ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

EVALUACIÓN Y AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO: DOMINIO ENTREGA DE SERVICIOS Y SOPORTE

POR: **SANDRA PATRICIA BALSECA ALCOCER**

MIGUEL EDUARDO CACHIMUEL QUEREMBÁS

SANGOLQUÍ, 29 ABRIL DEL 2008

DEDICATORIA

El presente trabajo lo dedico con mucho cariño a Dios por haberme fortalecido en mis estudios, y a mi familia por su sacrificio y afán de brindarme una educación y a la vez una profesión de la cual depende mi futuro.

Sandra Patricia Balseca Alcocer

DEDICATORIA

El presente proyecto está dedicado a Dios, mi familia y todas las personas que me han apoyado durante el transcurso de mi carrera estudiantil y de las que he aprendido y tomado un poco de sus conocimientos y experiencia para el enriquecimiento de mis pensamientos mediante los cuales podré desempeñar mis futuras actividades.

Miguel Eduardo Cachimuel Querembás

AGRADECIMIENTO

A todas las personas que con su apoyo incondicional hicieron posible el presente trabajo, a mis padres, compañero de Tesis y los ingenieros directores los cuales han sabido orientarme y dotarme de sabiduría y en especial a mi director de tesis Ing. Mario Ron, por su orientación durante el presente trabajo.

Sandra Patricia Balseca Alcocer

AGRADECIMIENTO

Agradezco a mis padres, mi compañera de tesis, los ingenieros directores, codirectores, informantes, docentes, mi familia, compañeros de carrera en la Escuela Politécnica del Ejército, quienes cada uno aportaron con un granito de arena para la consecución del presente proyecto de tesis.

Miguel Eduardo Cachimuel Querembás

ÍNDICE DE CONTENIDOS

RESUMEN I

CAPÍTULO I 1

AUDITORÍA INFORMÁTICA – PRESENTACIÓN DEL PROYECTO 1

1.1. Introducción 1

1.2. Antecedentes 2

1.3. Justificación 3

1.4. Objetivos del proyecto 4

1.4.1. Objetivo General 4

1.4.2. Objetivos Específicos. 4

1.5. Alcance 5

1.6. Metodología 6

CAPÍTULO II 7

MARCO TEÓRICO DE REFERENCIA 7

2.1. Auditoría Informática 7

2.1.1. Introducción 7

2.2. Ambiente de control 8

2.3. El proceso de la auditoría Informática 10

2.3.1. Planificación de la auditoría Informática 11

2.3.2. Ejecución de la auditoría Informática 15

2.3.3. Finalización de la auditoría Informática 16

2.4. Clasificación de los controles TI 19

2.4.1. Controles de Aplicación 19
2.4.2. Controles Generales 22

CAPÍTULO III 24

MODELO COBIT 24

3.1. Introducción 24

3.2. Productos COBIT 26
3.2.1. Resumen Ejecutivo 27
3.2.2. Marco Referencial 28
3.2.3. Objetivos de Control 28
3.2.4. Guía o Directriz de Auditoría 29
3.2.5. Prácticas de Control 30
3.2.6. Guías de Administración 30
3.2.7. Conjunto de Herramientas de Implementación 30

3.3. Generalidades del modelo COBIT 31
3.3.1. Marco de Trabajo de COBIT 31
3.3.1.1. Orientado a Negocios 31
3.3.1.2. Orientado a Procesos 35
3.3.1.3. Basado en Controles 38
3.3.1.4. Impulsado por Mediciones 39

3.4. Dominio Entrega de Servicios y Soporte 40
3.4.1. DS 1 DEFINICIÓN Y ADMINISTRACIÓN DE NIVELES DE SERVICIO 40
3.4.2. DS 2 ADMINISTRAR LOS SERVICIOS DE TERCEROS 41
3.4.3. DS 3 ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD 42
3.4.4. DS 4 ASEGURAR EL SERVICIO CONTINUO 43
3.4.5. DS 5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS 45
3.4.6. DS 6 IDENTIFICAR Y ASIGNAR COSTOS 47
3.4.7. DS 7 EDUCAR Y ENTRENAR A LOS USUARIOS 47
3.4.8. DS 8 APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN 48

3.4.9. DS 9 ADMINISTRACIÓN DE LA CONFIGURACIÓN 49
3.4.10. DS 10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES 49
3.4.11. DS 11 ADMINISTRACIÓN DE DATOS 50
3.4.12. DS 12 ADMINISTRACIÓN DE INSTALACIONES 51
3.4.13. DS 13 ADMINISTRACIÓN DE OPERACIONES 52

CAPÍTULO IV 53

4.1. Resumen Ejecutivo 53

4.2. Informe de Auditoría. 55

DS1. DEFINIR NIVELES DE SERVICIO 55
DS1.1. Marco de Referencia para el Acuerdo de Niveles de Servicio. 55
DS1.2. Definición de servicios 59
DS1.3. Procedimientos de Desempeño. 60
DS1.4. Monitoreo y Reporte 62
DS1.5.- Revisión de Acuerdos y Contratos de Nivel de Servicio 64
DS1.6. Programa de Mejoramiento del Servicio 65

DS2. ADMINISTRAR LOS SERVICIOS DE TERCEROS 67
DS2.1. Identificación de las relaciones con todos los proveedores 67
DS2.2. Relaciones con los Propietarios (usuarios dueños) 69
DS2.3. Calificación de Terceros 70
DS2.4. Continuidad de Servicios 72
DS2.5. Relaciones con la Seguridad 73
DS2.6. Monitoreo 74

DS3. ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD 76
DS3.1. Requerimiento de disponibilidad y desempeño 76
DS3.2. Plan de Disponibilidad 77
DS3.3. Monitoreo y Reporte 79
DS3.4. Manejo Proactivo del Desempeño. 80
DS3.5. Pronóstico de Carga de Trabajo 81
DS3.6. Administración de Capacidad de Recursos 82

DS4. ASEGURAR EL SERVICIO CONTINUO 84
DS4.1. Marco de Referencia de Continuidad de Tecnología de información ... 84
DS4.2. Estrategia y Filosofía del Plan de Continuidad de TI. 86
DS4.3. Almacenamiento de respaldo en el sitio alterno (Off-site)..... 87

DS5. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS..... 89
DS5.1. Administrar Medidas de Seguridad 89

DS6. IDENTIFICAR Y ASIGNAR COSTOS 93
DS6.1. Elementos Sujetos a Cargo o Cobro por su Uso.- 93

DS7. EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS.-..... 95
DS7.1. Identificación de necesidades de entrenamiento 95
DS7.2. Evaluación del entrenamiento recibido. 96

DS8. APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN..... 97
DS8.1. Help Desk 97

DS9. ADMINISTRACIÓN DE LA CONFIGURACIÓN..... 100
DS9.1. Repositorio de configuración y línea base.- 100
DS9.2. Identificación, mantenimiento y revisión de elementos de configuración 102

DS10. MANEJO DE PROBLEMAS E INCIDENTES 104
DS10.1. Escalamiento de problemas.- 104
DS10.2. Seguimiento de Problemas y Pistas de Auditoría.- 106
DS10.3. Autorización de Accesos temporales y emergentes.- 107
DS10.4. Prioridades de procesamiento de emergencia.- 109

DS11. ADMINISTRACIÓN DE DATOS 110
DS11.1. Sistema de administración de librerías de medios.-..... 110
DS11.2. Respaldo y restauración 112

DS12. ADMINISTRACIÓN DE INSTALACIONES..... 113
DS12.1. Seguridad Física.-..... 113
DS12.2. Escolta de Visitantes.- 115

DS13. ADMINISTRACIÓN DE OPERACIONES 117
DS13.1. Operaciones Remotas 117

CAPÍTULO V 119

CONCLUSIONES Y RECOMENDACIONES 119

5.1 CONCLUSIONES..... 119

5.2 RECOMENDACIONES 120

BIBLIOGRAFÍA 122

ANEXO A .....**ERROR! BOOKMARK NOT DEFINED.**

ESQUEMA DEL PROCESO DE AUDITORÍA INFORMÁTICA..... **Error! Bookmark not defined.**

ANEXO B .....**ERROR! BOOKMARK NOT DEFINED.**

MATRIZ DE IMPACTO.....**Error! Bookmark not defined.**

ÍNDICE DE FIGURAS

Figura 3.1. Productos de COBIT
Figura 3.2. Principios Básicos de COBIT
Figura 3.3. Cubo COBIT
Figura 3.4. Niveles e actividades de TI
Figura 3.5. Resumen de los procesos de TI y de COBIT Definidos en los cuatro dominios
Figura 3.6. Componentes de los objetivos de control
Figura 3.7. Esquema del Proceso del Dominio Entrega de Servicios y Soporte

Siglas y Abreviaturas

COBIT Objetivos de Control para Tecnologías de Información y Relacionadas

COSO Comité de Organizaciones patrocinadoras de la Comisión Treadway.

ESPE Escuela Politécnica del Ejército.

ISO Organización Internacional de Normalización.

ITIL Biblioteca de Infraestructura de Tecnologías de Información.

SGC Sistema de Gestión de Calidad.

TI Tecnología de información.

UDI Unidad de Desarrollo Institucional.

UTIC Unidad de Tecnologías de Información y Comunicaciones.

RESUMEN

El presente documento del proyecto, “Evaluación y Auditoría del Sistema de Información de la Escuela Politécnica del Ejército: Dominio Entrega de Servicios y Soporte”, describe los siguientes aspectos:

- La importancia que tienen en la actualidad los sistemas informáticos en la ejecución de los procesos de negocio de todas las empresas, puesto que reducen el tiempo de operación y optimizan los recursos a ser utilizados.

- Indica que una auditoría de sistemas es un proceso de revisión de la manera en la que se están administrando actualmente los sistemas y los controles implantados en los mismos, basado en un criterio o modelo de control y gobierno de TI establecido. Proceso que debe ser realizado de manera secuencial siguiendo las fases, Planificación, Ejecución y Finalización de la Auditoría.

- Abarca la descripción del Marco de Referencia utilizado en el desarrollo del proyecto, el cual es el Modelo COBIT, que sirve para mitigar los riesgos del negocio, mejorar las necesidades de control y aspectos técnicos, y está dirigido a los auditores informáticos, permitiendo además determinar el alcance de la tarea de auditoría e identificar los controles mínimos.

- Describe los criterios del Modelo COBIT, utilizados para realizar el relevamiento de la operación y administración del sistema de información de la Escuela Politécnica del Ejército; relevamiento con el cual se pudo detectar los errores potenciales que producen riesgos en la consistencia de la información, así como las recomendaciones que deberían ser implantadas por las autoridades de la institución evaluada, para mitigar los riesgos y cumplir los estándares de calidad a los que se encuentra sujeta.

CAPÍTULO I

AUDITORÍA INFORMÁTICA – PRESENTACIÓN DEL PROYECTO

1.1. Introducción

La evolución de los sistemas de información y comunicación en nuestro País, ha generado la necesidad de implementar la gestión de sistemas en las diferentes instituciones; para obtener seguridad, confiabilidad y escalabilidad en todos los ámbitos que a estas conciernen.

La velocidad con que los medios de comunicación progresan, han hecho que las empresas cada vez necesiten de más control sobre sus datos y los sistemas que estas utilizan, provocando con ello el que el procesamiento de la información y la rapidez con la que se realiza se vuelva de vital importancia.

La Escuela Politécnica del Ejército y su Unidad de Tecnología de la Información y Comunicación, han venido ejecutando varios proyectos relacionados con el área informática con el fin de apoyar a las distintas actividades que se desarrollan dentro de ella, por lo que se vuelve indispensable controlar se entreguen los servicios requeridos, exista una correcta capacitación para su uso y un adecuado soporte que permita la continuidad de las operaciones en caso de suscitarse cualquier tipo de problema o incidente. Esta ha sido la motivación por la que la Escuela Politécnica del Ejército ha considerado la necesidad de realizar una Auditoría Informática con el fin de enmendar fallas en el momento oportuno, que ocasionarían la entrega de resultados que no sean

satisfactorios para el usuario final o fallas en las operaciones, que podrían provocar la pérdida total de la información.

COBIT es un Marco de Referencia basado en las mejores prácticas y sistemas de información de auditoría y control de procesos y objetivos de tecnología de la Información que pueden ser implementados para controlar, auditar y administrar la organización de tecnología de la Información. Particularmente ayudará a entender y administrar los riesgos relacionados con la tecnología de la Información, la relación entre los procesos de administración, las preguntas técnicas, la necesidad de controles, los riesgos y su gestionamiento.

1.2. Antecedentes

La Escuela Politécnica del Ejército, al ser una institución educativa que se mantiene a la vanguardia en cuanto al campo tecnológico, desde hace algunos años ha venido ejecutando varios proyectos relacionados con el área informática, con el objeto de apoyar a las diferentes actividades que desarrollan en la misma, algunos de estos proyectos ya han sido implementados por lo que se encuentran brindado servicios informáticos, los que deben estar acorde a los requerimientos exigidos por los usuarios finales, con el respectivo soporte técnico y la capacitación para su correcta utilización. Estos servicios se encuentran centralizados en la unidad de gestión de las tecnologías en información y comunicaciones, que se encarga de la administración y gestión de las actividades TI, es decir, el análisis, desarrollo e implantación de los sistemas requeridos en la Escuela Politécnica del Ejército y se preocupa

por el adecuado funcionamiento de las aplicaciones existentes, las redes y comunicaciones.

1.3. Justificación

Una Auditoría de Sistemas permite la identificación de fallas, riesgos y el planteamiento de medidas correctivas; que de acuerdo a los antecedentes comentados anteriormente deben ser evaluados constantemente, la calidad de servicios que las aplicaciones e infraestructura tecnológica brindan a los usuarios finales, que se cuenten con políticas y estándares que permitan la pronta gestión de errores y corrección de problemas, y con planes de continuidad y contingencia que garanticen la continuidad de las operaciones en caso de desastres que puedan ocasionar la paralización total o parcial de los servicios tecnológicos e inclusive la pérdida de información.

Un proceso de Auditoría Informática tiene como objetivos la implantación de nuevos y mejores controles, que permitan entregar servicios tecnológicos con calidad y eficiencia, que a su vez permitirá que la Escuela Politécnica del Ejército alcance un mejor posicionamiento y acreditación dentro de las instituciones de este ramo tanto dentro como fuera del país, apoyando de esta manera a los distintos procesos que esta emprendiendo para alcanzar la visión que se ha planteado.

1.4. Objetivos del proyecto

1.4.1. Objetivo General

Realizar una Auditoría Informática de la Escuela Politécnica del Ejército, del dominio de Entrega de Servicios y Soporte definido en el modelo de Objetivos de Control COBIT (Control Objectives For Information and Related Technology), con el fin de determinar las medidas y controles adecuados para la correcta entrega de servicios tecnológicos, soporte técnico, capacitación y continuidad de las operaciones del Sistema de Información de la Escuela Politécnica del Ejército.

1.4.2. Objetivos Específicos.

- Presentar el marco teórico del Modelo COBIT.
- Describir la situación actual del área informática, las actividades y esfuerzos necesarios para lograr los objetivos propuestos de la Escuela Politécnica del Ejército.
- Evaluar la eficiencia y eficacia con que los Sistemas de Información, apoyan en la toma de decisiones a la empresa, considerando:

i) El nivel de detalle provisto por los "Objetivos de Control" y las "Directrices de Administración" de COBIT, principalmente enfocados en los criterios de efectividad, disponibilidad, confidencialidad e integridad.

ii) Políticas, procesos y procedimientos y prácticas de trabajo que serán evaluados a diferentes niveles de la organización, desde la Administración TI (Tecnología de Información) hasta el staff operacional, y complementando con trabajo más detallado en el ámbito de las diferentes plataformas operativas.

- Aplicar el Modelo COBIT en la auditoría de sistemas para la Escuela Politécnica del Ejército.

1.5. Alcance

El proyecto de plan de tesis "EVALUACIÓN Y AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO: DOMINIO ENTREGA DE SERVICIOS Y SOPORTE", realizará la revisión de los procesos para la entrega de servicios tecnológicos, capacitación y entrenamiento de los usuarios, soporte técnico y la continuidad de las operaciones puesto que se enfoca al dominio de Entrega de Servicios y Soporte.

De acuerdo a lo enunciado anteriormente, se procederá inicialmente con la recolección, agrupación y evaluación de evidencias para determinar la manera en la que se encuentran diseñados e implementados los controles del dominio Entrega de Servicios y Soporte en la Escuela Politécnica del Ejército, lo que nos dará una visión actual del sistema informático, para luego proceder a realizar las pruebas para comprobar si estos controles se están cumpliendo, posteriormente procederemos a definir los riesgos que

conlleva el ineficaz cumplimiento de estos controles o su falta de implementación, para por último emitir las recomendaciones que permitan mejorar el desempeño de los servicios e infraestructura tecnológica de la Escuela Politécnica del Ejército.

Este proyecto de tesis se ejecutará en la Escuela Politécnica del Ejército, con una duración de 22 semanas al final de las cuales se obtendrá un informe final en el que consten las condiciones encontradas y las respectivas recomendaciones de mejora para que puedan ser aplicadas según el criterio de las autoridades de la Escuela Politécnica del Ejército.

1.6. Metodología

La metodología en la que se basará el presente proyecto es COBIT, que ha sido escogida principalmente por su facilidad de adaptación a cualquier tipo de negocio, por lo que no presentará ninguna dificultad la adaptación para la revisión de los Sistemas de Información de la Escuela Politécnica del Ejército, además puesto que COBIT (Control Objectives For Information an Related Technology), es un modelo desarrollado basándose en las mejores prácticas de seguridad tecnológica y administración y control de la tecnología de la información (TI).

CAPÍTULO II

MARCO TEÓRICO DE REFERENCIA

2.1. Auditoría Informática

2.1.1. Introducción

Actualmente en todas las empresas y negocios de cualquier tamaño sus operaciones y procedimientos dependen de los sistemas informáticos, ya que gracias a ellos las organizaciones pueden realizar sus operaciones de manera más eficiente para brindar mejores servicios a sus clientes y conseguir más ventajas sobre sus competidores.

Las facilidades que brindan los sistemas informáticos pueden tener como inconveniente hacer más vulnerable la información importante de las organizaciones, por lo que se deben implantar controles para mantener segura la información y por ende se requiere de auditores especializados en sistemas informáticos que prueben que estos controles son efectivos y permiten que la información se procese de manera correcta. En consecuencia de esta situación se crea la necesidad de realizar periódicamente evaluaciones a los sistemas, o también llamadas, auditorías informáticas, con las cuales se pretende identificar y evaluar los controles implantados en los sistemas y minimizar los riesgos a los cuales las organizaciones que dependen de los sistemas informáticos se encuentran expuestas.

Una auditoría de sistemas es un proceso de revisión de la manera en la que se están administrando actualmente los sistemas y los controles implantados en los mismos, basado en un criterio o modelo de control y gobierno de TI[1] establecido (p. ej. COBIT, ITIL[2], ISO[3]), recolección de evidencias significativas y la emisión de una opinión independiente acerca de los controles evaluados. Esta opinión debe ser revisada por la gerencia de la entidad auditada, quien debe definir si está de acuerdo con la misma, puesto que en caso de estar en desacuerdo el auditor debe realizar una evaluación más exhaustiva a los puntos en desacuerdo, siendo este un escenario poco probable y deseado ya que los resultados emitidos por el auditor deben ser verificables por medio de las evidencias recolectadas que deben estar de acuerdo con las observaciones emitidas.

2.2. Ambiente de control

Basados en el "INFORME COSO[4] (COMMITTEE OF SPONSORING ORGANIZATIONS)" en el que se define un marco conceptual del control interno común para todas las organizaciones, que satisface las demandas generalizadas de todos los sectores involucrados, se identifica que el marco integrado de control consta de cinco componentes que son:

[1] TI: Tecnologías de Información.
[2] ITIL: Conjunto de bibliotecas que reúnen las mejores prácticas para la gestión de servicios de IT agrupadas en dos áreas Soporte al Servicio, Entrega al Servicio.
[3] ISO:Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar e implantar o mantener la seguridad de una organización
[4]COSO: Comité de las Organizaciones Auspiciantes de Control Interno.

- Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Monitoreo

Componentes de los cuales el Ambiente de Control constituye la base fundamental de los otros cuatro, ya que se refiere a la historia y cultura de la organización, es decir, integridad, valores éticos y competencias de las personas de la entidad, y el ambiente en el cual estas personas llevan a cabo sus funciones, características fundamentales en el sistema de control interno, sin las cuales los otros componentes colapsarían. Además dentro del Ambiente de Control se incluye la filosofía y estilo de operar de la gerencia, que influencian a la cultura, por ejemplo la asignación de autorizaciones y responsabilidades, desarrollo de sus empleados y las recomendaciones de la mesa directiva.

De acuerdo a esto es necesario realizar evaluaciones al ambiente de control que permitan identificar los riesgos y definir los controles para neutralizarlos, puesto que el núcleo principal de control son las personas, quienes si no tienen suficiente integridad, valores éticos y competencias, el resto de procesos posiblemente no funcionarán, por lo cual debe establecerse un adecuado ambiente de control sobre el que se desarrollan las operaciones de la organización evaluada.

2.3. El proceso de la auditoría Informática

El proceso de la auditoría informática es similar al de auditoría de estados financieros, en la cual los objetivos principales son, salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales, y la utilización de los recursos con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias. De manera semejante como sucede con la auditoría financiera en la auditoría informática se recogen evidencias, las cuales se analizan para identificar, la manera en la cual son salvaguardados los activos computarizados, la forma en la que se mantiene la integridad de los datos, como se logran los objetivos de la organización eficazmente y se usan los recursos consumidos eficientemente, pero esto no es un trabajo que se debe realizar de manera desorganizada sino que debe realizarse siguiendo procedimientos ordenados en las siguientes fases:

- Planificación de la Auditoría Informática
- Ejecución de la Auditoría Informática
- Finalización de la Auditoría Informática, las cuales detallaremos a continuación.

Es importante la participación de todas las áreas de la organización durante las fases del proyecto de auditoría puesto que son una pieza

fundamental para alcanzar objetivos concernientes a toda la organización como por ejemplo:

- Seguimiento a proyectos relacionados con tecnología informática
- Verificación y aseguramiento del cumplimiento de políticas inherentes a la tecnología informática.
- Aspectos de interés tecnológico para la gerencia.
- Apoyo en la definición, implantación y seguimiento de políticas, controles y procedimientos de auditoría financiera relacionados directa o indirectamente con la tecnología informática.
- Planes de capacitación en el uso y entendimiento de software de auditoría, herramientas de productividad, bases de datos y equipos de cómputo.
- Identificación de controles de interés para otros tipos de auditoría cuando evalúan áreas del negocio que se apoyan en informática.
- Apoyo en la definición, implantación y seguimiento de políticas, controles, procedimientos y estándares relativos a la administración informática.

2.3.1. Planificación de la auditoría Informática

Como todo proyecto implantado dentro de una organización, el proyecto de auditoría informática debe iniciar con una fase de

planeación en la cual participen todas las áreas de la organización para identificar los recursos necesarios que permitirán llevar a cabo este proyecto, como son, objetivos que se pretenden alcanzar con el proyecto, análisis costo/beneficio, personal humano que intervendrá en el proyecto, marco de referencia de Auditoría Informática que se va a utilizar (p. Ej. COBIT), basándose en varios objetivos fundamentales que son:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo
- Evaluación del proceso de datos,

Lo cual se resume en obtener un conocimiento inicial de la organización a evaluar, con especial énfasis en sus procesos informáticos basados en evaluaciones administrativas realizadas a los procesos electrónicos, sistemas y procedimientos, equipos de cómputo, seguridad y confidencialidad de la información, y aspectos legales de los sistemas y la información.

Una vez que se ha obtenido un conocimiento inicial de la organización se procede a establecer metas, programas de trabajo de auditoría, personal que intervendrá en el proyecto, presupuesto financiero, y las fechas y la manera como se presentarán los informes de las actividades de cumplimiento del proyecto, basados en la realidad de la organización evaluada.

También dentro del proceso de planificación de la Auditoría Informática se debe incluir y documentar por lo menos los siguientes aspectos:

- Se debe definir los objetivos y el alcance del trabajo.
- El relevamiento de información de las actividades a auditarse en la que se apoyará el análisis.
- Los recursos que se necesitarán para llevar a cabo el proyecto de auditoría.
- Los canales de comunicación necesarios entre los involucrados en el proyecto de auditoría.
- El procedimiento apropiado a utilizarse para realizar una inspección física que permita la obtención del conocimiento de la manera como se ejecutan las actividades y controles a auditar, así como de las áreas críticas en las que se debe poner mayor énfasis al realizar la auditoría.
- La declaración por escrito del programa de auditoría.
- Determinar los responsables de analizar los resultados de la auditoría, los plazos de tiempo en los que se deberá llevar a cabo el proyecto de auditoría y la forma en la que se presentarán los resultados de la misma.
- La aprobación del plan de trabajo de auditoría.

Una vez que se han definido estos aspectos se debe proceder a la realización de una fase de revisión preliminar, que es una fase de análisis inicial de los controles implantados en la organización por

medio de entrevistas al personal utilizando cuestionarios, revisión de documentación. Evidencias que le permitirán al auditor definir la manera en la que procederá durante la duración del proyecto de auditoría, pudiendo este decidirse por una de las siguientes 3 estrategias:

- Volver a la parte de planificación de la auditoría para rediseñar el trabajo de auditoría debido a que el personal elegido no cuenta con las suficientes capacidades técnicas.

- Proseguir con el desarrollo del Plan de Auditoría basándose en una estrategia de confianza en controles internos para lo cual se deberá revisar que los controles se encuentren adecuadamente implementados y se puedan reducir las pruebas sustantivas.

- Proseguir con el trabajo de auditoría con una estrategia de no confianza en controles debido a que puede ser más eficiente el realizar pruebas sustantivas desde el punto de vista costo-beneficio o que la implantación de controles informáticos produzcan un sobrecontrol cubriendo el mismo ámbito que los controles manuales de usuario.

2.3.2. Ejecución de la auditoría Informática

La ejecución de la auditoría Informática consiste principalmente en la recolección de información y evidencias suficientes, para fundamentar los comentarios, conclusiones y recomendaciones con respecto a la Administración de TI, lo cual se realiza utilizando diversas técnicas como las siguientes:

- Entrevistas
- Simulación
- Cuestionarios
- Análisis de la información documental entregada por el auditado
- Revisión y Análisis de Estándares
- Revisión y Análisis de la información de auditorías anteriores

El análisis de esta información deberá ser realizado utilizando el criterio profesional adquirido por la experiencia del equipo encargado del Proyecto de Auditoría, identificando cuando las evidencias obtenidas son suficientes para evidenciar el adecuado conocimiento de la entidad.

La información recabada debe ser completa y detallada para que pueda ser comprendida por el equipo de auditoría y permita la obtención de comentarios, conclusiones y recomendaciones, mediante su revisión.

La evidencia se clasifica de la siguiente manera:

a. Evidencia documental.

b. Evidencia física.

c. Evidencia analítica.

d. Evidencia testimonial.

Una vez que se ha recolectado información confiable sobre la cual se pueda evaluar a la organización, se debe proceder a probar la manera en la que han sido diseñados los controles en la organización, para lo cual el equipo de auditoría verificará la información procesada por medios electrónicos y utilizará métodos especializados de informática.

Se debe tomar en cuenta que para dar una opinión favorable acerca de los sistemas y determinar su confiabilidad en el procesamiento de la información, es necesario efectuar una revisión de los controles generales del computador, puesto que en la confiabilidad de ellos se basa el buen funcionamiento de los sistemas de aplicación.

2.3.3. Finalización de la auditoría Informática

El resultado de la auditoría Informática, se materializa en un informe de conclusiones que se debe redactar y entregar a la administración de la organización para su evaluación, por lo que

antes de la emisión del informe final se debe realizar varios borradores, que serán analizados en conjunto entre los auditores y la administración de la organización, para descubrir fallos en la evaluación de auditoría debido a la incorrecta comprensión de la organización por parte de los auditores.

La estructura del informe de conclusiones a entregarse a la administración de la organización es la siguiente:

- Debe iniciar con el período de tiempo en el que se ha realizado la evaluación.

- Indicar el equipo de auditoría que ha intervenido en la evaluación.

- Incluir los objetivos que se pretendieron alcanzar con la evaluación de auditoría.

- Posteriormente se debe indicar el Dominio del cual se ha realizado la evaluación de auditoría de acuerdo al marco de trabajo que utilizado, en este caso COBIT.

- Indicar el criterio sobre el cual se ha realizado la evaluación, en este caso el criterio recomendado por los objetivos de control definidos en COBIT.

- Identificar la condición en la que se encontró a la organización, o también conocida como observación.

- Identificar las causas que provocan la situación observada en la organización.

- Se debe incluir los efectos que puede provocar el hecho que se mantenga la situación actual identificada por los auditores en la organización.

- Incluir las recomendaciones que la administración debería adoptar para cumplir con el criterio de los objetivos de control, que permita reducir la posibilidad de ocurrencia de los efectos anotados anteriormente.

- Por último se debe incluir el punto de vista de la administración en la que se indique si tomarán en cuenta las recomendaciones emitidas y las fechas en las cuales estas serán adoptadas, lo cual facilitará la ejecución de un seguimiento posterior de la auditoría.

Se debe tomar en cuenta que en el informe final a ser presentado a la administración debe incluir los hechos importantes encontrados, puesto que la inclusión de objetivos irrelevantes no representa valor a la evaluación.

Un diagrama que resume el proceso de auditoría informática se puede observar en el Anexo A.

2.4. Clasificación de los controles TI

Al momento de realizar un proyecto de auditoría se desarrollan gran variedad de actividades de control para verificar la exactitud, integridad y autorización de las transacciones. Estas actividades pueden agruparse en dos grandes conjuntos de controles de los sistemas de información, los cuales son, controles de aplicación y los controles generales de la computadora. Sin embargo estos dos conjuntos de controles se encuentran estrechamente relacionados, puesto que los controles generales de la computadora son normalmente necesarios para soportar el funcionamiento de los controles de aplicación, además que de la efectividad de ambos depende el aseguramiento del procesamiento completo y preciso de información.

Por ejemplo, controles de seguridad de acceso efectivo para reducir el riesgo de acceso no autorizado a información sensible soportan el funcionamiento de los controles de aplicación.

2.4.1. Controles de Aplicación

La evaluación de los controles de aplicación es una actividad sumamente importante, puesto que la consistencia de la información

significativa para la organización depende de la seguridad de los sistemas en los cuales se procesa.

Los controles de aplicación son procedimientos manuales o automatizados que operan típicamente a nivel de los procesos de la organización. Los controles de aplicación pueden ser de naturaleza preventiva o de detección y están diseñados para asegurar la integridad de la información que se procesa en ellos. Debido a lo cual, los controles de aplicación se relacionan con los procedimientos utilizados para iniciar, registrar, procesar e informar las transacciones de la organización. Estas actividades de control ayudan a asegurar que las transacciones ocurridas, estén autorizadas y completamente registradas y procesadas con exactitud. Por ejemplo podemos incluir los controles implantados para verificar la validez del ingreso de datos dentro de los sistemas, controles que podemos evaluar mediante el seguimiento manual de los informes de excepción o la corrección en el punto de entrada de datos.

Debido al tamaño y complejidad de varios sistemas no siempre se los podrá revisar a todos, por lo que es necesario evaluar los sistemas de aplicación para considerar en el plan de auditoría los sistemas de aplicación que tienen un efecto significativo en el desarrollo de las operaciones de la organización, con el fin de realizar un análisis más profundo de estos sistemas. Existen varios parámetros que se debe

considerar para calificar los sistemas de aplicación, los cuales son los siguientes:

- Importancia de las transacciones procesadas.

- Potencial para el riesgo de error incrementado debido a fraude.

- Si el sistema sólo realiza funciones sencillas, como acumular o resumir información o funciones más complejas, como la iniciación y ejecución de transacciones.

- Tamaño y complejidad de los sistemas de aplicación.

Esta evaluación servirá de igual forma para definir el plan de auditoría a seguir, ya que si un sistema de aplicación es muy grande y complejo, sería conveniente dividirlo en subsistemas de acuerdo con las actividades principales de la organización que soporta cada subsistema para cubrir cada uno por separado. Por ejemplo, un sistema que efectúa transferencias electrónicas de fondos por pagos de órdenes de compra, a las cuentas bancarias de los proveedores, sería considerado un sistema complejo.

2.4.2. Controles Generales

Los controles generales de la computadora son políticas y procedimientos que se relacionan con muchos sistemas de aplicación y soportan el funcionamiento eficaz de los controles de aplicación, ayudando a asegurar la operación continua y apropiada de los sistemas de información. Los controles generales de la computadora mantienen la integridad de la información y la seguridad de los datos. Es por esto que antes de realizar una evaluación de los controles de aplicación, normalmente se actualiza la comprensión general de los controles del ambiente de procesamiento de la computadora y se emite una conclusión acerca de la eficacia de estos controles. Las actividades que se realizan para la evaluación de estos controles inician con entrevistas a la administración, luego de las cuales se tendrá un mejor capacidad para comprender y definir la estrategia y las pruebas que realizaremos sobre los controles. Posteriormente se debe determinar si los controles generales de la computadora se diseñan e implementan para soportar el procesamiento confiable de la información respecto a los controles que se han identificado, para lo cual se debe realizar lo siguiente:

- Evaluación del diseño de los controles, en la que se determinará que los controles evitan los riesgos para los que fueron diseñados.

- Determinar si los controles se han implementado, lo cual consiste en evaluar si los controles que se han diseñado, se están utilizando durante el tiempo de funcionamiento de la organización.

Es importante indicar que si durante el proceso de evaluación de estos controles se concluye que no son eficaces, se debe realizar indagaciones para identificar controles alternos que pueden ser eficaces.

CAPÍTULO III

MODELO COBIT

3.1. Introducción

La evolución de los sistemas de información y comunicación en el Ecuador, ha generado la necesidad de implementar la gestión de sistemas en las diferentes instituciones; para obtener seguridad, confiabilidad y escalabilidad en todos los ámbitos que a estas conciernen. Lo que provoca que las empresas cada vez necesiten más control sobre sus datos y los sistemas que estas utilizan.

De acuerdo a lo expuesto, es necesaria la utilización de una herramienta o modelo de control que ayude a la gerencia a comprender y administrar los riesgos asociados con tecnologías de información y tecnologías relacionadas.

Es por esto que en el presente proyecto de tesis se utilizó el Modelo COBIT versiones 3.0 y 4.0 ya que permite un enfoque distinto y actual de los sistemas, por cuanto los mira en su ámbito global, formado por procesos manuales e informáticos. Además incorpora aspectos de gestión de la calidad total, reingeniería de empresas e integra los dos modelos de control: los orientados a las Tecnologías de Información y los orientados a los Objetivos Empresariales.

El Modelo COBIT (Control Objetives for Information and Related Technologies) es un modelo de referencia basado en las mejores prácticas, sistemas de información de auditoría, control de procesos y objetivos de TI. El

cual tiene como objetivo principal el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de tecnologías de información.

El Modelo COBIT sirve para salvar las brechas entre riesgos de negocios, necesidades de control y aspectos técnicos y está dirigido a los auditores informáticos, además permite determinar el alcance de la tarea de auditoría e identificar los controles mínimos. Además es posible emplearla como una herramienta de autoevaluación del Área Informática ya que es aplicable a todos los tamaños y tipos de organización.

Se adoptó las versiones 3.0 y 4.0 del Modelo COBIT puesto que una vez que se realizó un análisis de todas las versiones de COBIT se identificaron las siguientes características en cada una de ellas.

- Versión 1.0: uso de estándares internacionales, las pautas y la investigación en las mejores prácticas condujeron al desarrollo de los objetivos del control.

- Versión 2.0: análisis de fuentes internacionales dedicados a la compilación, revisión e incorporación apropiada de los estándares técnicos internacionales, códigos de la conducta, estándares de calidad, estándares profesionales, y los requisitos de la industria, como se relacionan con el marco y con los objetivos del control individual.

- Versión 3.0: consiste en proveer a la gerencia un uso del marco de referencia, COBIT, para que de él pueda determinar las mejores opciones a ser puestas en práctica y las mejoras del control sobre su información y tecnología relacionada. Así como las pautas para la gerencia que incluyen modelos de madurez, factores críticos de éxito, indicadores dominantes de la meta e indicadores dominantes del funcionamiento relacionados con los objetivos del control.

- Versión 4.0: acentúa el cumplimiento regulador, ayuda a las organizaciones a aumentar el valor logrado de TI, ya que posee un enfoque más gerencial que permite la alineación y simplifica la puesta en práctica del Modelo COBIT.

Luego de este análisis se concluyó que las versiones 3.0 y 4.0 se basan en los principios de, "proporcionar la información que la empresa requiere para lograr sus objetivos"[5] y que "la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información"[6].

3.2. Productos COBIT

En el Modelo de COBIT los productos se han definido en tres niveles, los mismos que dan soporte a:

[5] COBIT versión 4.0
[6] COBIT versión 4.0

- Administración y consejos ejecutivos.
- Administración del negocio y de Tecnología de Información.
- Profesionales de gobierno, aseguramiento, control y seguridad, como se detalla en la siguiente figura.

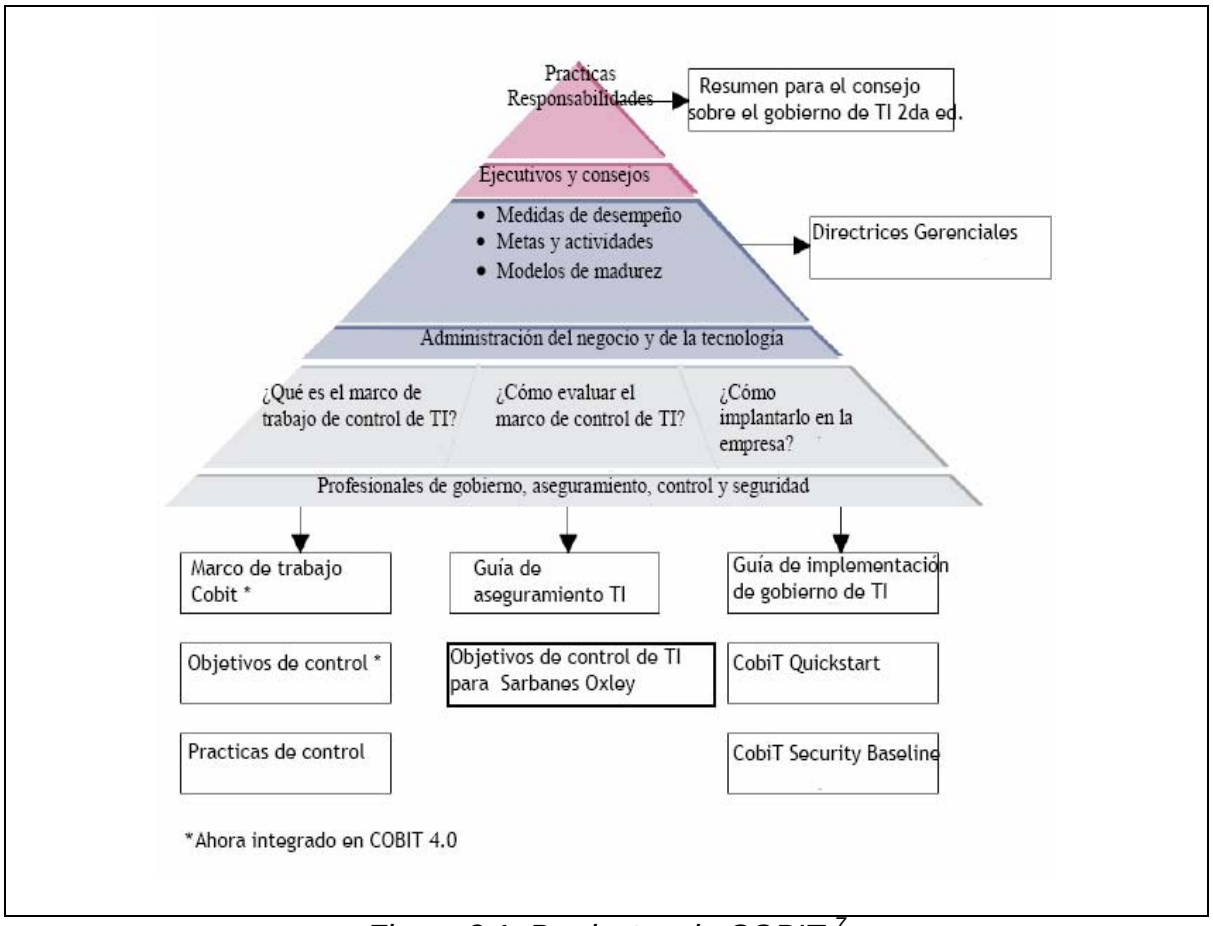

Figura 3.1. Productos de COBIT [7]

3.2.1. Resumen Ejecutivo

El Resumen Ejecutivo consiste en una descripción que proporciona una conciencia cuidadosa y el entendimiento de los conceptos claves del COBIT, es decir, un entendimiento más detallado de los conceptos y principios de auditoría de Sistemas, identificando los cuatro dominios del COBIT y sus 34 procesos de TI

[7] COBIT 4.0 español, IT Governance Institute, ISBN 1-933284-37-4, página 8.

correspondientes. Además ayuda a los ejecutivos a comprender porqué el gobierno de TI es importante, sus intereses y sus responsabilidades para su correcta administración.

3.2.2. Marco Referencial

El Marco Referencial COBIT es la base para el desarrollo de los demás elementos COBIT. El marco referencial explica como los procesos de TI deben entregar la información, que el negocio requiere para alcanzar sus objetivos, proporcionando al propietario de los procesos del negocio herramientas que faciliten el cumplimiento de esta responsabilidad.

El Marco Referencial permite también definir si la información procesada para cumplir con los objetivos del negocio se está adaptando a los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad), así como también define cuales de los recursos de TI (sistemas de aplicación, tecnología, instalaciones, datos) son importantes para apoyar a los objetivos de negocio.

3.2.3. Objetivos de Control

Un Objetivo de Control en TI es la definición del resultado o propósito que se desea alcanzar siguiendo procedimientos de control específicos dentro de una Actividad de Control de TI. Los Objetivos de Control de COBIT son los

requerimientos mínimos que debe cumplir un control de cada proceso de TI, para que sea definido como efectivo.

Los Objetivos de Control están definidos y orientados a los procesos, por medio del principio de reingeniería de negocios. Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. A los que se les debe analizar como un todo, ya que representan las características de un proceso bien administrado.

3.2.4. Guía o Directriz de Auditoría

Las Guías de Auditoría indican pautas y recomendaciones mediante las que la gerencia de la entidad auditada puede cumplir de una manera más óptima con los Objetivos de Control.

Estas Guías de Auditoría provistas por COBIT no son específicas sino son acciones genéricas que se pueden poner en práctica en mayor o menor grado dependiendo de la entidad y están orientadas para proveer a la gerencia actividades que le permitan, mantener bajo control la información de la empresa y sus procesos relacionados, monitorear el logro de las metas organizacionales, monitorear el desempeño de cada proceso de TI y llevar a cabo un benchmarking de los logros organizacionales.

3.2.5. Prácticas de Control

Las Prácticas de Control proveen guías para diseñar controles y cómo implementarlos, puesto que ayudan al personal encargado de diseñar e implementar controles específicos a administrar riegos en proyectos de TI. Además las Prácticas de Control ayudan a mejorar el rendimiento de TI ya que definen mejores prácticas para evitar el incumplimiento o mal uso de controles internos.

3.2.6. Guías de Administración

Las Guías de Administración o directrices gerenciales, contienen modelos de madurez asociado al gobierno de TI, que sirven para determinar en que posición se encuentra la organización. También las Guías de Administración proveen factores críticos de éxito específico, indicadores claves por objetivo e indicadores clave de desempeño, que son las mejores prácticas administrativas para alcanzar los Objetivos de Control en TI.

3.2.7. Conjunto de Herramientas de Implementación

El Conjunto de Herramientas COBIT proporciona lecciones aprendidas por aquellas organizaciones que aplicaron COBIT obteniendo resultados exitosos, las cuales pueden ser utilizadas por otras organizaciones.

Estas herramientas incluyen dos particularmente útiles:

- Diagnóstico de Sensibilización Gerencial (Management Awareness Diagnostic)
- Diagnóstico de Control en TI (IT Control Diagnostic), para proporcionar asistencia en el análisis del ambiente de control de TI en una organización.

3.3. Generalidades del modelo COBIT

3.3.1. Marco de Trabajo de COBIT

El modelo de COBIT fue creado para ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

3.3.1.1. Orientado a Negocios

El Modelo de COBIT es orientado a negocios ya que se encuentra diseñado para ser una guía para la gerencia, propietarios de los procesos de negocio, los proveedores de servicios, usuarios y auditores de TI. Además es el enfoque de control en TI que se lleva a cabo visualizando la información necesaria para dar soporte a los procesos del negocio. Siendo la Información el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos TI.

El Marco de Trabajo de COBIT ofrece herramientas para garantizar la alineación de la administración de TI con los requerimientos del negocio, basados en los principios básicos de COBIT. (Ver Figura 2)

Figura 3.2. Principios Básicos de COBIT[8]

En donde los requerimientos de información del negocio deben adaptarse a ciertos criterios de información, para que la misma permita cumplir con los objetivos de la organización, los cuales son:

- Efectividad: la información relevante y pertinente al proceso del negocio existe y es entregada a tiempo, correcta, consistente y utilizable.

- Eficiencia: es la optimización (más económica y productiva) de los recursos que se utilizan para la provisión de la información.

[8] COBIT 4.0 español, IT Governance Institute, ISBN 1-933284-37-4, página 15.

- Confidencialidad: es relativo a la protección de información sensitiva de acceso y divulgación no autorizada.

- Integridad: se refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas del negocio.

- Disponibilidad: accesibilidad a la información para los procesos del negocio en el presente y en el futuro, también salvaguardar los recursos y capacidades asociadas a los mismos.

- Cumplimiento: son las leyes, regulaciones, acuerdos contractuales a los que el proceso del negocio esta sujeto.

- Confiabilidad de la Información: proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con las responsabilidades de los reportes financieros.

Una vez que las metas del negocio se encuentran alineadas y han sido definidas, requieren ser monitoreadas para garantizar que la entrega cumple con las expectativas del negocio.

Los recursos de TI son:

- Datos: Todos los objetos de información interna y externa, estructurada o no, gráficas, sonidos, etc.

- Aplicaciones: los sistemas de información, que integran procedimientos manuales y sistematizados.

- Tecnología: incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

- Instalaciones: son recursos necesarios para alojar y dar soporte a los sistemas de información.

- Recursos Humanos: habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

Se deben gestionar todos los recursos de TI mediante un conjunto de procesos agrupados para lograr metas de TI que proporcionen la información que el negocio necesita para alcanzar sus objetivos. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT. (Ver figura 3).

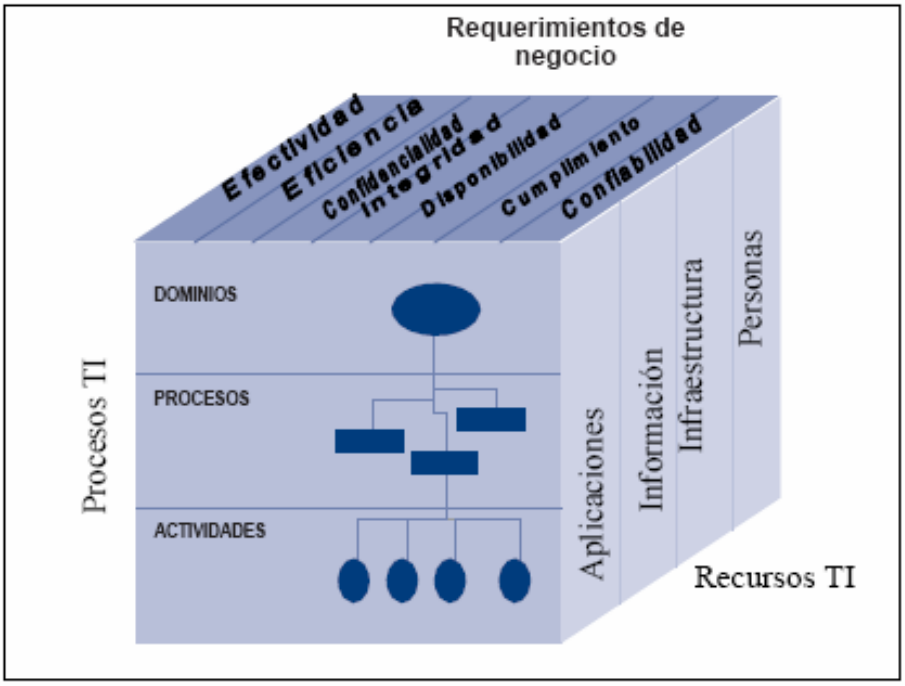

Figura 3.3. Cubo COBIT[9]

3.3.1.2. Orientado a Procesos

Se pueden diferenciar tres niveles de actividades en un proceso de TI:

- El nivel superior de agrupación son los dominios que son los procesos agrupados, los dominios en una estructura organizacional se denominan dominios de responsabilidad y se alinean con el ciclo de vida o administrativo de los procesos TI.

- En el nivel intermedio se encuentran los procesos, que son un conjunto de varias tareas y actividades.

[9] COBIT 4.0 español, IT Governance Institute, ISBN 1-933284-37-4, página 25.

- En el nivel bajo se hallan las actividades y tareas necesarias para alcanzar un resultado medible, es decir, son las actividades más discretas, como se puede observar en la siguiente figura.

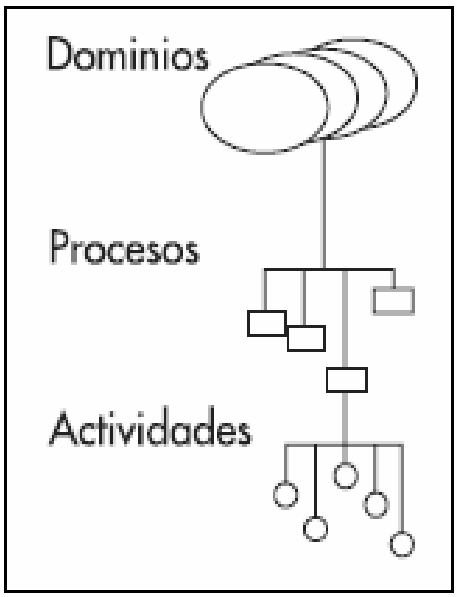

Figura 3.4. Niveles de actividades de TI.[10]

COBIT define las actividades de TI en un modelo de procesos en cuatro dominios. Estos dominios son:

- Planeación y Organización: cubre las estrategias, las tácticas, y la manera de identificar la forma en que TI puede contribuir al logro de los objetivos del negocio.

[10] COBIT 4.0 español, IT Governance Institute, ISBN 1-933284-37-4, página 25.

- Adquisición e Implementación: cubre las estrategias de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio.

- Entrega de Servicios y Soporte: incluye los procesos de entrega o distribución desde las operaciones tradicionales hasta el entrenamiento tomando en cuenta aspectos de seguridad y continuidad de las operaciones. Con el fin de entregar servicios. En donde se incluye el procesamiento de datos, los sistemas de aplicación, clasificados de forma frecuente como controles de aplicación.

- Monitorear y Evaluar: se debe evaluar de forma regular los procesos de control independientes, los mismos que son definidos por auditorías externas e internas o por fuentes alternativas. También abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno de TI.

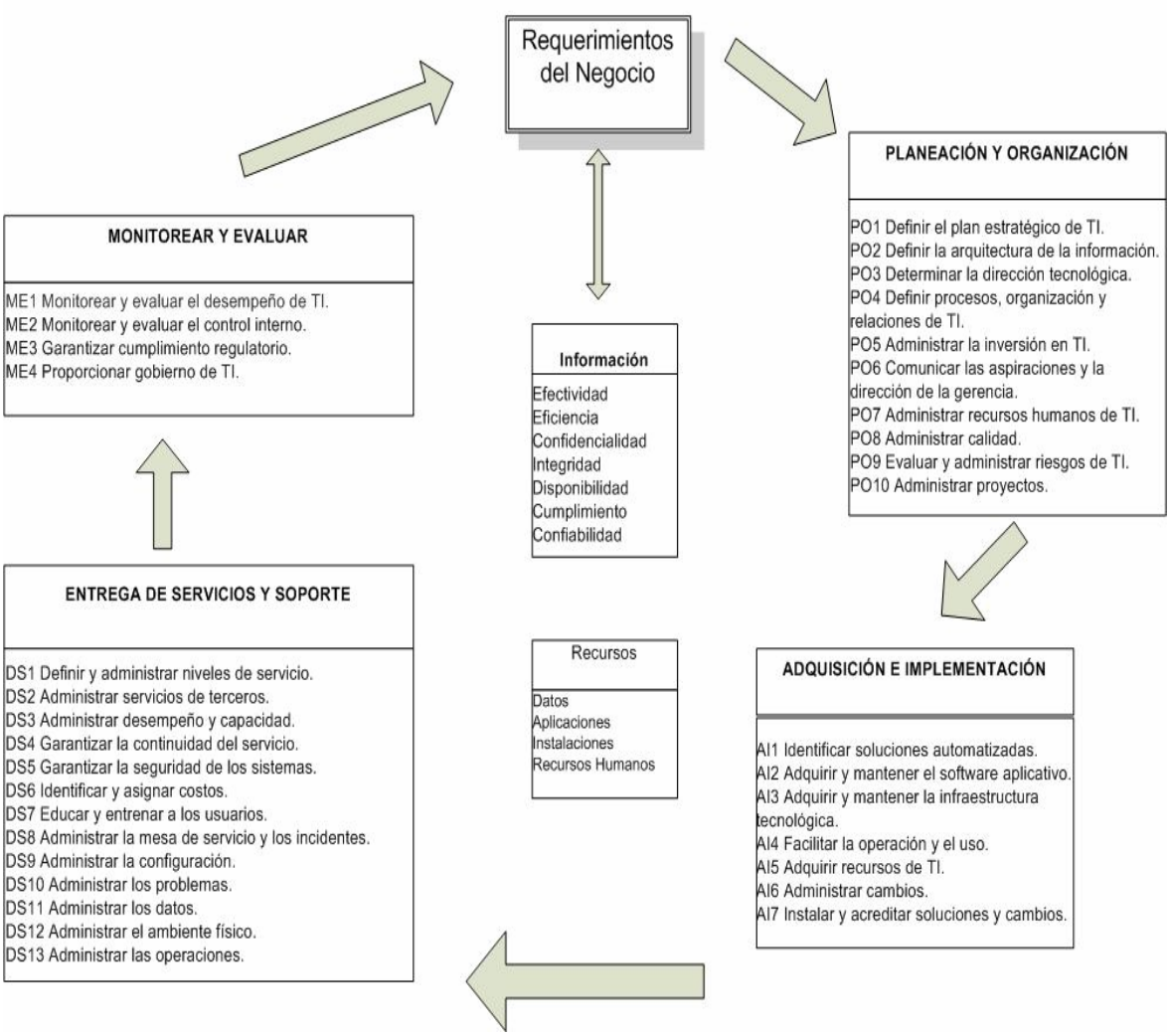

Fig. 3.5. Resumen de los Procesos de TI de COBIT Definidos en los cuatro Dominios[11]

3.3.1.3. Basado en Controles

El Modelo de COBIT se encuentra basado en los Objetivos de Control de TI, que es el resultado que se desea lograr al aplicar los procedimientos de control en las actividades de TI. Los Objetivos de Control son los requerimientos mínimos de un control efectivo de cada uno de los procesos de TI.

[11] COBIT 4.0 español, IT Governance Institute, ISBN 1-933284-37-4, página 26

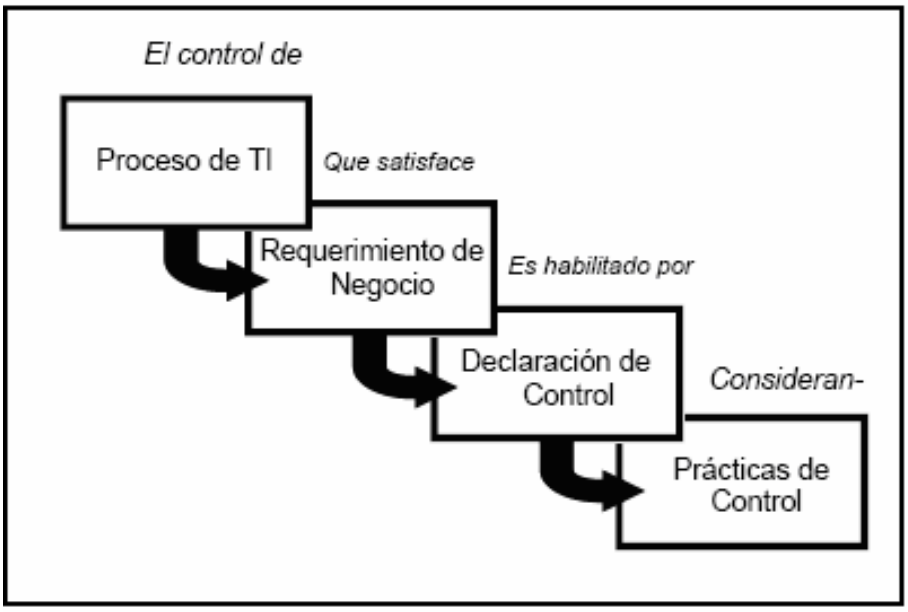

Figura. 3.6 Componentes de los Objetivos de Control[12]

Los Objetivos de Control se enfocan sobre objetivos 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.

3.3.1.4. Impulsado por Mediciones

Sirve para identificar cual es el estado de los sistemas de TI y decidir qué nivel de administración y control se debe realizar en el negocio. Basados en los siguientes temas que abarca COBIT:

- Modelos de madurez: ayudan a la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad del negocio.

[12] COBIT 3.0 Marco Referencial Español, IT Governance Institute**,** ISBN 1-933284-37-4, página 23

- Metas y mediciones de desempeño para los procesos de TI, que indican como los procesos satisfacen las necesidades del negocio y de TI. (balanced scorecard).

- Metas de actividades que faciliten el desempeño efectivo de los procesos.

3.4. Dominio Entrega de Servicios y Soporte

3.4.1. DS 1 DEFINICIÓN Y ADMINISTRACIÓN DE NIVELES DE SERVICIO

Establecer un entendimiento común del nivel de servicio requerido posibilitado por el establecimiento de acuerdos de nivel de servicio que formalizan los criterios de rendimiento contra los cuales se medirá la cantidad y la calidad del servicio que será medido, lo cual permita a la gerencia identificar deficiencias en el servicio prestado, enfocándose en la identificación de requerimientos de servicio.

En este proceso se toma en consideración los siguientes aspectos:

- Acuerdos o convenios formales
- Definición de responsabilidades
- Tiempos y volúmenes de respuesta
- Cargos
- Garantías de integridad.
- Acuerdos de confidencialidad

- Criterio de satisfacción del cliente
- Análisis costo-beneficio de los niveles de servicio requerido
- Monitoreo y reporte.

Los objetivos de control detallados de este proceso son:

DS 1.1. Marco de Referencia para el Acuerdo de Niveles de Servicio.

DS 1.2. Definición de Servicios.

DS 1.3. Procedimiento de Desempeño.

DS 1.4. Monitoreo y Reporte.

DS 1.5. Revisión de Acuerdos y Contratos de Nivel de Servicio.

DS 1.6. Programa de Mejoramiento del Servicio.

3.4.2. DS 2 ADMINISTRAR LOS SERVICIOS DE TERCEROS

La administración de servicios de terceros, se logra mediante una clara definición de roles, responsabilidades, y expectativas en los acuerdos con los proveedores. Este proceso se orienta a las relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.

Ya que con una buena administración de servicios de terceros se minimiza los riesgos del negocio asociados a los proveedores que no cumplen con los acuerdos.

En el proceso se toma en consideración lo siguiente:

- Acuerdos de servicio con terceras partes

- Administración de contrato
- Acuerdos de confidencialidad
- Requerimientos legales y regulatorios.
- Monitoreo y reporte de la entrega de servicio
- Análisis de riesgos de la empresa y de TI
- Ejecución de recompensas y sanciones
- Contabilidad organizacional interna y externa
- Análisis de costos y variaciones en los niveles de servicio

Los objetivos de control detallados de este proceso son:

DS 2.1. Interfases con Proveedores

DS 2.2. Relaciones con los Propietarios (usuarios dueños)

DS 2.3. Contratos con Terceros

DS 2.4. Calificación de Terceros

DS 2. 5. Contratos de Outsourcing

DS 2.6 Continuidad de Servicios

DS 2.7. Relaciones con la Seguridad

DS 2.8. Monitoreo

3.4.3. DS 3 ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD

Asegurar que la capacidad adecuada esté disponible y que se haga el mejor y el óptimo uso de ésta para satisfacer las necesidades requeridas de rendimiento a través de la recolección de datos, análisis y reporte sobre el rendimiento de los recursos. Con este proceso se provee un pronóstico de las necesidades futuras, basadas en los requerimientos de carga de

trabajo, almacenamiento y contingencias. Este proceso brinda seguridad en los recursos de información que soportan los requerimientos del negocio.

Se puede medir por medio del número de horas perdidas por usuario por mes, debidas a la falta de planeación de la capacidad, el porcentaje de picos donde se excede la meta de utilización.

En este proceso se toma en consideración los siguientes aspectos:

- Requerimientos de disponibilidad y desempeño
- Monitoreo y reporte automatizado
- Herramientas de modelado
- Administración de capacidad
- Disponibilidad de recursos
- Cambios en precio-rendimiento del hardware y software

Los objetivos de control detallados de este proceso son:

DS 3.1. Requerimientos de Disponibilidad y Desempeño

DS 3.2. Plan de Disponibilidad

DS 3.3. Monitoreo y Reporte

DS 3.4. Manejo Proactivo del Desempeño

DS 3.5. Pronóstico de Carga de Trabajo

DS 3.6. Administración de Capacidad de Recursos

3.4.4. DS 4 ASEGURAR EL SERVICIO CONTINUO

Asegurar que los servicios de TI estén disponibles cuando se requieran y que el impacto de su operación deficiente o interrumpida sea

mínimo en el negocio. Lo cual se hace posible a través del desarrollo y mantenimiento de un plan de continuidad de TI probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio.

Los aspectos a ser considerados en el proyecto de desarrollo y mantenimiento del Plan de Continuidad son:

- Clasificación de criticidad (severidad)
- Procedimientos alternativos
- Respaldo y recuperación
- Pruebas y entrenamiento sistemáticos y regulares
- Monitoreo y procesos de escalamiento
- Responsabilidades organizacionales internas y externas
- Activación de la continuidad del negocio, vuelta atrás (fallback) y plan de reactivación
- Actividades de administración de riesgos
- Análisis de puntos únicos de falla
- Administración de problemas

Los objetivos de control detallados de este proceso son:

DS 4.1. Marco de Referencia de Continuidad de Tecnología de información

DS 4.2. Estrategia y Filosofía del Plan de Continuidad de TI

DS 4.3. Contenido del Plan de Continuidad de TI

DS4.4. Reducción de requerimientos de Continuidad de Tecnología de información.

DS 4.5. Mantenimiento del Plan de Continuidad de Tecnología de Información.

DS4.6. Entrenamiento sobre el Plan de Continuidad de Tecnología de información.

DS 4.7. Distribución del Plan de Continuidad de TI

DS4.8. Procedimientos de respaldo de procesamiento alternativo para departamentos usuarios.

DS 4. 9. Recursos Críticos de Tecnología de Información

DS 4. 10. Sitio y Hardware de Respaldo

DS 4. 11. Almacenamiento de respaldo en el sitio alterno (Off-site)

DS 4. 12. Procedimiento de afinamiento del Plan de Continuidad

3.4.5. DS 5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad

Se toma en consideración los siguientes aspectos:

- Requerimientos de privacidad y confidencialidad
- Autorización, autenticación y control de acceso

- Identificación de usuarios y perfiles de autorización
- Necesidad de saber y necesidad de tener (need-to-know and need-to-have)
- Administración de llaves criptográficas
- Manejo, reporte y seguimiento de incidentes
- Prevención y detección de virus
- Firewalls
- Administración centralizada de seguridad
- Entrenamiento a los usuarios
- Herramientas para monitoreo del cumplimiento, pruebas de intrusión y reportes.

Los objetivos de control detallados de este proceso son:

DS 5.1. Administrar las medidas de seguridad.

DS 5.2. Identificación, Autenticación y Acceso

DS 5.3. Administración de Cuentas de Usuario

DS 5.4. Revisión Gerencial de Cuentas de Usuario

DS 5.5. Vigilancia de Seguridad

DS 5.6. Clasificación de Datos

DS 5.7. Reportes de Violación y de Actividades de Seguridad

DS 5.8 Confianza en Contrapartes

DS 5.9. Protección de las funciones de seguridad

DS 5.10. Prevención, Detección y Corrección de Software “Malicioso”

DS 5.11. Arquitectura de Firewalls y conexión a redes públicas

3.4.6. DS 6 IDENTIFICAR Y ASIGNAR COSTOS

Es necesario tener un sistema justo y equitativo para asignar costos de TI al negocio, el cual requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa.

Este proceso asegura un conocimiento correcto de los costos de los servicios de TI. Además incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios, que permita tomar decisiones más acertadas respecto al uso de los servicios de TI.

Para este proceso se toma en consideración los recursos identificables y medibles, los procedimientos y políticas de cargo, la tarifa de cargo, verificación de comprensión de beneficios.

Los objetivos de control detallados de este proceso son:

DS 6.1. Elementos Sujetos a Cargo o Cobro por su Uso

DS 6.2. Procedimientos de Costeo

DS 6.3. Procedimientos de Reversión de Cargos y Facturación a Usuarios

3.4.7. DS 7 EDUCAR Y ENTRENAR A LOS USUARIOS

Para una efectiva educación de todos los usuarios de sistemas de TI, incluyendo al personal dentro de TI, se requiere identificar las necesidades de entrenamiento de cada grupo de usuarios. Se debe identificar las necesidades incluyendo la definición y ejecución de una estrategia para llevar a cabo un buen entrenamiento que permita medir los

resultados. El tener un proceso efectivo de entrenamiento incrementa el buen uso de la tecnología disminuyendo los errores, incrementando la productividad y el cumplimiento de los controles.

Para poder cumplir con este proceso se debe tener en cuenta el plan de entrenamiento, inventario de las habilidades del personal y usuarios de TI, técnicas de concienciación, uso de nuevos métodos y tecnología de entrenamiento, productividad del personal y mantener una base de conocimientos.

Los objetivos de control detallados de este proceso son:

DS 7.1. Identificación de Necesidades de Entrenamiento

DS 7.2. Organización del Entrenamiento

DS 7.3. Evaluación del entrenamiento recibido

3.4.8. DS 8 APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN

Mediante este proceso se pretende asegurar que cualquier problema que experimente el usuario sea resuelto de manera apropiada a través de una facilidad de Help Desk que provee soporte y asesoramiento de primera línea. Este proceso incluye la creación de un registro de los servicios, en donde se específica el escalamiento de incidentes, análisis de tendencia, análisis de causas y resolución.

Los objetivos de control detallados de este proceso son:

DS8.1 Help Desk

DS8.2 Registro de Consulta de los Usuarios

DS8.3 Escalamiento de Consultas del Cliente

DS8.4 Monitoreo de Atención al Cliente

DS8.5 Análisis y Reporte de Tendencias

3.4.9. DS 9 ADMINISTRACIÓN DE LA CONFIGURACIÓN

Este proceso requiere establecer y mantener un repositorio de configuraciones completo y preciso, que incluye toda la información de la configuración inicial, normas, verificación y auditoría de la configuración y actualización del repositorio de configuración conforme se necesite.

El tener una buena administración de la configuración facilita la disponibilidad y minimiza los problemas de producción, permitiendo resolver los problemas de una manera eficiente.

Los objetivos de control detallados son:

DS 9.1. Repositorio de configuración y línea base

DS 9.2. Identificación, mantenimiento y revisión de elementos de configuración

3.4.10. DS 10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES

Una administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas.

El proceso de administración de problemas incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas.

Con un buen proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la satisfacción del usuario.

Los aspectos a considerarse en este proceso son las pistas de auditoría de problemas y soluciones, procedimiento de escalamiento, reportes de incidentes, accesibilidad a la información de la configuración, responsabilidades del proveedor, coordinación con la administración de cambios.

Los objetivos de control detallados de este proceso son:

DS 10.1. Sistema de Administración de Problemas

DS 10.2. Escalamiento de problemas

DS 10.3. Seguimiento de Problemas y Pistas de Auditoría

DS 10.4. Autorización de Accesos temporales y emergentes

DS 10.5. Prioridades de procesamiento de emergencia

3.4.11. DS 11 ADMINISTRACIÓN DE DATOS

Este proceso administra la librería de medios, respaldo, recuperación de datos y la eliminación apropiada de medios. Una buena administración de datos garantiza la calidad, oportunidad y disponibilidad de la información del negocio.

Para cumplir con este proceso se mide con la satisfacción del usuario con la disponibilidad de los datos, los porcentajes de restauraciones exitosas de

datos y número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados.

Los objetivos de control detallados son:

DS 11.1. Requerimientos del negocio para administración de datos

DS 11.2. Acuerdos de almacenamiento y conservación

DS 11.3. Sistema de administración de librerías de medios

DS 11.4. Eliminación

DS 11.5. Respaldo y restauración

DS 11.6. Requerimientos de seguridad para la administración de datos

3.4.12. DS 12 ADMINISTRACIÓN DE INSTALACIONES

La protección del Centro de Cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. Este proceso incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

Los objetivos de control detallados son:

DS 12.1. Seguridad Física

DS 12.2. Discreción sobre las Instalaciones de Tecnología de Información

DS 12.3. Escolta de Visitantes

DS 12. 4. Protección contra Factores Ambientales

DS 12. 5. Suministro Ininterrumpido de Energía

3.4.13. DS 13 ADMINISTRACIÓN DE OPERACIONES

Asegurar que las funciones importantes de soporte de TI se realicen regularmente y en la forma debida mediante un programa de actividades de soporte que es registrado y aprobado para la realización de todas las actividades.

Este proceso ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

DS 13.1. Manual de Instrucciones y Procedimientos de las Operaciones de Procesamiento.

DS 13.2. Programación de Trabajos

DS 13.3. Desviaciones de la Programación de Trabajos Estándar

DS 13.4. Operaciones Remotas

Esquema de Relaciones entre los Procesos y Objetivos de Control del Dominio Entrega de Servicios y Soporte

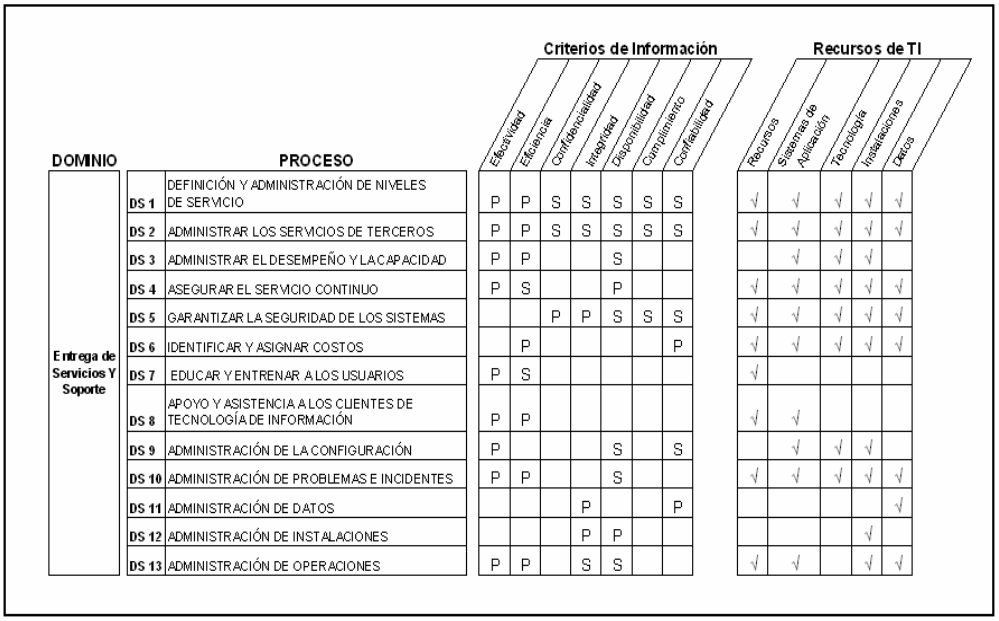

Fig. 3.7. Esquema de Procesos del Dominio Entrega de Servicios y Soporte[13]

[13] COBIT 3.0 Marco Referencial Español, IT Governance Institute**,** ISBN 1-933284-37-4, página 29

CAPÍTULO IV

4.1. Resumen Ejecutivo

La auditoría de sistemas es un examen crítico que debe ser realizado para evaluar que las áreas responsables del procesamiento de información se encuentren funcionando de manera eficiente y eficaz, y en caso de que no esté ocurriendo de esta manera proponer procedimientos o controles alternativos que permitan que se corrija esta situación.

Partiendo de este antecedente se ha aprobado y ejecutado el proyecto titulado "AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO: DOMINIO ENTREGA DE SERVICIOS Y SOPORTE", mediante el cual se realizó la evaluación de los procedimientos que sigue la Unidad de Tecnologías de Información y Comunicaciones para administrar, almacenar y dar soporte a los servicios de tecnología de la Escuela Politécnica del Ejército. A continuación, se detalla un resumen general acerca de la situación actual de la Unidad de Tecnologías de Información y Comunicaciones.

La causa principal de la que se derivan varias de las condiciones encontradas, es la falta de conciencia y conocimiento acerca de las mejores prácticas de control interno y auditoría de los sistemas de información por parte de las autoridades de la ESPE y el personal de la Unidad de Tecnologías de Información y Comunicaciones. De acuerdo a lo mencionado estas condiciones son:

- Las autoridades de la ESPE y la Unidad de TIC's, en conjunto con los proveedores externos y los usuarios no han realizado un análisis de los servicios de tecnología de la ESPE, basados en sus características básicas, operaciones que soportan y su nivel de importancia para la institución, lo cual impide que se definan niveles de servicio que regulen la disponibilidad y el funcionamiento adecuado de los servicios de tecnología brindados por la ESPE.

- El procedimiento de monitoreo del correcto funcionamiento de los servicios de tecnología brindados por la ESPE y sus proveedores, no se encuentra adecuadamente definido e implementado, puesto que, no se han designado específicamente personas encargadas de realizar esta actividad, los parámetros que se han utilizado para realizar el monitoreo no son adecuados y entendibles, y en los contratos con los proveedores de servicios de tecnología no se incluyen parámetros de disponibilidad de los servicios.

- La administración de las políticas de seguridad de la información no es adecuada, ya que la Unidad de TIC's, debería incluir las medidas de seguridad adoptadas por la ESPE en un plan de seguridad, de manera que en caso de la existencia de algún incidente o modificación errónea se pueda regresar a la configuración adecuada de los sistemas.

- La ESPE no ha considerado la realización de un plan de continuidad de la institución en el que se incluya análisis de las operaciones y servicios

críticos proporcionados, los recursos de hardware y software que permiten la ejecución de estas operaciones, riesgos naturales y tecnológicos que pueden afectar a los mencionados recursos, el personal clave encargado de la ejecución y recuperación de las operaciones, centros alternos de operación. Dentro de este plan se debe considerar la obtención y almacenamiento de respaldos de la información que permitan la recuperación inmediata de los datos.

4.2. Informe de Auditoría.

"AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO: DOMINIO ENTREGA DE SERVICIOS Y SOPORTE."

En conformidad con el Plan del proyecto de tesis, "Auditoría Informática del Sistema de Información de la Escuela Politécnica del Ejército", se ha realizado la revisión de los controles referentes al dominio de Entrega de Servicios y Soporte implantados en Tecnología de la Información y Comunicaciones de la Escuela Politécnica del Ejército, de la que se detalla a continuación las observaciones y recomendaciones resultantes, en base del modelo COBIT.

DS1. DEFINIR NIVELES DE SERVICIO

DS1.1. Marco de Referencia para el Acuerdo de Niveles de Servicio.

Observación DS1 La Escuela Politécnica del Ejército no posee niveles de servicio acordados entre los usuarios, la Unidad de Tecnología de la Información y Comunicaciones u otros proveedores de servicios.

Criterio

La alta gerencia deberá establecer un marco de referencia en donde presente la definición de acuerdos de niveles de servicio formales y determine el contenido mínimo: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia/recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio. Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos. El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y la cantidad de servicios ofrecida y los usuarios deberán ajustar la utilización de los servicios solicitados a los límites acordados.

Condición

- La Escuela Politécnica del Ejército no ha realizado un análisis que sirva para determinar niveles de servicio de tecnología con los usuarios, en los que se indique la calidad, la disponibilidad y el tiempo en el que se prestarán los mencionados servicios. (Evidencia: DIR-1 y DIR-2)
- Dentro del procedimiento de Soporte Técnico no se ha establecido el tiempo que debe haber transcurrido para que se escale el problema a un área especializada o externa de tecnología. (Evidencia: GT2-1)

- El procedimiento de Soporte Técnico no se encuentra correctamente difundido a todos los usuarios de la Escuela Politécnica del Ejército, puesto que en lugar de realizar la solicitudes de atención de problemas en primera instancia a la unidad de Help Desk, en varias ocasiones se realiza la solicitudes de solución de problemas a las unidades especializadas, las que atienden problemas pequeños que podrían ser solucionados en una instancia inferior y que restan productividad a las áreas especializadas.

Causa

- No existen, políticas, acuerdos y análisis, basados en la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario y plan de contingencia mediante los cuales se puedan definir acuerdos de niveles de servicio con los usuarios.
- El procedimiento mediante el cuál se brinda soporte técnico a los usuarios en el cual se indica que el primer nivel de atención de problemas es el área de Help Desk, no se encuentra correctamente difundido a todos los usuarios de la Escuela Politécnica del Ejército.

Efecto

- La falta de niveles de servicio acordados con los usuarios impide que se realicen evaluaciones a la Unidad de Tecnologías de Información y Comunicaciones y a sus funcionarios acerca de los servicios de tecnología que brindan a los usuarios, por medio de las cuales se pueden verificar las deficiencias y mejorar el desempeño de la Unidad de Tecnologías de Información y Comunicaciones.

- El no definir límites de tiempo desde el reporte de un problema con los servicios de tecnología hasta el escalamiento del mismo al área especializada de la Unidad de Tecnologías de Información y Comunicaciones, puede provocar que queden requerimientos de usuarios sin atención o en espera indefinida.
- El desconocimiento del procedimiento de reporte de problemas en los servicios de tecnología por los usuarios, provoca que se reporten de manera desorganizada los problemas a cualquier área de la Unidad de Tecnologías de Información y Comunicaciones, teniendo estas que dedicar la mayoría de su tiempo, a resolver problemas menores de soporte técnico que no les corresponden.

Recomendación DS1.-

- El Director de la Unidad de Desarrollo Institucional, deberá definir durante el año en curso, como política institucional el establecimiento de niveles de servicio de tecnologías de información.
- El Director de la Unidad de Tecnología de Información y Comunicaciones, durante el año en curso, debe elaborar los niveles de servicios de tecnología entre la Unidad de Tecnología de Información y Comunicaciones y los usuarios de acuerdo a la realidad de la Escuela Politécnica del Ejército, en los que se indique el tiempo en el que estos servicios deben estar disponibles, la clasificación de criticidad de los problemas que los afecten y el tiempo en el que se atenderá cada problema de acuerdo a la criticidad definida. Definirá además, la manera y el período en el que se evaluará el cumplimiento con los niveles de servicio

acordados. Dentro del procedimiento de Soporte Técnico, incluirá el tiempo en el que se deberá realizar el escalamiento de los problemas reportados a una área especializada de la Unidad de Tecnología de Información y Comunicaciones o a un proveedor de servicios de tecnología e implantará alertas que permitan controlar que ese tiempo se cumpla de manera adecuada, difundirá y capacitará a los usuarios acerca de la manera en la que se deben reportar los problemas con los servicios de tecnología de acuerdo al procedimiento de soporte técnico.

DS1.2. Definición de servicios

Observación DS2 La Escuela Politécnica del Ejército no posee un catálogo / portafolio de servicios en el cual se encuentren definidas las características básicas de los servicios y requerimientos del negocio.

Criterio

La institución debe contar con definiciones base de los servicios de TI sobre las características del servicio y los requerimientos del negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo / portafolio de servicios.

Condición

No existe evidencia de un portafolio de servicios de tecnología de información de la Escuela Politécnica del Ejército, al ser requerido a la Unidad de Tecnología de Información y Comunicaciones, únicamente fue recibido el listado de las aplicaciones en el que se indica el nombre de la aplicación, dependencia en la que funciona, el responsable de su mantenimiento y si fue

adquirido o desarrollado internamente en la Unidad.(Evidencia: DIR-1 y DIR-2).

Causa

- Falta de políticas al respecto del mantenimiento de un catálogo de servicios.
- No se mantiene definiciones básicas de las configuraciones, parámetros de calidad y disponibilidad de los servicios de tecnología de la Escuela Politécnica del Ejército.

Efecto

Deficiencia en el uso de tecnologías y falta de competitividad.

Recomendación DS2.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, durante el segundo trimestre del año en curso, deberá desarrollar un portafolio de servicios completo en el que se indique la disponibilidad y la calidad con la que se prestarán los servicios de TI.

DS1.3. Procedimientos de Desempeño.

Observación DS3 La Escuela Politécnica del Ejército, específicamente el área de Logística, no define de manera detallada y adecuada en los contratos los procedimientos y políticas de desempeño que deberían cumplir los proveedores de servicios de tecnología con la Escuela Politécnica del Ejército.

Criterio

Deberán definirse procedimientos que aseguren que la forma y las responsabilidades sobre las relaciones que rigen el desempeño (por ejemplo, acuerdos de confidencialidad) entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

Condición

Se realizó una revisión de varios contratos firmados con proveedores de tecnología, en los que se determinó que no se han definido políticas de desempeño, tampoco se encuentran definidas sanciones en el caso de incumplimiento con los contratos, que permitan controlar que la información entregada por la Escuela Politécnica del Ejército sea utilizada adecuadamente. (Evidencia: CON-1, CON-2, CON-3, CON-4)

Causa

El formato de los contratos que formaliza la Escuela Politécnica del Ejército con sus proveedores, tiene un estándar único sin importar el tipo de servicios contratados, en los servicios de tecnología no se consideran cláusulas de confidencialidad, calidad y desempeño.

Efecto

No se podría exigir el cumplimiento de los contratos de servicios entre los proveedores y la Escuela Politécnica del Ejército para que sean entregados de acuerdo a los requerimientos iniciales de la misma.

Recomendación DS3.-

El Director de la Unidad de Desarrollo Institucional, dentro del segundo trimestre del año en curso, deberá establecer y poner en ejecución políticas y normatividad e incluir dentro de los contratos, acuerdos de desempeño, cláusulas de confidencialidad y sanciones por incumplimiento de estas cláusulas, deberá designar a un funcionario encargado de verificar constantemente que estas cláusulas y sanciones se cumplan.

DS1.4. Monitoreo y Reporte

Observación DS4 No se ha designado una persona responsable de monitorear y reportar el cumplimiento de niveles de servicio.

Criterio

La Gerencia de la función de servicios de información, deberá designar a un Gerente de nivel de servicio, que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

Condición -

- No existe evidencia de un seguimiento a los servicios de tecnología prestados por proveedores externos y por la Unidad de Tecnología de Información y Comunicaciones de la Escuela Politécnica del Ejército; tampoco existe evidencia de un análisis de los problemas encontrados en los servicios de tecnología.

- No se realiza un monitoreo continuo de las hojas de control de soporte técnico, que permita detectar la existencia de fallas en el servicio recibido o casos no resueltos.
- No se mantiene un monitoreo continuo de la satisfacción del usuario de los servicios de soporte técnico prestados, únicamente cuando los técnicos realizan una actividad de soporte, llenan una hoja de control en la que el usuario califica el grado de satisfacción del servicio. (Evidencia: AUDI-ESPE-2007-ENT-001)
- No se realiza un monitoreo continuo y un control de los servicios prestados por proveedores externos que permita identificar deficiencias en el servicio y en base al cual solicitar mejoras en los servicios. (Evidencia: AUDI-ESPE-2007-ENT-001, AUDI-ESPE-2007-ENT-002).

Causa

La Unidad encargada de la administración de las tecnologías de información desconoce de estándares de buenas prácticas.

Efecto

Desconocimiento de la calidad de servicios prestada, errores o fallas en los mismos que permitan aplicar medidas correctivas para mejorar los servicios de tecnología, así como sanciones y garantías estipuladas en los contratos firmados entre los proveedores de servicios externos y la Escuela Politécnica del Ejército.

Recomendación DS4.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, desde le primer trimestre del año en curso, designará a un administrador de

nivel de servicio, quien será responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

DS1.5.- Revisión de Acuerdos y Contratos de Nivel de Servicio

Observación DS5 No se ha implementado procesos de revisión de cumplimiento de acuerdos y contratos de niveles de servicio.

Criterio

La Gerencia deberá implementar un proceso de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de servicios como terceras partes.

Condición

No existe un proceso de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de acuerdo a los problemas reportados durante el período de duración de los contratos; luego de realizar una revisión de la documentación de los contratos con los diferentes proveedores de servicios de la Escuela Politécnica del Ejército, no se encontró evidencia de algún procedimiento de revisión regular de convenios de servicios y contratos, con la Unidad de Tecnología de Información y Comunicaciones, los proveedores y los usuarios.

Causa

La Unidad de Tecnología de Información y Comunicaciones, no ha desarrollado políticas y normatividad referente al tema.

Efecto

Las condiciones con las que se prestan los servicios pueden estar obsoletas y deficientes, se impide el análisis del desempeño de los servicios de tecnología y sus proveedores, poniendo en riesgo la continuidad de las operaciones en caso de servicios críticos.

Recomendación DS5.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, debe definir procesos de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de servicios.

DS1.6. Programa de Mejoramiento del Servicio

Observación DS6 No se ha implementado un proceso para asegurar que los usuarios y los Coordinadores de la Unidad de Tecnología de Información y Comunicaciones concuerden regularmente en un programa de revisión y mejoramiento de los servicios y los niveles de servicio que los regulan.

Criterio

La Gerencia deberá implementar un proceso para asegurar que los usuarios y los Gerentes de nivel de servicio concuerden regularmente en un programa de mejoramiento del servicio con el fin de dar seguimiento a mejoras al nivel de servicio cuyo costo esté justificado.

Condición

- No se han definido programas de revisión y mejoramiento de los servicios de tecnología prestados.
- Dentro de la matriz gestión de acciones para la mejora continua se observó que no se registran todos los problemas atendidos por GT2 en un primer nivel de soporte.
- No se actualiza frecuentemente la matriz gestión de acciones para la mejora continua.
- En la revisión realizada al Sistema de Gestión de Calidad, se encontró una matriz de gestión de acciones para la mejora continua en la cuál se incluye la apertura de la acción, dentro de la que se encuentran la descripción del problema a mejorarse, la fuente de acción, la fecha de apertura, los resultados a esperarse, la unidad responsable, de su desarrollo y puesta en producción de la solución. (Evidencia: SGC.DI.121 -Octubre 29 2007), luego está la planificación de acciones, en la que se enumera las causas del problema y las soluciones propuestas, el control de avance en el que se detalla el porcentaje de la ejecución, fecha real de cierre, días de retraso y la justificación del retraso, por último se encuentra el control de las deficiencias en la que se detalla la fecha de control, revisión de las deficiencias, evidencia de los resultados logrados y si el problema reportado fue solucionado o se encuentra pendiente.

Causa

Falta de políticas y normatividad al respecto.

Efecto

- Desperdicio de tiempo del personal de soporte al atender problemas que se repiten constantemente en lugar de atender las causas de dichos problemas dando una solución definitiva.
- No se tiene una evaluación real del servicio que se está brindado o recibiendo y por tanto no se efectúa la mejora del servicio.

Recomendación DS6.-

El Director de la Unidad de Desarrollo Institucional, en el segundo trimestre del año en curso, debe implementar un proceso para asegurar que los usuarios y los encargados del nivel de servicio, concuerden regularmente en un programa de mejoramiento del servicio con el fin de dar seguimiento a mejoras al nivel de servicio cuyo costo esté justificado.

DS2. ADMINISTRAR LOS SERVICIOS DE TERCEROS

DS2.1. Identificación de las relaciones con todos los proveedores

Observación DS7 No se mantiene un control adecuado de proveedores.

Criterio

Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores.

Condición

Al revisar el listado de los proveedores facilitado por la Unidad de Logística se corroboró que no se tienen los suficientes datos de acuerdo al criterio de este objetivo. (Evidencia: UL-1 Listado de proveedores.)

Causa

- Falta de coordinación entre la Unidad de Tecnología de Información y Comunicaciones y la Dirección de Logística, para establecer el control de proveedores.
- Desconocimiento de las normas y procedimientos de adquisición de servicios y equipos por parte de las unidades señaladas.

Efecto

La falta de control de proveedores no permite mantener alertas que limiten la participación de proveedores incumplidos o que tengan problemas al prestar sus servicios o entregar sus productos.

Recomendación DS7.-

El Director de Logística, desde el primer trimestre del año en curso, mantendrá un registro actualizado de control de proveedores de tecnologías, en coordinación con el Director de la Unidad de Tecnología de Información y Comunicaciones.

DS2.2. Relaciones con los Propietarios (usuarios dueños)

Observación DS 8: La Escuela Politécnica del Ejército no realiza evaluaciones a los servicios prestados por proveedores externos, junto con los representantes de las empresas proveedoras de servicios de tecnología.

Criterio

La Gerencia de la organización del cliente, deberá establecer relaciones con quien sea responsable de asegurar la calidad de las relaciones con terceros.

Condición

- La Unidad de Desarrollo Institucional, no mantiene definidos procedimientos y buenas prácticas en las que se describa que se realizarán evaluaciones periódicas a los servicios de tecnología prestados por terceros
- No se realizan evaluaciones periódicas de los servicios de tecnología contratados por la Escuela Politécnica del Ejército a proveedores externos, lo cual impide llegar a nuevos acuerdos tomando en cuenta la evolución y cambios que suceden en la infraestructura de la Escuela Politécnica del Ejército y los avances tecnológicos frecuentes.
- No existe una planificación y coordinación adecuada de los recursos humanos de la Unidad de Tecnología de Información y Comunicaciones para monitorear los servicios de tecnología prestados por proveedores. (Evidencia: AUDI-ESPE-2007-ENT-002).

Causa

En la Unidad de Tecnologías de Información y Comunicaciones no poseen políticas y normatividad al respecto.

Efecto

- Que no se conozcan nuevas propuestas de mejoramiento de los servicios ofrecidos por los proveedores.
- No se pueden exigir mejoras a los proveedores, al momento que se detecten deficiencias en los servicios prestados.

Recomendación DS8.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, durante el año en curso, debe definir un procedimiento para establecer relaciones con terceros, a fin de revisar el desempeño actual de los servicios prestados, para luego definir oportunidades de mejora de los servicios de tecnología actuales.

DS2.3. Calificación de Terceros

Observación DS9 No se califica adecuadamente a los proveedores de tecnología entre al Unidad de Tecnología de Información y Comunicaciones y la Unidad de Logística.

Criterio

La Gerencia debe asegurar en forma previa a su selección, que los terceros potenciales cuentan con las calificaciones adecuadas a través de una

evaluación de su capacidad para proporcionar los servicios requeridos (due diligence).

Condición

No existe evidencia de monitoreo continuo sobre los servicios de TI prestados por terceros, a pesar de lo informado por el Director (E) de la Unidad de Tecnología de Información y Comunicaciones, en el memo Nº 2007-1164-ESPE-d-6, en el que se indica que si existe un monitoreo continuo sobre los servicios de TI prestados por terceros, sin embargo no existe informe alguno que sustente este hecho. (Evidencia: DIR-1)

Causa

Falta de supervisión de políticas y regulaciones en los servicios prestados por terceros personas.

Efecto

- Falta de garantías en los servicios de tecnología y equipos de tecnología adquiridos para la Escuela Politécnica del Ejército.
- Retraso en la entrega e instalación de los servicios y equipos de tecnología adquiridos.

Recomendación DS9.-

El Director de la Unidad de Desarrollo Institucional, desde el primer trimestre del año en curso, determinará y ejecutará un procedimiento para asegurar en forma previa a su selección, que los terceros potenciales cuentan con las calificaciones adecuadas a través de una evaluación de su capacidad para proporcionar los servicios requeridos.

DS2.4. Continuidad de Servicios

Observación DS10.- No existe un plan de continuidad de los servicios, en el cual se incluya acciones y medidas a tomarse para mitigar los riesgos de desastres que afecten a los servicios prestados por terceros.

Criterio

La gerencia deberá considerar el riesgo de negocios relacionado con la participación de terceros en términos de incertidumbre legal y con el concepto de interés sobre la continuidad y negociar contratos de depósito en garantía donde sea apropiado.

Condición

- En el plan de contingencias de tecnología de información y comunicaciones elaborado el 11 de Julio del 2006 no se analizan los riesgos que afecten a los servicios en outsourcing.
- No existe definido un plan de continuidad del negocio de la Escuela Politécnica del Ejército, tampoco en los contratos se definen políticas y estrategias que permitan la continuidad de estos servicios.

Causa

La Unidad de Tecnología de Información y Comunicaciones no ha definido políticas y normatividad al respecto.

Efecto

Puede ocurrir que en caso de un desastre, no se puedan recuperar estos servicios en un tiempo adecuado de acuerdo a las necesidades de la Escuela Politécnica del Ejército.

Recomendación DS10.-

El Director de la Unidad de Desarrollo Institucional, durante el año en curso, definirá e implantará políticas y normatividad para considerar el riesgo de negocios relacionados con la participación de terceros en términos de incertidumbre legal y con el concepto de interés sobre la continuidad y negociar contratos de depósito en garantía donde sea apropiado.

DS2.5. Relaciones con la Seguridad

Observación DS11.- Dentro de los contratos de servicios, no existen acuerdos de seguridad que permitan la continuidad de las operaciones y la confidencialidad de la información de la Escuela Politécnica del Ejército.

Criterio

La Gerencia deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de confidencialidad) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en línea con los requerimientos legales y regulatorios, incluyendo obligaciones.

Condición

En la Institución, no se firman contratos, en los que se incluyan acuerdos de seguridad y confidencialidad de la información con proveedores de servicios de tecnología y personal de la Unidad de Tecnología de Información y Comunicaciones. (Evidencia: CON-1 y CON-2)

Causa

Falta de políticas y normas para incluir cláusulas de seguridad y confidencialidad de la información.

Efecto

Eventual fuga de información confidencial e incremento en la vulnerabilidad de los sistemas informáticos de la Escuela Politécnica del Ejército.

Recomendación DS11.-

El Director de la Unidad de Desarrollo Institucional, dentro del año en curso, definirá un procedimiento para asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de confidencialidad) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en línea con los requerimientos legales y regulatorios, incluyendo obligaciones.

DS2.6. Monitoreo

Observación DS12.- No existe evidencia de monitoreo continuo de los servicios prestados por los proveedores externos de la Escuela Politécnica del Ejército.

Criterio

La Gerencia deberá establecer un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

Condición

- No existe evidencia de la realización de un monitoreo adecuado y periódico a los servicios prestados por terceros a pesar de que en el Reglamento Interno de Adquisiciones, Contratación de Servicios y Ejecución de Obras, en el artículo 25, especifica que se debe realizar de forma permanente evaluaciones a los proveedores y contratistas calificados y se debe mantener un registro actualizado con el resultado de las mismas y las acciones derivadas de ellas. (Evidencia: AUDI-ESPE-2007-ENT-014, SG-01 Reglamento Interno de Adquisiciones, Contratación de Servicios y Ejecución de Obras).
- No se definen cronogramas ni programas para realizar evaluaciones periódicas a los servicios prestados por terceros

Causa

Falta de supervisión en el cumplimiento del Reglamento Interno de Adquisiciones, Contratación de Servicios y Ejecución de Obras.

Efecto

Se puede renovar contratos con proveedores que no cumplen con estándares de calidad y no satisfacen las necesidades de la Escuela Politécnica del Ejército.

Recomendación DS12.-

El Director de la Unidad de Desarrollo Institucional, durante el año en curso, debe definir un procedimiento para efectuar evaluaciones periódicas a los servicios prestados por terceros y mediante los resultados de las mismas las unidades de Tecnología de Información y Comunicaciones y Logística

tomarán acciones correctivas que permitan mejorar los servicios o en su defecto seleccionar a proveedores mejor calificados.

DS3. ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD

DS3.1. Requerimiento de disponibilidad y desempeño

Observación DS13 No se realiza análisis de disponibilidad y desempeño de los servicios de tecnología.

Criterio

El proceso de administración, deberá asegurar que las necesidades del negocio con respecto a disponibilidad y desempeño de los servicios de información sean identificados y convertidos en requerimientos y términos de disponibilidad.

Condición

No se ha realizado un estudio de requerimientos tecnológicos de la Escuela Politécnica del Ejército, que sea la base para determinar la capacidad, disponibilidad y desempeño de los recursos de TI. (Evidencia: AUDI-ESPE-ENT-001, ADM-001)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Riesgo en el cumplimiento de los objetivos institucionales y desarrollo tecnológico.

Recomendación DS13.-

El Director de la Unidad de Desarrollo Institucional, durante el año en curso, debe solicitar la realización de un análisis de requerimientos tecnológicos de la Escuela Politécnica del Ejército basado en la disponibilidad y desempeño de los servicios de tecnología, que servirá como base para la adquisición o desarrollo de sistemas de información que garanticen el apoya a las metas y objetivos generales de la Escuela Politécnica del Ejército, y ayuden a satisfacer las necesidades tecnológicas del personal y usuarios de la Escuela Politécnica del Ejército; en este estudio de requerimientos se deberá considerar las oportunidades, cambios tecnológicos y definir la arquitectura de los sistemas de información.

DS3.2. Plan de Disponibilidad

Observación DS14.- No existe un plan en el que se describa los diferentes servicios de tecnología que brinda la Escuela Politécnica del Ejército por medio de la Unidad de Tecnología de Información y Comunicaciones, su período de disponibilidad y características adecuadas de desempeño.

Criterio

La Gerencia deberá asegurar el establecimiento de un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.

Condición

No se cuenta con un plan de disponibilidad de servicios de tecnología, con el cual se pueda controlar el tiempo en el que deben estar disponibles los

servicios de tecnología, cuya indisponibilidad resulta critica para las operaciones de la Escuela Politécnica del Ejército, las actividades a realizarse al momento en el que se detecte que un servicio no está disponible y el impacto de la no disponibilidad de los servicios, así como los responsables y las penalizaciones a los mismos.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- No se puede controlar el tiempo y las condiciones en el que los servicios de tecnología de la Escuela Politécnica del Ejército deben estar disponibles de manera adecuada para permitir el cumplimiento de las operaciones de la institución.
- Al no contar con acuerdos de disponibilidad de los servicios de tecnología no se puede mantener un plan de continuidad que indique cuales son los servicios críticos de la Escuela Politécnica del Ejército y que deben estar disponibles continuamente.

Recomendación DS14.-

El Director de la Unidad de Desarrollo Institucional, dentro del segundo trimestre del año en curso, en coordinación con el Director de la Unidad de Tecnología de Información y Comunicaciones, definirá dentro de un plan de disponibilidad, el tiempo y las características en las que deben estar disponibles los servicios de tecnología, los riesgos que pueden producirse al no contar con estos servicios de tecnología, los responsables de que los

servicios cumplan con estos parámetros y las penalizaciones a los mismos por el incumplimiento con el plan de disponibilidad.

DS3.3. Monitoreo y Reporte

Observación DS15.- No se realiza un monitoreo continuo del desempeño de los recursos de tecnología de información, en base a las características de disponibilidad y desempeño adecuados.

Criterio

La Gerencia, deberá implementar un proceso que asegure que el desempeño de los recursos de tecnología de información, sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

Condición

No existen procedimientos y actividades de monitoreo del desempeño de los recursos de tecnológicos de la Escuela Politécnica del Ejército y las actividades que deberían realizarse en caso de que los resultados del monitoreo no sean los adecuados.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Desempeño inadecuado de los recursos tecnológicos de la Escuela Politécnica del Ejército
- Aplicación tardía de acciones correctivas a los recursos tecnológicos, en el caso de que no exista el desempeño de manera adecuada.

Recomendación DS15.-

El Director de la Unidad de Desarrollo Institucional, desde el primer trimestre del año en curso, implementará un proceso que asegure que el desempeño de los recursos de tecnología de información, sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

DS3.4. Manejo Proactivo del Desempeño.

Observación DS16.- No se realiza un adecuado análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado de impacto y magnitud de los daños ocasionados.

Criterio

El proceso de administración del desempeño, deberá incluir la capacidad de pronóstico, para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado del impacto y magnitud del daño.

Condición

No existen procedimientos y actividades de monitoreo del desempeño de los recursos de tecnológicos de la Escuela Politécnica del Ejército y las actividades que deberían realizarse en caso de que los resultados de este monitoreo no sea adecuado.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Mitigación inadecuada y tardía de fallas presentadas por los servicios de tecnología y los problemas reportados por los usuarios en los sistemas de información.

Recomendación DS16.-

El Director de la Unidad de Desarrollo Institucional, durante el año en curso, deberá implantar un proceso de administración del desempeño, que incluirá la capacidad de pronóstico, para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado del impacto y magnitud del daño.

DS3.5. Pronóstico de Carga de Trabajo

Observación DS17.- No existen pronósticos de carga de trabajo.

Criterio

Deberán establecerse controles para asegurar que se preparen pronósticos de carga de trabajo con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad.

Condición

No se han definido controles que permitan pronosticar la carga de trabajo en el cual consten las tendencias de utilización de los recursos de tecnología.
(Evidencias: AUDI-ESPE-2007-ENT-001, AUDI-ESPE-2007-ENT-002, AUDI-ESPE-2007-ENT-005)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Identificación y planificación inadecuada de la capacidad y desempeño que deben proveer los sistemas de información a los usuarios de los mismos en la Escuela Politécnica del Ejército.

Recomendación DS17.-

El Director de la Unidad de Desarrollo Institucional, desde el primer trimestre del año en curso, establecerá controles para asegurar que se preparen pronósticos de carga de trabajo con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad de TI.

DS3.6. Administración de Capacidad de Recursos

Observación DS18.- No existen definidos procesos de planeación para la revisión del desempeño y capacidad del hardware.

Criterio

La Gerencia de la función de servicios de información, deberá establecer un proceso de planeación para la revisión del desempeño y capacidad del hardware, con el fin de asegurar que siempre exista una capacidad justificable económicamente, para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas, prescritas en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

Condición

No existe un cronograma de revisión del desempeño y capacidad de hardware que permita asegurar que siempre exista un capacidad justificable económicamente para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas. (Evidencias: AUDI-ESPE-2007-ENT- 001, AUDI-ESPE-2007-ENT-002, AUDI-ESPE-2007-ENT-005)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Riesgo en la continuidad del negocio y deficiencia en el desempeño.

Recomendación DS18.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, durante el año en curso, debe establecer un proceso de planeación para la revisión del desempeño y capacidad del hardware, con el fin de asegurar que siempre exista una capacidad justificable económicamente, para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas, prescritas en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

DS4. ASEGURAR EL SERVICIO CONTINUO

DS4.1. Marco de Referencia de Continuidad de Tecnología de información

Observación DS19.- No existe evidencia de políticas y normativa referentes a la continuidad de los servicios de TI.

Criterio

La Gerencia de TI, en cooperación con los propietarios de los procesos del negocio, debe definir un marco de referencia de continuidad en el que consten los roles, responsabilidades, la metodología a seguir basada en riesgo, las reglas y la estructura para documentar el plan de continuidad, así como los procedimientos de aprobación.

El plan de continuidad del negocio, debe proveer a la organización la habilidad para continuar operando los procesos críticos definidos, a un nivel menor al normal aceptado por la Gerencia, en ocasiones en las que se produzcan eventos que ocasionen la paralización de los servicios informáticos.

Condición

La Escuela Politécnica del Ejército no posee un plan de continuidad realizado en base a una metodología definida, un análisis de riesgos de la información y los recursos tecnológicos más importantes; el plan de contingencia que se ha definido para la Escuela Politécnica del Ejército y en el cual se indica las acciones a ser llevadas a cabo al momento de que se produzcan desastres se encuentra desactualizado. (Evidencia: AMD – 1 Plan de Contingencias de Tecnologías de Información y Comunicaciones)

Causa

- Existe desconocimiento de la importancia del desarrollo e implantación de un Plan de Continuidad del Negocio.
- No se ha realizado un análisis de las operaciones de la Escuela Politécnica del Ejército, en el que se considere la información y las operaciones críticas de las áreas que forman parte de la Institución.

Efecto

- Riesgo de no mantener la continuidad de las operaciones de la Escuela Politécnica del Ejército, en el caso de la ocurrencia de desastres.
- Incremento de los costos implicados en la recuperación de la operatividad de los sistemas y datos.
- Errores en el procesamiento de transacciones en el período de contingencia.

Recomendación DS19.-

El Director de la Unidad de Desarrollo Institucional, durante el segundo trimestre del año en curso, en cooperación con los propietarios de los procesos del negocio, definirá políticas y normatividad en el que consten los roles, responsabilidades, la metodología a seguir basada en riesgo, las reglas y la estructura para documentar el plan de continuidad, así como los procedimientos de aprobación, el plan de continuidad del negocio, proveerá a la organización la habilidad para continuar operando los procesos críticos definidos, a un nivel menor al normal aceptado, en ocasiones en las que se produzcan eventos que ocasionen la paralización de los servicios informáticos.

DS4.2. Estrategia y Filosofía del Plan de Continuidad de TI.

Observación DS20.- No se mantienen políticas, estrategia y filosofía acerca del mantenimiento de la continuidad de las operaciones de la Escuela Politécnica del Ejército.

Criterio

La Gerencia deberá garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa para asegurar consistencia. Aún más, el plan de continuidad de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.

Condición

- No existe evidencia de políticas, análisis, marco teórico, metodología o algún procedimiento que se haya realizado por parte de la Unidad de Desarrollo Institucional, que pueda servir de base para el desarrollo del Plan de Continuidad General de la Escuela Politécnica del Ejército.
- No existe evidencia de coordinaciones realizadas entre la Unidad De Tecnología de Información y Comunicaciones y otras unidades, para iniciar un Plan de Continuidad de TI, que permita reaccionar en el caso de no se encuentren disponibles los servicios de tecnología. (Evidencias: AUDI-ESPE-2007-ENT-005, DIN-01.)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Riesgo de no mantener la continuidad de las operaciones de la Escuela Politécnica del Ejército, en el caso de la ocurrencia de desastres.
- Incremento de los costos implicados en la recuperación de la operatividad de los sistemas y datos
- Errores en el procesamiento de transacciones en el período de contingencia

Recomendación DS20.-

El Director de la Unidad de Desarrollo Institucional, durante el año en curso, debe establecer un procedimiento para garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la Escuela Politécnica del Ejército para asegurar consistencia. El plan de continuidad de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.

DS4.3. Almacenamiento de respaldo en el sitio alterno (Off-site)

Observación DS21.- No se ha definido los intervalos de tiempo para obtener respaldos de información, basados en análisis de su criticidad.

Criterio

El almacenamiento externo de copias de respaldo, documentación y otros recursos tecnológicos de información, catalogados como críticos, debe ser establecido para soportar el plan de recuperación y continuidad del negocio.

- Los propietarios de los procesos del negocio y el personal de la función de TI deben involucrarse en determinar que recursos de respaldo deben ser almacenados en el sitio alterno. La instalación de almacenamiento externo debe contar con medidas ambientales para los medios y otros recursos almacenados.

  El sitio de almacenamiento externo debe tener un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. La Gerencia de TI debe asegurar que los acuerdos/contratos del sitio alterno son periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental.

Condición

- La definición de los períodos de obtención de respaldos descritos en el Plan de Contingencias de Tecnologías de Información y Comunicaciones, se ha llevado a cabo sin antes realizar un análisis de la criticidad de la información respaldada. (Evidencia: AMD-1) y los respaldos mensuales se mantienen en el disco duro del servidor del que se obtuvo el respaldo hasta que se genere el respaldo trimestral. (Evidencias: AMD-1, AUDI-ESPE-2007-ENT-016).

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Riesgo de pérdida de información importante y vulnerable referente a las operaciones de la Escuela Politécnica del Ejército.

Recomendación DS21.-

El Director de la Unidad de Desarrollo Institucional, durante el año en curso, debe establecer políticas y normativas, para garantizar que los responsables de los procesos del negocio y el personal de la función de TI, se determinen los recursos de respaldo que deben ser almacenados en el sitio alterno. La instalación de almacenamiento externo contará con medidas ambientales para los medios y otros recursos almacenados; y tendrá un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. Los acuerdos/contratos del sitio alterno serán periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental.

DS5. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

DS5.1. Administrar Medidas de Seguridad

Observación DS22 No se ha definido un plan de seguridad en el que se describan las políticas adoptadas por la Escuela Politécnica del Ejército.

Criterio

- La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI, implementar el plan de seguridad de TI, actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI, evaluar el impacto de las solicitudes de cambio en la seguridad de TI, monitorear la implementación del plan de seguridad de TI

y alinear los procedimientos de seguridad de TI a otras políticas y procedimientos

- El acceso lógico y el uso de los recursos de TI deberá restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso, para evitar que personal no autorizados, tengan acceso a los recursos de cómputo
- La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.
- La Gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso. Se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental.
- La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectados, tanto interna como externamente y se debe actuar de una manera oportuna.
- La Gerencia deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad, mediante una

decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación de datos.

- La administración de la función de servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas.
- Todo el hardware y software relacionado con seguridad, debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas.
- Con respecto al software malicioso, la Gerencia deberá establecer un marco de referencia adecuado y medidas de control preventivas, detectivas y correctivas para responder y reportar su presencia.
- Se deberá contar con Firewalls adecuados para proteger contra negación de servicios y cualquier acceso no autorizado a los recursos internos si existe conexión con Internet u otras redes públicas.

Condición

- No se ha implementado un Plan de Seguridad de TI, que contenga las definiciones de los requisitos de seguridad de la Escuela Politécnica del Ejército y que permitan a los usuarios desempeñar adecuadamente sus funciones.
- No existe evidencia de políticas de seguridad lógica definidas para el Active Directory, que restrinjan el acceso de personal no autorizado a los sistemas de información. (Evidencia: MEM-3)

- No existe evidencia de procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario.
- No existe evidencia de procedimientos aprobados formalmente, que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.
- No existe evidencia de procedimientos para establecer revisiones periódicas de los derechos de acceso asignados los usuarios. (Evidencia AUDI-ESPE-2007-ENT-002)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Incremento en la vulnerabilidad de los sistemas de tecnología de la Escuela Politécnica del Ejército, que causarían sustracción o daño en la información crítica a nivel de hardware y software.
- Interrupciones en los servicios informáticos, causadas por virus y ataques informáticos.
- Accesos indebidos a información crítica lo cual impide preservar la integridad de los datos.
- Pérdida de confidencialidad de datos y privacidad de clientes y usuarios.
- Disminución de la confianza de clientes y usuarios con respecto a la integridad de la información.

Recomendación DS22.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, establecerá políticas y procedimientos, para administrar y monitorear la seguridad en TI, de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI, implementar el plan de seguridad de TI, actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI, evaluar el impacto de las solicitudes de cambio en la seguridad de TI, monitorear la implementación del plan de seguridad de TI y alinear los procedimientos de seguridad de TI a otras políticas y procedimientos.

DS6. IDENTIFICAR Y ASIGNAR COSTOS

DS6.1. Elementos Sujetos a Cargo o Cobro por su Uso.-

Observación DS23.- No se realizan análisis para identificar y controlar el correcto uso de los elementos de tecnología sujetos a cargos.

Criterio

La Gerencia de TI, en coordinación con la alta Gerencia, deberá asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los usuarios. Los usuarios deberán ser capaces de controlar el uso de los servicios de información y de los niveles de facturación asociados.

Condición

No existe evidencia, que nos permita corroborar la realización de un análisis costo beneficio, de los servicios de tecnología prestados por la Unidad de Tecnología de Información y Comunicaciones (Evidencia: AUDI-ESPE-2007-ENT-005).

No ha existido coordinación con la Unidad de Desarrollo Institucional, para realizar un análisis acerca de los servicios prestados por la Unidad de Tecnología de Información y Comunicaciones; esto ha impedido identificar aquellos servicios sujetos a costo o el gasto que representa para la Escuela Politécnica del Ejército su mala utilización.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Desconocimiento y desconfianza en la inversión de TI.

Recomendación DS23.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, determinará e implantará políticas y normativa que permita asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los usuarios. Los usuarios deberán ser capaces de controlar el uso de los servicios de información y de los niveles de facturación asociados.

DS7. EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS.-

DS7.1. Identificación de necesidades de entrenamiento

Observación DS24 No existe evidencia de procedimientos para identificación de necesidades de entrenamiento a usuarios.

Criterio

La Gerencia deberá establecer y mantener procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.

Condición

- No se ha realizado una evaluación al personal de la Unidad de Tecnología de Información y Comunicaciones, con respecto al desempeño de sus funciones (Evidencia: DIR-2, AUDI-ESPE-2007-ENT-005).
- El plan de capacitación de la Unidad de Tecnología de Información y Comunicaciones no se realiza en base a las deficiencias detectadas por evaluaciones realizadas al personal, sino en base a los pedidos del Director de la Unidad .(Evidencia: AUDI-ESPE-2007-ENT-004)
- No existe evidencia de procedimientos o planes establecidos para capacitar a usuarios de los sistemas de información.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Uso inadecuado de los sistemas de información o acceso inapropiado a estos.

Recomendación DS24.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, establecerá políticas y normativa para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.

DS7.2. Evaluación del entrenamiento recibido.

Observación DS25.- No existe evidencia de la evaluación del entrenamiento recibido.

Criterio

Al finalizar el entrenamiento, evaluar el contenido del entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

Condición

- No existe evidencia de la evaluación del entrenamiento recibido por usuarios para el uso apropiado de los servicios de TI. (Evidencia: AUDI-ESPE-2007-ENT-005).
- La Unidad de Talento Humano no realiza ninguna prueba sobre los conocimientos adquiridos en los cursos y solo emite los certificados de aprobación. (Evidencia: AUDI-ESPE-2007-ENT-013).

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Uso inadecuado de los sistemas de información o acceso inapropiado a estos.

Recomendación DS25.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, definirá e implantará políticas y procedimientos para que, al finalizar el entrenamiento, se evalúe el contenido del mismo respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

DS8. APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN

DS8.1. Help Desk

Observación DS26.- No se ha definido un procedimiento adecuado para el reporte y solución de problemas de los usuarios.

Criterio

Deberá establecerse un procedimiento de soporte para usuarios dentro de una función de Help Desk, puesto que los usuarios deben contar con una sección dentro de la Unidad de TI, que sirva como contacto para resolver problemas reportados que tienen relación con el uso de los sistemas en aplicación, dificultades en el procesamiento de transacciones inusuales, fallas del hardware, errores en la lógica del sistema de aplicación o problemas de red, para los cuales el área de Help Desk debe registrar el contacto inicial y

cualquier acción subsecuente en una bitácora de problemas, lo cual ayuda a la gerencia a monitorear tendencias y estadísticas de problemas de manera tal que se pueda aplicar un enfoque proactivo a la resolución de problemas.

Condición

- No existe evidencia de análisis de tendencias, en base de bitácoras de problemas reportados en el área de Help Desk, mediante el cual se pueda dar soluciones a los problemas recurrentes.
- No se mantiene un cronograma de revisiones periódicas para determinar que todos los incidentes fueron solucionados correctamente, en el tiempo oportuno y que no existen pendientes.
- No se ha designado formalmente al encargado de la administración del área de Help Desk (Evidencia Nº MEM -01).
- El procedimiento de reporte y solución de problemas e incidentes no se encuentra correctamente difundido entre los usuarios, razón por la cual los mismos no siguen el procedimiento adecuado. (Evidencia: GT2.1)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Si los problemas no son manejados de manera efectiva, la entidad podría desperdiciar recursos en asuntos sin importancia y/o los usuarios bien podrían no utilizar el sistema como se pretende.

- La falta de un registro y control de los problemas e incidentes, puede ocasionar que existan problemas que no se hayan resuelto debidamente y a tiempo.
- El desconocimiento del procedimiento de reporte y solución de problemas e incidentes ocasiona que no todos los problemas e incidentes se reporten de manera adecuada y sean atendidos oportunamente.
- Riesgo en la calidad de servicio de TI, en apoyo a los objetivos institucionales.

Recomendación DS26.-

- El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, establecerá políticas y procedimientos para monitorear tendencias y estadísticas de problemas de manera tal que se pueda aplicar un enfoque proactivo a la resolución de problemas.
- El Director de la Unidad de Tecnología de Información y Comunicaciones, desde el segundo trimestre del año en curso, pondrá en práctica cronogramas de revisiones periódicas de los incidentes reportados para determinar que todos los incidentes fueron solucionados correctamente, en el tiempo oportuno. Actualizará el procedimiento de reporte y solución de problemas y lo difundirá a los usuarios y personal de la Escuela Politécnica del Ejército.
- El Director de Talento Humano, en forma inmediata designará de manera formal al encargado del área de Soporte Técnico ó contratar a un Encargado de manera definitiva.

DS9. ADMINISTRACIÓN DE LA CONFIGURACIÓN

DS9.1. Repositorio de configuración y línea base.-

Observación DS27.- No existe un repositorio de la configuración base de hardware y software.

Criterio

Establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

Condición

- No existe evidencia de algún procedimiento para registrar la configuración base de los nuevos sistemas de aplicación y de las modificaciones realizadas a los mismos para mantener una configuración base. (Evidencia: AUDI-ESPE-2007-ENT-002, AUDI-ESPE-2007-ENT-003)
- No existe evidencia de una bitácora, en donde se especifique la configuración base de todo el hardware y software en el que se procesa la información de la Escuela Politécnica del Ejército. (Evidencia: DIR-2).
- No existen planes de rollback que permita regresar a la configuración base de los sistemas de hardware y software cuando se requiere instalar o

modificar nuevos equipos. (Evidencia: AUDI-ESPE-2007-ENT-002, AUDI-ESPE-2007-ENT-003)

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Pérdida de información crítica de la institución, al momento de implantar nuevas versiones de los sistemas de información instalados lo cual podría impedir la ejecución normal de las operaciones de la Escuela Politécnica del Ejército.

Recomendación DS27.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, desde el segundo trimestre del año en curso, establecerá un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluirá hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

DS9.2. Identificación, mantenimiento y revisión de elementos de configuración

Observación DS28.- No existe evidencia de algún procedimiento para identificar y dar mantenimiento a las configuraciones de los sistemas y equipos de la Escuela Politécnica del Ejército.

Criterio

La organización debe contar con procedimientos en orden para,

- Identificar elementos de configuración y sus atributos
- Registrar elementos de configuración nuevos, modificados y eliminados
- Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones.
- Actualizar los elementos de configuración existentes en el repositorio de versiones de configuración
- Prevenir la inclusión de software no-autorizado

Estos procedimientos deben brindar una adecuada autorización y registro de todas las acciones.

Revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar periódicamente contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de

licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse.

Condición

- No existe evidencia de un documento formalmente aprobado dentro del SGC, en el que se registren las modificaciones y nuevas versiones de los sistemas implantados en la Escuela Politécnica del Ejército. (Evidencia: AUDI-ESPE-2007-ENT-005).
- No existe evidencia de un procedimiento para registrar la configuración base de los nuevos sistemas de aplicación y de las modificaciones realizadas a los mismos para mantener una configuración base. (Evidencia: AUDI-ESPE-2007-ENT-002, AUDI-ESPE-2007-ENT-003, MEM-2, ADM-1).
- No existe evidencia de un procedimiento para verificar periódicamente, que los usuarios no hayan instalado software no licenciado.
- No se evidenciaron políticas configuradas en el Active Directory. (Evidencia: MEM No.2007-187-ESPE-c-f-mr. Memo enviado a GT3 el 15 de noviembre del 2007).

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Alto riesgo en la continuidad de las operaciones, en caso de desastre.
- Problemas legales que enfrente la institución por software ilegalmente utilizado, virus y mal uso de licenciamiento.

Recomendación DS28.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, establecerá políticas y normativa para que la Escuela Politécnica del Ejército cuente con procedimientos en orden para identificar elementos de configuración y sus atributos, registrar elementos de configuración nuevos, modificados y eliminados, identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones, actualizar los elementos de configuración existentes en el repositorio de versiones de configuración, prevenir la inclusión de software no-autorizado; estos procedimientos deben brindar una adecuada autorización y registro de todas las acciones.

DS10. MANEJO DE PROBLEMAS E INCIDENTES

DS10.1. Escalamiento de problemas.-

Observación DS29.- No existe evidencia de un procedimiento de escalamiento de problemas reportados a la Unidad de Tecnología de Información y Comunicaciones.

Criterio

La gerencia deberá definir e implementar procedimientos de escalamiento de problemas, para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el proceso de escalamiento para la activación del plan de continuidad de TI.

Condición

- No se encuentra difundido apropiadamente el procedimiento de Soporte Técnico establecido por el SGC al personal de la Escuela Politécnica del Ejército. (Evidencia: AUDI-ESPE-2007- 001).
- No existe evidencia que se sigue el procedimiento de Soporte Técnico cuando se presentan problemas en los servicios prestados por la Unidad de Tecnología de Información y Comunicaciones. (Evidencias: SCG, GT2).
- No existe un registro en el que se incluyan los problemas escalados a otras unidades y a proveedores o consultores externos. (Evidencia: AUDI-ESPE-2007-ENT-001)
- No existen definidas políticas para la realización del monitoreo de la calidad de los servicios prestados por los proveedores y las áreas especializadas al resolver problemas reportados por los usuarios de la Escuela Politécnica del Ejército.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Pérdida de tiempo en las unidades especializadas en atender problemas mínimos.
- Pérdida de dinero al solicitar soporte externo a proveedores cuando este no lo amerita.

Recomendación DS29.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, establecerá e implantará políticas y normativa de escalamiento de problemas, para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el proceso de escalamiento para la activación del plan de continuidad de TI.

DS10.2. Seguimiento de Problemas y Pistas de Auditoría.-

Observación DS30.- No existe un proceso para seguimiento de problemas y pistas de auditoría.

Criterio

El sistema de administración de problemas deberá proporcionar adecuada pistas de auditoría que permitan el seguimiento de un incidente a partir de sus causas (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

Condición

- No existe evidencia del diseño e implantación de un sistema de administración de problemas que provea pistas de auditoría, que permitan dar seguimiento a los problemas presentados en las aplicaciones de los sistemas.

- No se evidenció la existencia de un proceso para administrar los cambios de las aplicaciones y configuraciones nuevas de los equipos informáticos.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Riesgo de repetición de incidentes por falta de seguimiento, que pueden afectar a la continuidad del servicio.

Recomendación DS30.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, debe establecer políticas y procedimientos para estructurar el sistema de administración de problemas, el que deberá proporcionar adecuadas pistas de auditoría que permitan el seguimiento de un incidente a partir de sus causas (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

DS10.3. Autorización de Accesos temporales y emergentes.-

Observación DS31.- No existe registro de autorizaciones de acceso temporal o de emergencia.

Criterio

Las autorizaciones de acceso temporal y de emergencia deberán ser documentadas en formularios estándar y mantenidas en archivo, aprobadas

por los gerentes apropiados, comunicadas de forma segura a la función de seguridad y las mismas deberán terminarse automáticamente después de un período predeterminado.

Condición

- No tiene políticas del uso de los accesos emergentes, debido a que el encargado del mantenimiento de las aplicaciones posee permisos de administrador. (Evidencia: AUDI-ESPE-2007-ENT-003).
- No se evidenció la existencia de un procedimiento de seguridad que indique quienes son las personas autorizadas para realizar cambios emergentes en los recursos de TI.
- El director de la Unidad de Tecnología de Información y Comunicaciones no tiene conocimiento de cuando se hace un cambio emergente en las aplicaciones, ya que no existe un registro con los datos de la persona, fecha, y motivo de dicho cambio.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Riesgo de cambios no autorizados, sabotaje, suspensiones de servicio sin que se pueda detectar estos hechos.

Recomendación DS31.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, definirá e implantará políticas para reglamentar las autorizaciones de acceso temporal y de emergencia, que deberán ser

documentadas en formularios estándar y mantenidas en archivo, aprobadas por los gerentes apropiados, comunicadas de forma segura a la función de seguridad y deberán terminarse automáticamente después de un período predeterminado.

DS10.4. Prioridades de procesamiento de emergencia.-

Observación DS32.- No existe evidencia de un procedimiento en donde se especifique la priorización de emergencias.

Criterio

La Gerencia de TI debe establecer, documentar y aprobar mediante el uso de programas adecuados las prioridades de procesamiento de emergencia.

Condición

- No existe evidencia de algún documento, en donde se identifique la prioridad de los problemas o modificaciones reportadas como emergentes, ni un análisis del impacto del suceso sobre la organización, el esfuerzo requerido y costo para su implementación.
- No existe un procedimiento para la toma de decisiones cuando se presente una emergencia. (Evidencia: DIR-2).

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Demora en atención de problemas graves que requieren una solución inmediata por solucionar problemas de menor prioridad que pueden esperar una solución.

Recomendación DS32.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, establecerá documentará y aprobará mediante el uso de programas adecuados las prioridades de procesamiento de emergencia.

DS11. ADMINISTRACIÓN DE DATOS

DS11.1. Sistema de administración de librerías de medios.-

Observación DS33.- No existe evidencia de un procedimiento para mantener el inventario de los recursos críticos de software y hardware de la Escuela Politécnica del Ejército.

Criterio

Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

Condición

- No existe evidencia de un inventario de todas las configuraciones de los componentes de hardware y versiones de las aplicaciones implantadas en

la Escuela Politécnica del Ejército. (Evidencias: AUDI-ESPE-2007-ENT-002, AUDI-ESPE-2007-ENT-005)

- No existe un sitio en la Unidad de Tecnología de Información Y Comunicaciones en donde se guarden los archivos de las configuraciones de los componentes de hardware y versiones de las aplicaciones implantadas en la Escuela Politécnica del Ejército. (Evidencia: DIR-2).
- No se ha definido un procedimiento de almacenamiento de los componentes de hardware y versiones de las aplicaciones implantadas en la institución.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Riesgo de pérdida de continuidad en las operaciones; no se puede aplicar el plan de contingencia.
- No se puede dar una solución oportuna, al presentarse un problema en los componentes de hardware y versiones de las aplicaciones implantadas.

Recomendación DS33.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, definirá e implementará procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

DS11.2. Respaldo y restauración

Observación DS34.- No existe la evidencia de un procedimiento para la administración de respaldos y recuperación.

Criterio

Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

Condición

- No está completamente definida la política para respaldar la información de los servidores de la Escuela Politécnica del Ejército, de acuerdo a un criterio de periodicidad; se verificó que en la ocasión cuando hubo fallas en el servidor en el que se encontraba instalada la aplicación financiera Olympo, no se pudo restaurar la información desde los medios magnéticos en los que se obtuvieron los respaldos de esta aplicación. (Evidencia:FIN-01).
- No se sigue un procedimiento para realizar los respaldos de los servicios prestados por la Unidad de Tecnología de Información Y Comunicaciones, que sirva para documentar las configuraciones de software y configuraciones de hardware controladas.
- No existe evidencia de un procedimiento de recuperación de la información.(Evidencia: AUDI-ESPE-2007-ENT-005).

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Pérdida de datos sensibles para la Escuela Politécnica Del Ejército.
- Desperdicio de recursos al tener que generar información ya ingresada en el sistema.
- Generación incorrecta de información manual para suplir a la información perdida.
- Riesgo en la continuidad de las operaciones.

Recomendación DS34.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del año en curso, definirá e implementará procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. En los procedimientos, se verificará el cumplimiento de los procedimientos de respaldo y la capacidad y el tiempo requerido para tener una restauración completa y exitosa, se probará los medios de respaldo y el proceso de restauración.

DS12. ADMINISTRACIÓN DE INSTALACIONES

DS12.1. Seguridad Física.-

Observación DS 35.- No existe evidencia de políticas y procedimientos de seguridad física.

Criterio

Deberán establecerse medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información, incluyendo el uso de dispositivos de información off-site, en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deben abarcar no sólo el área que contenga el hardware del sistema, sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por vandalismo.

Condición

- No existe evidencia de políticas de seguridad implantadas en el Centro de Cómputo de la Escuela Politécnica del Ejército. (Evidencia: AUDI-ESPE-2007-ENT-005).
- No existen un plan de mantenimiento a los equipos de seguridad.(Evidencia: DIR2)
- No se ha definido procedimientos de revisión del cumplimiento de los controles de acceso al Centro de Cómputo. (Evidencia: DIR2).

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

- Acceso indebido al Sistema de Información.
- Perdida de equipos, información y daños al Sistema de Información.

Recomendación DS35.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, desde el segundo trimestre del año en curso, establecerá medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información, incluyendo el uso de dispositivos de información off-site, en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deben abarcar no sólo el área que contenga el hardware del sistema, sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por vandalismo.

DS12.2. Escolta de Visitantes.-

Observación DS 36.- No existe un procedimiento de escolta de visitantes al ingreso al centro de Cómputo.

Criterio

Deberán establecerse procedimientos apropiados, que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información, sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

Condición

- No existe evidencia de un procedimiento para ingreso de personal visitante al Centro de Cómputo de la Escuela Politécnica del Ejército, ni registro en donde se indique el motivo del acceso y la fecha y duración del mismo .(Evidencia: DIR-2)
- No se han definido políticas de control referentes a la administración del Centro de Cómputo.

Causa

Falta de políticas y normatividad relativa al tema.

Efecto

Riesgo de sabotaje, daño o robo que puedan producirse en los equipos que se encuentran en el Centro de Cómputo.

Recomendación DS36.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, desde el segundo trimestre del año en curso, establecerá procedimientos apropiados, que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información, sean escoltadas por

algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

DS13. ADMINISTRACIÓN DE OPERACIONES

DS13.1. Operaciones Remotas

Observación DS37.- La calidad de las operaciones remotas entre los Centros de Apoyo con los sistemas de información implantados en el campus Sangolquí de la Escuela Politécnica del Ejército, es deficiente.

Criterio

Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la instalación remota sean identificadas e implementadas.

Condición

Al visitar Centros de Apoyo de la Escuela Politécnica del Ejército, se evidenció que los enlaces de comunicación provistos con los sistemas de información centrales, no son adecuados, porque no se puede enviar guías de educación a distancia, realizar matrículas, descargar archivos de guías y consultas a los tutores vía Web. (Evidencia: AUDI-ESPE-2007-ENT-008, Entrevista al coordinador del Centro de apoyo de Quevedo.)

Causa

No se realiza monitoreo ni evaluación de la calidad de los enlaces de comunicación remotas, para mejorar las características de servicio y cumplir

con las necesidades de los usuarios y estudiantes de los Centros de Apoyo de la Escuela Politécnica del Ejército.

Efecto

Pérdida de información importante en las actividades académicas de los alumnos de los Centros de Apoyo, cuando es enviada a la Escuela Politécnica del Ejército Sangolquí, provocando retrasos y errores en las evaluaciones y registro de los alumnos.

Recomendación DS37.-

El Director de la Unidad de Tecnología de Información y Comunicaciones, desde el segundo trimestre del año en curso, establecerá procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la instalación remota sean identificadas e implementadas.

El grado de criticidad de las recomendaciones emitidas anteriormente se pueden observar en la matriz de impacto que se encuentra en el Anexo B.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Actualmente la informática sirve como apoyo para la sistematización de las áreas de negocio tales como la administración y el manejo de la contabilidad y la nómina, lo cual causa como efecto que sea necesaria la realización periódica de un ejercicio práctico y formal de la auditoría en informática que permita asegurar que los recursos informáticos se están utilizando de manera adecuada para lograr los objetivos de la institución auditada.

- El ámbito de auditoría ofrece gran cantidad de herramientas y modelos que se pueden tomar como referencia para definir la manera en la que el gobierno de TI o la alta gerencia de una institución debe actuar para administrar adecuadamente los recursos y operaciones de los sistemas informáticos.

- Uno de los modelos más utilizados para ejecutar procesos de auditoría informática, es el marco de referencia COBIT, puesto que se puede adaptar a todas las organizaciones sin importar el tamaño y la actividad principal del negocio. Además cuenta con herramientas que ayudan a satisfacer múltiples tareas como la determinación de riesgos, definición de controles, buenas prácticas en la ejecución de los procesos y actividades que permitan optimizar la inversión de la información y evaluar el desempeño de las actividades y los recursos de tecnología de información.

- Concluimos que actualmente en nuestro medio no se pone real énfasis en temas referentes a, auditoría informática, controles y seguridad, en el desarrollo y desempeño de las actividades relacionadas con los recursos de tecnología de información, lo que ocasiona que no se tenga un conocimiento adecuado en estos temas y no se cuente con personal especializado para planificar y ejecutar estas tareas.

- La administración de las instituciones debe preocuparse de definir una persona que se encargue de la planificación y ejecución de las tareas de auditoría y evaluación periódica de los sistemas de información, mediante las que se pueda mantener estadísticas constantes del desempeño de los sistemas de información y de las personas y proveedores que son responsables de su adecuado mantenimiento.

5.2 RECOMENDACIONES

- Se recomienda capacitar al personal de las organizaciones en aspectos de seguridad y control de tecnología para que en base a los conocimientos adquiridos propongan estrategias adecuadas de administración y gobierno de TI, entiendan la importancia de evaluar los controles y den una apertura favorable a la realización de auditorías informáticas.

- Es recomendable la adopción de herramientas adecuadas en las que se base el personal de la de Tecnología de Información y Comunicaciones para la

administración de los recursos de tecnología, por ejemplo COBIT, la cual debe ser definida oficialmente como el marco de administración de tecnología.

- Se debe poner gran énfasis a los procedimientos de control y seguridad de la información puesto que hoy por hoy se ha constituido en un bien sumamente importante y la Escuela Politécnica del Ejército debería incentivar en sus estudiantes la investigación y análisis de las diferentes técnicas que pueden utilizarse para la detección, mitigación de riesgos y aseguramiento de la información.

- Es recomendable que las organizaciones adopten como una buena práctica, la planificación y la realización de ejercicios periódicos de auditoría informática, los cuales además de evaluar los sistemas de información deben hacer un seguimiento de recomendaciones señaladas por consultores externos para mejorar su situación actual.

BIBLIOGRAFÍA

- Auditoría Informática, Gonzalo Alonso Rivas, 1998 ediciones Díaz de Santos ISBN 84-87189-13.
- Auditoría en Informática Un enfoque metodológico y práctico, Lic. Enrique Hernández Hernández, 2002 editorial continental ISBN 970-24-0042-2.
- Auditoría informática, Echenique García José Antonio, segunda edición.
- Auditoría informática, Piattini Velthuis Mario Gerardo y Del Peso Navarro Emilio, segunda edición.
- COBIT versión 3 y 4
- http://www.network-sec.com/COBIT_DS
- http://itil.osiatis.es/
- http://www.reddeabastecimiento.org/COBIT%204.pdf
- http://www.auditoríasistemas.com/
- http://www.audit.gov.tw/span/span2-2.htm
- Auditoría Mario B. Ron Resumen
- "Evaluación de los Sistemas de Tecnología Informática y Revisión de las Seguridades de Plataforma Específica para la empresa EMAPA-I"/ Andrea M. Tobar.
- WHITTINGTON, O. Ray, PANY Kurt, Auditoría: Un enfoque Integral, Irwin McGrawHill, 12ª. Edición, Santa Fe de Bogota, Colombia, 2000
- Normas de Auditoría Interna emitidas por el The Institute of Internal Auditors
- Enciclopedia de la Auditoría, Grupo Editorial Océano, Barcelona, España, 1999
- MEIGS, Principios de Auditoría, Editorial Diana México 1975.

BIOGRAFÍA

SANDRA PATRICIA BALSECA ALCOCER

INFORMACIÓN PERSONAL

Cédula: 171550678-6

Fecha de nacimiento: Quito, Mayo 23 de 1982

Estado civil: Soltera

Teléfonos: 2 224-313

084056179

Dirección: Santa María # 710 y Juan de Velasco

Correo electrónico: sandy2pa@hotmail.com

sandy2pa@yahoo.es

EDUCACIÓN

Básica

Unidad Educativa “María Auxiliadora”

Bachillerato

Unidad Educativa “María Auxiliadora”

Unidad Educativa Experimental “Academia Almirante Nelson”

Bachiller en Ciencias Básicas – Especialidad Físico Matemático

Superior

ESCUELA POLITÉCNICA DEL EJÉRCITO

Ingeniería de Sistemas e Informática

ESTUDIOS ADICIONALES Y SEMINARIOS:

ESCUELA POLITÉCNICA DEL EJÉRCITO

“I Seminario de Inteligencia Artificial NeuroEspe-2004”

"II Congreso Nacional de Redes De Comunicación ESPnet 2004"

Módulos de Certificación CISCO CCNA, Escuela Politécnica del Ejército.

EXPERIENCIA LABORAL

2005 - 2008 Tribunal Supremo Electoral Dirección de Sistemas Informáticos.

IDIOMAS

INGLES: Nivel Medio, Aprobada suficiencia Idioma Inglés, Escuela Politécnica del Ejército – Sangolquí

MIGUEL EDUARDO CACHIMUEL QUEREMBÁS

INFORMACIÓN PERSONAL

Cédula: 171402060-7

Fecha de nacimiento: Quito, Abril 29 de 1982

Estado civil: Soltero

Teléfonos: 3160-523

098328844

Dirección: Urbanización Nueva Tola 2

Correo electrónico: hellspawn629@yahoo.com.ar

mcachimuel@deloitte.com

EDUCACIÓN:

2000 – 2007: Estudios Superiores, Escuela Politécnica del Ejército - Sangolquí, Facultad de Ingeniería en Sistemas e Informática.

1994 - 2000: Estudios Secundarios, Academia Militar "Borja #3", especialización "Físico – Matemático"**.**

1988 – 1994: Estudios Primarios, Pensionado "San Vicente".

ESTUDIOS ADICIONALES Y SEMINARIOS:

2007: Capacitación acerca de, Control Interno, Administración del Ambiente de Procesamiento del Computador, Revisiones de Controles Automáticos en Ciclos de Negocios, Deloitte & Touche – Ecuador

2006: Módulos de Certificación CISCO CCNA, Escuela Politécnica del Ejército.

2004: I Seminario de Inteligencia Artificial NeuroESPE – 2004, Escuela Politécnica del Ejército.

2004: Hands on Lab Microsoft Office 2003, Compueducación Ejecutiva.

2004: Seminario de Seguridad a Nivel de la Red Interna y en las Aplicaciones con ISA Server 2004 y Herramientas de Microsoft Windows Server 2003 para Gestión de Seguridad, Microsoft TechNet.

2004: II Congreso Nacional de Redes de Comunicación ESPEnet 2004, Escuela Politécnica del Ejército.

2003: Curso de Excel 2000, NEW HORIZONS.

2002: Curso de Internet y Diseño de Páginas Web, programación HTML, SECAP.

EXPERIENCIA LABORAL

2007: Deloitte & Touche Auditor Informático – Junior A

- Auditoría Interna de Sistemas –Banco Pichincha
- Revisión de Controles de los Sistemas:
  - Corporación Financiera Nacional
  - Banco del Estado
  - Empresa del Centro Histórico de Quito
  - Sucasa
  - Ecuador Bottling Company
  - Lafarge - Ecuador
  - Banco Ecuatoriano de la vivienda

2006: Intser, Soporte Técnico y Helpdesk, administrador de red "Corporación Participación Ciudadana", con Windows 2000 Server, ISA Server 2000, estaciones de trabajo con Windows XP, seguridad con paquetes Symantec y firewalls Symantec.

2004: Binaria Sistemas, Practicante en el Área de Consultorías Microsoft, Ayudando en soporte a usuarios, migración de sistemas de Windows NT 4.0 a Windows 2003 Server.

2002: Binaria Sistemas, Vendedor, Marca Compaq.

2000: Ayudante de Instalación de Cableado.

1999: Notaría 36 de la Dra. Ximena Borja de Navas, Digitador.

IDIOMAS:

INGLES: Nivel Medio, Aprobada suficiencia Idioma Inglés, Escuela Politécnica del Ejército – Sangolquí.