sin que para esto sea necesario conocimientos de lenguajes de programación o de administración de base de datos.
- Únicamente aquellas personas autorizadas para ello podrán acceder al sistema. La autorización consistirá en que los usuarios poseerán un nombre de usuario y una contraseña válidos en el sistema.
- Las licencias de uso del software de la aplicación, servidores, lenguajes de programación, sistemas operativos, etc. deberán ser lo menos restrictiva posible.

6.3.1.1. ENTORNO TECNOLÓGICO DEL SISTEMA

- El entorno tecnológico del sistema podrá ser el Sistema Operativo Windows o Linux, además las aplicaciones desarrolladas deberán ser programadas en lenguaje PHP con base de datos MySQL, debido a que esta plataforma es la más utilizada para los sistemas desarrollados en la corporación.

- Refiriéndonos a las interfaces de usuario, las aplicaciones deberán utilizar interfaces amigables y simples.

6.3.2. IDENTIFICACIÓN DE USUARIOS

Los usuarios involucrados en el uso o aplicación de la Guía Automatizada CObIT son:

- **Auditor de Sistemas:** Quien ejecutará la auditoria en todas sus fases.
- **Personal de la Institución:** En primera instancia tenemos a todo el personal que labora en la institución, ya que ellos formarán parte del módulo de Usuarios TI de la Guía Automatizada.
- **Departamento de Informática:** Director/ Gerente, personal de Soporte de Software, Hardware y Comunicaciones, y Soporte al Usuario, como dependencia responsable de todos los procesos de TI del Gobierno Provincial

6.3.3. ESTABLECIMIENTO DE REQUISITOS

En esta fase determinaremos los requisitos generales de los módulos anteriormente descritos, con el fin de facilitar el análisis de los mismos. La Guía Automatizada de la Metodología CObIT deberá cumplir con los siguientes requisitos:

Funcionales:

- Mediante la Guía Automatizada de la implementación de CObIT, valorar los controles instanciados en la Dirección de Informática versus controles de la Normativa de manera individual.
- Evaluar el Control Interno mediante encuestas (Evaluación del Gobierno de TI).
- Generar reportes y estadísticas de los controles y encuestas aplicadas.
- Impresión de dichos reportes.

Rendimiento:

- Permitir aplicar cada uno de sus módulos tanto de Controles como Encuestas (Evaluación de Gobierno de TI) de manera individual.
- Generar en reportes la tabulación automática y presentación de resultados estadísticos de forma inmediata.

Implantación:

- La aplicación deberá brindar una interacción amigable y manejable al usuario.
- El software de aplicación contendrá la suficiente información de ayuda tanto para el manejo de sus opciones como para la interpretación de resultados.
- La Guía Automatizada de la implementación de CObIT, se la realizará cumpliendo el aspecto legal como la Metodología implantada lo es en si.

Disponibilidad:

- La Guía Automatizada de CObIT podrá ser utilizado por el Auditor, o Gerente de TI o usuarios en cualquier instancia que lo creyere necesario, permitiendo compararlos contra el ambiente de TI existente y planeado en

la organización, con lo cual podrá determinar lo que esta logrando y si el caso amerita aplicar las medidas correctivas necesarias.

- La Guía Automatizada podrá ser utilizada en diferentes plataformas como son Windows y Linux.
- El sistema podrá ser actualizado y adaptable a versiones posteriores a esta.

Hardware y Software:

Procesador	Procesador Pentium IV de 1.4 Ghz (Recomendado Superior Procesador Pentium IV de 2.0 Ghz).
Memoria	2 Gb (Recomendado 4 Gb)
Disco duro	1 Gb de espacio disponible mínimo.
Periféricos (E/S)	Teclado, mouse, monitor resolución 1024 x 678 Mega píxeles o mayor para una mejor visualización)
Conexión a redes	Tarjeta de Red
~~Conexión a Internet~~	~~No requerida~~
Explorador web	Internet Explorer versión 7 en adelante o Mozilla Firefox versión 3 en adelante.
SGBD	Base de datos de MySQL 5.0.1 o superior
Lenguaje de programación	PHP versión 5 hasta PHP versión 5.3 Se requiere: • php-xml, para lectura del Descriptor de la Base de Datos. • php-gd: para generación dinámica de imágenes para reportes.
Servidor	Servidor web Apache 2.2 en adelante
Sistema operativo	Windows XP o superior, Linux cualquier distribución (Recomendado Debian)

Tabla 6.1. Requerimientos de Hardware y Software mínimos para el sistema.

6.3.4. ANÁLISIS MEDIANTE DIAGRAMAS DE CASOS DE USO

Una vez se han descrito los requisitos del sistema se procederá a realizar el análisis de casos de uso, con los que podremos describir las interacciones entre usuarios y que interfaces utilizarán.

ACTORES DEL SISTEMA	CASOS DE USO
Administrador	Panel de Control
	Ingresos
	Controles CObIT
	Finalizar Controles CObIT
	Resultados Controles CObIT
Usuario general de TI	Test

Tabla 6.2. Casos de uso del sistema.

6.3.4.1. DIAGRAMA DE CASOS DE USO PARA EL MODULO GOBIERNO DE TI

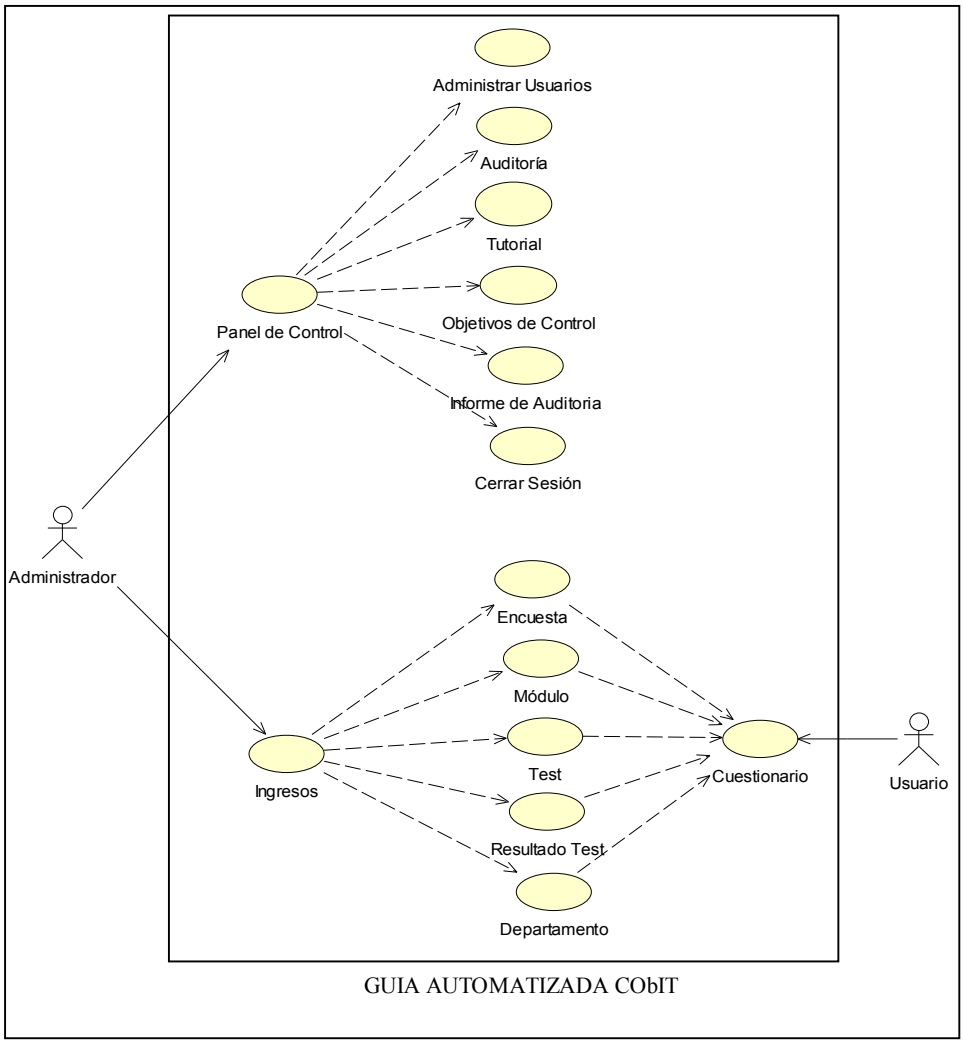


Fig. 6.2. Caso de uso del Gobierno de TI.

CASO DE USO	CU-001 Gobierno de TI	
ACTORES	Administrador, Usuario de TI	
PRECONDICIÓN	El administrador y usuario han iniciado sesión. Hay un test disponible.	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Administrador elige Panel de Control para: administrar usuarios, auditar, entre otras opciones. 2. Administrador elige Ingresos, publica Test. 3. Usuario ingresa al Sistema para evaluación.	1. El sistema muestra opciones para: administrar usuarios, auditar, entre otras opciones. 2. El sistema muestra opciones de Ingresos para: Test, encuestas, etc. 3. Muestra Test publicado por el Administrador.
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador no publica test.	
POSTCONDICIÓN	La aplicación fue agregada exitosamente en el lugar deseado.	

Tabla 6.3. Caso de uso del Gobierno de TI.

6.3.4.1.1. CASOS DE USO PARA PANEL DE CONTROL

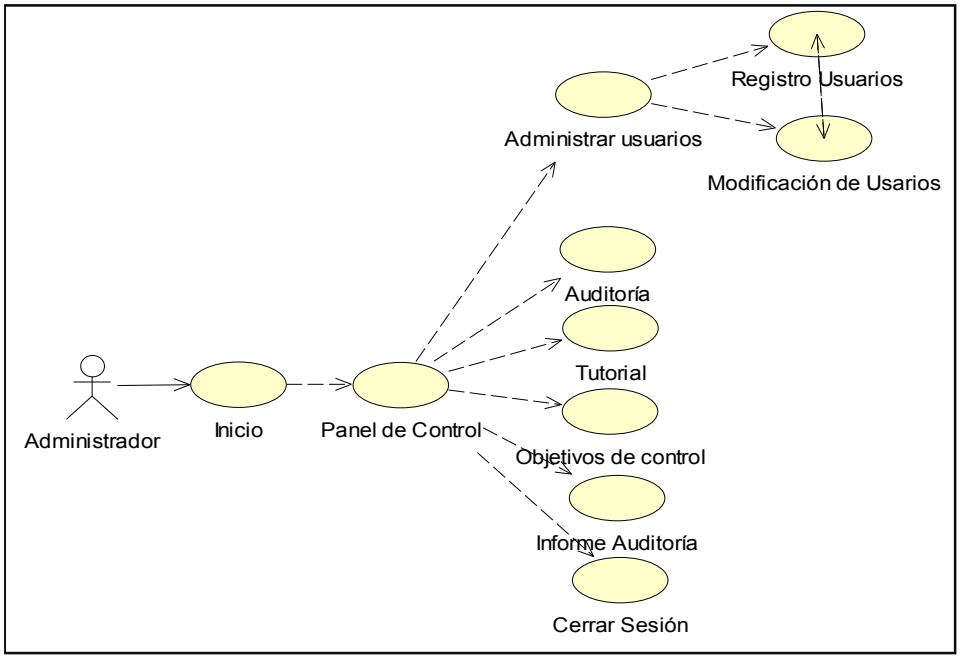


Fig. 6.3. Caso de uso Panel de Control.

CASO DE USO	CU-002 Panel de Control	
ACTORES	Administrador	
PRECONDICIÓN	El administrador ha iniciado sesión	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Administrador inicia sistema.	1. El sistema muestra opciones de panel de control y menu
	2. Elige Administrador Usuarios.	2. El sistema despliega información para: registro de nuevos usuarios o modificación de la información de los ya registrados.
	3. Administrador selecciona Auditoría	3. Se muestra información de los cambios realizados en el sistema y base de datos por el administrador del sistema.
	4. Administrador selecciona Tutorial	4. Se despliega información sobre el sistema y sus componentes en formato html.
	5. Administrador selecciona Objetivos de control.	5. El sistema muestra un archivo en formato pdf sobre información de los Objetivos de control de la Metodología CObIT.
	6. Administrador elige Informe de Auditoría.	6. El sistema muestra ventana de descarga de archivo en formato Microsoft Word, documento base para elaboración de informe final.
	7. Administrador elige cerrar sesión.	7. Salida del sistema.
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador no ingresa al sistema.	

Tabla 6.4. Caso de uso de Panel de Control.

6.3.4.1.2. CASOS DE USO PARA INGRESOS

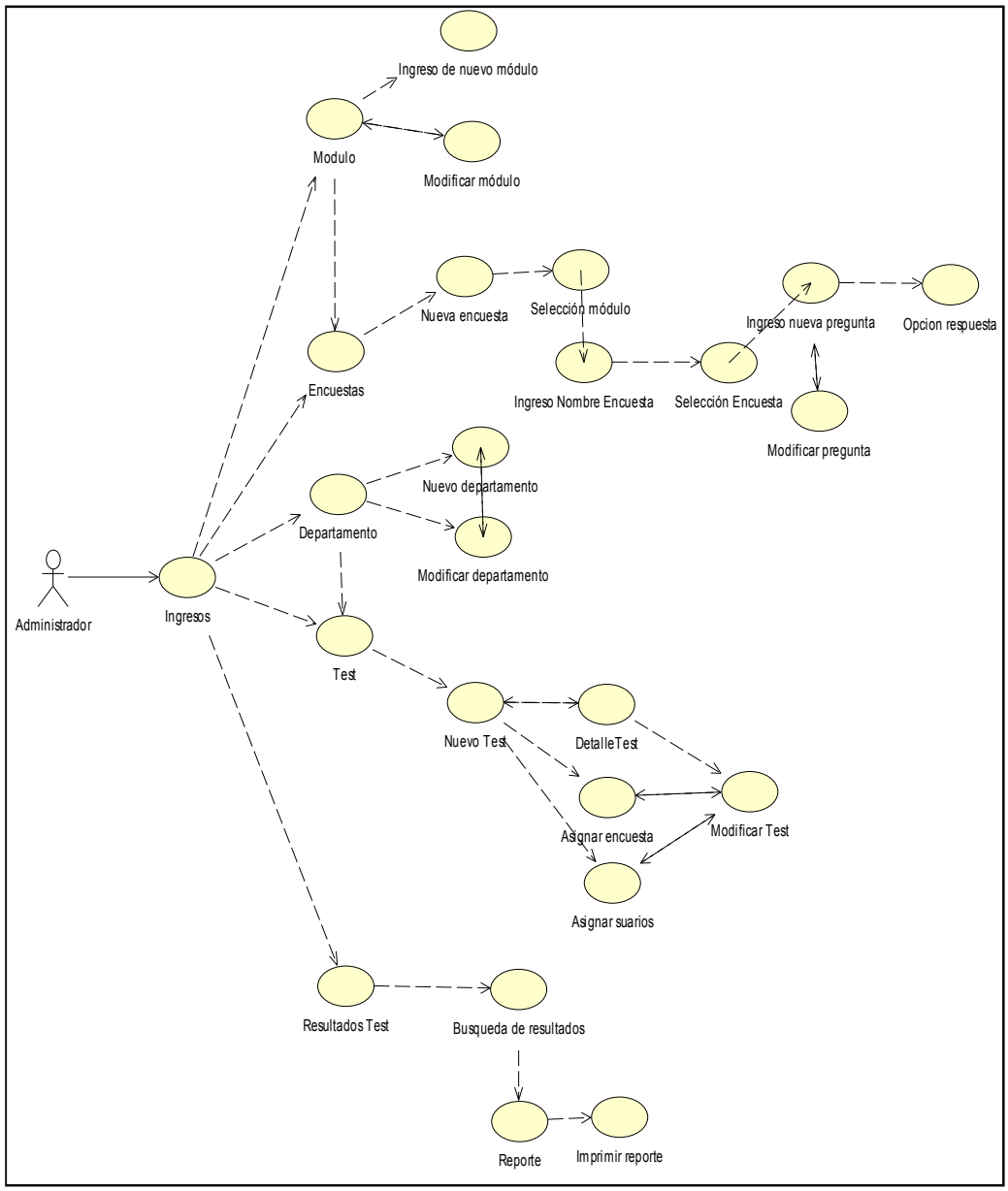


Fig. 6.4. Caso de uso Ingresos.

CASO DE USO	CU-003 Ingresos	
ACTORES	Administrador	
PRECONDICIÓN	El administrador ha iniciado sesión	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Administrador inicia sistema.	1. El sistema muestra opciones de panel de control y menú
	2. Elige Menú Ingresos.	2. El sistema despliega menú de opciones: Módulo, Encuesta, Departamento, Test, Resultado Test.
	3. Selecciona Módulo	3. El sistema despliega información para registro de un nuevo módulo que contendrá una o varias encuestas. También pueden modificarse los ya existentes.
	4. Selección Encuestas	4. Se despliega información para registro de nueva encuesta o modificación de encuestas ya registradas. Pueden añadirse o modificarse nuevas preguntas.
	5. Elección Departamento.	5. El sistema muestra información para registro de nuevos departamentos o modificación de registros existentes.
	6. Elección Test.	6. El sistema genera información para creación de un nuevo test, asignación de detalles como fecha y hora, asignación de encuestas y usuarios participantes. La modificación solo se podrá realizar antes de la publicación de un test.
	7. Selección Resultado Test.	7. Se generan resultados de acuerdo a la búsqueda realizad por departamento. Se muestran todos los test realizados a dicha dependencia.
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador no publica Test.	
POSTCONDICIÓN	Los ingresos y publicación de test se realizaron exitosamente en el lugar deseado	

Tabla 6.5. Caso de uso de Ingresos.

6.3.4.2. DIAGRAMAS DE CASOS DE USO PARA EL MÓDULO CONTROLES CObIT

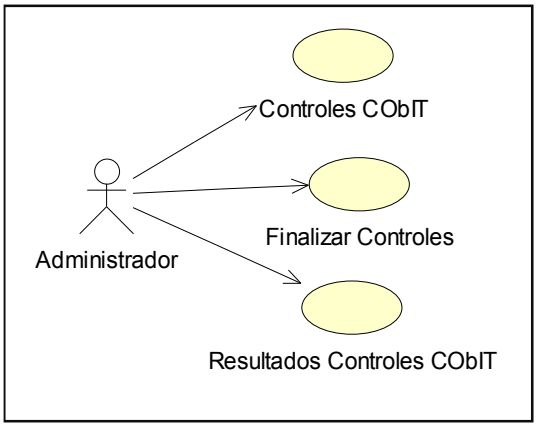


Fig. 6.5. Caso de uso Módulo Controles CObIT.

CASO DE USO	CU-004 Controles CObIT	
ACTORES	Administrador	
PRECONDICIÓN	El administrador ha iniciado sesión	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Administrador inicia sistema.	1. El sistema muestra opciones de panel de control y menú
	2. Selecciona Controles CObIT.	2. Opción para evaluación de los controles en os 4 dominios de CObIT.
	3. Selección Finalizar Controles CObIT.	3. Finalizar evaluación de controles.
	4. Selección Resultados Controles.	4. Reportes de las evaluaciones de control aplicadas
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador realiza controles.	
POSTCONDICIÓN	Las evaluaciones de control se realizan exitosamente.	

Tabla 6.6. Caso de uso de Controles CObIT.

6.3.4.2.1. CASOS DE USO PARA CONTROLES CObIT

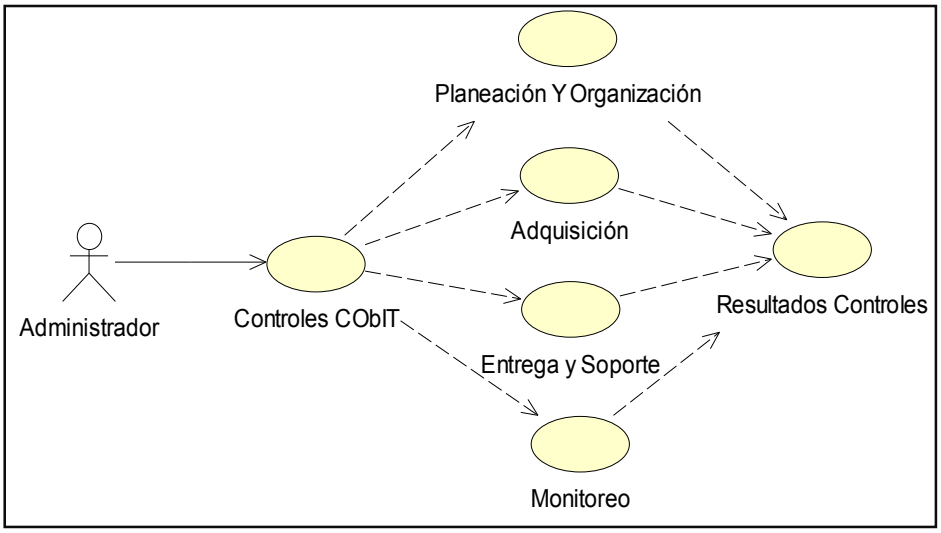


Fig. 6.6. Caso de uso Controles CObIT.

CASO DE USO	CU-005 Controles CObIT	
ACTORES	Administrador	
PRECONDICIÓN	El administrador ha iniciado sesión	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Administrador inicia sistema.	1. El sistema muestra opciones de panel de control y menú
	2. Selecciona Controles CObIT.	2. El sistema genera las opciones para Evaluar los controles CObIT en los dominios de: Planeación y Organización, Adquisición e Implementación, Entrega y Soporte y, Monitoreo. Estos se relacionan directamente con los resultados CObIT.
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador no realiza controles.	
POSTCONDICIÓN	Las evaluaciones de control CObIT se realizan exitosamente.	

Tabla 6.7. Caso de uso de Evaluación controles CObIT.

6.3.4.2.2. CASOS DE USO PARA FINALIZAR CONTROLES CObIT

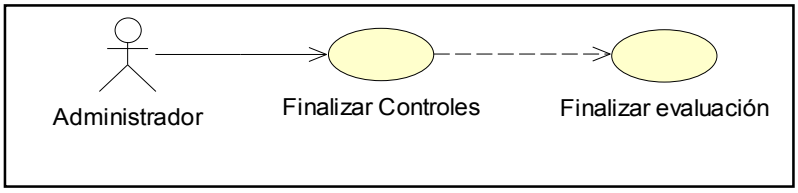


Fig. 6.7. Caso de uso Finalizar Controles CObIT.

CASO DE USO	CU-006 Finalizar Controles CObIT	
ACTORES	Administrador	
PRECONDICIÓN	El administrador ha iniciado sesión	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Administrador inicia sistema.	1. El sistema muestra opciones de panel de control y menú
	2. Selecciona Finalizar Controles CObIT.	2. El sistema finaliza la evaluación en curso de los controles CObIT, con ello los datos se guardan para posterior reporte.
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador no realiza controles.	
POSTCONDICIÓN	Se finaliza la evaluación de controles CObIT se realizan exitosamente.	

Tabla 6.8. Caso de uso de Finalizar controles CObIT.

6.3.4.2.3. CASOS DE USO PARA RESULTADOS CONTROLES CObIT

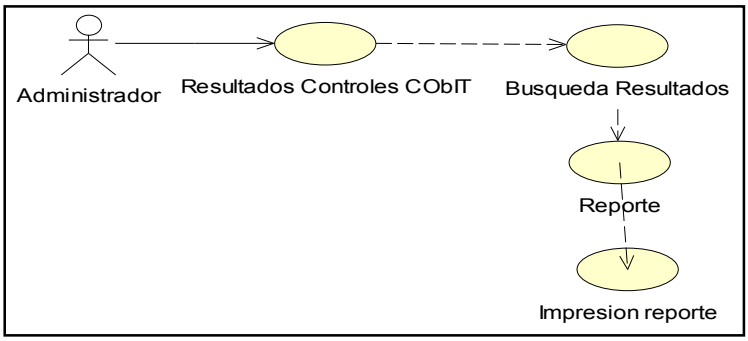


Fig. 6.8. Caso de uso Resultados Controles CObIT.

CASO DE USO	CU-007 Resultados Controles CObIT	
ACTORES	Administrador	
PRECONDICIÓN	El administrador ha iniciado sesión	
CURSO NORMAL	**ACTOR**	**SISTEMA**
	1. Selección opción Resultados Controles CObIT. 2. Selección Impresión	1. El sistema muestra casillas de búsqueda por fecha de las evaluaciones realizadas. 2. Se envían los reportes a impresión.
CURSO ALTERNO	**ACTOR**	**SISTEMA**
	El administrador no realiza controles.	
POSTCONDICIÓN	Se visualizan e imprimen los reportes de controles CObIT exitosamente.	

Tabla 6.9. Caso de uso de Resultados controles CObIT.

6.3.5. DEFINCIÓN DE INTERFACES DE USUARIO

Previo y durante el desarrollo de la aplicación de CObIT, se pudo determinar el tipo de usuarios a quienes la Guía Automatizada de CObIT ira orientada, así como también se pudo establecer las interfaces a ser aplicadas para cada caso.

6.3.5.1. PERFILES DE USUARIO PARA LA GUÍA AUTOMATIZADA DE CObIT

La Guía Automatizada de CObIT podrá ser utilizada por usuarios que tengan las siguientes características:

- Usuarios con perfil técnico, con conocimientos básicos en Tecnologías de la Información.
- Usuarios con nociones cimentadas de Auditoría, principalmente de la Metodología CObIT.

- Usuarios Auditores, puesto que la herramienta permitirá soportar su opinión y/o proporcionar concejos a la administración sobre los controles internos.
- Usuarios Gerentes o Administradores de TI, como ayuda para lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.
- Usuarios de TI, para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

6.3.5.2. ESPECIFICACIONES GENERALES DE LA INTERFAZ DE USUARIO

La Guía Automatiza de la implantación de CObIT tendrá las siguientes características:

- El acceso a la aplicación y su uso se realizará a través de un navegador web.
- Las interfaces serán simples e intuitivas de manera que se reduzca al mínimo la capacitación.
- Para la edición del contenido se realizará a través de formularios web en los que se demostrará la información ya existente para modificarla o ingresar nueva.
- Como se ha mencionado anteriormente la Guía Automatizada de CObIT, tendrá 4 módulos, cada unos de los cuales podrán ser ejecutados de manera independiente de cualquier otro módulo, sin embargo jamás ejecutarse dos módulos al tiempo.
- Los reportes generados por los módulos de Evaluación de Gobierno de TI, Controles de TI e Informe CObIT, podrán ser enviados a su respectiva impresión para posterior sustentación del informe de resultados.

- En caso de no requerirse impresión directa de los reportes de los módulos de Evaluación del Gobierno de TI y Controles de TI, los reportes también podrán ser enviados a formato PDF.

Fig. 6.9. Interfaz de usuario de la Guía Automatizada de CObIT

6.4. DISEÑO DEL SISTEMA

En esta fase obtendremos modelos y especificaciones que definan nuestra aplicación en referencia al análisis realizado en inciso anterior. Estas actividades nos permiten determinar las especificaciones de desarrollo e integración. Los resultados a obtener serán:

- La definición del modelo arquitectónico del sistema, identificando componentes, e interacciones.
- Identificación de subsistemas, sus requisitos de integración y funcionalidades cubiertas.
- Examinar los casos de uso aplicados de los subsistemas anteriormente identificados, para reflejar el modelo y especificaciones definidos.

- Determinar los requisitos necesarios para proceder con éxito a la implementación del sistema.

6.4.1. ARQUITECTURA GENERAL DEL SISTEMA

En la arquitectura del sistema, se han determinado dos partes fundamentales y muy bien diferenciadas en el desarrollo de la aplicación. Por un lado se encuentra la Evaluación de Gobierno de las Tecnologías de la Información (encuestas) y por otro la aplicación de los Controles de TI de CObIT.

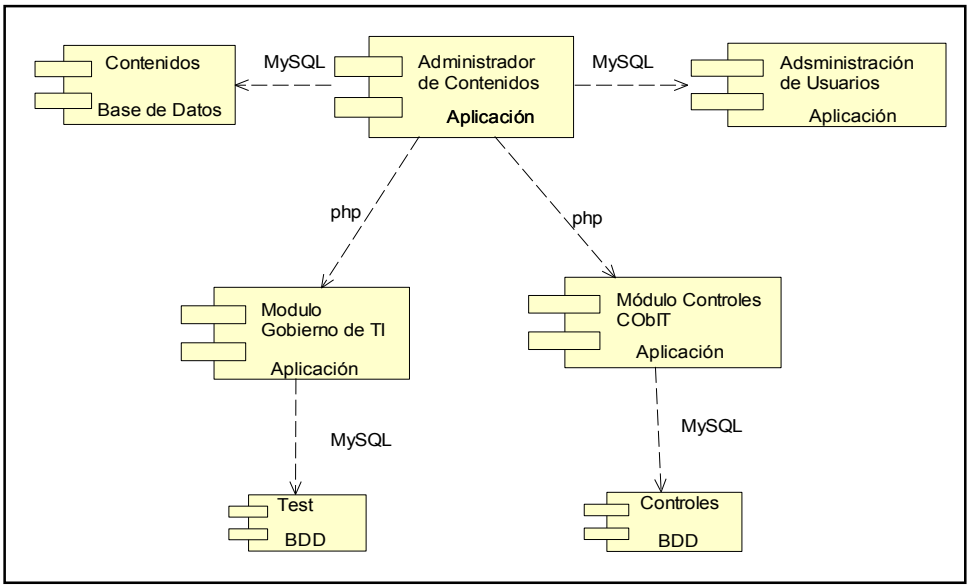


Fig. 6.11. Arquitectura General del Sistema

Evaluación del Gobierno de TI	
Contiene encuestas módulos diferentes aplicables a cada uno de los miembros del departamento de Informática y Usuarios de TI respectivamente. Evalúa y proporciona resultados de manera individual Genera impresión a documento o PDF	Resultados

Tabla 6.10. Especificaciones del módulo Evaluación del Gobierno de TI

Objetivos de Control de CObIT	
Compuesto por los 4 dominios (submódulos) de CObIT. Cada domino consta de 4 a 11 evaluaciones de controles respectivamente. Las evaluaciones de controles contienen de 3 a 30 items a ser calificados Evalúa y proporciona resultados de manera individual por dominio. Genera impresión a documento o PDF	Resultados

Tabla 6.11. Especificaciones del módulo Objetivos de Control de CObIT

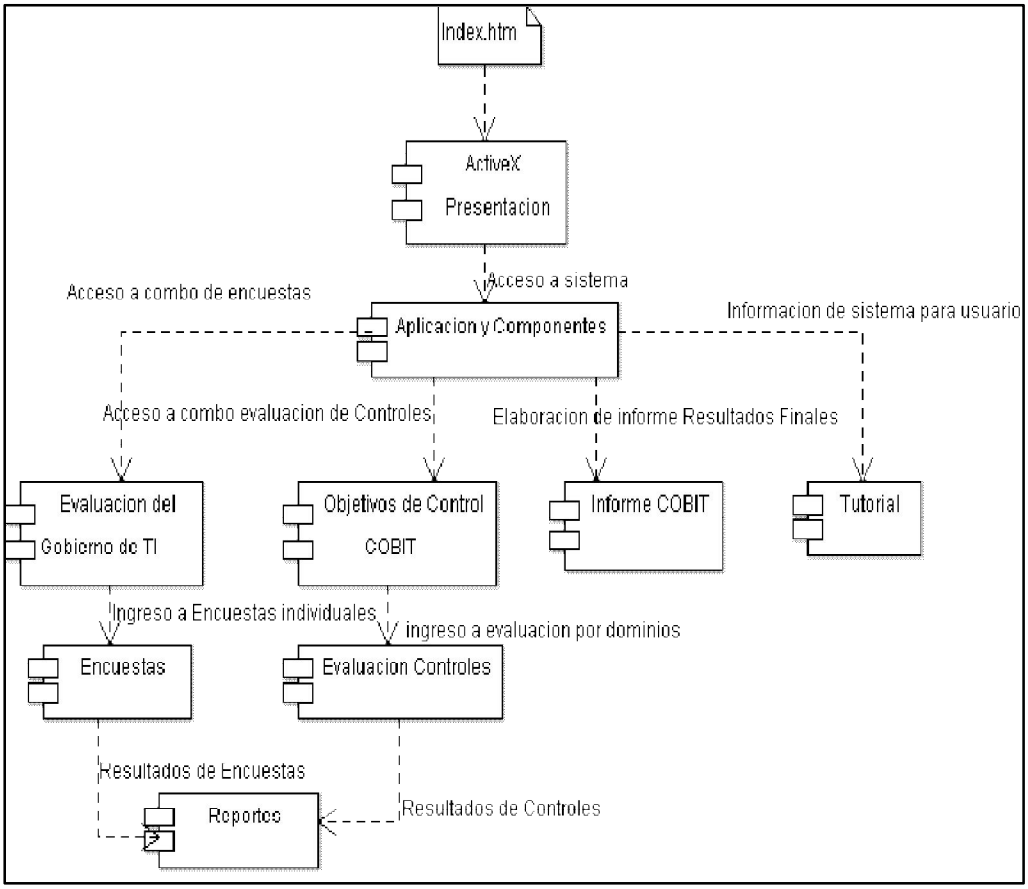


Fig. 6.12. Diagrama de Componentes del Sistema

6.5. DESARROLLO DEL SISTEMA

El objetivo de esta fase la construcción ordenada del sistema posterior al estudio de viabilidad, análisis y diseñado realizado.

Para el desarrollo se utilizarán metodologías conocidas en las que se da preferencias a la agilidad del ciclo de vida del proyecto, pudiendo también adaptar otras normas que se adapten a nuestras necesidades y realidad, y que nos ayuden a determinar el inicio y fin del desarrollo en completa sincronía con las diferentes actividades que se realicen, con el fin de que el proyecto se encuentre en condiciones de implantación.

Las actividades dentro e esta fase que nos permitirán alcanzar nuestros objetivos son:

- Especificación y estudio de alternativas de los componentes de software o librerías a utilizarse.
- Implementar el entorno de desarrollo.
- Desarrollar pruebas unitarias.
- Desarrollar los componentes necesarios.
- Realizar la documentación.
- Pruebas de integración del sistema.
- Aprobar el sistema.

Con ello, se dará aprobación al sistema para que pueda ser implementado.

6.5.1. DESARROLLO

Se instanciará el entorno de desarrollo que nos permitan llevar a cabo con la planificación del desarrollo, identificando las siguientes áreas:

- Preparación el entorno de generación y desarrollo.
- Generación del código de los componentes o procedimientos.

A partir de la planificación del desarrollo, se procederá a:

- Instalar el IDE de desarrollo Zend Studio en el equipo de desarrollo como para la generación del código del sistema.
- Determinar un conjunto de preferencias de funcionamiento del editor, tamaño de tabulación, estilo de código, etc.
- Generación de código a partir de los diagramas de casos de uso y las pruebas desarrolladas en la elaboración de código.
- Ejecución de pruebas unitarias concurrentes con el desarrollo.

Para el presente proyecto, se realizó el respetivo plan de pruebas para verificar su funcionalidad y cumplimiento con requerimientos solicitados.

Las pruebas realizadas a la aplicación se realizaran en base a criterios de: integración, implantación y aceptación en cada una de sus versiones, a los módulos y en al sistema en forma unitaria (caja blanca y caja negra); cuyos resultados en cada una de sus fases permitirán comprobar que el proyecto se ha realizado correctamente y que se cumple con los requerimientos solicitados por el cliente.

6.6. IMPLANTACIÓN

En esta fase, no es más que el paso a producción del sistema desarrollado, lo cual requerirá una cuidada planificación de actividades.

Una vez que el sistema ha sido probado a nivel de integración, la implantación se limita en este caso a realizar la instalación de los servicios en el

servidor definitivo junto con los datos que especifican para el funcionamiento de la aplicación.

Con ello cual se procede lo siguiente:

- Comprobar el funcionamiento de los servicios en el servidor designado.
- Instalar los componentes desarrollados en el servidor designados.
- Comprobar la existencia del gestor de la base de datos así como los usuarios y sus respectivos permisos.
- Crear la base de datos, la estructura de sus tablas y cargar datos iniciales.

Luego que se ha comprobado que la instalación se ha realizado correctamente, ejecutaremos las pruebas de implantación como pueden ser:

- Navegación completa a través de todo el sitio web, tomando datos acerca del tiempo de respuesta.
- Comprobar la integridad de datos en los distintos módulos de presentación de resultados del sistema.

Por lo tanto podemos acotar que CObIT está diseñado para ser la herramienta que ayude a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas, proporcionando a gerentes, interventores, y usuarios de Tecnologías de la Información medidas generalmente aceptadas, indicadores, procesos y las mejores prácticas para maximizar las ventajas sacadas por el empleo de tecnología de información y desarrollo de la gobernación apropiada de las Tecnologías de la Información en la empresa.

Sin duda, la aplicación de esta metodología a través de la guía automatizada que propone el presente proyecto, nos facilitará establecer un buen Gobierno de las Tecnologías de la Información y Comunicaciones, con las medidas técnicas, humanas y organizativas que CObIT contempla, permitiéndonos no solo una adecuada administración del riesgo, sino el establecer, implantar, monitorear y

mantener un Sistema de Gestión de Seguridad de la Información (SGSI) en la Dirección de Informática del Gobierno Provincial de Imbabura, garantizando de esta manera beneficios y ventaja competitiva en la Corporación.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. VERIFICACIÓN DE LA HIPÓTESIS

"La implementación de la Metodología CObIT, permitirá el uso eficiente de los recursos TI, garantizando seguridad y control sobre el rendimiento de las mismas, maximizando los beneficios y minimizando las inversiones en tecnología de información, para cumplir con los objetivos institucionales del Gobierno Provincial de Imbabura"

El uso de un estándar internacional como lo es la Metodología CObIT (*Objetivos de Control para la Información y las Tecnologías Relacionadas*) aplicada a la auditoría y seguridad informática a través de la Guía la Automatizada, nos permite obtener una administración efectiva de TI, ayudando a satisfacer las múltiples necesidades de la Administración, y los controles necesarios en aspectos técnicos.

Con ello la Dirección de Informática, podrá implementar los correctivos, establecer nuevos objetivos, alinear en consecuencia sus procesos y asegurar el cumplimiento de los objetivos institucionales, garantizando así, la obtención a largo plazo de los beneficios esperados de la tecnología de información (TI), en el Gobierno Provincial de Imbabura.

En consecuencia, lo anteriormente expuesto indica que la hipótesis planteada se cumple satisfactoriamente en su totalidad.

7.2. CONCLUSIONES

- En el ámbito de la Auditoría Informática y debido a los diversos cambios en la tecnología, inevitablemente ha generado en ella cambios de manera drástica en los últimos años, por ello el dominio de diversos conocimientos integrados se ha tornado indispensable para el auditor, de manera que faciliten la comprensión de los hechos resultantes en la administración y gestión informática.
- Es importante reconocer que las Normas Internacionales de Auditoría, son una base fundamental para una mejor comprensión de ciertos criterios relacionados con el trabajo de auditoría, que en la mayoría de lineamientos, Normas o Guías para la Auditoría Informática no suelen estar especificados.
- Un conocimiento y cumplimiento del código de ética profesional, es esencial para el desarrollo del trabajo de auditoría, por lo tanto el auditor deberá adoptar dichas normas, además de las que rijan su colegiado o formación profesional.
- Se debe tener claras nociones de las leyes o regulaciones que presidan en la entidad a ser auditada, para evitar posteriores complicaciones.
- La ausencia de una normativa de seguridad para una adecuada evaluación y control de los recursos de TI, generan no solo un incremento del riesgo operativo, sino el sobredimensionamiento o subdimensionamiento de dichos recursos en las entidades.
- La aplicación de la Guía Automatizada de CObIT, proporciona un marco de referencia para la efectiva administración de los recursos y criterios de TI, dichos controles constituyen una herramienta útil para la gestión, más no un sustituto de ésta.
- La Metodología CObIT, provee políticas claras y buenas prácticas para la seguridad y control, basadas en la perspectiva de la auditoría,

convirtiéndose en una verdadera guía para profesionales que incurran en el ámbito de la Auditoría Informática.

- La Guía Automatizada de CObIT, cumple con propiedades metodológicas debidamente sustentadas, por lo que es considerada como una metodología válida y correctamente estructurada.

7.3. RECOMENDACIONES

- Facilitar el acceso a la documentación y demás información para el desarrollo del trabajo de auditoría, para logar una mejor aplicación de las Evaluaciones de Gobierno de TI y Controles de CObIT.
- Capacitar a los auditores internos de la entidad, en el uso de herramientas computacionales a través de cursos, conferencias y pasantías.
- Realizar auditorías concurrentes en la Dirección de Informática del Gobierno Provincial de Imbabura.
- Proveer de todos los recursos de hardware que sean necesarios para el desarrollo e implementación de la Metodología CObIT.
- El personal a ser auditado, debe mostrar total apertura y colaboración al staff de auditoría.
- Aplicar regularmente la Evaluación de Gobierno de TI y los Controles de CObIT, a fin de corregir de forma inmediata las diferentes falencias que pudieren existir en control interno, de manera que garanticen la efectividad y eficiencia de los controles implementados.
- Con la realización de este trabajo práctico, hemos determinado que toda empresa, pública o privada, que posean Sistemas de Información medianamente complejos, deben de someterse a controles, ya que su éxito radica en eficiencia y eficacia de sus sistemas de información.

BIBLIOGRAFÍA

CAPÍTULO I

LIBROS

- **[LIB.001]**
  Biblioteca personal. Auditoría Informática, Un enfoque profesional, 2004.
  Definiciones y conceptos básicos de Auditoría.

- **[LIB.002]**
  Hackers los piratas del Chip y del Internet, Claudio Hernández, 2001.
  Seguridad informática, tipos de hackers, características generales sobre violaciones a las seguridades.

INTERNET

- **[WWW.001]**
  www.monografías.com/trabajos14/auditoria/auditoria.shtml
  Definiciones, clasificación de la auditoría,

- **[WWW.002]**
  http://www.scampus.org/lección/auditorias03
  Conceptos básicos.

- **[WWW.003]**
  http://www.monografías.com/trabajos/auditoriainfo/auditoinformatica.htm
  Herramientas y técnicas de auditoría informática,

- **[WWW.004]**
  http://www.eurologic.es/conceptos/canbasics.htm
  Criterios de Seguridad Informática

- **[WWW.005]**
  http:www.eurologic.es/conceptos/conbasics.html
  Tipos de ataque a la Seguridad Informática

- **[WWW.006]**
  http://www.monografias.com/trabajos/hackers/hackers.shtml
  Herramientas de Hacking

- **[WWW.007]**
  http://virusprot.com/articulo.html
  Herramientas de Hacking

- **[WWW.008]**
  http://www.es.wikipedia.org/wiki/seguridad_informatica.html
  Técnicas de aseguramiento

CAPÍTULO II

LIBROS

- **[LIB.003]**
  NORMAS INTERNACIONALES DE AUDITORÍA, Federación Internacional de Contadores Públicos, Edición 2008.
  Estándar internacional de Normas de Auditoría y ámbitos de aplicación.

INTERNET

- **[WWW.009]**
  http://www.isaca.org.ec/codigo-etica.htm
  Código de ética para la Auditoría Informática

CAPÍTULO III

LIBROS

- **[LIB.006]**

  Auditoría Informática, un enfoque práctico, Editorial RAMA.

  Fundamentos de Auditoria Informática.

- **[LIB.007]**

  Fundamentos para el desarrollo de Proyectos con UML Y CMM, José A. Rubio, 2004.

  Conceptos de CMM y CMM-I

INTERNET

- **[WWW.0010]**

  http:es.wikipedia.org/wiki/information-technology-infraestructure-library.html

  Información sobre ITIL, fundamentos.

- **[WWW.011]**

  http://www.getronics.es/asl.html

  Descripción del modelo ASL, estructura.

- **[WWW.012]**

  http://www.es.wikipedia.org/wiki/project_management_institute.html

  Conceptos y modelo PMI

- **[WWW.013]**

  http://www.lean-sigma.es/desarrollo-de-la-estructura-sixsigma.php

  Modelo SixSigma.

- **[WWW.014]**
  http://www.sarbanes-oxley-forum.com
  Orígenes de Sarbanes Oxley y COSO

- **[WWW.015]**
  www.iso27000.es
  Evolución de ISO, de BS7799 a 27000 e información

- **[WWW.016]**
  http://www.channelplanet.com/index.php?idcategoria=11752\Mex+Seguridad+en+Informacion\Resumen\Que+es+un+BS7799.xalter
  Análisis de controles de BS7799

CAPÍTULO IV

LIBROS

- **[LIB.008]**
  Information Systems Audit and Control Association (ISACA) - IT Governance Institute. "Governance Guides and Audit for Information and Related Technology" – Executive Summary, 3^{era} Edición.
  Resumen Ejecutivo de CObIT, lineamientos generales.

- **[LIB.009]**
  Information Systems Audit and Control Association (ISACA) - IT Governance Institute. "Governance Guides and Audit for Information and Related Technology" – Framework, 3^{era} Edición.
  Marco de Referencial CObIT para las Tecnologías de la Información.

- **[LIB.010]**
  Information Systems Audit and Control Association (ISACA) - IT Governance Institute. "Governance Guides and Audit for Information and Related Technology" – Control Objetives, 3era Edición.
  Objetivos de Control de CObIT.

- **[LIB.011]**
  Information Systems Audit and Control Association (ISACA) - IT Governance Institute. "Governance Guides and Audit for Information and Related Technology" – Audit Guidelines, 3era Edición.
  Directrices de Auditoría CObIT.

- **[LIB.012]**
  Information Systems Audit and Control Association (ISACA) - IT Governance Institute. "Governance Guides and Audit for Information and Related Technology" – Management Guidelines, 3era Edición
  Directrices Gerenciales CObIT.

INTERNET

- **[WWW.017]**
  http://www.isaca.org/Template.cfm?Section=Overview_and_History&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=32415
  Información general de ISACA

CAPÍTULO V

LIBROS

- **[LIB.014]**
  Informe de Auditoría, realizado en la Dirección de Tecnologías de la Información y Comunicaciones del Gobierno Provincial de Imbabura.

- **[LIB.015]**

  Constitución Política del Ecuador, ref Art 228

  Legislación aplicada a los Gobiernos Seccionales

- **[LIB.016]**

  Biblioteca personal, Documentación de la Dirección de Informática del Gobierno Provincial de Imbabura – Orgánico Funcional. Antecedentes de tecnología del 2002 hasta la fecha

  Documentos de información general.

INTERNET

- **[WWW.018]**

  http://www.imbabura.gov.ec

  Pagina del Gobierno Provincial, información de la institución.

GLOSARIO

- **AICPA**

  Instituto Americano de Contadores Públicos Certificado. (*American Institute of Certified Public Accountants)*

- **CCEB**

  Criterios comunes para seguridad en tecnología de información. (*Common Criteria for Information Technology Security)*

- **CICA**

  Instituto Canadiense de Contadores. (*Canadian Institute of Chartered Accountants*)

- **CISA**

  Auditor Certificado de Sistemas de Información. (*Certified Information Systems Auditor*)

- **Control**

  Políticas, procedimientos, prácticas y estructuras organizacionales, diseñados para proporcionar una seguridad razonable de que los objetivos del negocio serán alcanzados y que eventos no deseados serán prevenidos o detectados y corregidos.

- **COSO**

  Comité de Organizaciones Patrocinadoras de la Comisión de Intercambio. "Tradeway" (*Committee of Sponsoring Organisations of the Tradeway Commission).*

- **DRI**

  Instituto Internacional de Recuperación de Desastres. (*Disaster Recovery Institute International*)

- **DTI**

  Departamento de Comercio e Industria del Reino Unido. (*Department of Trade and Industry of the United Kingdom)*

- **EDIFACT**

  Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria (*Electronic Data Interchange for Administration, Commerce and Trade*)

- **EDPAF**

  Fundación de Auditores de Procesamiento Electrónico de Datos (*Electronic Data Processing Auditors Foundation*), ahora **ISACF.**

- **ESF**

  Foro Europeo de Seguridad (*European Security Forum*), cooperación de 70+ multinacionales europeas principalmente con el propósito de investigar problemas de seguridad y control comunes de TI.

- **GAO**

  Oficina General de Contabilidad de los EUA. (*U.S. General Accounting Office*)

- **I4**

  Instituto Internacional de Integridad de Información. (*International Information Integrity Institute*), asociación similar a ESF, con metas similares, pero con base principalmente en los Estados Unidos y dirigida por el Instituto de Investigaciones de Stanford (*Stanford Research Institute)*

- **IBAG**

  Grupo Consultivo de Negocios Infosec (*Infosec Business Advisory Group*), representantes de la industria que asesoran al Comité Infosec. Este Comité está compuesto por funcionarios de los gobiernos de la Comunidad Europea y asesora a la Comisión Europea sobre cuestiones de seguridad de TI.

- **IFAC**

  Federación Internacional de Contadores. (*International Federation of Accountants*)

- **IIA**

  Instituto de Auditores Internos. (*Institute of Internal Auditors*)

ANEXOS

ANEXO I

GUÍA RÁPIDA DE USUARIO

El apartado de este anexo explica la operativa a seguir para la correcta utilización de la aplicación aautomatizada del estudio de la Metodología CObIT.

En las páginas siguientes se especificará en forma general y desde el punto de vista del usuario, el funcionamiento de la Guía Automatizada de la implementación de CObIT.

La aplicación reside por completo en un servidor, podrá ser accedido vía web.

Como primera instancia se abre la página de acceso al sistema, el Administrador se da de alta en el mismo para acceder a las aplicaciones.

Una vez que el usuario ha seleccionado el ingreso, se despliega en pantalla todos los módulos que el aplicativo contiene, en la cual podrá seleccionar entre las opciones siguientes:

- Evaluación del Gobierno de TI: Inicio, Ingresos.
- Objetivos de Control CObIT: Controles CObIT, Finalizar Controles CObIT, Resultados CObIT

EVALUACIÓN DEL GOBIERNO DE TI

Al iniciar la aplicación o seleccionar la opción ***Inicio*** del Menú Principal, se despliega en pantalla el Panel de Control, donde el Administrador podrá acceder a tareas como:

- Administrar Usuarios: Ingresar nuevos o modificar registros de usuarios.
- Auditoría: Donde se lleva un registro de todas las acciones realizadas por el Administrador realizadas en el Sistema.
- Tutorial: Muestra un manual de usuario del sistema.
- Objetivos de Control: Archivo PDF como soporte en la evaluación de los Controles CObIT.
- Informe de Auditoría: Modelo de informe de auditoría.

En la Evaluación del Gobierno de TI, el usuario podrá aplicar las encuestas según sea el caso. Las encuestas se encuentran contempladas en el menú ***Ingresos***.

En esta sección las encuestas se han divido en secciones denominadas módulos como sigue:

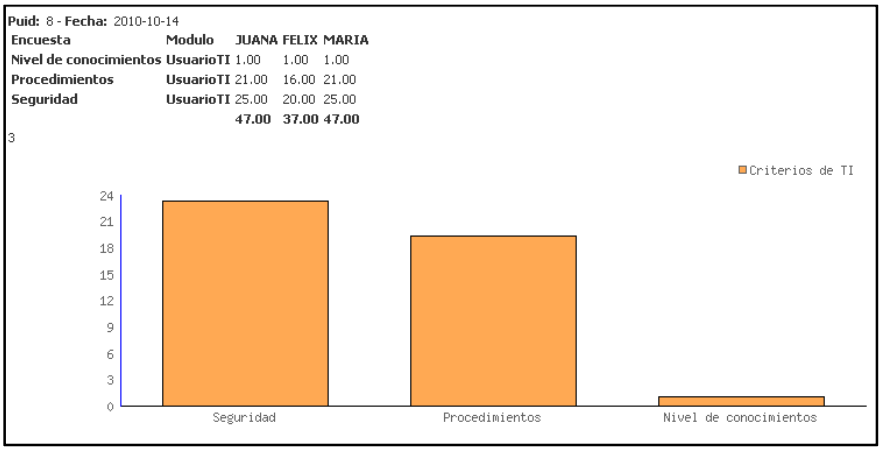
- Gestión y Dirección de TI
- Software y desarrollo
- Hardware y Comunicaciones
- Help Desk
- Usuario de TI

Los cuales contienen las respectivas encuestas de acuerdo al caso. El Administrador del sistema podrá ingresar como nuevos registros o modificar:

- Módulos
- Encuestas
- Departamentos
- Test

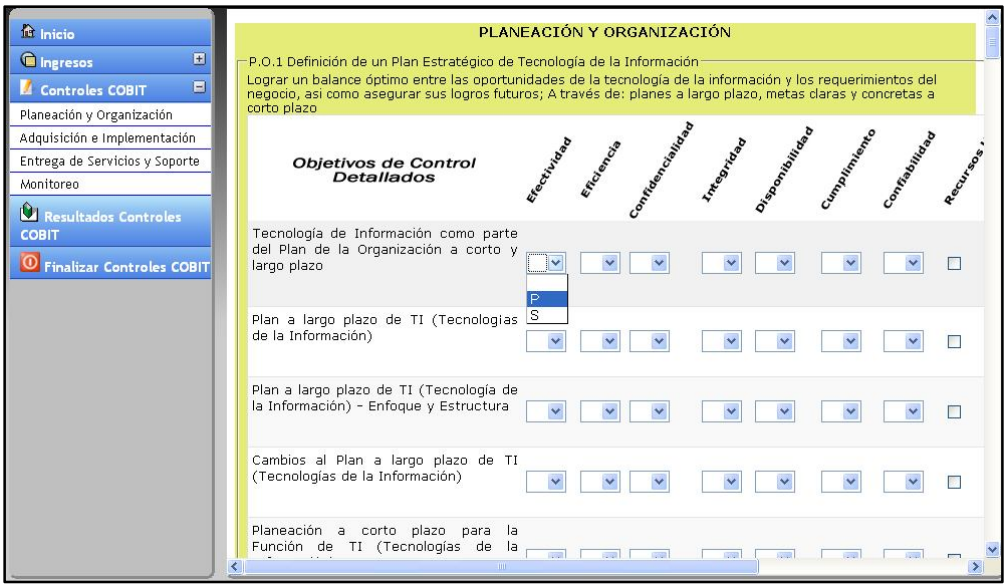
De similar forma se podrá publicar un nuevo Test, este contendrá las encuestas que el Administrador asigne y que serán aplicados al personal.

Cuando se ha realizado el Test, se podrán visualizar los resultados obtenidos en forma tabulada, para su posterior impresión.



Todas las encuestas se ejecutan de similar forma, presentando las mismas funcionalidades para cada uno de los casos.

CONTROLES CObIT



En esta sección se evalúan todos los controles CObIT. El usuario podrá evaluar:

- Planeación y Organización
- Adquisición e Implementación

- Entrega y Soporte
- Monitoreo

Cada uno de los dominios contiene los controles de alto nivel, que son 318 en total.

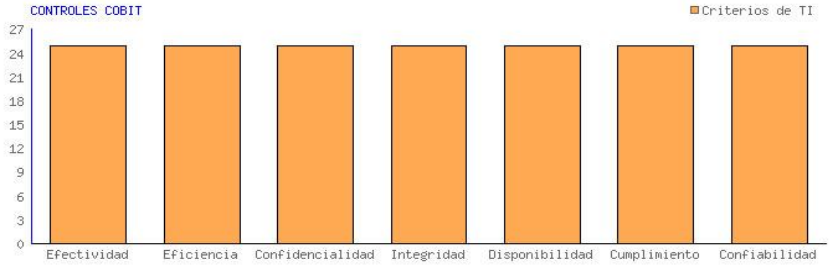
Para evaluar los controles de cada uno de los dominios, se debe seleccionar el dominio a ejecutar. Estos como se ha mencionado poseen los procesos que a cada uno atañe y los controles de alto nivel correspondientes. El usuario únicamente deberá seleccionar entre las opciones presentadas.

Al igual que en la Evaluación del Gobierno de TI, ninguno de los módulos (dominios) de los controles pueden ejecutarse independientemente de otro, puesto que se realiza reportes de toda la encuesta aplicada al auditado, además el usuario podrá calificar el riesgo, nivel de desempeño e importancia de cada módulo evaluado, de acuerdo a su criterio.

Una vez aplicados los controles, se procede a generar los reportes, que nos presentan los resultados en forma cualitativa el nivel de control existente, así como estadísticas de los Recurso y Criterios de TI, en los cuales han impactado los controles de alto nivel.

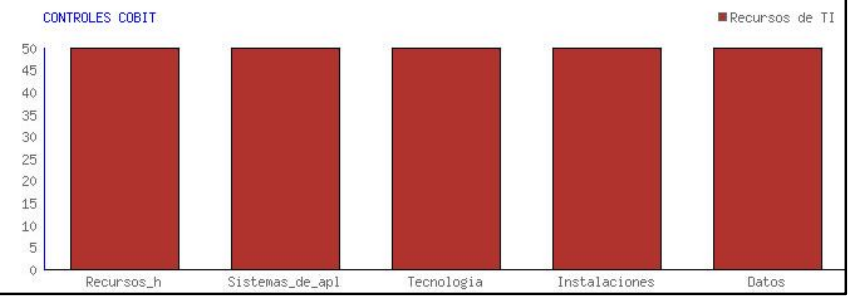
PLANEACIÓN Y ORGANIZACIÓN

CRITERIOS DE TI	PUNTAJE	RESULTADO
Efectividad	25.00	Inferior a lo estimado en: 75 pts.
Eficiencia	25.00	Inferior a lo estimado en: 33 pts.
Confidencialidad	25.00	Superior a lo estimado en: 15 pts.
Integridad	25.00	Inferior a lo estimado en: 4 pts.
Disponibilidad	25.00	Superior a lo estimado en: 17 pts.
Cumplimiento	25.00	Superior a lo estimado en: 9 pts.
Confiabilidad	25.00	Superior a lo estimado en: 7 pts.
TOTAL	175	



RECURSOS DE TI	PUNTAJE	RESULTADO
Recursos Humanos	50.00	Inferior a lo estimado en: 41 pts.
Sistemas de Aplicación	50.00	Inferior a lo estimado en: 11 pts.
Tecnología	50.00	Inferior a lo estimado en: 6 pts.
Instalaciones	50.00	Inferior a lo estimado en: 6 pts.
Datos	50.00	Superior a lo estimado en: 24 pts.
TOTAL	250	

Nivel de Control en Recursos de TI: Aceptable. Porcentaje Obtenido: 86%



Posteriormente, dichos resultados pueden ser enviados su respectiva impresión

Una vez se han realizado las evaluaciones del Gobierno de TI y los Controles CObIT, se procederá ha realizar el informe de Auditoría, ya que los resultados obtenidos de la Guía Automatizada serán una fuente de sustentación para la opinión del auditor.

ANEXO II

PROGRAMA DE AUDITORIA

FASE Nº1: PLANIFICACIÓN DE LA AUDITORÍA			
OBJETIVO: Planificar la Auditoría a la Dirección de Informática del GPI			
Nº	**PROCEDIMIENTOS**	**AUDITOR**	**FECHA**
1.1	Realizar el plan de auditoría a desarrollarse en la Dirección de Informática del Gobierno Provincial de Imbabura		
1.2.	Determinar el alcance y objetivos de la auditoría		

FASE Nº2: ESTUDIO PRELIMINAR			
OBJETIVO: Conocer la entidad y la Dirección de Informática			
Nº	**PROCEDIMIENTOS**	**AUDITOR**	**FECHA**
2.1.	Conocimiento general del Gobierno Provincial de Imbabura		
2.1.1.	Recopilar la normativa legal		
2.1.2.	Recopilar datos y estructura organizacional del Gobierno Provincial de Imbabura		
2.1.3.	Plan Estratégico de la entidad – revisión		
2.2.	Conocimiento general de la Dirección de Informática		
2.2.1.	Conocer la organización de la Dirección de Informática		
2.2.1.1.	Recopilar datos y estructura organizacional de la Dirección de Informática.		
2.2.1.2.	Plan Estratégico Informático – revisión		
2.2.2.	Conocimiento de la tecnología informática		
2.2.2.1.	Conocer los sistemas en funcionamiento		
2.2.2.2.	Supervisión de seguridades físicas y respaldo de recursos.		
2.2.3.	Evaluación de Satisfacción de usuarios		
2.2.4.	Elaboración de papeles de trabajo y comentarios		

FASE Nº3: EVALUACIÓN DE RESPONSABILIDADES Y CONTROLES INTERNOS			
OBJETIVO: Evaluar el nivel de Gobernabilidad de TI existente			
Nº	**PROCEDIMIENTOS**	**AUDITOR**	**FECHA**
3.1.	Aplicación de Encuesta a usuarios de Sistemas y Aplicaciones existentes		
3.2.	Aplicar encuestas de acuerdo al orgánico funcional de la Dirección de Informática del Gobierno Provincial		
3.3.	Elaborar papeles de trabajo y comentarios respectivos.		

FASE Nº4: EVALUACIÓN DE LOS CONTROLES DE TI CObIT			
OBJETIVO: Evaluar el nivel de control de TI existente con los Objetivos de Control de CObIT			
Nº	**PROCEDIMIENTOS**	**AUDITOR**	**FECHA**
4.1.	Aplicación Controles CObIT en la Dirección de Informática del Gobierno Provincial de Imbabura		
4.2.	Elaborar papeles de trabajo y comentarios respectivos.		

FASE Nº5: PRESENTACIÓN DE RESULTADOS			
OBJETIVO: Evaluar el nivel de control de TI existente con los Objetivos de Control de CObIT			
Nº	**PROCEDIMIENTOS**	**AUDITOR**	**FECHA**
5.1.	Citar los comentarios con sus respectivos hallazgos.		
5.2.	Formular conclusiones y recomendaciones.		

El trabajo de auditoría realizado a la Dirección de Informática del Gobierno Provincial de Imbabura, se aplicó en las fases anteriormente señaladas, cumpliéndose con todas las etapas concernientes para la ejecución de la misma.

En lo referente a la evaluación del Control interno, se aplicaron cuestionarios a todos los funcionarios de la Dirección de Informática, así como a usuarios de Sistemas, tal como el Sistema de Costos y Administración Directa, y demás usuarios de TI en general. Dichos cuestionarios fueron elaborados en base a las

guías y criterios de la Metodología CObIT, los mismos que forman parte de la Gobernabilidad de TI.

Para los resultados y tabulación final del control interno, se establecieron valores regidos por la Norma ISO 9126 e IEEE1028 "Standar for Software Reviews and Audits", de lo cual se determinó:

CALIFICACIÓN	PORCENTAJE	CATEGORÍA
Correcto	100-95	SATISFACTORIO
Aceptable	85-94	SATISFACTORIO
Mejorable	75-84	ACEPTABLE
Deficiente	65-74	INSATISFACTORIO
Muy Deficiente	Menos de 65	INSATISFACTORIO

Estas calificaciones son las que rigen el módulo de Gobernabilidad de TI de la Guía Automatizada de CObIT, mostrándonos en los reportes en nivel de control existente en la entidad.

Aplicado lo anterior, se pudo establecer los siguientes valores cuantitativos, tanto para el desempeño, importancia y riesgo, en cada uno de los cuestionarios individuales:

CRITERIO: DESEMPEÑO	CALIFICACIÓN/NIVEL
Excelente	5
Muy Bueno	4
Satisfactorio	3
Regular	2
Deficiente	1

CRITERIO: IMPORTANCIA	CALIFICACIÓN/NIVEL
Muy Importante	5
Importante	4
Moderadamente Importante	3
Desconoce / No esta seguro.	2
No importante	1

CRITERIO: RIESGO	CALIFICACIÓN/NIVEL
Alto	4
Medio	3
Razonable	2
Bajo	1

Según el puntaje y porcentaje obtenido, se asignan los niveles correspondientes a los criterios de: desempeño, importancia y riesgo, tal como se muestra a continuación:

- Porcentaje obtenido en evaluaciones: 97%. Por lo tanto en desempeño, importancia y riesgo le corresponde:
  Desempeño: Excelente; Importancia: Muy Importante; Riesgo: Bajo.

Estos últimos valores, el auditor los asignará en base a los resultados obtenidos en las evaluaciones aplicadas y al estudio preliminar realizado en la entidad auditada y su control interno.

De similar manera, estos criterios son tomados para la evaluación de los Controles de CObIT en la Dirección de Informática en cada uno de sus aspectos, indispensables para la ejecución de la 3^{era} y 4^{ta} fases de auditoría y para la elaboración de las respectivas conclusiones y recomendaciones en base a los hallazgos y resultados obtenidos.

ANEXO III

RESULTADOS DE LA APLICACIÓN DE LA GUÍA AUTOMATIZADA CObIT

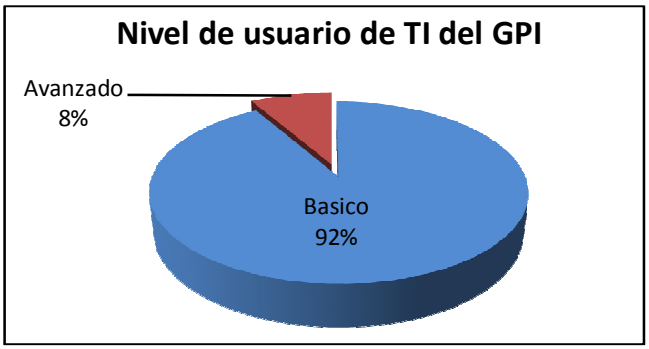
EVALUACIÓN DEL GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – USUARIOS TI

Como primera instancia se evaluó a los Usuarios de las Tecnologías de la Información de la institución, para luego proceder con la evaluación de la Dirección de TIC´s del GPI.

Evaluación de los Usuarios de las Tecnologías de la Información

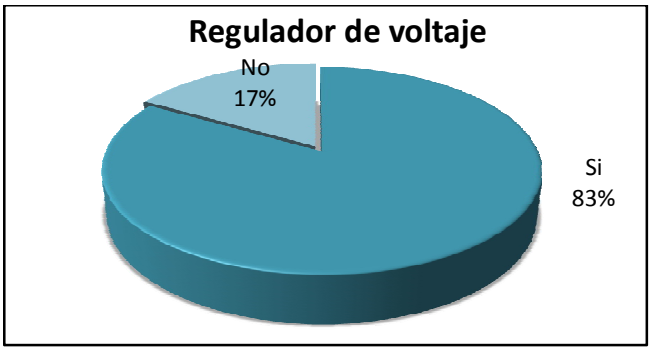
A continuación presentamos los resultados obtenidos en cada una de las preguntas realizadas a los usuarios de TI del Gobierno Provincial de Imbabura. Estas se encuentran contenidas en las encuestas de: Nivel de Conocimientos, Procedimientos, Seguridad y Servicios respectivamente.

1. De acuerdo a sus conocimientos en computación e informática, en que nivel de usuario se ubica usted: Básico, Medio o Avanzado.



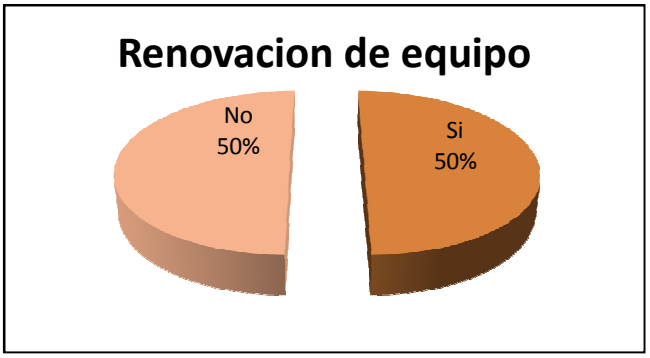
El nivel de conocimientos en un 92% es Básico, mientras que el 8% es avanzado.

2. ¿Su computador cuenta con regulador de voltaje o ups?



Un 83% de los usuarios tienen ups o regulador, un 17% no posee nada.

3. Durante el tiempo que lleva en la institución, su equipo de computación ha sido renovado:

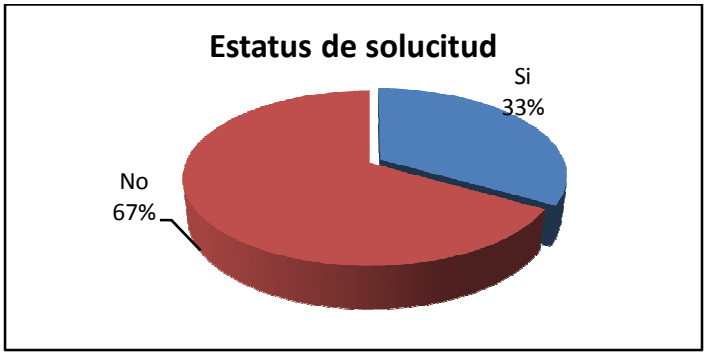


El 50% de equipos han sido renovados, el otro 50% no.

4. Cuando se solicitan cambios de equipo, instalación o actualización de programas se realiza:

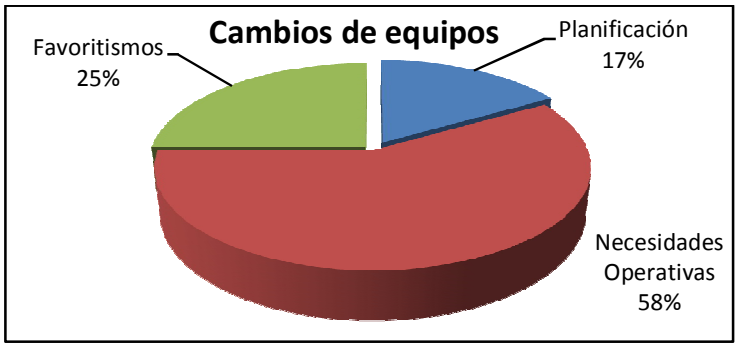
El 64% de los usuarios realiza petición verbal, mientras que el 36% realiza una solicitud.

5. Si usted solicita dichos cambios ¿La dirección de informática le informa oportunamente del estado de su solicitud?



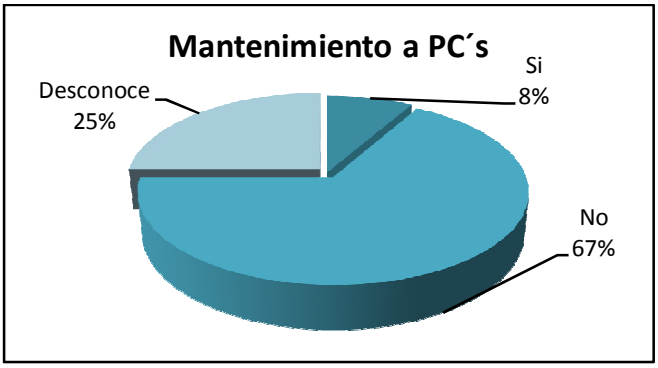
De los usuarios que han realizado solicitud de cambios o actualización de programas, el 67% no permanece informado de su petición, el 33% se le comunica el estado de su solicitud.

6. A su criterio, cual es la razón por la que se realizan los cambios de equipos en la institución:



De los usuarios encuestados un 58% piensa que los cambios se realizan por necesidades operativas, un 25% por favoritismos y el 17% por una planificación.

7. ¿Sabe usted si existe un cronograma para mantenimiento preventivo (limpieza) a computadores en la institución?

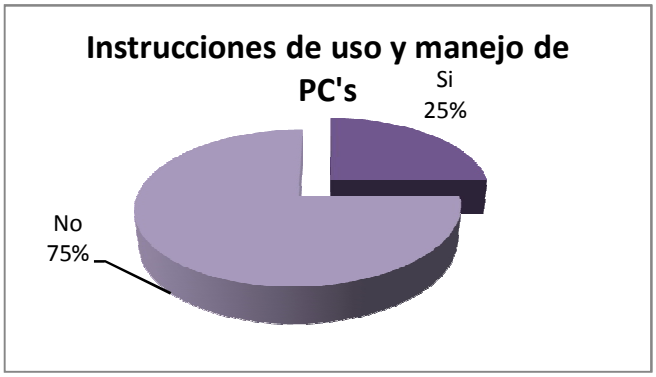


El 67% de los encuestados dice que no existe un programa de mantenimiento, el 25% desconoce, y un 8% asegura que si hay un programa.

8. Con que frecuencia se realiza mantenimiento o limpieza a su computador en la institución:

El 92% de los usuarios reciben mantenimiento solo cuando se daña el equipo, mientras que el 8% no recibe ningún mantenimiento.

9. ¿La Dirección de Informática le ha proporcionado instrucciones de operación para el cuidado y manejo del computador?



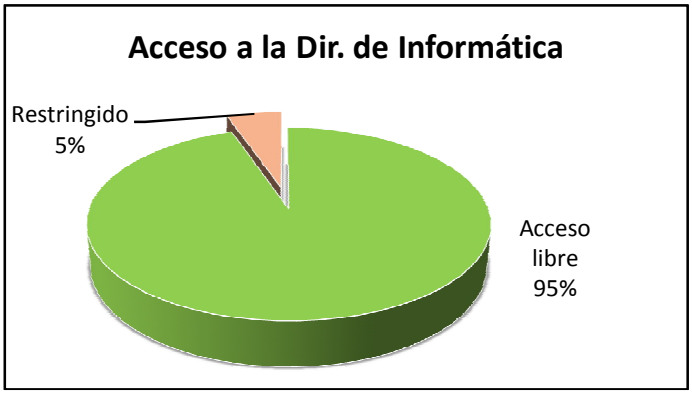
De los usuarios encuestados el 75% no ha recibido instrucciones de uso y manejo, el 25% si.

10. ¿La Dirección de Informática le ha comunicado que existe personal específico responsable del Soporte Técnico en la institución?:

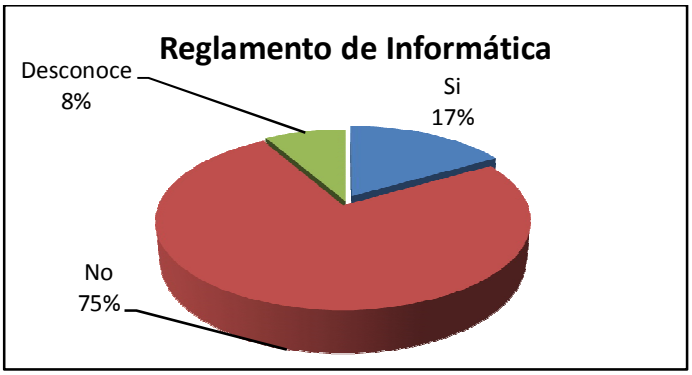
El 75% de los usuarios desconoce que exista personal específico para soporte técnico, el 25% está informado al respecto.

11. El ingreso al departamento de informática por parte del personal de la institución es:

De los usuarios encuestados el 95% tiene acceso libre a todas las dependencias de la Dirección de Informática, mientras que el 5% anotan es restringido.



12. ¿Es de su conocimiento si en la Dirección de informática existe algún reglamento?



Referente al reglamento de la Dirección de TIC´s, el 75% no sabe de la existencia de un reglamento, el 17% si sabe cual es el reglamento, y el 8% desconoce si existe o no un reglamento.

13. ¿En el departamento de Informática existen carteles con prohibiciones de fumar, tomar alimentos y refrescos?

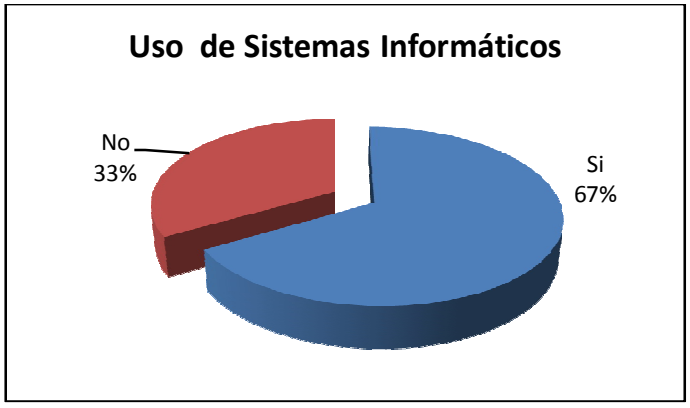
El 87% de los encuestados señala que no existen prohibiciones, el 9% desconoce el que existan, el 4% afirman que si.

14. ¿Considera usted que se cumplen dichas prohibiciones?

De los usuarios encuestados el 90% señalan que no se cumplen las prohibiciones del reglamento, mientras que el 10% aseguran que si se cumplen.

15. ¿Utiliza usted algún sistema informático en particular (contabilidad, bodega, tesorería, u otro)?

El 67% de los encuestados utilizan algún sistema informático, el 33% de los usuarios restantes no utiliza.

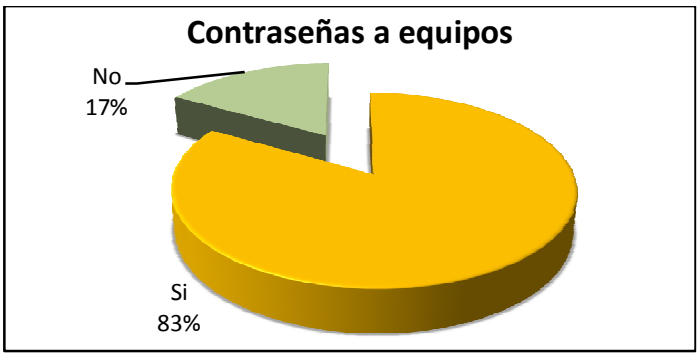


16. ¿Existen Prohibiciones sobre la instalación o uso de programas no autorizados en los equipos de la institución?

El 75% de los usuarios señalan existen prohibiciones, el 25% indican no existir dichas restricciones.

17. ¿Cree que es conveniente que los equipos estén protegidos con contraseñas?

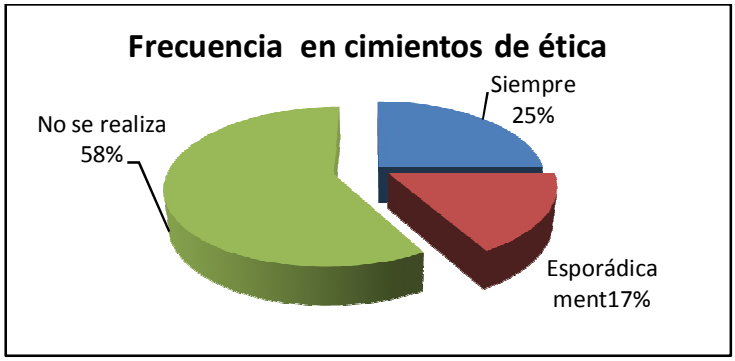
El 83% de los encuestados señalan que se debe tener contraseñas en los equipos, el 17% restante no lo considera necesario.



18. ¿El departamento de informática le ha brindado capacitación en temas relacionados con Seguridad de la Información?

El 92% de los usuarios no ha recibido capacitación en temas de seguridad de la información, mientras que el 8% si la ha recibido.

19. En la institución con que frecuencia se fomenta la conciencia, honradez y ética en el personal:

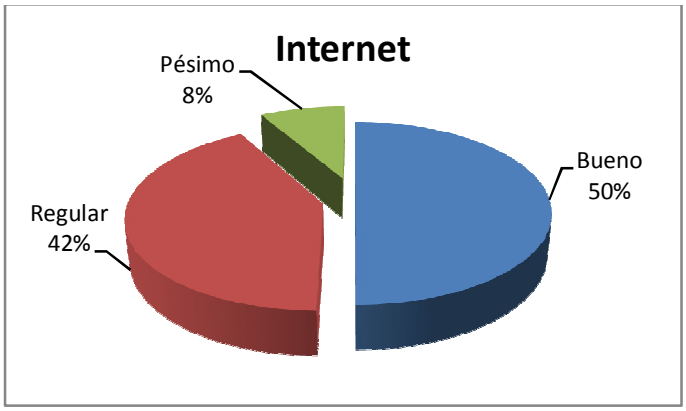


De los usuarios encuestados el 58% señalan que no se realiza, el 25% siempre se fomenta, y el 17% indica que esporádicamente se topan estos temas.

20. Con que frecuencia se entrena al personal para casos de incidentes o desastres (incendios, temblores):

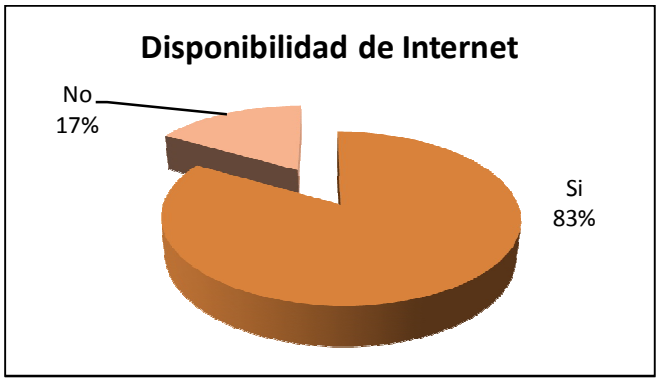
El 100% de los encuestados indican que no se han realizado ningún tipo de entrenamiento en caso de incidentes.

21. ¿Cómo califica el servicio de internet?



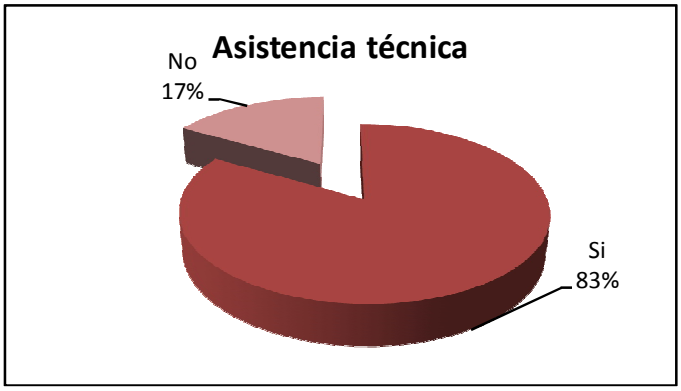
El 50% de los usuarios señalan que el servicio es bueno, el 42% que el servicio es regular, y el 8% que es pésimo.

22. ¿Considera que el servicio de internet debe estar disponible a cualquier hora y para cualquier usuario?



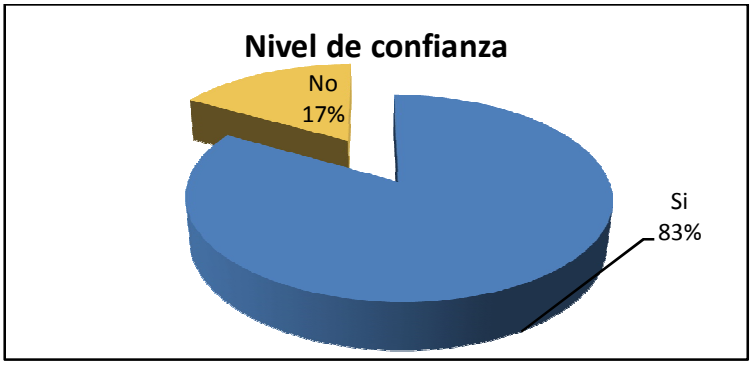
El 83% de los usuarios indican la necesidad de que el internet esté disponible, mientras que el 17% opina que debe ser restringido.

23. ¿El Departamento de Informática le brinda atención cuándo usted lo requiere?



El 83% de los usuarios encuestados reciben oportunamente asistencia técnica, mientras que el 17% no la reciben a tiempo.

24. ¿Tiene usted la suficiente confianza como para presentar su queja sobre fallas en los equipos?

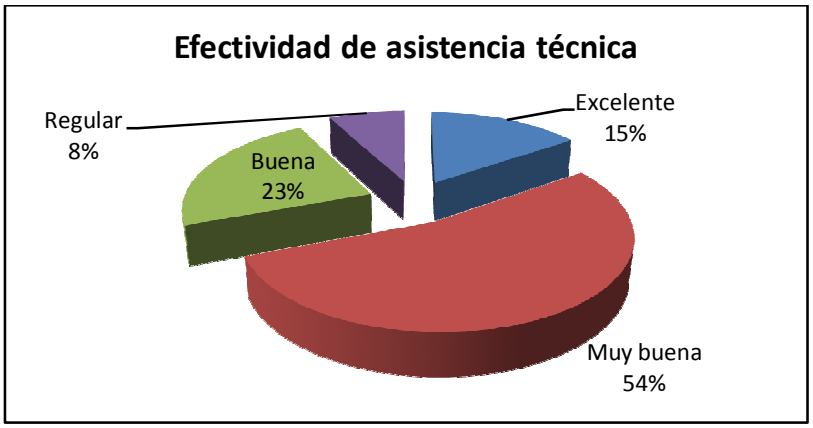


El 83% de los usuarios presentan sin inconveniente sus peticiones, el 17% no tienen la confianza necesaria para presentar sus quejas.

25. Cuando usted solicita asistencia técnica al departamento de informática, lo hace a:

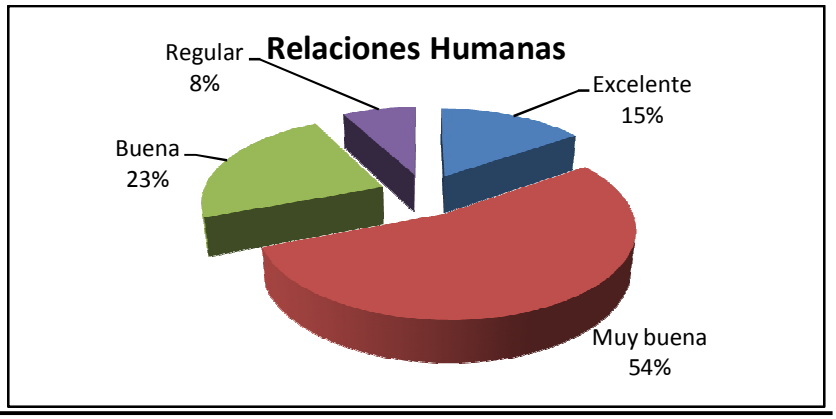
De los usuarios encuestados al solicitar soporte técnico el 70% lo solicita a cualquier miembro de informática, mientras que el 30% lo hace al personal designado a esta tarea.

26. ¿Cuál es la efectividad del(os) técnico(s) para resolver los problemas de mantenimiento?



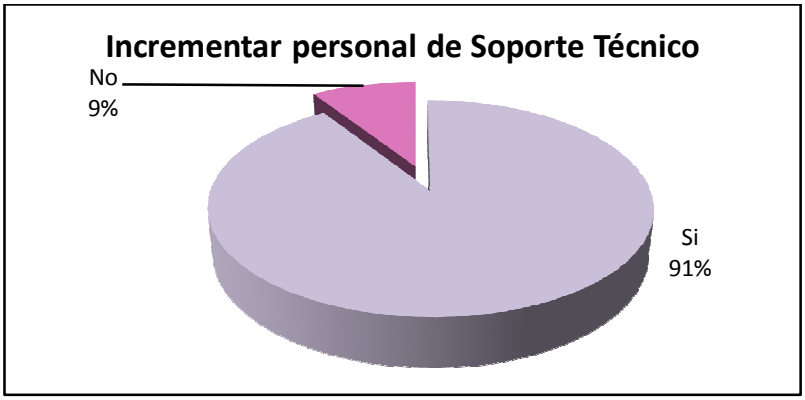
El 59% de los usuarios opina que es muy buena, el 25% señalan es buena, el 8% excelente y el 8% que es mala.

27. En Relaciones Humanas, el personal de informática con respecto al personal de la institución es:



Respecto a Relaciones humanas el 54% de los usuarios opina que es Muy buena, el 23% Buena, el 15% Excelente y el 8% Regular.

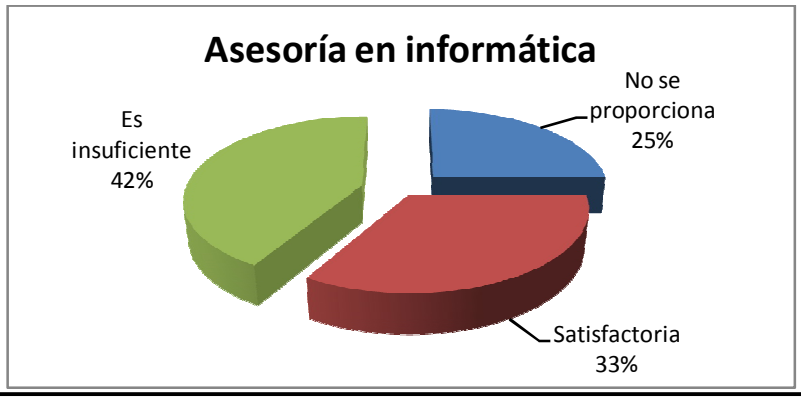
28. ¿Considera usted que debe existir mas personal de informática para brindar asistencia técnica a la institución?



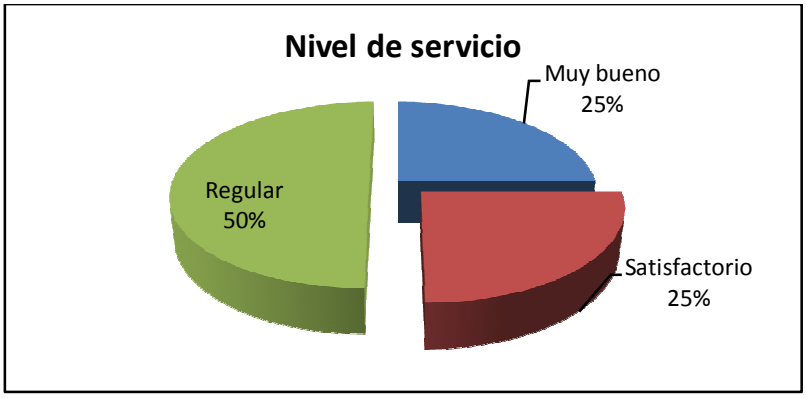
De los usuarios encuestados el 91% consideran se debe incrementar el personal para un mejor servicio, el 9% no lo considera necesario.

29. ¿Qué piensa de la asesoría que se imparte sobre informática por parte del departamento de Informática de la institución?

El 42% de los usuarios señalan que la asesoría es insuficiente, el 33% que es satisfactoria, mientras que el 25% indican que no se proporciona la asesoría adecuada.



30. ¿Como valora usted el servicio que presta el departamento de Informática a la institución?



De los usuarios encuestados el 50% opina que el nivel de servicio es Regular, el 25% que es Satisfactorio mientras que el otro 25% lo califica de Muy Bueno.

Luego de haber aplicado la Evaluación del Gobierno de TI en el departamento de Informática, se obtuvo los siguientes resultados:

Evaluación de la Dirección de TIC´s

Evaluación del Gobierno de TI	CATEGORÍA	
Gestión y Dirección de Sistemas	Importancia: 96,42%	Desempeño: 77,14 %
Software y Desarrollo	Importancia 85.71%	Desempeño 65.71%
Hardware y Comunicaciones	Importancia 87,5 %	Desempeño 70 %
Help Desk	Importancia 90 %	Desempeño 80 %

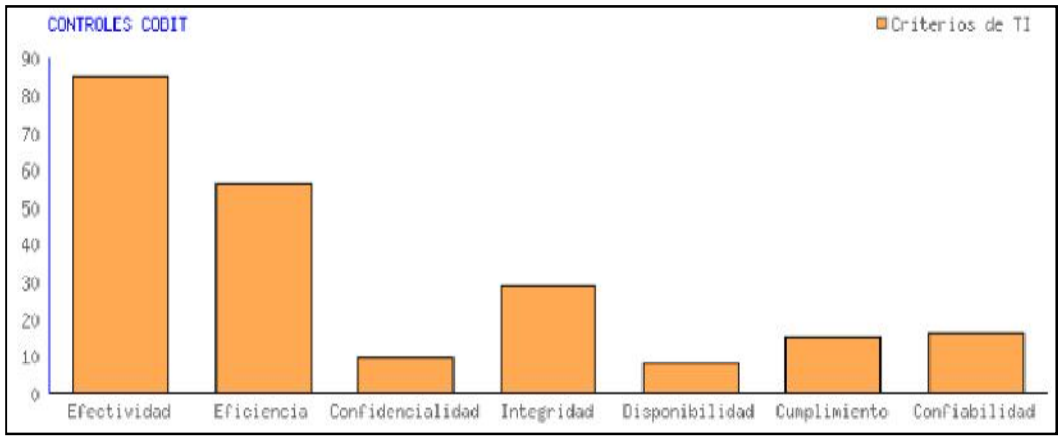
RESULTADOS TOTALES:

CRITERIO	Importancia	Desempeño	Nivel de Control	Nivel de Riesgo
Total	89,90%	92,49%	Aceptable	Bajo
Categoría	Importante	Satisfactorio		

Dándonos como resultado un nivel ***SATISFACTORIO***, lo que muestra que el nivel de Gobernabilidad de TI es aceptable.

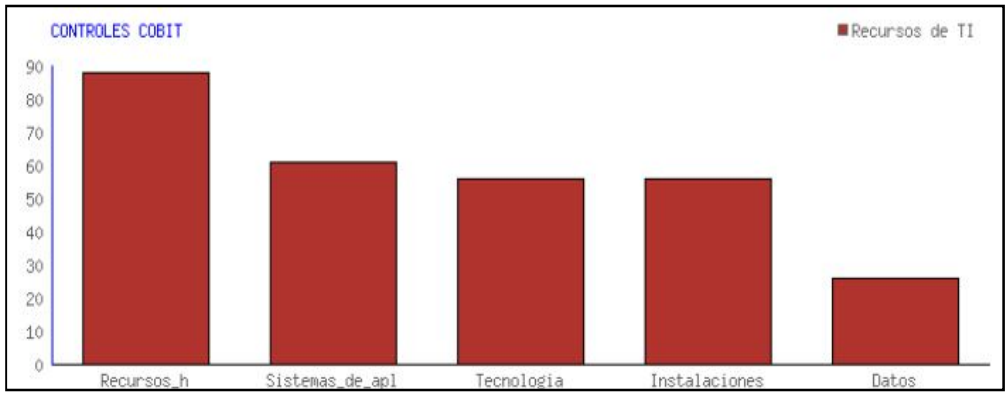
EVALUACIÓN DE LOS CONTROLES COBIT

PLANEACION Y ORGANIZACIÓN



CRITERIOS DE TI	PUNTAJE	RESULTADO
Efectividad	85.50	Inferior a lo estimado en: 14.5 pts.
Eficiencia	56.00	Inferior a lo estimado en: 2 pts.
Confidencialidad	9.50	Inferior a lo estimado en: 0.5 pts.
Integridad	29.00	Correcto
Disponibilidad	8.00	Correcto
Cumplimiento	15.00	Inferior a lo estimado en: 1 pts.
Confiabilidad	16.50	Inferior a lo estimado en: 1.5 pts.
TOTAL	219.5	

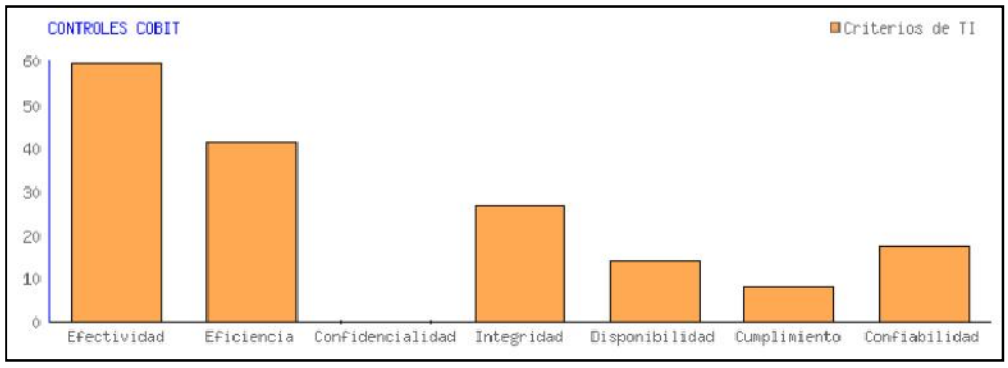
Nivel de Control en Criterios de TI: Aceptable. Porcentaje Obtenido: 92%



RECURSOS DE TI	PUNTAJE	RESULTADO
Recursos Humanos	88.00	Inferior a lo estimado en: 3 pts.
Sistemas de Aplicación	61.00	Correcto
Tecnología	56.00	Correcto
Instalaciones	56.00	Correcto
Datos	26.00	Correcto
TOTAL	287	

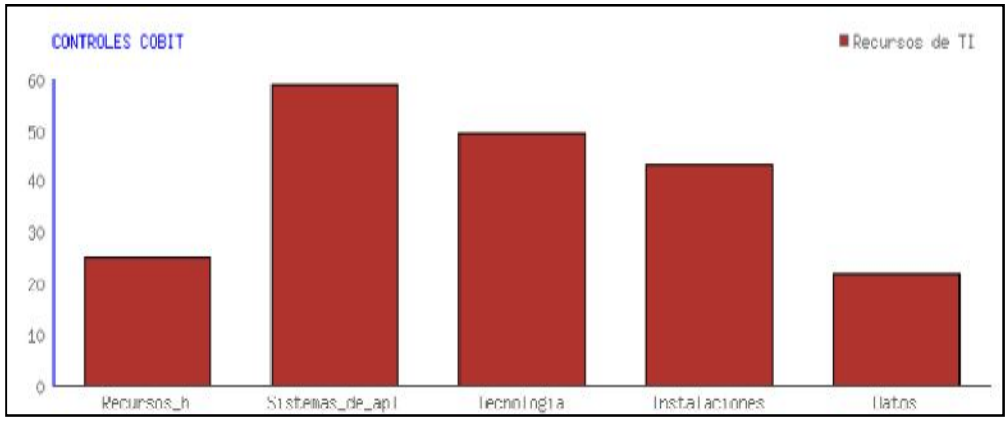
Nivel de Control en Recursos de TI: Correcto. Porcentaje Obtenido: 98%

ADQUISICIÓN E IMPLEMENTACIÓN



CRITERIOS DE TI	PUNTAJE	RESULTADO
Efectividad	59.50	Inferior a lo estimado en: 8.5 pts.
Eficiencia	41.50	Inferior a lo estimado en: 3.5 pts.
Confidencialidad	0.00	Correcto
Integridad	27.00	Inferior a lo estimado en: 2 pts.
Disponibilidad	14.00	Inferior a lo estimado en: 1 pts.
Cumplimiento	8.00	Inferior a lo estimado en: 3 pts.
Confiabilidad	17.50	Superior a lo estimado en: 2.5 pts.
TOTAL	167.5	

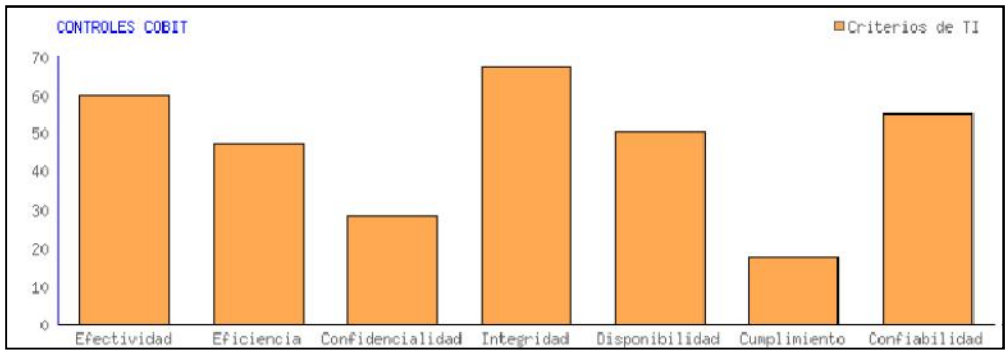
Nivel de Control en Criterios de TI: Aceptable. Porcentaje Obtenido: 92%



RECURSOS DE TI	PUNTAJE	RESULTADO
Recursos Humanos	25.00	Inferior a lo estimado en: 1 pts.
Sistemas de Aplicación	59.00	Inferior a lo estimado en: 2 pts.
Tecnología	49.50	Inferior a lo estimado en: 1.5 pts.
Instalaciones	43.00	Inferior a lo estimado en: 1 pts.
Datos	22.00	Correcto
TOTAL	198.5	

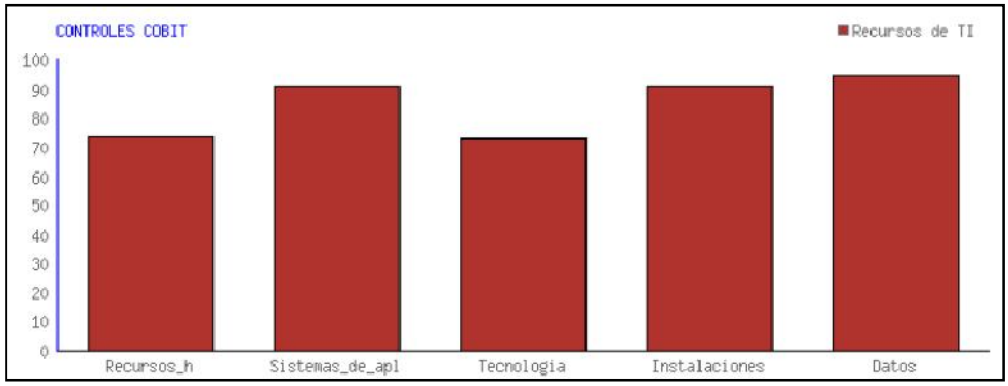
Nivel de Control en Recursos de TI: Correcto. Porcentaje Obtenido: 97%

ENTREGA DE SERVICIOS Y SOPORTE



CRITERIOS DE TI	PUNTAJE	RESULTADO
Efectividad	60.00	Inferior a lo estimado en: 6 pts.
Eficiencia	47.50	Inferior a lo estimado en: 5.5 pts.
Confidencialidad	28.50	Inferior a lo estimado en: 0.5 pts.
Integridad	67.50	Inferior a lo estimado en: 1.5 pts.
Disponibilidad	50.50	Inferior a lo estimado en: 6.5 pts.
Cumplimiento	17.50	Inferior a lo estimado en: 0.5 pts.
Confiabilidad	55.00	Correcto
TOTAL	326.5	

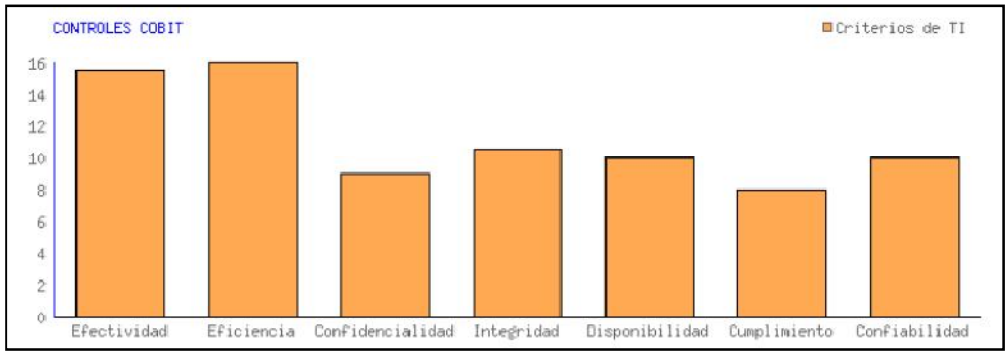
Nivel de Control en Criterios de TI: Aceptable. Porcentaje Obtenido: 94%



RECURSOS DE TI	PUNTAJE	RESULTADO
Recursos Humanos	70.00	Inferior a lo estimado en: 3 pts.
Sistemas de Aplicación	86.00	Inferior a lo estimado en: 1 pts.
Tecnología	73.00	Inferior a lo estimado en: 1 pts.
Instalaciones	87.00	Inferior a lo estimado en: 1 pts.
Datos	95.00	Correcto
TOTAL	411	

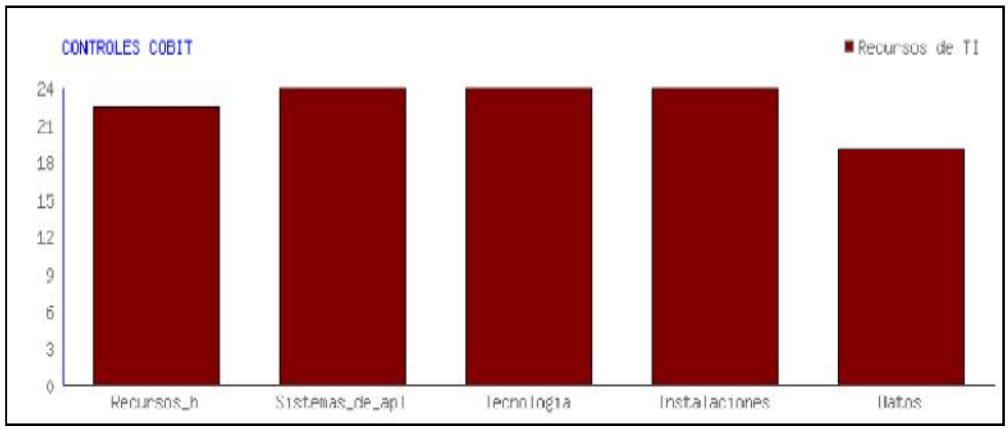
Nivel de Control en Recursos de TI: Correcto. Porcentaje Obtenido: 98%

MONITOREO



CRITERIOS DE TI	PUNTAJE	RESULTADO
Efectividad	15.50	Inferior a lo estimado en: 8.5 pts.
Eficiencia	16.00	Inferior a lo estimado en: 6 pts.
Confidencialidad	9.00	Inferior a lo estimado en: 3 pts.
Integridad	10.50	Inferior a lo estimado en: 1.5 pts.
Disponibilidad	10.00	Inferior a lo estimado en: 2 pts.
Cumplimiento	8.00	Inferior a lo estimado en: 4 pts.
Confiabilidad	10.00	Inferior a lo estimado en: 2 pts.
TOTAL	79	

Nivel de Control en Criterios de TI: Mejorable. Porcentaje Obtenido: 75%



RECURSOS DE TI	PUNTAJE	RESULTADO
Recursos Humanos	22.50	Inferior a lo estimado en: 1.5 pts.
Sistemas de Aplicación	24.00	Correcto
Tecnología	24.00	Correcto
Instalaciones	24.00	Correcto
Datos	19.00	Inferior a lo estimado en: 5 pts.
TOTAL	113.5	

Nivel de Control en Criterios de TI: Correcto. Porcentaje Obtenido: 95%

ANEXO IV

ENCUESTAS PARA EL GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

MÓDULO GESTIÓN/ DIRECCIÓN DE SISTEMAS.

- Encuesta I: Organización de TI
- Encuesta II: Arquitectura de TI
- Encuesta III: Procesamiento de Datos
- Encuesta IV: Planes de Contingencia
- Encuesta VI: Inventarios
- Encuesta VI: Personal y Procedimientos
- Encuesta VII: Seguridad.

MÓDULO: SOFTWARE Y DESARROLLO DE SISTEMAS.

- Encuesta I: Organización de TI
- Encuesta II: Arquitectura de TI
- Encuesta III: Procesamiento de Datos
- Encuesta IV: Planes de Contingencia
- Encuesta VI: Inventarios
- Encuesta VI: Personal y Procedimientos
- Encuesta VII: Seguridad

MÓDULO: HARDWARE Y COMUNICACIONES.

- Encuesta I: Organización de TI
- Encuesta II: Infraestructura de TI
- Encuesta IV: Planes de Contingencia
- Encuesta V: Inventarios
- Encuesta VI: Personal y Procedimientos
- Encuesta VII: Seguridad

MÓDULO: HELP DESK (ASISTENCIA TECNICA A USUARIO)

- Encuesta I: Organización de TI
- Encuesta II: Hardware
- Encuesta III: Software
- Encuesta IV: Planes de Contingencia
- Encuesta V: Inventarios
- Encuesta VI: Personal y Procedimientos
- Encuesta VII: Seguridad

MODULO: USUARIO DE TI

- Encuesta I: Nivel de Conocimientos
- Encuesta II: Procedimientos
- Encuesta III: Seguridad
- Encuesta IV: Servicios

Parámetro NS = No Sabe o Desconoce.

MÓDULO: GESTIÓN/ DIRECCIÓN DE SISTEMAS

ENCUESTA I: ORGANIZACIÓN DE TI

1.1. ¿Existe un Plan estratégico Informático de Tecnología de la Información (TI) para la institución?
Si ☐ No ☐ NS☐

1.2. ¿Existe o se han tomado estándares o modelos de referencia para llevar a cabo la planificación estratégica de TI?
Si☐ No☐ NS☐

1.3. ¿Hay cambios programados en el uso de modelos de referencia para la planificación estratégica de Ti? P.ej.: Conversión de ITIL a 27001
Si☐ No☐ NS☐

1.4. ¿El Plan Estratégico de TI contempla los requisitos y metas estratégicas de la Tectología de la Información (TI) a largo y corto plazo?
Si☐ No☐ NS☐

1.5. ¿En el plan estratégico de TI se establecen procesos para adaptación a cambios a largo plazo de la institución?
Si☐ No ☐ NS☐

1.6. ¿El plan estratégico de TI contiene planes operacionales a corto y mediano plazo respecto a departamento de informática?
Si☐ No☐ NS☐

1.7. ¿Con que frecuencia se realiza evaluación y monitoreo del plan estratégico de TI?
3 meses ☐ No se realiza ☐
6 meses ☐ Desconoce ☐
Anual ☐

1.8. ¿Los cambios realizados al plan estratégico de TI son documentados?
Si☐ No☐ NS☐

1.9. ¿El personal de informática tiene conocimiento del plan estratégico de TI: misión, visión, objetivos?
Si☐ No☐ NS☐

1.10. ¿Se realizan reportes a la alta gerencia respecto al cumplimiento de metas?
Si☐ No ☐ NS ☐

1.11. ¿Los ejecutivos administrativos de la institución han considerado la importancia que tiene la planeación estratégica de TI?
Si☐ No☐ NS☐

1.12. ¿Existe la asignación correspondiente de presupuesto para TI en la institución?
Si ☐ No ☐ NS☐

1.13. La asignación de presupuesto se realiza cada:
6 meses ☐ Otra ☐
Anual ☐ Desconoce ☐

1.14. ¿Se realizan estudios de costo-beneficio en relación al presupuesto asignado para TI?
Si☐ No☐ NS☐

1.15. ¿La institución cuenta con una planificación de infraestructura tecnológica?
Si☐ No☐ NS☐

1.16. ¿La adquisición de Hardware y Software son establecidos en base a la planeación de infraestructura tecnológica?
Si☐ No☐ NS☐

1.17. ¿Se realizan estudios de factibilidad previa implementación de software, hardware y demás infraestructura tecnológica en la institución?
Si☐ No☐ NS☐

1.18. ¿Existe una lista de implementación de proyectos de sistemas con fechas programadas?
Si☐ No☐ NS☐

1.19. ¿Se realizan estudios de costo-beneficio de cada uno los proyectos de software?
Si☐ No☐ NS☐

1.20. ¿Están los proyectos contemplados en el plan estratégico de TI?
Si☐ No☐ NS☐

1.21. ¿Se utilizan técnicas adecuadas para controlar el avance de proyectos de sistemas?
Si☐ No☐ NS☐

1.22. Según su criterio ¿Cómo califica usted a la Planeación Estratégica de TI de la institución?

Excelente	☐	Regular	☐
Muy Buena	☐	Desconoce	☐
Satisfactoria	☐		

ENCUESTA II: ARQUITECTURA DE LA INFORMACIÓN

2.1. ¿Posee la institución un modelo de arquitectura de la información definido?
Si☐ No☐ NS☐

2.2. ¿Existe o se ha utilizado algún estándar o normativa para el modelado de arquitectura de TI?
Si☐ No☐ NS☐

2.3. ¿Hay cambios planificados en el uso de modelos de referencia para la arquitectura de la información? P.ej.: Conversión de ITSM a BS1500
Si☐ No☐ NS☐

2.4. Dichos cambios ¿Se encuentran debidamente documentados?
Si☐ No☐ NS☐

2.5. ¿El modelo de arquitectura de TI se encuentra formalmente documentado?
Si☐ No☐ NS☐

2.6. ¿El modelo, se encuentra actualizado?
Si☐ No☐ NS☐

2.7. Como valora usted al modelo de arquitectura de la Tecnología de la Información de la institución:

Excelente	☐	Regular	☐
Muy Buena	☐	Desconoce	☐
Satisfactoria	☐		

2.8. ¿Existe una clasificación General de datos corporativos de acuerdo a su criticidad(sensitivos) e importancia?
Si☐ No☐ NS☐

2.9. ¿La clasificación distingue criterios como: Riesgos para el negocio, Riesgos para el servicio prestado a clientes y riesgo de parálisis de la Gestión de la Institución?
Si☐ No☐ NS☐

2.10. ¿Se han implementado niveles de seguridad para cada una de las clasificaciones de datos?
Si☐ No☐ NS☐

2.11. ¿Existe Diccionario de datos y sintaxis de programas y/o Sistemas de la institución?
Si☐ No☐ NS☐
2.12. ¿El Diccionario de datos incorpora reglas de sintaxis de los datos?
Si☐ No☐ NS☐
2.13. ¿Al realizar modificaciones o cambios a Sistemas Aplicativos el Diccionario de datos y sintaxis de programas se actualiza oportunamente?
Si ☐ No ☐ NS☐

ENCUESTA III: PROCESAMIENTO DE DATOS

3.1. ¿Se utiliza alguna metodología del ciclo de vida para el desarrollo sistemas?
Si☐ No☐ NS☐
3.2. ¿Los nuevos sistemas/programas desarrollados son sometidos a pruebas operacionales?
Si☐ No☐ NS☐
3.3. ¿Las pruebas realizadas a Sistemas o Programas se rigen por alguna normativa?
Si☐ No ☐ NS☐
3.4. ¿Se documentan los resultados de las pruebas realizadas a los sistemas/programas?
Si☐ No ☐ NS ☐
3.5. ¿En el desarrollo de sistemas/programas se utilizan estándares o métricas de calidad?
Si☐ No ☐ NS☐
3.6. ¿Se aplican técnicas o métodos de diseño en la creación de proyectos de software? P.ej.: UML
Si☐ No☐ NS☐
3.7. ¿Las especificaciones de los programas de cada proyecto son detalladas por escrito?
Si☐ No☐ NS☐
3.8. De acuerdo al orden ¿Quiénes intervienen al diseñar un sistema?
( ) usuario y analista
( ) usuario, gerente del departamento y analista
( ) gerente del departamento y analista
( ) otros
3.9. ¿Se supervisan los nuevos programas o modificaciones que se encuentran en producción?
Si☐ No☐ NS☐
3.10. ¿Se entregan manuales de referencia y soporte adecuados a los usuarios de cada proyecto de desarrollo?
Siempre ☐ No se realiza ☐
Ocasionalmente ☐ Desconoce ☐
3.11. ¿Cuándo se realizan modificaciones a sistemas o programas se actualizan los manuales de usuario?
Si☐ No☐ NS☐
3.12. ¿Se encuentran documentados todos los programas aplicativos que posee la institución?
Si☐ No☐ NS☐

3.13. ¿Existen manuales de procedimientos e instrucciones de operación para todos los programas que acceden a la base de datos?
Si☐ No☐ NS☐

3.14. ¿Existe un DBA responsable del manejo, administración, integridad y privacía de los datos en las Bases de Datos existentes?
Si☐ No☐ NS☐

3.15. ¿El DBA es responsable de los cambios en el diseño de las Bases de Datos?
Si☐ No☐ NS☐

3.16. ¿Se encuentran definidos y documentados los procedimientos para corrección de errores en la salida de datos?
Si☐ No☐ NS☐

3.17. Actualmente los procesos operacionales de la institución dependen de los Sistemas aplicativos existentes en:
Mucho☐ No dependen ☐
Poco ☐ Desconoce ☐

3.18. ¿Se han establecido políticas sobre derechos de propiedad intelectual que cubra el desarrollo de software de la institución?
Si☐ No☐ NS☐

3.19. ¿Se han adquirido productos de Software de terceras partes?
Si☐ No☐ NS☐

3.20. ¿La adquisición de software se norma en base a procedimientos y estándares específicos?
Si☐ No☐ NS☐

3.21. ¿Los contratos de adquisición de software se encuentran documentados?
Si☐ No☐ NS☐

3.22. ¿Se evalúa el impacto del nuevo software adquirido sobre el rendimiento del(os) sistema(s) en general?
Si☐ No☐ NS☐

ENCUESTA IV: PLANES DE CONTINGENCIA Y CONTINUIDAD

4.1. ¿Existen estudios de análisis de riesgos de la Tecnología de la Información para la institución?
Si☐ No☐ NS☐

4.2. ¿En dichos estudios se han identificado y medido todos los riesgos de TI en la institución?
Si☐ No☐ NS☐

4.3. ¿Existen planes de Contingencia y Continuidad que permitan mitigar dichos riesgos y sus posibles alternativas?
Si☐ No☐ NS☐

4.4. ¿Los Planes de Contingencia y Continuidad toman en consideración el plan a mediano y largo plazo de Tecnología de la Información?
Si☐ No☐ NS☐

4.5. ¿Los Planes de Contingencia y Continuidad garantizan el buen funcionamiento del Repositorio o Diccionario de Datos?
Si☐ No☐ NS☐

4.6. ¿El Plan de Contingencia incluye un Plan de Recuperación de desastres (DRP)?
Si☐ No☐ NS☐

4.7. ¿El Plan de Contingencias establece procedimientos de respaldo y recuperación de datos de los Sistemas Aplicativos y Bases de datos?
Si☐ No☐ NS☐

4.8. Con que frecuencia se realizan los respaldos:

Diariamente	☐	No se realiza	☐
Semanalmente	☐	Desconoce	☐
Mensualmente	☐	Otro	☐

4.9. ¿Se encuentran documentados dichos procedimientos de respaldo y recuperación?
Si☐ No☐ NS☐

4.10. ¿El Plan de Continuidad de TI establece políticas para restablecer el funcionamiento operacional (caídas del sistema) de la institución en el menor tiempo?
Si☐ No☐ NS☐

4.11. ¿Se han realizado pruebas al Plan de Continuidad de TI para evaluar su efectividad?
Si☐ No☐ NS☐

4.12. ¿Establece el Plan de Continuidad de TI guías detalladas para su utilización?
Si☐ No☐ NS☐

4.13. ¿El Plan de Continuidad se encuentra actualizado?
Si☐ No☐ NS☐

4.14. Valore según su criterio el nivel de implementación del Plan de Contingencia en la institución:

Excelente	☐	Regular	☐
Muy Bueno	☐	Desconoce	☐
Satisfactorio	☐		

ENCUESTA V: INVENTARIOS

5.1. ¿Existe inventario de Software, Hardware y Datos de la institución?
Si☐ No☐ NS☐

5.2. ¿Se identifica quienes son los propietarios de los elementos en el inventario?
Si☐ No☐ NS☐

5.3. ¿Existe un criterio para evaluar cuales son los elementos críticos del inventario?
Si☐ No☐ NS☐

5.4. ¿En el inventario se encuentran registrados adecuadamente los costos de estos?
Si☐ No☐ NS☐

5.5. El inventario se almacena en :

Papel	☐	Sistema	☐
Otro	☐	Desconoce	☐

5.6. ¿Existen copias de respaldo del inventario?
Si☐ No☐ NS☐

5.7. ¿Se encuentran etiquetadas e inventariadas las licencias de Software de los PC's de la Institución?
Si☐ No☐ NS☐

5.8. ¿Dichas licencias tienen los respaldos correspondientes?
Si☐ No☐ NS☐

5.9. ¿Existe registro de archivos o dispositivos que se prestan y la fecha en que se devolverán?
Si☐ No☐ NS☐

5.10. ¿Las solicitudes de cambio de Software o Hardware están sujetos a procedimientos formales establecidos?
Si☐ No☐ NS☐

5.11. ¿Son estas solicitudes categorizadas de acuerdo a su prioridad?
Si☐ No☐ NS☐

5.12. ¿Se tiene un procedimiento específico para los cambios de emergencia?
Si☐ No☐ NS☐

5.13. ¿Se han realizado revisiones del inventario por un especialista (auditor, consultor, experto en informática) externo a la institución?
Si☐ No☐ NS☐

ENCUESTAVI: PERSONAL Y PROCEDIMIENTOS

6.1. ¿Se han designado roles o funciones específicas dentro del departamento de informática?
Si☐ No☐ NS☐

6.2. ¿Las funciones y roles del personal de informática son asignadas por escrito?
Si☐ No☐ NS☐

6.3. ¿Se han establecido normas o políticas dentro del departamento de informática?
Si☐ No☐ NS☐

6.4. ¿El reglamento está a la vista del usuario?
Si☐ No☐ NS☐

6.5. ¿El personal da cumplimiento a las políticas establecidas en el departamento de informática?
Si☐ No☐ NS☐

6.6. ¿El departamento de Informática tiene código de ética o conducta?
Si☐ No☐ NS☐

6.7. Cómo considera usted la promoción e incentivos al personal de informática:
Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐

6.8. ¿Se estudia la evolución del mercado y la adaptación de los usuarios a esa evolución?
Si☐ No☐ NS☐

6.9. El personal de informática es evaluado en sus competencias cuando:
Va ser promovido ☐ No se evalúa ☐
Contratado ☐ Otro ☐
Transferido ☐

6.10. ¿Se brinda formación al personal de informática y se planifica ésta con asistencia a cursos, seminarios, etc?
Si☐ No☐ NS☐

6.11. Con que frecuencia se capacita al personal de informática sobre nuevas tendencias en TI (hardware/ software):
Continuamente ☐ No se capacita ☐
Ocasionalmente ☐ Desconoce ☐

6.12. ¿Se aplican estándares ergonomía para el personal de informática?
Si☐ No☐ NS☐

6.13. ¿Se aplican estándares de ergonomía para el personal que labora en la institución?
Si☐ No☐ NS☐

6.14. ¿Hay personal de informática específico para brindar asistencia técnica a la institución?
Si☐ No☐ NS☐

6.15. ¿Se ha capacitado al personal de informática en temas relacionados con Seguridad de la Información y ética?
Si ☐ No ☐ NS ☐

6.16. ¿El personal de otras dependencias de la institución han sido capacitados en temas básicos de Seguridad de la Información y ética?
Si ☐ No ☐ NS ☐

6.17. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática?
Si ☐ No ☐ NS ☐

6.18. Con que frecuencia se entrena al personal para casos de incidentes o desastres:
6 meses ☐ Anual ☐
9 meses ☐ No se realiza ☐

6.19. ¿Se lleva un monitoreo del nivel de servicio y desempeño del Departamento de Informática en la institución?
Si ☐ No ☐ NS ☐

6.20. ¿Se utilizan indicadores de desempeño para evaluar dichos servicios?
Si ☐ No ☐ NS ☐

6.21. Como valora usted el servicio que presta el departamento de Informática a la institución:
Excelente ☐ Pobre ☐
Muy bueno ☐ No esta seguro ☐
Satisfactorio ☐

ENCUESTAVII: SEGURIDAD

7.1. ¿Se ha asignado personal específico para la seguridad lógica y física de TI?
Si ☐ No ☐ NS ☐

7.2. Con que frecuencia se fomenta la cultura de honradez, ética y conciencia sobre la Seguridad de TI en el departamento de informática:
Siempre ☐ No se realiza ☐
Ocasionalmente ☐ Desconoce ☐

7.3. En los usuarios de TI de la Institución con que frecuencia se fomenta la honradez, ética y conciencia sobre la Seguridad de TI:
Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

7.4. ¿Se restringe el acceso a los lugares asignados para servidores de datos?
Si ☐ No ☐ NS ☐

7.5. ¿Existen controles de protección para el hardware y software relacionado con la seguridad de la institución?
Si ☐ No ☐ NS ☐

7.6. ¿Se controla el trabajo fuera de horario?
Si ☐ No ☐ NS ☐

7.7. ¿Se ha instruido al personal en caso de que alguien intente ingresar sin autorización?
Si ☐ No ☐ NS ☐

7.8. Existe alarma para:
Detectar fuego(calor o humo) en forma automática ☐
Avisar en forma manual la presencia del fuego ☐
Otros ☐
No existe ☐

7.9. En que lugar se encuentra la alarma:
En el departamento de informática ☐
En el cuarto frío ☐

En otros lados ☐

7.10. ¿Se registra el acceso de personas ajenas al departamento de informática?
Si☐ No☐ NS☐

7.11. ¿Son controladas las visitas y demostraciones en el departamento de informática?
Si☐ No☐ NS☐

7.12. Existe control para el acceso al departamento de informática a través de:
Identificación personal ☐ No se controla ☐
Tarjeta magnética ☐ Desconoce ☐
Claves de acceso ☐

7.13. ¿El mantenimiento o trabajos de software o hardware realizados por terceros o proveedores es supervisado o monitoreado?
Si☐ No☐ NS☐

7.14. ¿Los proveedores son sujetos a evaluaciones o calificación para su selección?
Si☐ No☐ NS☐

7.15. ¿Los contratos convenidos con los proveedores garantizan la continuidad del servicio para la institución?

Si No NS
☐ ☐ ☐

7.16. ¿Se tienen acuerdos de confidencialidad con los proveedores?
Si☐ No☐ NS☐

7.17. ¿Los servicios de TI prestados por los proveedores o terceros son sujetos a evaluaciones de efectividad?
Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

7.18. ¿Se solicitan certificaciones/acreditaciones independientes de los proveedores de servicios de TI?
Si☐ No☐ NS☐

7.19. ¿Se evalúa periódicamente la seguridad y los controles internos que se encuentran operando?
Si☐ No☐ NS☐

7.20. El área de almacenamiento de respaldos de Sistemas, Hardware y Datos esta ubicado:
En el mismo edificio del departamento ☐
En otro lugar ☐

7.21. ¿Existe un administrador de sistemas que controle a los usuarios y sus perfiles?
Si☐ No☐ NS☐

7.22. Gestiona el DBA los accesos a las distintas instancias de las bases de datos?
Si☐ No☐ NS☐

7.23. ¿Esta restringido el acceso al entorno de desarrollo?
Si☐ No☐ NS☐

7.24. ¿Se lleva registro de los incidentes, problemas y errores operacionales suscitados?
Si☐ No☐ NS☐

7.25. ¿Son investigadas y documentadas las causas de los incidentes?

Si☐ No☐ NS☐

7.26. ¿Con que frecuencia se hace limpieza del cuarto de servidores y de los ductos de aire?
Trimestral ☐ Semestral ☐
Anual ☐ No se realiza ☐

7.27. ¿Los locales asignados a los servidores de datos tienen cerradura especial?
Si☐ No☐ NS☐

7.28. ¿Existen medidas de protección contra factores ambientales como fuego y agua de los servidores?
Si☐ No☐ NS☐

7.29. ¿La institución posee suministro ininterrumpido de energía?
Si☐ No☐ NS☐

7.30. ¿Se evalúa el impacto del nuevo hardware adquirido sobre el rendimiento de las aplicaciones y sistemas existentes en general de la institución?

Si ☐ No☐ NS☐

7.31. ¿Se han ejecutado planes de auditoría al Departamento de Informática?

Si☐ No☐ NS☐

7.32. ¿La auditoría es ejecutada por personal independiente a la institución?

Si☐ No ☐ NS☐

7.33. ¿El personal que audita es técnicamente certificado o acreditado en Auditoría de Sistemas de Información?

Si☐ No ☐ NS☐

MÓDULO: SOFTWARE Y ADMINISTRACIÓN DE SISTEMAS

ENCUESTA I: ORGANIZACIÓN DE TI

1.1. ¿El departamento de informática tiene plan estratégico de TI?
Si☐ No☐ NS☐

1.2. ¿Es de su conocimiento la misión, visión y objetivos del plan estratégico de TI?
Si☐ No☐ NS☐

1.3. Como califica usted a la planeación estratégica de TI en la institución:
Muy Importante ☐ Desconoce ☐
Algo Importante ☐ No Importante ☐
Poco Aplicable ☐

1.4. ¿Se han establecido normas o políticas dentro del departamento de informática?
Si☐ No☐ NS☐

1.5. ¿El reglamento está a la vista del usuario?
Si☐ No☐ NS☐

1.6. ¿El personal da cumplimiento a las políticas establecidas en el departamento de informática?
Si☐ No☐ NS☐

1.7. ¿La institución cuenta con una planificación de infraestructura tecnológica?
Si☐ No☐ NS☐

1.8. ¿La adquisición de Software son establecidos en base a la planeación de infraestructura tecnológica?
Si☐ No☐ NS☐

1.9. ¿Se realizan estudios de factibilidad tecnológica previa implementación/ modificación de software en la institución?
Si☐ No☐ NS☐

ENCUESTA II: ARQUITECTURA DE LA INFORMACIÓN

2.1. ¿Posee la institución un modelo de arquitectura de la información definido?
Si☐ No☐ NS☐

2.2. ¿Existe o se ha utilizado algún estándar o normativa para el modelado de arquitectura de TI?
Si☐ No☐ NS☐

2.3. ¿Hay cambios planificados en el uso de modelos de referencia para la arquitectura de la información? P.ej.: Conversión de ITSM a BS1500
Si☐ No☐ NS☐

2.4. Dichos cambios ¿Se encuentran debidamente documentados?
Si☐ No☐ NS☐

2.5. ¿El modelo de arquitectura de TI se encuentra formalmente documentado?
Si☐ No☐ NS☐

2.6. ¿El modelo, se encuentra actualizado?
Si☐ No☐ NS☐

2.7. Como valora usted al modelo de arquitectura de la Tecnología de la Información de la institución:
Excelente ☐ Regular ☐
Muy Buena ☐ Desconoce ☐
Satisfactoria ☐

2.8. ¿Existe una clasificación General de datos corporativos de acuerdo a su criticidad (sensitivos) e importancia?
Si☐ No☐ NS☐

2.9. ¿La clasificación distingue criterios como: Riesgos para el negocio, Riesgos para el servicio prestado a clientes y riesgo de parálisis de la Gestión de la Institución?
Si☐ No☐ NS☐

2.10. ¿Se han implementado niveles de seguridad para cada una de las clasificaciones de datos?
Si☐ No☐ NS☐

2.11. ¿Existe Diccionario de datos y sintaxis de programas y/o Sistemas de la institución?
Si☐ No☐ NS☐

2.12. ¿El Diccionario de datos incorpora reglas de sintaxis de los datos?
Si☐ No☐ NS☐

2.13. ¿Al realizar modificaciones o cambios a Sistemas Aplicativos el Diccionario de datos y sintaxis de programas se actualiza oportunamente?
Si☐ No☐ NS☐

2.14. ¿Se ha establecido alguna configuración base de elementos(software) autorizados para los equipos de la institución?
Si☐ No☐ NS☐

2.15. A que factor obedecen mas las innovaciones software realizadas en la institución:
Planificación ☐ ☐ Desconoce
Necesidades operativas ☐

2.16. ¿Se utiliza algún estándar o normativa para la implementación de software en la institución?
Si☐ No☐ NS☐

ENCUESTA III: PROCESAMIENTO DE DATOS

3.1. ¿Se utiliza alguna metodología del ciclo de vida para el desarrollo sistemas?
Si☐ No☐ NS☐

3.2. ¿Existe un diseño físico y lógico de las Bases de Datos?
Si☐ No☐ NS☐

3.3. ¿Las Bases de datos se encuentran organizadas con criterios relacionales?
Si☐ No☐ NS☐

3.4. ¿Dispone también el Diccionario de datos un diseño físico y lógico?
Si☐ No☐ NS☐

3.5. ¿Es el DBA responsable del desarrollo, mantenimiento y control del Diccionario de Datos?
Si☐ No☐ NS☐

3.6. ¿Los nuevos sistemas/programas desarrollados son sometidos a pruebas operacionales?
Si☐ No☐ NS☐

3.7. ¿Las pruebas realizadas a Sistemas o Programas se rigen por alguna normativa?
Si☐ No☐ NS☐

3.8. ¿Se documentan los resultados de las pruebas realizadas a los sistemas/programas?
Si☐ No☐ NS☐

3.9. ¿En el desarrollo de sistemas/programas se utilizan estándares o métricas de calidad?
Si☐ No☐ NS☐

3.10. ¿Se aplican técnicas o métodos de diseño en la creación de proyectos de software? P.ej.: UML
Si☐ No☐ NS☐

3.11. ¿Las especificaciones de los programas de cada proyecto son detalladas por escrito?

Si☐ No☐ NS☐

3.12. De acuerdo al orden ¿Quiénes intervienen al diseñar un sistema?

( ) usuario y analista
( ) usuario, gerente del departamento y analista
( ) gerente del departamento y analista
( ) otros

3.13. ¿Existe una lista de implementación de proyectos de sistemas/programas se toman en cuenta el tiempo y recursos?

Si☐ No☐ NS☐

3.14. ¿Se supervisan los nuevos programas o modificaciones que se encuentran en producción?

Si☐ No☐ NS☐

3.15. ¿Se entregan manuales de referencia y soporte adecuados a los usuarios de cada proyecto de desarrollo?

Siempre ☐ No se realiza ☐
Ocasionalmente ☐ Desconoce ☐

3.16. ¿Cuándo se realizan modificaciones a sistemas o programas se actualizan los manuales de usuario?

Si☐ No☐ NS☐

3.17. ¿Se evalúa si las necesidades del usuario son satisfechas por el sistema?

Si☐ No☐ NS☐

3.18. ¿Se encuentran documentados todos los programas aplicativos que posee la institución?

Si☐ No☐ NS☐

3.19. ¿Existen manuales de procedimientos e instrucciones de operación para todos los programas que acceden a la base de datos?

Si☐ No☐ NS☐

3.20. ¿Se realizan revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?

Si☐ No☐ NS☐

3.21. ¿El mantenimiento de sistemas/programas se contemplan dentro de la metodología de ciclo de vida de estos?

Si☐ No☐ NS☐

3.22. ¿Existe un DBA responsable del manejo, administración, integridad y privacía de los datos en las Bases de Datos existentes?

Si☐ No☐ NS☐

3.23. ¿El DBA es responsable de los cambios en el diseño de las Bases de Datos?

Si☐ No ☐ NS☐

3.24. ¿Se encuentran definidos y documentados los procedimientos para corrección de errores en la salida de datos?

Si☐ No☐ NS☐

3.25. Actualmente los procesos operacionales de la institución dependen de los Sistemas aplicativos existentes en:

Mucho☐ No dependen ☐
Poco ☐ Desconoce ☐

3.26. ¿Se han establecido políticas sobre derechos de propiedad intelectual que cubra el desarrollo de software de la institución?

Si☐ No☐ NS☐

3.27. ¿Se han adquirido productos de Software de terceras partes?

Si☐ No☐ NS ☐

3.28. ¿La adquisición de software se norma en base a procedimientos y estándares específicos?

Si☐ No☐ NS ☐

3.29. ¿Los contratos de adquisición de software se encuentran documentados?
Si☐ No☐ NS☐

3.30. ¿Se evalúa el impacto del nuevo software adquirido sobre el rendimiento del(os) sistema(s) en general?
Si☐ No☐ NS☐

ENCUESTA IV: PLANES DE CONTINGENCIA Y CONTINUIDAD

4.1. ¿Existen estudios de análisis de riesgos de la Tecnología de la Información para la institución?
Si☐ No☐ NS☐

4.2. ¿En dichos estudios se han identificado y medido todos los riesgos de TI en la institución?
Si☐ No☐ NS☐

4.3. ¿Existen planes de Contingencia y Continuidad que permitan mitigar dichos riesgos y sus posibles alternativas?
Si☐ No☐ NS☐

4.4. ¿Los Planes de Contingencia y Continuidad toman en consideración el plan a mediano y largo plazo de Tecnología de la Información?
Si☐ No☐ NS☐

4.5. ¿Los Planes de Contingencia y Continuidad garantizan el buen funcionamiento del Repositorio o Diccionario de Datos?
Si☐ No☐ NS☐

4.6. ¿El Plan de Contingencia incluye un Plan de Recuperación de desastres (DRP)?
Si☐ No☐ NS☐

4.7. ¿El Plan de Contingencias establece procedimientos de respaldo y recuperación de datos de los Sistemas Aplicativos y Bases de datos?
Si☐ No☐ NS☐

4.8. Con que frecuencia se realizan los respaldos:
Diariamente ☐ No se realiza ☐
Semanalmente ☐ Desconoce ☐
Mensualmente ☐

4.9. El lugar de almacenamiento de respaldos de la BDD de los Sistemas Aplicativos esta situado:
En el mismo edificio del departamento ☐
En otro lugar ☐
Desconoce ☐

4.10. ¿Se encuentran documentados dichos procedimientos de respaldo y recuperación?
Si☐ No☐ NS☐

4.11. ¿El Plan de Continuidad de TI establece políticas para restablecer el funcionamiento operacional (caídas del sistema) de la institución en el menor tiempo?
Si☐ No☐ NS☐

4.12. ¿Se han realizado pruebas al Plan de Continuidad de TI para evaluar su efectividad?
Si☐ No☐ NS☐

4.13. ¿Establece el Plan de Continuidad de TI guías detalladas para su utilización?
Si☐ No☐ NS☐

4.14. ¿El Plan de Continuidad se encuentra actualizado?
Si☐ No☐ NS☐

4.15. ¿Se ha brindado asesoría o entrenamiento respecto al Plan de Continuidad de TI?
Si☐ No☐ NS☐

4.16. ¿Se ha realizado estudios del posible efecto de cargas normales de trabajo y los picos sobre los requerimientos de software?
Si☐ No☐ NS☐

4.17. ¿Los contratos convenidos con proveedores de software garantizan la continuidad del servicio para la institución?
Si☐ No☐ NS☐

4.18. ¿Se han implementado niveles de seguridad (firewalls) para el Software/ programas y datos de la institución?
Si☐ No☐ NS☐

4.19. ¿Se revisa y monitorea el desempeño y capacidad del software (Sistemas Aplicativos, BDDD, etc) continuamente?
Si☐ No☐ NS☐

4.20. Valore según su criterio el nivel de implementación del Plan de Contingencia en la institución:

Excelente ☐ Regular ☐
Muy Bueno ☐ Desconoce ☐
Satisfactorio ☐

ENCUESTA V: INVENTARIOS

5.1. ¿Los Sistemas Aplicativos, archivos y demás software de la institución se encuentra inventariado?
Si☐ No☐ NS☐

5.2. ¿Se identifica quienes son los propietarios de los elementos en el inventario?
Si☐ No☐ NS☐

5.3. ¿Existe un criterio para evaluar cuales son los elementos críticos del inventario?
Si☐ No☐ NS☐

5.4. ¿En el inventario se encuentran registrados adecuadamente los costos de estos?
Si☐ No☐ NS☐

5.5. El inventario se almacena en :

Papel ☐ Sistema aplicativo☐
Óptico ☐ Desconoce ☐

5.6. ¿Existen copias de respaldo del inventario?
Si☐ No☐ NS☐

5.7. ¿Se encuentran etiquetadas e inventariadas las licencias de Software de los PC's de la Institución?
Si☐ No☐ NS☐

5.8. ¿Dichas licencias tienen los respaldos correspondientes?
Si☐ No☐ NS☐

5.9. ¿Existe un inventario de manuales y documentación de software existente?
Si☐ No☐ NS☐

5.10. ¿Las solicitudes de cambio de Software/programas están sujetos a procedimientos formales establecidos?
Si☐ No☐ NS☐

5.11. ¿Son estas solicitudes categorizadas de acuerdo a su prioridad?
Si ☐ No ☐ NS ☐

5.12. ¿Se tiene un procedimiento específico para los cambios de emergencia?
Si☐ No☐ NS☐

5.13. ¿Se han realizado revisiones del inventario por un especialista (auditor, consultor, experto en informática) externo a la institución.
Si☐ No☐ NS☐

ENCUESTA VI: PERSONAL Y PROCEDIMIENTOS

6.1. ¿Se le han asignado responsabilidades o funciones específicas en el Departamento de Informática?
Si☐ No☐ NS☐

6.2. ¿Las funciones y roles que desempeña le han sido asignadas formalmente por escrito?
Si☐ No☐ NS☐

6.3. ¿El departamento de Informática tiene código de ética o conducta?
Si☐ No☐ NS☐

6.4. ¿Se vigilan la moral y comportamiento del personal de informática?
Si☐ No☐ NS☐

6.5. Cómo considera usted la promoción e incentivos al personal de informática:
Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐

6.6. Sus competencias técnicas y profesionales son evaluadas:
Continuamente ☐ No se evalúa ☐
Ocasionalmente ☐ Otro ☐

6.7. ¿Se brinda formación al personal de informática con asistencia a cursos, seminarios, etc?
Si☐ No☐ NS☐

6.8. Con que frecuencia se capacita al personal de informática sobre nuevas tendencias en TI (hardware/ software):
Continuamente ☐ No se capacita ☐
Ocasionalmente ☐ Desconoce ☐

6.9. ¿Ha recibido capacitación en temas relacionados con Seguridad de la Información y ética?
Si ☐ No☐ NS☐

6.10. Con que frecuencia se entrena al personal para casos de incidentes o desastres:
6 meses ☐ Anual ☐
9 meses ☐ No se realiza ☐

6.11. ¿Se cuenta con un directorio actualizado de todo el personal de Informática?
Si☐ No☐ NS☐

6.12. ¿Se tiene en un sitio visible un directorio con números de emergencia?
Si☐ No☐ NS☐

6.13. ¿El departamento de informática tiene salida de emergencia?
Si☐ No☐ NS☐

6.14. ¿Existen prohibiciones de fumar, tomar alimentos y refrescos en el departamento de informática?
Si☐ No☐ NS☐

6.15. ¿Se cuenta con carteles en lugares visibles que recuerden dichas prohibiciones?
Si☐ No☐ NS☐

6.16. Valore la formación y capacitación recibida por el departamento de informática:

Excelente ☐ Pobre ☐
Muy buena ☐ No esta seguro ☐
Satisfactoria ☐

6.17. Durante el tiempo que lleva en la institución ¿Ha recibido incentivos o promoción en su carrera profesional?

Si☐ No☐ NS☐

6.18. ¿Presenta informes a la Gerencia de Sistemas del desempeño de sus actividades asignadas y realizadas?

Si☐ No☐ NS☐

6.19. Cómo considera usted la promoción e incentivos al personal de informática:

Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐

6.20. ¿Se aplican estándares ergonomía para departamento de informática?

Si☐ No☐ NS☐

6.21. ¿Se lleva un monitoreo del nivel de servicio y desempeño del Departamento de Informática en la institución?

Si☐ No☐ NS☐

6.22. ¿Se utilizan indicadores de desempeño para evaluar dichos servicios?

Si☐ No☐ NS☐

6.23. Como valora usted el servicio que presta el departamento de Informática a la institución:

Excelente ☐ Pobre ☐
Muy bueno ☐ No esta seguro ☐
Satisfactorio ☐

ENCUESTA VII: SEGURIDAD

7.1. ¿Se ha asignado personal específico para la seguridad lógica y física de TI?

Si☐ No☐ NS☐

7.2. Con que frecuencia se fomenta la cultura de honradez, ética y conciencia sobre la Seguridad de TI en el departamento de informática:

Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

7.3. En los usuarios de TI de la Institución con que frecuencia se fomenta la honradez, ética y conciencia sobre la Seguridad de TI:

Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

7.4. ¿Se restringe el acceso a los lugares asignados para servidores de datos?

Si☐ No☐ NS☐

7.5. ¿Los locales asignados a los servidores de datos tienen cerradura especial?

Si☐ No☐ NS☐

7.6. ¿Existe un sistema de alarma que para la detección de intrusos en el departamento de informática?

Si☐ No☐ NS☐

7.7. ¿Existen políticas para la obtención de archivos de respaldo de la BDD?

Si☐ No☐ NS☐

7.8. ¿Se han establecido privilegios de acceso para la información a usuarios?

Si☐ No☐ NS☐

7.9. ¿Existen controles/permisos para asegurar que la identificación y derechos de acceso a los sistemas son de forma única y centralizada?
Si☐ No☐ NS☐

7.10. En caso de transgresión, ¿Se registra las violaciones a los controles y seguridades?
Si☐ No☐ NS☐

7.11. ¿Se realizan reportes de estas violaciones a la Gerencia de Sistemas?
Si☐ No☐ NS☐

7.12. ¿Se han realizado investigaciones o seguimientos de las transgresiones?
Si☐ No☐ NS☐

7.13. ¿Se controla el trabajo fuera de horario?
Si☐ No☐ NS☐

7.14. ¿Se ha instruido al personal en caso de que alguien intente ingresar sin autorización?
Si☐ No☐ NS☐

7.15. ¿Existe algún sistema para detección de incendios en el cuarto servidores?
Si☐ No☐ NS☐

7.16. ¿Se tienen instalados extintores manuales de incendios?
Si☐ No☐ NS☐

7.17. ¿Se ha capacitado sobre el uso y tipo de extintor a utilizar, dependiendo de la situación?
Si☐ No☐ NS☐

7.18. ¿El material del techo falso del Departamento de Informática es ignifugante?
Si☐ No☐ NS☐

7.19. ¿El departamento de informática cuenta con una salida de emergencia?
Si☐ No☐ NS☐

7.20. ¿La institución posee suministro ininterrumpido de energía?
Si☐ No☐ NS☐

7.21. ¿Se registra el acceso de personas ajenas al departamento de informática?
Si☐ No☐ NS☐

7.22. ¿Son controladas las visitas y demostraciones en el departamento de informática?
Si☐ No☐ NS☐

7.23. Existe control para el acceso al departamento de informática a través de:
Identificación personal ☐ No se controla ☐
Tarjeta magnética ☐ Desconoce ☐
Claves de acceso ☐

7.24. ¿Se tienen acuerdos de confidencialidad con los proveedores de Software?
Si☐ No☐ NS☐

7.25. ¿Los servicios de TI prestados por los proveedores o terceros son sujetos a evaluaciones de efectividad?
Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

7.26. ¿Los servicios o trabajos realizados por terceros o proveedores es monitoreado/supervisado?
Si☐ No☐ NS☐

7.27. ¿Se solicitan certificaciones/acreditaciones independientes de los proveedores de servicios de TI?
Si☐ No☐ NS☐

7.28. ¿Se evalúa periódicamente la seguridad y los controles internos que se encuentran operando?
Si☐ No☐ NS☐

7.29. ¿Se utiliza algún software antivirus corporativo específico en los PC's de la institución?

Si☐ No☐ NS☐

7.30. Con que frecuencia se realizan actualizan del antivirus en la institución:

Diario (Automático)☐ No se realiza ☐

Semanal ☐ Desconoce ☐

7.31. ¿Se ha implementado políticas que restrinjan el uso de software personal y no licenciado?

Si☐ No☐ NS☐

7.32. El software no autorizado que se encuentra instalado en equipos ¿es eliminado?

Siempre ☐ No se elimina ☐

Ocasionalmente ☐ Desconoce ☐

7.33. ¿Se monitorea o supervisa los equipos de la institución para evitar que los usuarios instalen software no autorizado?

Si☐ No☐ NS☐

7.34. ¿Se restringe el acceso de personal no autorizado a manuales, documentación, librería, y otros medios?

Si☐ No☐ NS☐

7.35. ¿Existen controles para impedir el acceso a información sensitiva desechada o transferida?

Si☐ No☐ NS☐

7.36. ¿Se verifica regularmente la integridad de los datos almacenados en archivos y otros medios?

Si☐ No☐ NS☐

7.37. ¿Se han ejecutado planes de auditoría al Departamento de Informática?

Si☐ No☐ NS☐

7.38. ¿La auditoría es ejecutada por personal independiente a la institución?

Si☐ No☐ NS☐

7.39. ¿El personal que audita es técnicamente certificado o acreditado en Auditoría de Sistemas de Información?

Si☐ No☐ NS☐

MÓDULO HARDWARE Y COMUNICACIONES

ENCUESTA I: ORGANIZACIÓN DE TI

1.1. ¿El departamento de informática tiene plan estratégico de TI?
Si☐ No☐ NS☐

1.2. ¿Es de su conocimiento la misión, visión y objetivos del plan estratégico de TI?
Si☐ No☐ NS☐

1.3. Como califica usted a la planeación estratégica de TI en la institución:
Muy Importante ☐ Desconoce ☐
Algo Importante ☐ No Importante ☐
Poco Aplicable ☐

1.4. ¿Se han establecido normas o políticas dentro del departamento de informática?
Si☐ No☐ NS☐

1.5. ¿El reglamento está a la vista del usuario?
Si☐ No☐ NS☐

1.6. ¿El personal da cumplimiento a las políticas establecidas en el departamento de informática?
Si☐ No☐ NS☐

1.7. ¿El departamento de Informática tiene código de ética?
Si☐ No☐ NS☐

1.8. ¿La institución cuenta con una planificación de infraestructura tecnológica?
Si☐ No☐ NS☐

1.9. ¿La adquisición de Hardware y demás equipamiento son establecidos en base a la planeación de infraestructura tecnológica?
Si☐ No☐ NS☐

1.10. ¿Se realizan estudios de factibilidad previa implementación de hardware y demás infraestructura tecnológica en la institución?
Si☐ No☐ NS☐

ENCUESTA II: INFRAESTRUCTURA LOCATIVA Y OPERACIONAL

2.1. ¿Posee la institución un modelo de arquitectura de red y comunicaciones?
Si☐ No☐ NS☐

2.2. ¿Se utiliza algún estándar o normativa para el modelado de arquitectura de redes?
Si☐ No☐ NS☐

2.3. De los siguientes, que estándar o normativa utiliza para redes y comunicaciones:
EIA/TIA☐ IEEE ☐
UM4 ☐ Ninguna ☐

2.4. ¿El modelado y sus procesos se encuentran formalmente documentados?
Si☐ No☐ NS☐

2.5. ¿El modelo, se encuentra correctamente actualizado?
Si☐ No☐ NS☐

2.6. ¿Se aplican normativas para la distribución de equipos de conectividad y comunicaciones?
Si☐ No☐ NS☐

2.7. ¿Se cuenta con un sistema central de aire acondicionado?
Si☐ No☐ NS☐

2.8. ¿La ductería para líneas eléctricas, telefónicas o de datos están claramente identificadas?
Si☐ No☐ NS☐

2.9. ¿Las líneas eléctricas del departamento de informática son independientes del resto de las instalaciones eléctricas?
Si☐ No☐ NS☐

2.10. ¿La instalación eléctrica del departamento de informática tienen conexión a tierra de acuerdo a normas internacionales?
Si☐ No☐ NS☐

2.11. ¿Existen planos de las instalaciones eléctricas?
Si☐ No☐ NS☐

2.12. ¿Existen planos de las instalaciones de red y telefónicas?
Si☐ No☐ NS☐

2.13. ¿Se cuenta con suficiente espacio para la distribución de servidores y demás equipos de comunicaciones en la institución?
Si☐ No☐ NS☐

2.14. ¿Los equipos cuentan con regulador de voltaje?
Si☐ No☐ NS☐

2.15. ¿Se mantiene un stock de partes, piezas y suministros para la red?
Si☐ No☐ NS☐

2.16. ¿La iluminación del área de Informática es adecuada?
Si☐ No☐ NS☐

2.17. A que factor obedecen mas las innovaciones tecnológicas de hardware realizadas en la institución:
Planificación ☐ ☐ Desconoce
Necesidades operativas ☐

2.18. ¿Las solicitudes de cambio de Hardware están sujetos a procedimientos formales?
Si☐ No☐ NS☐

2.19. ¿Los solicitantes de los cambios permanecen informados del estatus de su solicitud?
Si☐ No☐ NS☐

2.20. ¿Se tiene un procedimiento específico para los cambios de emergencia de hardware?
Si ☐ No ☐ NS ☐

2.21. ¿Se realizan estudios de factibilidad previa implementación de infraestructura tecnológica en la institución?
Si☐ No☐ NS☐

2.22. ¿Se utiliza alguna normativa para la adquisición e implementación del hardware en la institución?
Si☐ No☐ NS☐

2.23. ¿Se evalúa el impacto del nuevo hardware adquirido sobre el rendimiento de las aplicaciones y sistemas existentes en general de la institución?
Si ☐ No☐ NS☐

2.24. ¿Hay personal de informática específico para brindar asistencia técnica a la institución?
Si☐ No☐ NS☐

2.25. ¿Existe un programa para realizar mantenimiento preventivo al hardware de la institución?
Si☐ No☐ NS☐

2.26. Con que frecuencia se realiza el mantenimiento:
6 meses ☐ No se realiza ☐
Anual ☐ Desconoce ☐

2.27. ¿Se tiene determinado un lugar específico para papelería y herramientas de trabajo?

Si☐ No☐ NS☐

2.28. ¿Existe un lugar asignado para mantenimiento o reparación de equipos?

Si☐ No☐ NS☐

2.29. ¿Existen instructivos y procedimientos de operación para encender el computador cuando se va la energía o en operaciones normales?

Si☐ No☐ NS☐

2.30. ¿Con que frecuencia se hace limpieza en el cuarto de servidores y de los ductos de aire?

6 meses ☐ No se realiza ☐
Anual ☐ Desconoce ☐

2.31. Según su criterio valore el nivel de implementación tecnológica en la institución:

Excelente ☐ Pobre ☐
Muy buena ☐ Desconoce ☐
Satisfactoria ☐

ENCUESTA III: PLANES DE CONTINGENCIA Y CONTINUIDAD

3.1. ¿Se han realizado estudios de análisis de riesgos de la Tecnología de la Información para la institución?

Si☐ No☐ NS☐

3.2. ¿En dichos estudios se han identificado y medido todos los riesgos de TI de la institución?

Si☐ No☐ NS☐

3.3. ¿Existen planes de Contingencia y Continuidad que permitan mitigar dichos riesgos y sus posibles alternativas?

Si☐ No☐ NS☐

3.4. ¿El Plan de Contingencia incluye un Plan de Recuperación de desastres (DRP)?

Si☐ No☐ NS☐

3.5. ¿El Plan de Continuidad de TI establece políticas para restablecer el funcionamiento operacional (caídas del sistema) de la institución en el menor tiempo?

Si☐ No☐ NS☐

3.6. ¿Se encuentra diseñada la red de de comunicación de tal manera que no afecte totalmente la caída de algún dispositivo de comunicación?

Si☐ No☐ NS☐

3.7. ¿Se han realizado pruebas al Plan de Continuidad de TI para evaluar su efectividad?

Si☐ No☐ NS☐

3.8. ¿Establece el Plan de Continuidad de TI guías detalladas para su utilización?

Si☐ No☐ NS☐

3.9. ¿El Plan de Continuidad se encuentra actualizado?

Si☐ No☐ NS☐

3.10. ¿Se ha brindado asesoría o entrenamiento respecto al Plan de Continuidad de TI?

Si No NS

3.11. Valore según su criterio el nivel de implementación del Plan de Contingencia en la institución:

Excelente ☐ Regular ☐
Muy Bueno ☐ Desconoce ☐
Satisfactorio ☐

3.12. ¿Se han realizado estudios del posible efecto de cargas normales de trabajo y los picos sobre los requerimientos de equipos?
Si☐ No☐ NS☐

3.13. ¿Existen implantados mecanismos de tolerancia de fallas para los servicios de información?
Si ☐ No ☐ NS☐

3.14. ¿Se revisa y monitorea el desempeño y capacidad del hardware continuamente?
Si☐ No☐ NS☐

3.15. ¿Se dispone de equipos auxiliares en caso de caída o avería del equipo principal?
Si ☐ No ☐ NS☐

3.16. ¿Se lleva registro de los incidentes, problemas u errores en el funcionamiento de equipos?
Si☐ No☐ NS☐

3.17. ¿Son investigadas y documentadas las causas de los incidentes?
Si☐ No☐ NS☐

3.18. ¿Se verifica y registra frecuentemente la temperatura y la humedad de local de servidores?
Si☐ No☐ NS ☐

3.19. ¿Se mide con frecuencia la tensión e intensidad de la corriente eléctrica?
Si☐ No☐ NS ☐

ENCUESTA IV: INVENTARIOS

4.1. ¿Los PC's, equipos de red y demás Hardware de la institución está inventariado y etiquetado?
Si☐ No☐ NS ☐

4.2. ¿Se identifica quienes son los propietarios de los elementos en el inventario?
Si ☐ No ☐ NS ☐

4.3. ¿Existe un criterio para evaluar cuales son los elementos críticos del inventario?
Si☐ No☐ NS ☐

4.4. ¿En el inventario se encuentran registrados adecuadamente los costos de estos?
Si☐ No☐ NS ☐

4.5. El inventario se almacena en :
Papel ☐ Sistema aplicativo☐
Óptico ☐ Desconoce ☐

4.6. ¿Existen copias de respaldo del inventario?
Si ☐ No ☐ NS ☐

4.7. ¿Existe registro de los dispositivos o equipos (proyectores, portátil, etc.) que se prestan y la fecha en que se devolverán?
Si☐ No☐ NS☐

4.8. ¿Las solicitudes de cambio de Hardware en la institución están sujetos a procedimientos formales establecidos?
Si☐ No☐ NS☐

4.9. ¿Son estas solicitudes categorizadas de acuerdo a su prioridad?
Si☐ No☐ NS☐

4.10. ¿Se tiene un procedimiento específico para los cambios de emergencia?
Si☐ No☐ NS☐

4.11. ¿Se han realizado revisiones del inventario por un especialista (auditor, consultor, experto en informática) externo a la institución.
Si☐ No☐ NS☐

ENCUESTA V: PERSONAL Y PROCEDIMIENTOS

5.1. ¿Se le han asignado responsabilidades o funciones específicas en el Departamento de Informática?
Si☐ No☐ NS☐
5.2. ¿Las funciones y roles que desempeña le son asignadas formalmente por escrito?
Si☐ No☐ NS☐
5.3. ¿Se han establecido normas o políticas en el departamento de informática?
Si☐ No☐ NS☐
5.4. ¿Se da cumplimiento a dichas políticas establecidas?
Si☐ No☐ NS☐
5.5. ¿El departamento de Informática tiene código de ética o conducta?
Si☐ No☐ NS☐
5.6. ¿Se vigilan la moral y comportamiento del personal de informática?
Si☐ No☐ NS☐
5.7. Cómo considera usted la promoción e incentivos al personal de informática:
Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐
5.8. Sus competencias técnicas y profesionales son evaluadas:
Continuamente ☐ No se evalúa ☐
Ocasionalmente ☐ Desconoce ☐
5.9. ¿Se brinda formación al personal de informática con asistencia a cursos, seminarios, etc.?
Si☐ No☐ NS☐
5.10. Con que frecuencia se capacita al personal de informática sobre nuevas tendencias en TI (hardware/ software):
Continuamente ☐ No se capacita ☐
Ocasionalmente ☐ Desconoce ☐
5.11. ¿Ha recibido capacitación en temas relacionados con Seguridad de la Información y ética?
Si ☐ No☐ NS☐

5.12. Con que frecuencia se entrena al personal para casos de incidentes o desastres:
6 meses ☐ Anual ☐
9 meses ☐ No se realiza ☐
5.13. ¿Se cuenta con un directorio actualizado de todo el personal de Informática?
Si☐ No☐ NS☐
5.14. ¿Se tiene en un sitio visible un directorio con números de emergencia?
Si☐ No☐ NS☐
5.15. ¿El departamento de informática tiene salida de emergencia?
Si☐ No☐ NS☐
5.16. ¿Existen prohibiciones de fumar, tomar alimentos y refrescos en el departamento de informática?
Si☐ No☐ NS☐
5.17. ¿Se cuenta con carteles en lugares visibles que recuerden dichas prohibiciones?
Si☐ No☐ NS☐

5.18. Valore la formación y capacitación recibida por el departamento de informática:

Excelente ☐ Pobre ☐
Muy buena ☐ No esta seguro ☐
Satisfactoria ☐

5.19. Durante el tiempo que lleva en la institución ¿Ha recibido incentivos o promoción en su carrera profesional?

Si☐ No☐ NS☐

5.20. ¿Presenta informes a la Gerencia de Sistemas del desempeño de sus actividades asignadas y realizadas?

Si☐ No☐ NS☐

5.21. Cómo considera usted la promoción e incentivos al personal de informática:

Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐

5.22. ¿Se aplican estándares ergonomía para departamento de informática?

Si☐ No☐ NS☐

5.23. ¿Se lleva un monitoreo del nivel de servicio y desempeño del Departamento de Informática en la institución?

Si☐ No ☐ NS ☐

5.24. ¿Se utilizan indicadores de desempeño para evaluar dichos servicios?

Si☐ No☐ NS☐

5.25. Como valora usted el servicio que presta el departamento de Informática a la institución:

Excelente ☐ Pobre ☐
Muy bueno ☐ No esta seguro ☐
Satisfactorio ☐

ENCUESTA VI: SEGURIDAD

6.1. ¿Se ha asignado personal específico para la seguridad lógica y física de TI?

Si☐ No☐ NS☐

6.2. Con que frecuencia se fomenta la cultura de honradez, ética y conciencia sobre la Seguridad de TI en el departamento de informática:

Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

6.3. En los usuarios de TI de la Institución con que frecuencia se fomenta la honradez, ética y conciencia sobre la Seguridad de TI:

Siempre ☐ No se realiza ☐
Esporádicamente ☐ Desconoce ☐

6.4. ¿Se restringe el acceso a los lugares asignados para servidores de datos?

Si☐ No☐ NS☐

6.5. ¿Los locales asignados a los servidores de datos tienen cerradura especial?

Si☐ No☐ NS☐

6.6. ¿Existe un sistema de alarma que para la detección de intrusos en el departamento de informática?

Si☐ No☐ NS☐

6.7. ¿Se controla el trabajo fuera de horario?

Si☐ No☐ NS☐

6.8. ¿Se ha instruido al personal en caso de que alguien intente ingresar sin autorización?

Si☐ No☐ NS☐

6.9. ¿Existe algún sistema para detección de incendios en el cuarto servidores?
Si☐ No☐ NS☐

6.10. ¿El local de servidores cuenta con detectores de humedad?
Si☐ No☐ NS☐

6.11. ¿La ductería utilizada para los diferentes tipos de cableado es ignifugante?
Si☐ No☐ NS☐

6.12. ¿Todas las líneas de comunicación están aseguradas para prevenir que sean interceptadas?
Si☐ No☐ NS☐

6.13. ¿Se tienen instalados extintores manuales de incendios?
Si ☐ No☐ NS☐

6.14. ¿Se ha capacitado sobre el uso y tipo de extintor a utilizar, dependiendo de la situación?
Si☐ No☐ NS☐

6.15. ¿El material del techo falso del Departamento de Informática es ignifugante?
Si☐ No☐ NS☐

6.16. ¿El departamento de informática cuenta con una salida de emergencia?
Si☐ No☐ NS☐

6.17. ¿La institución posee suministro ininterrumpido de energía?
Si☐ No☐ NS☐

6.18. ¿Se registra el acceso de personas ajenas al departamento de informática?
Si☐ No☐ NS☐

6.19. ¿Son controladas las visitas y demostraciones en el departamento de informática?
Si ☐ No ☐ NS ☐

6.20. ¿Se restringe el acceso y controla el acceso a los equipos de la red por personas no autorizadas?
Si☐ No☐ NS☐

6.21. ¿Existe un manual de sobre seguridades físicas de la red?
Si☐ No☐ NS☐

6.22. Existe control para el acceso al departamento de informática a través de:

Identificación personal	☐	No se controla	☐
Tarjeta magnética	☐	Desconoce	☐
Claves de acceso	☐		

6.23. ¿El mantenimiento o trabajos de hardware realizados por terceros/ proveedores es supervisado o monitoreado?
Si☐ No☐ NS☐

6.24. ¿Los proveedores de equipamiento tecnológico son sujetos a evaluaciones o calificación para su selección?
Si☐ No☐ NS☐

6.25. ¿Los contratos convenidos con los proveedores garantizan la continuidad del servicio para la institución?
Si☐ No ☐ NS☐

6.26. ¿Se tienen acuerdos de confidencialidad con los proveedores?
Si☐ No☐ NS☐

6.27. ¿Los servicios de TI prestados por los proveedores o terceros son sujetos a evaluaciones de efectividad?

Siempre	☐	No se realiza	☐
Esporádicamente	☐	Desconoce	☐

6.28. ¿Se solicitan certificaciones/acreditaciones independientes de los proveedores de servicios de TI?
Si☐ No☐ NS☐

6.29. ¿Se evalúa periódicamente la seguridad y los controles internos que se encuentran operando?

Si☐ No☐ NS☐

6.30. ¿Son investigadas y documentadas las causas de incidentes en equipos?

Si☐ No☐ NS☐

6.31. ¿Con que frecuencia se hace limpieza del cuarto de servidores y de los ductos de aire?

Trimestral	☐	Semestral	☐
Anual	☐	No se realiza	☐

6.32. ¿Se restringe el acceso de personal no autorizado a manuales, documentación, librería, y otros medios?

Si☐ No☐ NS☐

6.33. ¿Se han ejecutado planes de auditoría al Departamento de Informática?

Si☐ No☐ NS☐

6.34. ¿La auditoría es ejecutada por personal independiente a la institución?

Si☐ No☐ NS☐

6.35. ¿El personal que audita es técnicamente certificado o acreditado en Auditoría de Sistemas de Información?

Si☐ No☐ NS☐

MÓDULO: HELP DESK

ENCUESTA I: ORGANIZACIÓN DE TI

1.1. ¿El departamento de informática tiene plan estratégico de TI?
Si ☐ No ☐ NS ☐

1.2. ¿Es de su conocimiento la misión, visión y objetivos del plan estratégico de TI?
Si☐ No☐ NS☐

1.3. Como califica usted a la planeación estratégica de TI en la institución:
Muy Importante ☐ Desconoce ☐
Algo Importante ☐ No Importante ☐
Poco Aplicable ☐

1.4. ¿Se han establecido normas o políticas dentro del departamento de informática?
Si☐ No☐ NS☐

1.5. ¿El reglamento está a la vista del usuario?
Si ☐ No ☐ NS ☐

1.6. ¿El personal da cumplimiento a las políticas establecidas en el departamento de informática?
Si☐ No ☐ NS☐

1.7. ¿La institución cuenta con una planificación de infraestructura tecnológica?
Si ☐ No ☐ NS ☐

1.8. ¿La adquisición de Software y Hardware son establecidos en base a la planeación de infraestructura tecnológica?
Si☐ No ☐ NS ☐

1.9. ¿Se realizan estudios de factibilidad tecnológica previa implementación/ modificación de software y hardware en la institución?
Si☐ No ☐ NS ☐

ENCUESTA II: HARDWARE

2.1. ¿Posee la institución un modelo de arquitectura de la información definido?
Si☐ No ☐ NS☐

2.2. ¿Posee la institución un modelo de arquitectura de red y comunicaciones?
Si☐ No ☐ NS☐

2.3. ¿Se aplican normativas para la distribución de equipos de conectividad y comunicaciones?
Si☐ No☐ NS☐

2.4. ¿Se cuenta con un sistema central de aire acondicionado?
Si☐ No☐ NS☐

2.5. ¿La ductería para líneas eléctricas, telefónicas o de datos están claramente identificadas?
Si☐ No ☐ NS☐

2.6. ¿Las líneas eléctricas del departamento de informática son independientes del resto de las instalaciones eléctricas?
Si☐ No☐ NS☐

2.7. ¿Existen planos de las instalaciones eléctricas?
Si☐ No☐ NS☐

2.8. ¿Existen planos de las instalaciones de red y telefónicas?
Si ☐ No ☐ NS☐

2.9. ¿Se cuenta con suficiente espacio para la distribución de servidores y demás equipos de comunicaciones en la institución?
Si☐ No☐ NS☐

2.10. ¿Los equipos de la institución cuentan con regulador de voltaje?
Si ☐ No ☐ NS ☐

2.11. ¿Se mantiene un stock de partes, piezas y suministros para la red?
Si ☐ No ☐ NS ☐

2.12. ¿La iluminación del área de Informática es adecuada?
Si ☐ No ☐ NS ☐

2.13. A que factor obedecen mas las innovaciones de Hardware realizadas en la institución:
Planificación ☐ Desconoce ☐
Necesidades operativas ☐

2.14. ¿Las solicitudes de cambio de Hardware están sujetas a procedimientos formales?
Si☐ No☐ NS☐

2.15. ¿Los solicitantes de los cambios permanecen informados del estatus de su solicitud? Si ☐ No ☐ NS ☐

2.16. ¿Se tiene un procedimiento específico para los cambios de emergencia de hardware? Si ☐ No ☐ NS ☐

2.17. ¿Se evalúa el impacto del nuevo hardware adquirido sobre el rendimiento de las aplicaciones y sistemas de la institución?
Si ☐ No ☐ NS ☐

2.18. ¿Existe un programa para realizar mantenimiento preventivo al hardware de la institución?
Si ☐ No ☐ NS ☐

2.19. Con que frecuencia se realiza el mantenimiento:
6 meses ☐ No se realiza ☐
Anual ☐ Desconoce ☐

2.20. ¿Se tiene determinado un lugar específico para papelería y herramientas de trabajo?
Si☐ No☐ NS☐

2.21. ¿Existe un lugar asignado para mantenimiento o reparación de equipos?
Si ☐ No ☐ NS ☐

2.22. ¿Existen instructivos/procedimientos de operación para encender el PC cuando se va la energía o en operaciones normales?
Si☐ No☐ NS☐

2.23. ¿Con que frecuencia se hace limpieza en el cuarto de servidores y de los ductos de aire?
6 meses ☐ No se realiza ☐
Anual ☐ Desconoce ☐

2.24. Según su criterio valore el nivel de implementación tecnológica en la institución:
Excelente ☐ Pobre ☐
Muy buena ☐ Desconoce ☐
Satisfactoria ☐

ENCUESTA III: SOFTWARE

3.1. ¿Existe Diccionario de datos y sintaxis de programas y/o Sistemas de la institución?
Si☐ No☐ NS☐

3.2. ¿El Diccionario de datos incorpora reglas de sintaxis de los datos?
Si☐ No☐ NS☐

3.3. ¿Se entregan manuales de referencia y soporte adecuados a los usuarios de cada proyecto de desarrollo?

Siempre ☐ No se realiza ☐
Ocasionalmente ☐ Desconoce ☐

3.4. ¿Cuándo se realizan modificaciones a sistemas o programas se actualizan los manuales de usuario?

Si☐ No☐ NS☐

3.5. ¿Se evalúa si las necesidades del usuario son satisfechas por el sistema?

Si☐ No☐ NS☐

3.6. ¿Se encuentran documentados todos los programas aplicativos que posee la institución?

Si☐ No☐ NS☐

3.7. ¿Existe un DBA responsable del manejo, administración, integridad y privacía de los datos en las Bases de Datos existentes?

Si☐ No☐ NS☐

3.8. Actualmente los procesos operacionales de la institución dependen de los Sistemas aplicativos existentes en:

Mucho ☐ No dependen ☐
Poco ☐ Desconoce ☐

3.9. ¿Se ha establecido alguna configuración base de elementos(software) autorizados para los equipos de la institución?

Si☐ No☐ NS☐

3.10. ¿Se utiliza algún estándar o normativa para la implementación de software en la institución?

Si☐ No☐ NS☐

3.11. ¿Son las solicitudes de cambio de Software (programas) sujetas también a procedimientos formales?

Si☐ No☐ NS☐

3.12. ¿Los solicitantes de los cambios permanecen informados del estatus de su solicitud? Si☐ No☐ NS☐

3.13. ¿Se da mantenimiento a los programas y aplicaciones de en forma regular?

Si☐ No☐ NS☐

3.14. ¿Se han adquirido productos de Software de terceras partes?

Si☐ No☐ NS☐

ENCUESTA IV: PLANES DE CONTINGENCIA Y CONTINUIDAD

3.15. ¿Existen estudios de análisis de riesgos de la Tecnología de la Información para la institución?

Si☐ No☐ NS☐

3.16. ¿En dichos estudios se han identificado y medido todos los riesgos de TI en la institución?

Si☐ No☐ NS☐

3.17. ¿Existen planes de Contingencia y Continuidad que permitan mitigar dichos riesgos y sus posibles alternativas?

Si☐ No☐ NS☐

3.18. ¿El Plan de Contingencias establece procedimientos de respaldo y recuperación de datos de los Sistemas Aplicativos y Bases de datos?

Si☐ No☐ NS☐

3.19. Con que frecuencia se realizan los respaldos:

Diariamente ☐ No se realiza ☐
Semanalmente ☐ Desconoce ☐
Mensualmente ☐

3.20. El lugar de almacenamiento de respaldos de la BDD de Sistemas Aplicativos esta situado:

En el mismo edificio del departamento ☐
En otro lugar ☐
Desconoce ☐

3.21. ¿Se encuentran documentados dichos procedimientos de respaldo y recuperación?

Si☐ No☐ NS☐

3.22. ¿Se han realizado pruebas al Plan de Continuidad de TI para evaluar su efectividad?

Si☐ No☐ NS☐

3.23. ¿Establece el Plan de Continuidad de TI guías detalladas para su utilización?

Si☐ No☐ NS☐

3.24. ¿El Plan de Continuidad se encuentra actualizado?

Si☐ No☐ NS☐

3.25. ¿Se ha brindado asesoría o entrenamiento respecto al Plan de Continuidad de TI?

Si☐ No☐ NS☐

3.26. ¿Se han implementado niveles de seguridad (firewalls) para el Software/ programas y datos de la institución?

Si☐ No☐ NS☐

3.27. ¿Se han realizado estudios del posible efecto de cargas normales de trabajo y los picos sobre los requerimientos de equipos?

Si☐ No☐ NS☐

3.28. ¿Se revisa y monitorea el desempeño y capacidad del hardware continuamente?

Si☐ No☐ NS☐

3.29. ¿Se dispone de equipos auxiliares en caso de caída o avería del equipo principal?

Si☐ No☐ NS☐

3.30. ¿Se verifica y registra frecuentemente la temperatura y la humedad de local de servidores?

Si☐ No☐ NS☐

3.31. ¿Se mide con frecuencia la tensión e intensidad de la corriente eléctrica?

Si ☐ No ☐NS ☐

3.32. Valore según su criterio el nivel de implementación del Plan de Contingencia en la institución:

Excelente ☐ Regular ☐
Muy Bueno ☐ Desconoce ☐
Satisfactorio ☐

ENCUESTA V: INVENTARIOS

4.1. ¿Los PC's, equipos de red y demás Hardware de la institución está inventariado y etiquetado?

Si ☐ No☐ NS ☐

4.2. ¿Se identifica quienes son los propietarios de los elementos en el inventario?

Si ☐ No☐ NS ☐

4.3. ¿Los Sistemas Aplicativos, archivos y demás software de la institución se encuentra inventariado?

Si ☐ No☐ NS ☐

4.4. ¿Se identifica quienes son los propietarios de los elementos en el inventario?

Si ☐ No☐ NS ☐

4.5. ¿Existe un criterio para evaluar cuales son los elementos críticos del inventario?
Si ☐ No☐ NS ☐

4.6. ¿En el inventario se encuentran registrados adecuadamente los costos de estos?
Si ☐ No☐ NS ☐

4.7. El inventario se almacena en :
Papel ☐ Sistema aplicativo☐
Óptico ☐ Desconoce ☐

4.8. ¿Existen copias de respaldo del inventario?
Si ☐ No☐ NS ☐

4.9. ¿Se encuentran etiquetadas e inventariadas las licencias de Software de los PC's de la Institución?
Si☐ No☐ NS☐

4.10. ¿Dichas licencias tienen los respaldos correspondientes?
Si☐ No☐ NS ☐

4.11. ¿Existe un inventario de manuales y documentación de software existente?
Si ☐ No☐ NS ☐

4.12. ¿Existe registro de archivos o dispositivos que se prestan y la fecha en que se devolverán?
Si ☐ No☐ NS ☐

4.13. ¿Se lleva un registro de los de programas, archivos, datos, papelería, etc , al que no se le va dar uso?
Si☐ No☐ NS☐

4.14. ¿Existe un stock mínimo de materiales necesarios (tinta, cds, papel, etc) en el departamento de informática?
Si☐ No☐ NS☐

4.15. ¿Se han realizado revisiones del inventario por un especialista (auditor, consultor, experto en informática) externo a la institución.
Si☐ No☐ NS☐

ENCUESTA VI: PERSONAL Y PROCEDIMIENTOS

4.16. ¿Se le han asignado responsabilidades o funciones específicas en el Departamento de Informática?
Si ☐ No☐ NS☐

4.17. ¿Las funciones y roles que desempeña le han sido asignadas formalmente por escrito?
Si☐ No☐ NS☐

4.18. ¿El departamento de Informática tiene código de ética o conducta?
Si ☐ No☐ NS☐

4.19. ¿Se vigilan la moral y comportamiento del personal de informática?
Si ☐ No☐ NS ☐

4.20. Cómo considera usted la promoción e incentivos al personal de informática:
Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐

4.21. Sus competencias técnicas y profesionales son evaluadas:
Continuamente ☐ No se evalúa ☐
Ocasionalmente ☐ Desconoce ☐

4.22. ¿Se brinda formación al personal de informática con asistencia a cursos, seminarios, etc?
Si☐ No☐ NS☐

4.23. Con que frecuencia se capacita al personal de informática sobre nuevas tendencias en TI (hardware/ software):
Continuamente ☐ No se capacita ☐
Ocasionalmente ☐ Desconoce ☐

4.24. ¿Ha recibido capacitación en temas relacionados con Seguridad de la Información y ética?
Si ☐ No☐ NS☐

4.25. Con que frecuencia se entrena al personal para casos de incidentes o desastres:
6 meses ☐ Anual ☐
9 meses ☐ No se realiza ☐

4.26. ¿Se cuenta con un directorio actualizado de todo el personal de Informática?
Si☐ No☐ NS☐

4.27. ¿Se tiene en un sitio visible un directorio con números de emergencia?
Si☐ No☐ NS☐

4.28. ¿El departamento de informática tiene salida de emergencia?
Si☐ No☐ NS☐

4.29. ¿Existen prohibiciones de fumar, tomar alimentos y refrescos en el departamento de informática?
Si☐ No☐ NS☐

4.30. ¿Se cuenta con carteles en lugares visibles que recuerden dichas prohibiciones?
Si☐ No☐ NS☐

4.31. ¿Se da cumplimiento con estas restricciones?
Si☐ No☐ NS☐

4.32. Valore la formación y capacitación recibida por el departamento de informática:
Excelente ☐ Pobre ☐
Muy buena ☐ No esta seguro ☐
Satisfactoria ☐

4.33. Durante el tiempo que lleva en la institución ¿Ha recibido incentivos o promoción en su carrera profesional?
Si☐ No☐ NS☐

4.34. ¿Presenta informes a la Gerencia de Sistemas del desempeño de sus actividades asignadas y realizadas?
Si☐ No☐ NS☐

4.35. Cómo considera usted la promoción e incentivos al personal de informática:
Muy Importante ☐ No importante ☐
Poco Importante ☐ Desconoce ☐
Poco Aplicable ☐

4.36. ¿Se aplican estándares ergonomía para departamento de informática?
Si☐ No☐ NS☐

4.37. Cuando el usuario lo requiere, ¿se brinda la asistencia técnica necesaria?
Si☐ No☐ NS☐

4.38. En el departamento de informática, la asistencia técnica la realiza:
Personal asignado ☐ Otros ☐
Todos ☐

4.39. ¿Se realiza escalabilidad de rango para dar solución a peticiones de mayor complejidad?
Si☐ No☐ NS☐

4.40. ¿Se lleva un registro de las consultas realizadas por los usuarios?
Si☐ No☐ NS☐

4.41. ¿Se lleva un monitoreo del nivel de servicio y desempeño del Departamento de Informática en la institución?

Si☐ No ☐ NS☐

4.42. ¿Se utilizan indicadores de desempeño para evaluar dichos servicios?

Si☐ No☐ NS☐

6.28. Como valora usted el servicio que presta el departamento de Informática a la institución:

Excelente	☐	Pobre	☐
Muy bueno	☐	No esta seguro	☐
Satisfactorio	☐		

ENCUESTA VII: SEGURIDAD

5.1. ¿Se ha asignado personal específico para la seguridad lógica y física de TI?

Si☐ No☐ NS☐

5.2. Con que frecuencia se fomenta la cultura de honradez, ética y conciencia sobre la Seguridad de TI en el departamento de informática:

Siempre	☐		☐
Esporádicamente	☐	Desconoce	☐

5.3. En los usuarios de TI de la Institución con que frecuencia se fomenta la honradez, ética y conciencia sobre la Seguridad de TI:

Siempre	☐		☐
Esporádicamente	☐	Desconoce	☐

5.4. ¿Se restringe el acceso a los lugares asignados para servidores de datos?

Si☐ No☐ NS☐

5.5. ¿Los locales asignados a los servidores de datos tienen cerradura especial?

Si☐ No☐ NS☐

5.6. ¿Existe un sistema de alarma que para la detección de intrusos en el departamento de informática?

Si☐ No☐ NS☐

5.7. ¿Se controla el trabajo fuera de horario?

Si☐ No☐ NS☐

5.8. ¿Se ha instruido al personal en caso de que alguien intente ingresar sin autorización?

Si☐ No☐ NS☐

5.9. ¿Existe algún sistema para detección de incendios en el cuarto servidores?

Si☐ No☐ NS☐

5.10. ¿Se tienen instalados extintores manuales de incendios?

Si☐ No☐ NS☐

5.11. ¿Se ha capacitado sobre el uso y tipo de extintor a utilizar, dependiendo de la situación?

Si☐ No☐ NS☐

5.12. ¿El material del techo falso del Departamento de Informática es ignifugante?

Si☐ No☐ NS☐

5.13. ¿El departamento de informática cuenta con una salida de emergencia?

Si☐ No☐ NS☐

5.14. ¿La institución posee suministro ininterrumpido de energía?

Si☐ No☐ NS☐

5.15. ¿Se registra el acceso de personas ajenas al departamento de informática?

Si☐ No☐ NS☐

5.16. ¿Son controladas las visitas y demostraciones en el departamento de informática?
Si☐ No☐ NS☐

5.17. Existe control para el acceso al departamento de informática a través de:
Identificación personal ☐ No se controla ☐
Tarjeta magnética ☐ Desconoce ☐
Claves de acceso ☐

7.18. ¿Los servicios o trabajos realizados por terceros o proveedores es monitoreado/supervisado?
Si☐ No☐ NS☐

7.19. ¿Se evalúa periódicamente la seguridad y los controles internos que se encuentran operando?
Si☐ No☐ NS☐

7.20. ¿Se lleva registro de los incidentes, problemas/ errores operacionales en equipos?
Si ☐ No☐ NS☐

7.21. ¿Son investigadas y documentadas las causas de dichos incidentes?

7.22. ¿Se utiliza algún software antivirus específico en los PC's de la institución?

7.23. Con que frecuencia se realizan actualizan del antivirus en la institución:
Diario (Automático☐ No se realiza ☐
Semanal ☐ ☐

7.24. ¿Se ha implementado políticas que restrinjan el uso de software personal y no licenciado?
Si☐ No☐ NS☐

7.25. El software no autorizado que se encuentra instalado en equipos ¿es eliminado?
Siempre ☐ No se elimina ☐
Ocasionalmente ☐ Desconoce ☐

7.26. ¿Se monitorea o supervisa los equipos de la institución para evitar que los usuarios instalen software no autorizado?
Si☐ No☐ NS☐

7.27. ¿Se restringe el acceso de personal no autorizado a manuales, documentación, librería, y otros medios?
Si☐ No☐ NS☐

7.28. ¿Existen controles para impedir el acceso a información sensitiva desechada o transferida?
Si☐ No☐ NS☐

7.29. ¿Se verifica regularmente la integridad de los datos almacenados en archivos y otros medios?
Si☐ No☐ NS☐

7.30. ¿Se han ejecutado planes de auditoría al Departamento de Informática?
Si ☐ No☐ NS☐

7.31. ¿La auditoría es ejecutada por personal independiente a la institución?
Si☐ No ☐ NS☐

7.32. ¿El personal que audita es técnicamente certificado o acreditado en Auditoría de Sistemas de Información?
Si☐ No ☐ NS☐

MÓDULO: USUARIO TI

ENCUESTA I: NIVEL DE CONOCIMIENTOS

1. De acuerdo a sus conocimientos en computación e informática, en que nivel de usuario se ubica usted:
   - ☐ Básico: Office, internet y otros programas de escritorio.
   - ☐ Avanzado: Instalar programas, completo dominio de Office e internet.
   - ☐ Experto: Programación, mantenimiento de equipos, redes, etc.

ENCUESTA II: PROCEDIMIENTOS

1. ¿Su computador cuenta con regulador de voltaje o ups?
   Si ☐ No ☐ NS☐
2. ¿Durante el tiempo que lleva en la institución, su equipo de computación ha sido renovado?
   1 Vez ☐
   2 ó 3 ☐
   Mas de 3 ☐
3. Cuando se solicitan cambios de equipo, instalación o actualización de programas se realiza:
   Formalmente (escrito) ☐
   Petición verbal ☐
4. Si usted solicita dichos cambios ¿La dirección de informática le informa oportunamente del estado de su solicitud?
   Si ☐ No ☐ NS ☐
5. A su criterio, cual es la razón por la que se realizan los cambios de equipos en la institución:
   Planificación ☐ Favoritismo ☐
   Solo cuando se daña ☐
6. ¿Sabe usted si existe un cronograma para mantenimiento preventivo (limpieza) a computadores en la institución?
   Si☐ No☐ NS ☐
7. Con que frecuencia se realiza el mantenimiento a computadores:
   6 meses ☐ No se realiza ☐
   Anual ☐ Solo cuando se daña el equipo ☐
8. ¿La Dirección de Informática le ha proporcionado instrucciones de operación para el cuidado y manejo del computador?
   Si☐ No☐ NS☐
9. ¿La Dirección de Informática le ha comunicado que existe personal específico responsable del Soporte Técnico de la Institución?
   Si ☐ No☐ NS ☐

ENCUESTA III: SEGURIDAD

1. El ingreso al departamento de informática por parte del personal de la institución es:
   Restringido ☐
   Es necesaria una autorización ☐
   Se accede libremente ☐
2. ¿Es de su conocimiento si en la Dirección de informática existe algún reglamento?
   Si ☐ No☐ NS ☐

3. ¿En el departamento de Informática existen carteles con prohibiciones de fumar, tomar alimentos y refrescos?
   Si ☐ No☐ NS ☐
4. ¿En el departamento de Informática existen carteles con prohibiciones de fumar, tomar alimentos y refrescos?
   Si ☐ No ☐ NS
5. ¿Considera usted que se cumplen dichas prohibiciones?
   Si☐ No☐ NS☐
6. ¿Utiliza usted algún sistema informático en particular (contabilidad, bodega, tesorería, u otro)?
   Si ☐ No ☐ NS ☐
7. Existen Prohibiciones sobre la instalación o uso de programas no autorizados en los equipos de la institución
   Si ☐ No ☐ NS ☐
8. ¿El departamento de Informática le ha brindado temas relacionados con Seguridad de la Información?
   Si ☐ No ☐ NS ☐
9. En la institución con que frecuencia se fomenta la honradez, ética y conciencia sobre la Seguridad de la información en el personal
   Siempre ☐ No se realiza ☐
   Esporádicamente ☐ Desconoce ☐
10. Con que frecuencia se entrena al personal para casos de incidentes o desastres (incendios, temblores):
    6 meses ☐ Anual ☐
    9 meses ☐ No se realiza ☐

ENCUESTA IV: SERVICIOS

1. ¿Cómo califica el servicio de internet?
   Excelente ☐ Regular ☐
   Muy buena ☐ Mala ☐
   Buena ☐
2. ¿Considera que el servicio de internet debe estar disponible a cualquier hora y para cualquier usuario?
   Si ☐ No ☐ NS ☐
3. Departamento de Informática le brinda atención cuándo usted lo requiere?
   Si☐ No☐ NS ☐
4. ¿Tiene usted la suficiente confianza como para presentar su queja sobre fallas en los equipos?
   Si ☐ No☐ NS☐
5. Cuando usted solicita asistencia técnica al departamento de informática, lo hace a
   Personal asignado para Soporte Técnico ☐
   Cualquier miembro de informática ☐
   Otros ☐
6. ¿Cuál es la efectividad del(os) técnico(s) para resolver los problemas de mantenimiento?
   Excelente ☐ Regular ☐
   Muy buena ☐ Mala ☐
   Buena ☐
7. En Relaciones Humanas, el personal de informática con respecto al personal de la institución es:
   Excelente ☐ Regular ☐
   Muy buena ☐ Mala ☐
   Buena ☐

8. ¿Considera usted que debe existir mas personal de informática para brindar asistencia técnica a la institución?
   Si ☐ No☐ NS ☐
9. ¿Qué piensa de la asesoría que se imparte sobre informática?
   No se proporciona☐ Satisfactoria ☐
   Es insuficiente ☐ Excelente ☐
10. Como valora usted el servicio que presta el departamento de Informática a la institución:
    Excelente ☐ Regular ☐
    Muy bueno ☐ Malo ☐
    Satisfactorio ☐