ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

Carrera en Ingeniería en Contabilidad y Auditoría CPA.

TESIS DE GRADO

Previa a la obtención del Título de:

Ingeniero en Contabilidad y Auditoría CPA.

TEMA:

"Auditoría a la Gestión de las Tecnologías de la Información al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012".

AUTOR:

Enrique Marcelo Beltrán Bravo

Riobamba – Ecuador

2014

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo, "Auditoría a la Gestión de las Tecnologías de la Información al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012" ha sido revisado en su totalidad quedando autorizada su presentación.

Ing. Jimena Catalina Viteri Ojeda	Ing. Carlos Alfredo Ebla Olmedo
DIRECTOR DE LA TESIS	**MIEMBRO DEL TRIBUNAL**

CERTIFICADO DE RESPONSABILIDAD

Las ideas expuestas en el presente trabajo de investigación y que aparecen como propias es responsabilidad absoluta del Autor.

ENRIQUE MARCELO BELTRÁN BRAVO

DEDICATORIA

En primer lugar dedico este trabajo a papito Dios por cada día de vida que nos permite estar junto a las personas que más quiero.

A mi papi Rosendo y a mi mami María que ha sido el soporte y el ejemplo a seguir, por sus consejos y el esfuerzo día a día para que sus hijos sean los mejores.

A mis hermanos Carlos, Elizabeth, Cynthia y en especial a Edgar Rosendo que por cuestiones de la vida se nos adelantó y estoy seguro de que desde ahí nos cubre con sus bendiciones, y por su apoyo incondicional en todo momento.

A mis sobrinos Heidi, Jhair y sobre todo Andy que me demuestra con su ternura e inocencia que con las cosas más sencillas de la vida uno puede ser la persona más feliz del mundo. Gracias por haber llegado a mi vida mis amores.

AGRADECIMIENTO

Agradezco de todo corazón a mis padres que con cada gota de sudor me demostraron que nada en la vida viene fácil y hay dar todo de mí para poder alcanzar mis sueños y anhelos.

A mis hermanos y sobrinos son razón de superación e inspiración para cumplir con todos mis objetivos y metas, por estar siempre ahí incondicionalmente.

A la escuela superior politécnica de Chimborazo que me abrió las puertas y me permitió obtener los conocimientos necesarios para ejercer una carrera que será el sustento de mi vida.

De manera especial a los docentes Ing. Jimena Catalina Viteri Ojeda y al Ing. Carlos Ebla Olmedo, por todo su apoyo, conocimiento y paciencia que me han permitido culminar con éxito este trabajo.

RESUMEN

La presente auditoría a la Gestión de las Tecnologías de la Información (AGTI) al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012, se la realizo con el fin de evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.

Se utilizaron diferentes métodos de investigación tales como método narrativo, descriptivo, observación directa, encuestas, entrevistas, los cuales permitieron obtener información veraz, segura y adecuada, que permitió establecer la situación actual del departamento.

Se aplicaron cuestionarios de control interno por cada una de los componentes del Subgrupo 410 que establece la Contraloría General del Estado, mediante a las cuales se evidenciaron inconsistencias en la gestión de las tecnologías de la información, para mitigar el nivel de riesgo detectado, se desarrolló un plan de mejoras el cual se detalla en la fase III del informe final de auditoría, cuya aplicación por parte de los directivos departamentales ayudaran enormemente en el cumplimiento de los estándares analizados.

Las recomendaciones emitidas en el presente informe de auditoría se realizaron con la finalidad de que se tomen las medidas correctivas necesarias en beneficio del crecimiento departamental y por ende del crecimiento institucional.

SUMMARY

This audit to Management of Information Technologies (AMIT) to the Telematics and Systems Department "DESITEL" of ESPOCH in Riobamba, in Chimborazo Province, in 2012, was performed to evaluate and measure the level of compliance on the Management of Information Technologies.

Different research methods such as narrative method, descriptive, direct observation, surveys and interviews were used which allowed to obtain accurate, reliable and adequate information and established the current status of the Department.

Internal control questionnaires were applied for each of the components of the Sub-group 410 established by the Government Accountability Office, whereby, inconsistencies were evident in the management of information technology. To mitigate the level of risk detected an improvement plan was developed, which is detailed in the phase III of final audit report, which application by the department managers will greatly help in meeting the standards analyzed.

The recommendations issued in this audit report are made in order that the necessary corrective actions are taken for departmental growth and therefore the institutional growth.

ÍNDICE DE CONTENIDOS

Título **Pág.**

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

No	Título	Pág.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

CAPÍTULO I:

CAPÍTULO: 1

1. El Problema

1.1 Antecedentes del problema

A continuación se detallan algunas de las debilidades que fundamentan el tema de investigación:

Cobertura limitada de internet para los estudiantes, docentes y empleados, debido a que las conexiones de red de Desitel son intermitentes, lo cual provoca lentitud en acceso al internet.

De la misma manera el portal de calificaciones tiende a colapsar de manera frecuente, lo que produce inquietud y enojo al no tener la información requerida en el tiempo estimado. La información en muchos de los casos son intercambiadas con otros estudiantes, o cambios sin autorización de datos como contraseñas, matriculas. Lo que ocasiona malestar, inseguridad y pérdida de tiempo en el curso normal de sus actividades.

1.1.1 Formulación del problema de investigación

¿Cómo incide la realización de una auditoría informática en la determinación de hallazgos para mejorar la gestión de las tecnologías de la información y comunicación?

1.1.2 Delimitación del problema

Delimitación por el campo de aplicación

- Campo: Control
- Área: Auditoría
- Aspecto: Auditoría a la Gestión de las Tecnologías de la Información.

Temporal: El tiempo de la investigación será de diciembre 2013 a mayo 2014.

Espacial: La investigación se realizará al departamento de sistemas y telemática "DESITEL" de la ESPOCH.

1.2 Objetivos

1.2.1. Objetivo general

Realizar una Auditoría a la Gestión de las Tecnologías de la Información(AGTI) al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012, con el fin de evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.

1.2.2. Objetivos específicos

1. Realizar un diagnóstico situacional del departamento, con el propósito principal de determinar las Fortalezas, Oportunidades, Debilidades y Amenazas, con la aplicación de Normas de la Tecnología de Información.
2. Evaluar el sistema de control interno mediante la aplicación de las normas de control interno emitidas en el grupo 410 acerca de las tecnologías de la información establecidas por la contraloría general del estado, como elemento principal que direccione la investigación.
3. Presentar el Informe de Auditoría Informática al departamento de sistemas y telemática DESITEL.

1.3 Justificación de la investigación

La Auditoría a la Gestión de las Tecnologías de la Información se ha constituido, en uno de los modelos de planificación y gestión que mayor interés ha despertado entre los directivos; debido a que se trata de un modelo de enfoque u orientación estratégica que da una solución clara y práctica, y cuyo objetivo se ha centrado en proporcionar un conjunto de herramientas que faciliten el logro del éxito competitivo en el largo plazo.

Al realizar el tema de investigación al DESITEL se crea un aporte teórico muy importante que servirá de base para nuevos estudios relacionados al tema, generando así el progreso del departamento , de la ESPOCH y la sociedad, al ayudarse de herramientas de control que permitan un mejor manejo institucional, siendo aplicable a la práctica.

Por lo tanto, es necesario adoptar las Normas de Control Interno para Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos especificadas en el grupo 410 acerca del uso de las normas de Tecnologías de la Información T.I, emitidas por la Contraloría General del Estado, para corregir posibles debilidades en la aplicación de dichas normas vigentes y se vean reflejadas en el desarrollo del departamento.

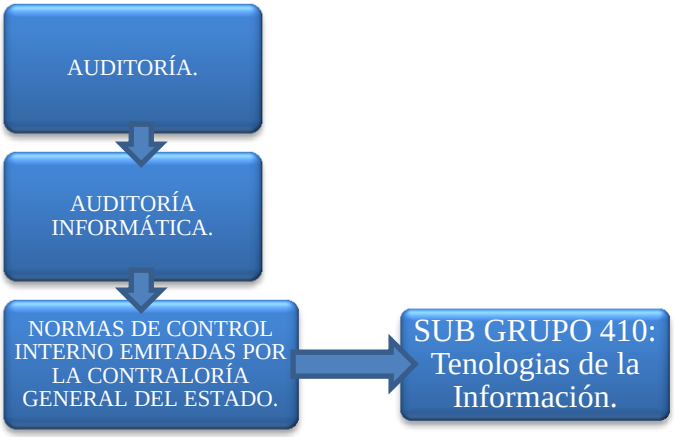
CAPÍTULO II:

2. Marco Teórico

2.1 Hilo conductor

El hilo conductor que se detalla a continuación es la guía a seguir para la formación del marco teórico, abarcando temas como: auditoria, auditoria informática y normas de la contraloría, los cuales se convierten en el fundamento teórico para el desarrollo del tema investigativo.

Figura No 1: Hilo Conductor



Fuente: Auditoria Informática.
Elaborado por: Autor

2.2. Auditoría

Es un examen objetivo, sistemático y profesional de las operaciones administrativas o financieras, tecnológicas, efectuado con posterioridad a su ejecución, con la finalidad de verificarlas y evaluarlas emitiendo como resultado un informe que contenga observaciones, conclusiones y recomendaciones. (McGraw, 2000)

Podemos descomponer este concepto en los siguientes elementos fundamentales:

Figura No 2: Conceptualización de Auditoría

EXAMEN OBJETIVO	Analiza los hechos ocurridos descartando cualquier practicidad de supuestos.
EXAMEN SISTEMÁTICO	Por cuanto su ejecución obedece a procesos científicamente diseñados.
EXAMEN PROFESIONAL	Por cuanto lo realizan profesionales en auditoria o contaduría pública, también pudiendo ser efectuadas por profesionales de áreas a fin.

Fuente: (López Hermoso, 2013)

Elaborado por: Autor

2.2.1. Clasificación de las auditorías

Existen varias formas de clasificar a la auditoría, simplemente si se piensa en las áreas de especialización, éstas darían una clasificación extensa y válida. Sin embrago, en esta ocasión se mencionarán dos tipos, las cuales pueden aportar elementos de interés en su posterior estudio.

La auditoría de gestión, está orientada a la evaluación de aspectos relacionados con la eficiencia y productividad de las operaciones de una organización. Este tipo de auditoría, al igual que la integral que se menciona a continuación, puede ser desempeñada tanto por auditores externos como internos.

Constituye objeto de la auditoría de gestión, el proceso administrativo, las actividades de apoyo y operativas; la eficiencia, efectividad y economía en el empleo de los recursos humanos, financieros, ambientales, tecnológicos y de tiempo; y el cumplimiento de las atribuciones institucionales.

La auditoría integral, se realiza con el fin de evaluar en su totalidad los objetivos que existen en una organización, es decir, los relacionados con información financiera, salvaguardar los activos, eficiencia y normativa, entre otros. Este tipo de auditorías también pueden ser realizadas tanto por auditores externos como internos (McGraw, 2000).

En ninguna de las clasificaciones anteriores se mencionó de manera específica a la auditoría de las tecnologías de información y comunicaciones. Esto es así, porque esta

disciplina no excluye a ninguna de las auditorías mencionadas, por el contrario, todas ellas deben integrar a la auditoría en tecnologías de información para efectuar revisiones específicas derivadas del uso de la tecnología de información en los servicios públicos.

En síntesis la aplicación del concepto de auditoria dentro de una organización nos permite conocer la situación en la que se encuentra, esta debe ser ejecutada por un profesional externo e independiente, lo cual ayudara a reflejar la legitimidad del proceso y su veracidad.

2.3 Auditoría informática

Para adentrarse en el proceso de una auditoría a las tecnologías de la información y comunicaciones, es requisito imprescindible comprender los conceptos de sistemas, información y tecnologías de las comunicaciones los cuales se detallaran a continuación.

Al lograr una visión y conocimientos del entorno informático, el auditor juzgará, de manera suficiente, la naturaleza de la problemática y riesgos a los cuales se verá enfrentado al planificar y realizar la auditoría.

2.3.1. Definición de auditoría informática

Es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de- una forma puntual y objetiva, a instancias de 1a dirección y con la intención de ayudar a mejorar conceptos como la seguridad, eficiencia y rentabilidad del servicio informático (López Hermoso, 2013).

2.3.2. Auditoría de tecnología de información

La Auditoría de Tecnología de Información es el proceso de recolectar y evaluar la evidencia para determinar si los Sistemas de Información y los recursos relacionados (base de datos, redes, aplicaciones, personal, infraestructura, presupuesto, etc.) protegen adecuadamente los activos, mantienen los datos y la integridad del Sistema de Información, proveen información relevante y confiable. Además de asegurar que las Tecnología de

Información coadyuven a los objetivos organizacionales y que los eventos no deseados serán detectados oportunamente para ser evitados.[1]

Organizaciones internacionales la definen como un examen sistemático del uso, de los recursos y los flujos de información, verificado con las personas y los documentos existentes, con el propósito de establecer la medida en que éstos están contribuyendo a los objetivos organizativos. [2]

Constituye pues, un diagnóstico sobre el uso de la información dentro de la organización; De forma sintética podemos indicar que:

- Implica una revisión del uso de la información dentro de la organización.
- Identifica y mapea los recursos de información disponibles.
- Determina qué información es esencial, por qué y para quién.
- Cómo se utiliza y se comparte.
- Establece los costes y valor de la información.
- Evalúa la eficacia y eficiencia del sistema de información existente.
- Las necesidades actuales y uso de la información por áreas y colectivos.
- La efectividad de la utilización y distribución del recurso.
- Identifica las posibles lagunas, inconsistencias y duplicidades.
- La existencia de nuevos recurso.
- Los puntos débiles y oportunidades del sistema.
- El comportamiento y prácticas de los usuarios respecto de la información.

2.3.3. Auditoría de gestión a las Tics

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestra) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información,

[1] (Alfaro, 2008)
[2] Propuesta por la Information Resources Management Network (IRM), un grupo de trabajo vinculado a la británica Association for Information Management (Aslib) y recientemente renombrado como Knowledge and Information Resources Management Network (Kimnet).

efectividad de los controles establecidos y la optimización de los recursos tecnológicos. (OLACEFs, 2011)

2.3.4. Objetivos de la auditoría informática

Según (Tamayo Alzate, 2010), la evaluación a los sistemas computacionales, a la administración al centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos:

i. Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
ii. Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.

2.3.5. Características de los sistemas de información

Si se tuviera que resumir con una sola frase, el principal objetivo de un sistema de información dentro de una organización, se podría afirmar que éste se encarga de entregar la información oportuna y precisa, con la presentación y el formato adecuados a la persona que la necesita dentro de la organización, para tomar una decisión o realizar alguna operación y justo en el momento en que esta persona necesita disponer de dicha información. Actualmente, la información debe ser considerada uno de los recursos más valiosos de una organización y el sistema de información es el encargado de que ésta sea gestionada siguiendo criterios de eficiencia y eficacia.

La información será útil para la organización, en la medida que facilite la toma de decisiones, por lo que ha de cumplir una serie de requisitos, entre los cuales cabe destacar:

Figura No 3: Características de los sistemas de información

Fuente: (Tamayo Alzate, 2010).

Elaborado por: Autor

Exactitud: La información ha de ser precisa y libre de errores.

Completitud: La información debe contener todos aquellos hechos que pudieran ser importantes.

Economicidad: El costo en que se debe incurrir para obtener la información debería ser menor que el beneficio proporcionado por ésta a la organización.

Confianza: Para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes de información.

Relevancia: La información ha de ser útil para la toma de decisiones. En este sentido, conviene evitar todos aquellos hechos que sean superfluos o que no aporten ningún valor.

Nivel de detalle: La información debe presentar el nivel de detalle indicado a la decisión a que se destina. Se debe proporcionar con la presentación y el formato adecuados para que resulte sencilla y fácil de manejar.

Verificabilidad: La información ha de poder ser contrastada y comprobada en todo momento**.** [3]

Por otra parte, no se debe olvidar que el exceso de información también puede ser causa de problemas, suponiendo un obstáculo en vez de una ayuda para la toma de decisiones.

[3] OLACEFS (XIV CONCURSO ANUAL DE INVESTIGACIÓN "Auditoria de Gestión a las Tecnologías de la Información y Comunicación"

Es así como la información y el conocimiento que acumulan las organizaciones, deben ser considerados como un recurso más, al mismo nivel que el capital, los bienes, las instalaciones o el personal.

En consecuencia, es necesario protegerlo y controlarlo adecuadamente, para que pueda contribuir a la realización de los objetivos y metas fijados por la organización.

2.3.6. Estructura de los sistemas de información

Los sistemas de información están compuestos por diferentes elementos que interaccionan entre sí, entre los cuales se pueden encontrar cinco componentes fundamentales: personas, actividades, datos, redes y tecnología.

Las personas engloban a los propietarios del sistema (entendiendo como tales, a aquellas personas que patrocinan y promueven el desarrollo de los sistemas de información), a los usuarios (directivos, ejecutivos medios, jefes de equipo, personal administrativo), a los diseñadores y a los desarrolladores.

Los datos constituyen la materia prima empleada para crear información útil.

Dentro de las actividades, se incluyen los procesos que se llevan a cabo en la organización y las actividades de procesamiento de datos y generación de información que sirven de soporte a las primeras.

En el componente redes, se analizan la descentralización de la organización, la distribución de los restantes componentes elementales en los lugares más útiles (oficinas, dependencias, delegaciones, etc.), así como la comunicación y coordinación entre dichos lugares.

Por último, el componente tecnología, hace referencia tanto al hardware como el software de un sistema de información. Se pone de manifiesto la existencia de una interrelación entre los elementos propios de la organización y los sistemas de información.

2.3.7 Procesos de los sistemas de información

La captura de datos puede ser manual o automatizada y, en general, es conveniente realizarla en el momento en que se produce el hecho al que está asociado.

En la etapa de proceso, se transforman los datos de entrada del sistema en información útil, mediante una serie de operaciones de cálculo, agregación, comparación, filtrado, presentación, etc. Estas operaciones, generalmente son realizadas con la ayuda de sistemas informáticos. La información útil se plasma en una serie de documentos, informes y gráficos, para ser distribuida a las personas adecuadas dentro de la organización. Esta información, así como los datos de partida, se almacenan generalmente, en un soporte informático para poder ser reutilizados en cualquier momento.

La retroalimentación (feedback) de la información obtenida en todo este proceso, se puede utilizar para realizar ajustes y detectar posibles errores en la captura de los datos y/o en su transformación.

2.3.8 Clasificación de los sistemas de información

Por lo general, las clasificaciones más extendidas de los sistemas de información suelen agrupar éstos en función de su propósito. De una forma muy global, puede considerarse que existen dos propósitos básicos para los sistemas:

Soporte a las actividades operativas: Que da lugar a sistemas de información para actividades más estructuradas (aplicaciones contables, ventas, adquisiciones y, en general, lo que se denomina "gestión empresarial" o también sistemas que permiten el manejo de información menos estructurada: aplicaciones ofimáticas, programas técnicos para funciones de ingeniería, etc.

Soporte a las decisiones y el control de gestión: Que puede proporcionarse desde las propias aplicaciones de gestión empresarial (mediante salidas de información existentes) o a través de aplicaciones específicas.

Los sistemas de soporte a las actividades operativas, surgen para automatizar actividades operacionales intensivas en el manejo de datos. Concretamente, se centran en áreas como administración (contabilidad y facturación) y gestión de personal, extendiéndose a otras actividades como la venta, la compra o la producción. Estos permiten recoger los datos básicos en las operaciones y se les denomina sistema de procesamiento transaccional.

Actualmente, estos sistemas forman parte de lo que normalmente las organizaciones denominan como su "Sistema de Gestión Empresarial" o ERP (Enterprise Resources Planning).

Los sistemas de información para la toma de decisiones, permiten sacar provecho a los datos recogidos por los sistemas transaccionales, siendo capaces de proporcionar información para la gestión. Estos sistemas, permiten generar informes para los directivos de la organización, con el propósito de mejorar el control de gestión de las distintas áreas funcionales. De este modo, se consigue agilizar el proceso de toma de decisiones, al proporcionar la información necesaria de forma rápida, precisa y fiable.

Los sistemas de soporte a la dirección son los que asisten a los directivos de las organizaciones en todos los aspectos de un proceso de toma de decisiones: generación de alternativas, análisis de ellas, simulación de resultados que se obtendrían con cada una de ellas, etc. Se puede afirmar que estos sistemas van un paso más allá que los sistemas de información tradicionales.

2.3.9 Tipos de auditoría informática

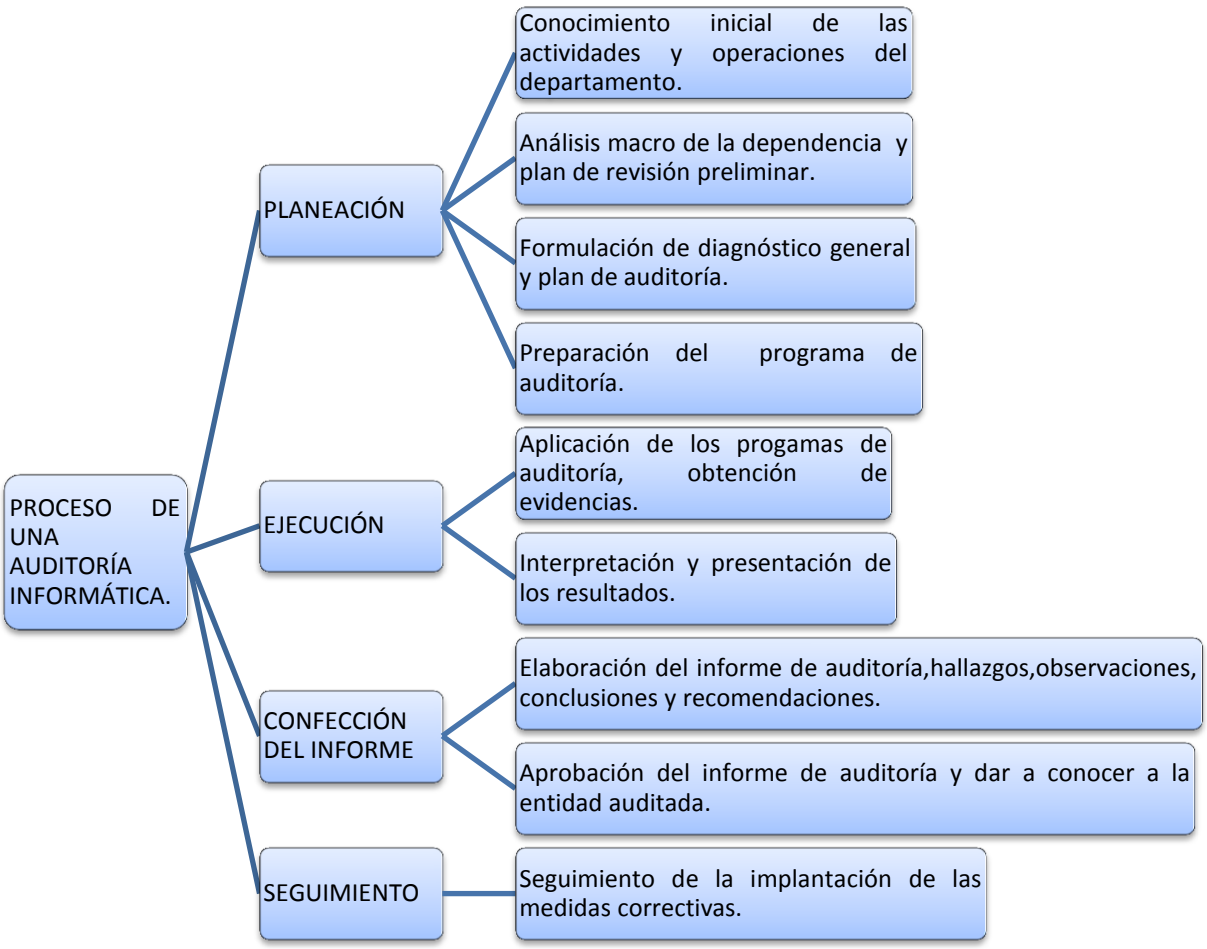
Dentro de la auditoría informática (Rivas, 1998) destaca los siguientes tipos que formaran parte de nuestra investigación:

- Auditoría de la seguridad: referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- Auditoría de la seguridad física: referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta.
- Auditoría de la seguridad lógica: comprende los métodos de autenticación de los sistemas de información.

2.3.10. Proceso de una auditoría informática

El proceso una auditoria informática se desarrolla en las fases y etapas que se detallan a continuación:

[1]**Figura No 4:** Proceso de una Auditoría Informática



Fuente: (Tamayo Alzate, 2010)

Elaborado por: Autor

Los puntos anteriormente mencionados no hablan sobre la auditoria informática, donde se especifica su clasificación, planificación ejecución entre otros, los cuales son los puntos claves a seguir en la planificación de la auditoría de tecnologías de información[4].

[4] Muñoz Razo Carlos. Auditoría en Sistemas Computacionales, Primera Edición, 2002 (pág. 186 y 236)

2.4 Normas de control interno para la auditoría informática

Para el siguiente tema de investigación tomaremos como base las Normas de Control Interno de la Contraloría General del Estado, emitidas para la aplicación de forma obligatoria a las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos.

Establecidas en el grupo 400, subgrupo 410, normas referentes a las Tecnologías de la Información para la evaluación del control interno (Contraloria General del Estado, 2009).

SUB GROP 410.- Tecnología de la Información

410-01 Organización informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional. La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo. Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones

Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo. La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal. La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410–03 Plan informático estratégico de tecnología

La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno. El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario. La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes

de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico. El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria. La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran. Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización. Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos. Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos. La unidad de tecnología de información deberá promover y establecer convenios

con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

410-05 Modelo de información organizacional.

La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes. El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente. Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos

La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.

2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.

3. La formulación de los proyectos considerará el *Costo Total de Propiedad CTP*; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios

relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.

4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.

5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.

6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.

7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.

8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.

9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.

10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo

La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso

contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.

4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos

y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.

7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.

8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica

La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el

plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

410-09 Mantenimiento y control de la infraestructura tecnológica

La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.

2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.

3. Control y registro de las versiones del software que ingresa a producción.

4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.

5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.

8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;

2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado.

3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;

4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;

5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.

6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;

7. Consideración y disposición de sitios de procesamiento alternativos.

8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado. Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la

responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.

2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.

3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.

4. Plan de recuperación de desastres que comprenderá:

Actividades previas al desastre (bitácora de operaciones)

Actividades durante el desastre (plan de emergencias, entrenamiento)

Actividades después del desastre.

5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.

6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

7. El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.

2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.

3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.

4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.

5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.

6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.

7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.

8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.

9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.

10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad. La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran. La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos. La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet

La unidad de tecnología de información considerará el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.

410-15 Capacitación informática

Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

410-16 Comité informático

Para la creación de un comité informático institucional, se considerarán los siguientes aspectos:

El tamaño y complejidad de la entidad y su interrelación con entidades adscritas.

La definición clara de los objetivos que persigue la creación de un comité de informática, como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad.

La conformación y funciones del comité, su reglamentación, la creación de grupos de trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.

410-17 Firmas electrónicas

Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento. El uso de la firma electrónica en la administración pública se sujetará a las garantías, reconocimiento, efectos y validez señalados en estas disposiciones legales y su normativa secundaria de aplicación. Las servidoras y servidores autorizados por las instituciones del sector público podrán utilizar la firma electrónica contenida en un

mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público que ocupan. Los aplicativos que incluyan firma electrónica dispondrán de mecanismos y reportes que faciliten una auditoría de los mensajes de datos firmados electrónicamente.

a) Verificación de autenticidad de la firma electrónica

b) Coordinación interinstitucional de formatos para uso de la firma electrónica

Con el propósito de que exista uniformidad y compatibilidad en el uso de la firma electrónica, las entidades del sector público sujetos a este ordenamiento coordinarán y definirán los formatos y tipos de archivo digitales que serán aplicables para facilitar su utilización. Las instituciones públicas adoptarán y aplicar los estándares tecnológicos para firmas electrónicas que las entidades oficiales promulguen, conforme a sus competencias y ámbitos de acción.

c) Conservación de archivos electrónicos

Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros, bajo la responsabilidad del usuario y de la entidad que los generó. Para ello se establecerán políticas internas de manejo y archivo de información digital.

d) Actualización de datos de los certificados de firmas electrónicas

Las servidoras y servidores de las entidades, organismos y dependencias del sector público titulares de un certificado notificarán a la entidad de certificación de Información sobre cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado. Cuando un servidor público deje de prestar sus servicios temporal o definitivamente y cuente con un certificado de firma electrónica en virtud de sus funciones, solicitará a la entidad de certificación de información, la revocación del mismo, además, el superior jerárquico ordenará su cancelación inmediata. El dispositivo portable seguro será considerado un bien de la entidad o dependencia pública y por tanto, a la cesación del servidor, será devuelto con la correspondiente acta de entrega recepción.

e) Seguridad de los certificados y dispositivos portables seguros

Los titulares de certificados de firma electrónica y dispositivos portables seguros serán responsables de su buen uso y protección. Las respectivas claves de acceso no serán divulgadas ni compartidas en ningún momento. El servidor solicitará la revocación de su certificado de firma electrónica cuando se presentare cualquier circunstancia que pueda comprometer su utilización.

f) Renovación del certificado de firma electrónica

El usuario solicitará la renovación del certificado de firma electrónica con la debida anticipación, para asegurar la vigencia y validez del certificado y de las actuaciones relacionadas con su uso.

g) Capacitación en el uso de las firmas electrónicas

La entidad de certificación capacitará, advertirá e informará a los solicitantes y usuarios de los servicios de certificación de información y servicios relacionados con la firma electrónica, respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados. Esta capacitación facilitará la comprensión y utilización de las firmas electrónicas, en los términos que establecen las disposiciones legales vigentes.

CAPÍTULO III:

3. Marco Metodológico

Al fin de obtener la información referente al tema de investigación se utilizo los siguientes tipos, métodos, técnicas e instrumentos los cuales se detallan a continuación:

3.1. Tipos de estudios de investigación

Los tipos de investigación que se utilizaron para la realización de la Auditoría a la Gestión de las Tecnologías de la Información son los que se detallan a continuación:

- **Exploratoria:** Por medio de la aplicación de este tipo de investigación se obtuvieron los datos, elementos e información suficiente que sirvieron para dar inicio a la auditoria a la Gestión de las Tecnologías de la Información.
- **Descriptiva:** Por medio de la investigación descriptiva se llegó a conocer las situaciones predominantes del DESITEL a través de la descripción exacta de las actividades, objetos, procesos y personas.
- **Explicativa:** Se aplicó a partir de la determinación de los hallazgos existentes en cada una de las áreas del DESITEL, dando a conocer las causas y efectos que se encuentran plasmadas en el informe final.

3.2. Métodos, técnicas e instrumentos

3.2.1 Métodos de investigación

- **Método Científico:** El tema investigativo se baja en las normas de control interno emitidas por la Contraloría General del Estado establecidas en el Sub grupo 410, a las cuales se sujetan todas las Instituciones del sector público.

- **Método Deductivo:** Se establecieron conclusiones lógicas a partir se obtención de los resultados adquiridos de la aplicación de la AGTI a los departamentos del DESITEL.

- **Método Analítico:** Con la información recopilada obtenida y en cada procedimiento aplicado en el desarrollo de la auditoría en el cual se fija el respectivo análisis a fin de determinar si es o no un hallazgo.

3.2.2 Técnicas e instrumentos de investigación

- **Análisis Documental:** Ese Se hizo el análisis al Plan Integral Informático y al reglamento existente al cual se rigen el personal existente en el DESITEL. **Entrevista:** Se realizó para obtener la información general la cual se convirtió en la base para dar inicio a la auditoria a la Gestión de Tecnologías de la Información.

- **Encuesta:** Se utilizó en la planificación específica en donde se obtuvo un conocimiento más específico de las áreas existentes del DESITEL.

- **Cuestionario:** Se aplicó en la evaluación del Sistema del Control Interno el cual ayuda a la obtención de los hallazgos existentes en el DESITEL.

3.3. Diagnóstico situacional

Previo al análisis FODA dentro del Departamento de Sistemas y Telemática, se hizo una exploración de la información dentro de la Escuela Superior Politécnica de Chimborazo, por medio de la aplicación de encuestas que se realizaron a las autoridades, técnicos, conserjes del departamento, directores de escuela y estudiantes de la ESPOCH, cuya información servirá de base para este análisis.

3.4 Análisis FODA

El análisis FODA consiste en conocer las fortalezas, oportunidades, debilidades y amenazas, y con esto manejar de una manera eficiente las fortalezas y oportunidades existentes para este análisis y disminuir al máximo el riesgo de las debilidades y amenazas que nos ayudara a tener un control interno sólido.

3.5 Planificación para la matriz FODA.

Objetivo: Determinar los pasos a seguir para determinar las fortalezas, oportunidades, debilidades y amenazas existente en el departamento de Sistemas y Telemática "DESITEL".

3.6. Recopilación de información para el análisis FODA

La recopilación de información para el análisis FODA se obtuvo del resultado de la investigación a cada una de las direcciones de las facultades Escuela Superior Politécnica de Chimborazo en el cual se determinó que el número de total de estudiantes es 12355, como se muestra en la siguiente tabla.

Tabla No 1: Número de estudiantes.

FACULTAD	No DE ESTUDIANTES
Administración de Empresas	2959
Ciencias	1855
Ciencias Pecuarias	884
Informática y Electrónica	2152
Mecánica	1295
Salud Pública	2319
Recursos Naturales	891

FUENTE: DESITEL
ELABORADO: Autor

Una vez determinada la población se procede con el cálculo de la muestra:

Dónde:

n= tamaño de la muestra a encontrar.

Z: nivel de confianza.

p: variable positiva.

q: variable negativa.

N: tamaño de la muestra.

E: error de margen.

$$n=\frac{z^2\,Npq}{(\mathrm{N}-1)E^2+Z^2pq}$$

$$n=\frac{1{,}96^2*12355*0{,}5*0{,}5}{(12355-1)0{,}05^{\ 2}+1{,}96Z^2*0{,}5*0{,}5}$$

$$n = \mathbf{373}\ \textbf{Encuestas}$$

3.6.1 Determinación de la matriz FODA

En la siguiente tabla se determinan cada una de las fortalezas, debilidades, oportunidades y amenazas existentes en las diferentes áreas del departamento, con la finalidad de establecer la situación actual del DESITEL.

Tabla No 2: Matriz FODA

FORTALEZAS	DEBILIDADES
F1: Experiencia en mantenimiento software y hardware de equipos electrónicos y de Telecomunicaciones.	**D1:** Falta de infraestructura Física.
F2: Dominio de sistemas de videoconferencias.	**D2:** Falta de personal para cubrir con el plan de mantenimiento anual en la Espoch.
F3:Trabajo en Equipo	**D3:** Falta de plan de capacitación y especialización
F4: Experiencia en instalación de redes informáticas. (Hardware).	**D4:** Falta de recursos económicos y materiales para cubrir imprevistos de último momento en las diferentes dependencias de la ESPOCH.
F5: Personal identificado con la institución	**D5:** Falta de accesorios de cómputo, en la bodega institucional.
F6: Zonas Wifi para los usuarios institucionales	**D6:** No existen repuestos para los equipos electrónicos ni de telecomunicaciones en la bodega
F7: Red de Telefonía IP	**D7:** Inequitativa distribución de responsabilidades.
F8: Personal con experiencia	**D8:** Poca comunicación entre el área y las dependencias.
F9: Dominio de sistemas de videoconferencias.	**D9:** Desprestigio departamental
F10: Dominio de varias aplicaciones informáticas para el soporte institucional	**D10:** Falta de cobertura Wifi para cumplir los indicadores de acreditación
OPORTUNIDADES	**AMENAZAS**
O1: El avance tecnológico proporciona un abanico de posibilidades que pueden ayudar a las actividades académicas y administrativas	**A1:** Disminución en el apoyo financiero.
O2: Auditorías externas a la Gestión de Tecnologías de la Información.	**A2:** Cortes de energía no programados
O3: Convenios con instituciones nacionales.	**A3:** Universidades que brindan servicios y productos de software.
O4: Convenios con instituciones internacionales.	**A4:** Desastres naturales.
FUENTE: DESITEL **ELABORADO:** Autor	

3.6.2. Matriz FODA y su impacto

A continuación se especifica el impacto que tiene cada una de las fortalezas, debilidades, oportunidades y amenazas en relación a las funciones y actividades que se desarrollan dentro del departamento DESITEL.

Tabla No 3: Matriz FODA y su Impacto

FORTALEZAS	IMPACTO
F1: Experiencia en mantenimiento software y hardware de equipos electrónicos y de Telecomunicaciones.	No permitir la obsolescencia de los equipos tecnológicos.
F2: Dominio de sistemas de videoconferencias.	Mejora interacción Docente-Estudiante
F3: Trabajo en Equipo	Apoyo coordinado en todas las áreas
F4: Experiencia en instalación de redes informáticas. (Hardware).	Seguridad del correcto funcionamiento.
F5:Personal identificado con la institución	Cumple con las necesidades requeridas
F6:Zonas Wifi para los usuarios institucionales	Acceso a navegar en la web.
F7: Red de Telefonía IP	Acceso al internet
F8: Personal con experiencia	Seguridad en las actividades.
F9: Dominio de sistemas de videoconferencias.	Aporte al desarrollo académico.
F10: Dominio de varias aplicaciones informáticas para el soporte institucional	Permite el normal desarrollo de las actividades tecnologías.
DEBILIDADES	**IMPACTO**
D1: Falta de infraestructura Física.	No permite el desarrollo funcional.
D2: Falta de personal para cubrir con el plan de mantenimiento anual en la Espoch.	Falta de cumplimiento de las actividades ya establecidas.
D3: Falta de plan de capacitación y especialización	Rezagarse con lo referente al avance tecnológico.
D4: Falta de recursos económicos y materiales para cubrir imprevistos de último momento.	Demora en cumplimiento de las actividades del área.
D5: Falta de accesorios de cómputo, en la bodega institucional.	Abastecimiento deficiente.
D6: No existen repuestos para los equipos electrónicos ni de telecomunicaciones en la bodega	Causa la obsolescencia de los equipos.
D7: Inequitativa distribución de responsabilidades en las distintas áreas.	Personal sobrecargado e ineficiente.
D8: Poca comunicación entre el área y las dependencias.	Ningún tipo de coordinación.
D9: Desprestigio departamental	Pérdida de confianza de los usuarios.
D10: Falta de cobertura Wifi.	Inconformidad de los usuarios.

OPORTUNIDADES	IMPACTO
O1: El avance tecnológico.	Proporciona un abanico de posibilidades.
O2: Auditorías externas a la Gestión de Tecnologías de la Información**.**	Determinar las vulnerabilidades existentes en el departamento.
O3: Convenios con instituciones nacionales**.**	Adquirir nuevos conocimientos en aspectos tecnológicos.
O4: Convenios con instituciones internacionales.	Estudio minucioso de estrategias a aplicar en beneficio de la institución.
AMENAZAS	**IMPACTO**
A1: Disminución en el apoyo financiero.	No ayuda a cubrir las demandas informáticas
A2: Cortes de energía no programados	Daño permanente en los equipos.
A3: Universidades que brindan servicios y productos de software.	Perder el estatus del departamento.
A4: Desastres naturales.	Pérdida permanente o parcial tanto de información como equipos informáticos.
FUENTE: DESITEL **ELABORADO:** Autor	

4.6.3. Análisis interno.

Este análisis se realiza al interior del departamento donde se combinan las posibilidades de crecimiento y desarrollo plasmadas en las fortalezas y sus falencias evidenciadas en las debilidades.

Tabla No 4: Fortalezas y Debilidades

FORTALEZAS	DEBILIDADES
F1: Experiencia en mantenimiento software y hardware de equipos electrónicos y de Telecomunicaciones.	**D1**: Falta de infraestructura Física.
F2: Dominio de sistemas de videoconferencias.	**D2**: Falta de personal para cubrir con el plan de mantenimiento anual en la Espoch.
F3:Trabajo en Equipo	**D3:** Falta de plan de capacitación y especialización
F4: Experiencia en instalación de redes informáticas. (Hardware).	**D4:** Falta de recursos económicos y materiales para cubrir imprevistos de último momento en las diferentes dependencias de la ESPOCH.
F5: Personal identificado con la institución	**D5**: Falta de accesorios de cómputo, en la bodega institucional.
F6: Zonas Wifi para los usuarios institucionales	**D6**: No existen repuestos para los equipos electrónicos ni de telecomunicaciones en la bodega

F7: Red de Telefonía IP **F8:** Personal con experiencia **F9:** Dominio de sistemas de videoconferencias. **F10**: Dominio de varias aplicaciones informáticas para el soporte institucional	**D7**: Inequitativa distribución de responsabilidades en las distintas áreas. **D8:** Poca comunicación entre el área y las dependencias. **D9**: Desprestigio departamental **D10**: Falta de cobertura Wifi para cumplir los indicadores de acreditación
FUENTE: DESITEL **ELABORADO:** Autor	

4.6.3.1 Matriz de Medios Internos

En base a las calificaciones mencionadas se realiza la ponderación de las fortalezas y debilidades del departamento cuyos resultados de muestran en la siguiente tabla:

Tabla No 5: Calificación Medios Internos

1	Debilidad Grave
2	Debilidad Menor
3	Equilibrio
4	Fortaleza Menor
5	Fortaleza Mayor

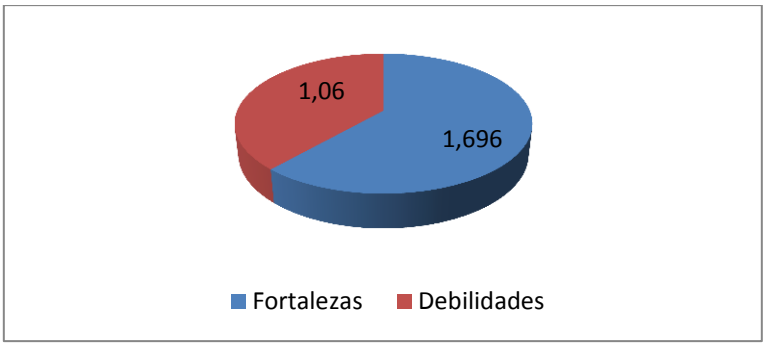
FUENTE: **DESITEL**
ELABORADO: **Autor**

Tabla No 6: Ponderación Fortalezas y Debilidades.

No	Factores Claves Externos	Ponderación	Calificación	Resultados
FORTALEZAS				
1	Experiencia en mantenimiento software y hardware de equipos electrónicos y de Telecomunicaciones.	0,050	5	**0,25**
2	Dominio de sistemas de videoconferencias.	0,050	4	**0,20**
3	Trabajo en Equipo	0,050	3	**0,15**
4	Experiencia en instalación de redes informáticas. (Hardware).	0,050	5	**0,25**
5	Personal identificado con la institución	0,050	3	**0,15**
6	Zonas Wifi para los usuarios institucionales	0,050	3	**0,15**
7	Red de Telefonía IP	0,050	4	**0,20**
8	Personal con experiencia	0,050	5	**0,25**
9	Dominio de sistemas de videoconferencias.	0,050	3	**0,15**
10	Dominio de varias aplicaciones informáticas para el soporte institucional	0,050	4	**0,20**

DEBILIDADES				
1	Falta de infraestructura Física.	0,050	1	**0,05**
2	Falta de personal para cubrir con el plan de mantenimiento anual en la Espoch.	0,050	1	**0,05**
3	Falta de plan de capacitación y especialización	0,050	2	**0,10**
4	Falta de recursos económicos y materiales para cubrir imprevistos de último momento en las diferentes dependencias de la ESPOCH.	0,050	3	**0,15**
5	Falta de accesorios de cómputo, en la bodega institucional.	0,050	3	**0,15**
6	No existen repuestos para los equipos electrónicos ni de telecomunicaciones en la bodega	0,050	2	**0,10**
7	Inequitativa distribución de responsabilidades en las distintas áreas.	0,050	2	**0,10**
8	Poca comunicación entre el área y las dependencias.	0,050	2	**0,10**
9	Desprestigio departamental	0,050	1	**0,05**
10	Falta de cobertura Wifi para cumplir los indicadores de acreditación	0,050	2	**0,10**
		1	**58**	**2,90**
FUENTE: **DESITEL** ELABORADO: **Autor**				

Gráfico No1: Ponderación de la Matriz de Medios Internos



FUENTE: **DESITEL**
ELABORADO: **Autor**

Una vez realizada la ponderación de la matriz de medios internos utilizando la una escala antes mencionada se obtuvo una ponderación de 2,90, lo que determina que se tiene una debilidad menor.

4.6.4. Análisis externo

En este análisis se determinan factores externos al departamento, donde las oportunidades permiten tener ventajas competitivas y las amenazas sino son atendidas pueden atentar contra la permanencia del departamento.

Tabla No 7: Oportunidades y Amenazas

OPORTUNIDADES	AMENAZAS
O1: El avance tecnológico. **O2:** Auditorías externas a la Gestión de Tecnologías de la Información. **O3:** Convenios con instituciones nacionales. **O4:** Convenios con instituciones internacionales.	**A1**: Disminución en el apoyo financiero. **A2:** Cortes de energía no programados **A3:** Universidades que brindan servicios y productos de software. **A4**: Desastres naturales.
FUENTE: DESITEL **ELABORADO:** Autor	

4.6.4.1 Matriz de Medios Externos

En base a las calificaciones mencionadas se realiza la ponderación de las oportunidades y amenazas del departamento cuyos resultados de muestran en la siguiente tabla:

Tabla No 8: Calificación Medios Externos

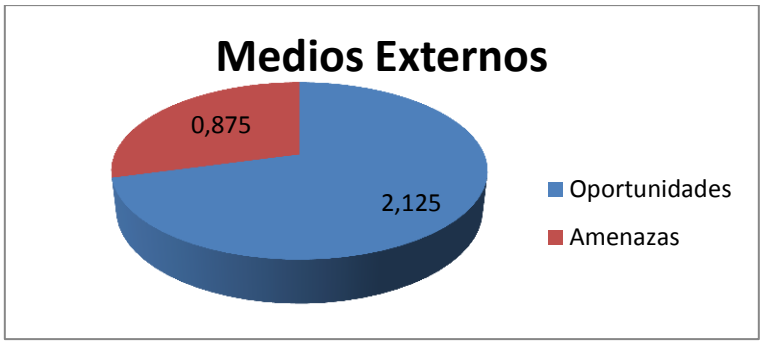
1	Amenaza Grave
2	Amenaza Menor
3	Equilibrio
4	Oportunidad Menor
5	Oportunidad Mayor

FUENTE: **DESITEL**
ELABORADO: **Autor**

Tabla No 9: Ponderación Oportunidades y Amenazas

No	Factores Claves Externos	Ponderación	Calificación	Resultados
OPORTUNIDADES				
1	El avance tecnológico.	0,125	3	**0,375**
2	Auditorías externas a la Gestión de Tecnologías de la Información.	0,125	4	**0,50**
3	Convenios con instituciones nacionales.	0,125	5	**0,625**
4	Convenios con instituciones internacionales.	0,125	5	**0,625**
AMENAZAS				
1	Disminución en el apoyo financiero.	0,125	2	**0,25**
2	Cortes de energía no programados	0,125	1	**0,125**
3	Universidades que brindan servicios y productos de software.	0,125	2	**0,25**
4	Desastres naturales.	0,125	2	**0,25**
		1	**24**	**3**
FUENTE: DESITEL **ELABORADO:** Autor				

Gráfico No 2: Ponderación de Matriz de Medios Externos



FUENTE: **DESITEL**
ELABORADO: **Autor**

Una vez realizado la ponderación a la matriz de medios externos utilizando la escala antes mencionada se obtuvo una ponderación de 3, lo que determina que las oportunidades tienen el mismo porcentaje que las amenazas.

CAPITULO IV

4. Auditoría

4.1 Desarrollo de la Auditoría

4.1.1 Planificación

Tabla No 10: Cronograma de Auditoría

N°	ACTIVIDADES A DESARROLLAR	DICIEMBRE 2013 – MARZO 2014															
		DICIEMBRE 2013				ENERO 2014				FEBRERO 2014				MARZO 2014			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**PLANIFICACIÓN**																
2	Cronograma de Auditoría																
3	Orden de Trabajo																
4	**PLANIFICACIÓN PRELIMINAR**																
5	**PLANIFICACIÓN ESPECÍFICA**																
6	Memorándum																

7	Programas de Trabajo																	
8	Papeles de Trabajo																	
9	**EVALUACIÓN DEL SISTEMA CONTROL INTERNO**																	
10	Evaluación de Riesgo																	
11	**ELABORACIÓN DE HALLAZGOS**																	
12	Hallazgos relevantes																	
12	**ELABORACIÓN DEL DICTÁMEN DE AUDITORÍA**																	
15	**CONCLUSIONES Y RECOMENDACIONES**																	

Fuente: Planificación de la Auditoría
Elaborado por: Marcelo Beltrán

4.1.2. Orden de trabajo

ORDEN DE TRABAJO N°001

Riobamba, 4 de diciembre del 2013

Ing. Paul Bernal

DIRECTOR DESITEL

Presente

Reciba un atento y cordial saludo de parte Marcelo Beltrán y a la vez pedirle de la manera más comedida la autorización para la realización de la Auditoría a la Gestión de las Tecnologías de la Información al Departamento de Sistemas y Telemática "Desitel" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, Periodo 2012, para lo cual informo a usted que la Auditoría Informática se lo desarrollará en base a las Normas de Control Interno emitidas por la Contraloría General del Estado, con el fin de medir el Grado de Cumplimiento sobre las Tecnologías de Información.

El tiempo que dispondrá para su ejecución será de 30 días laborables, contados a partir de la fecha y concluido el mismo servirá presentar el informe respectivo.

Los objetivos de la Auditoría Informática buscaran: Evaluar el grado de eficiencia y eficacia sobre el sistema de control interno establecido por la entidad ante los sistemas informáticos. Verificar el cumplimiento de las disposiciones legales, reglamentarias y normativas vigentes para su aplicación. El seguimiento y evaluación del cumplimiento de recomendaciones de auditorías anteriores (en caso de haberlas) y los resultados se harán conocer mediante el informe de auditoría que incluirá comentarios, conclusiones y recomendaciones.

Atentamente

Ing. Jimena Viteri

SUPERVISORA

4.1.3. Planificación preliminar

4.1.3.1 Conocimiento del departamento y su área informática.

La Escuela Superior Politécnica de Chimborazo (ESPOCH), tiene su origen en el Instituto tecnológico Superior de Chimborazo, creado mediante Ley No.6090, expedida por el Congreso Nacional, el 18 de abril de 1969. Inicia sus actividades académicas el 2 de mayo de 1972 con las Escuelas de Ingeniería Zootécnica, Nutrición y Dietética e Ingeniería Mecánica. Se inaugura el 3 de abril de 1972.

La Escuela Superior Politécnica de Chimborazo, en el mes de julio del 2003 aprobó mediante resolución del H. Consejo Politécnico la reestructuración orgánica funcional de la institución, misma que involucró a las diferentes dependencias administrativas y académicas con la finalidad de lograr una administración moderna y eficiente en sus diferentes ámbitos.

Este cambio determino que las tareas académicas encargadas al Departamento de Cómputo y Sistemas se vinculen directamente a las diferentes facultades y las funciones técnicas de asesoría, desarrollo de soluciones tecnológicas en el área informática se integren en el Departamento de Sistemas y Telemática mismas que se encontraban divididas en el comité Informático y el Departamento de Cómputo y Sistemas.

Misión

Proporcionar servicios integrales de calidad en las áreas de desarrollo organizacional y sistemas de información a la ESPOCH y entidades externas, utilizando tecnología

de punta, con personal capacitado, estándares de calidad y una participación activa y eficaz del usuario.

Visión

Convertirse en un departamento líder en el desarrollo e incorporación de tecnologías de la Información y comunicación, que soporten las demandas de generación, procesamiento y tratamiento de la información a través de redes de comunicación a nivel interno y externo.

Objetivos

- Definir estándares de procesos y documentación de las actividades informáticas de la institución.
- Planificar, dirigir y controlar el procesamiento automático de datos.
- Determinar las prioridades de trabajo.
- Establecer normas y políticas de trabajo para el procesamiento automático de información.
- Establecer programas de capacitación.
- Asesorar a los departamentos y usuarios de los recursos informáticos.
- Desarrollar e implantar sistemas que automaticen el procesamiento de información.
- Requerir la adquisición de HW y SW justificando su necesidad en su área.
- Administrar el personal técnico que se encuentra involucrado en las actividades informáticas

Funciones

- Presentar al H. Consejo Politécnico el Plan Informático Anual.
- Desarrollar y mantener los sistemas informáticos administrativos, académicos y de la organización.
- Apoyar los procesos de modernización administrativa, académica y de gestión institucionales.
- Administrar el correo electrónico, redes computacionales y todos los recursos informáticos de hardware y software.
- Proporcionar servicios de mantenimiento de Hardware y Software a la ESPOCH y la colectividad.
- Proporcionar servicios de identificación digital y otras especialidades a la ESPOCH y la sociedad.
- Mantener la información electrónica actualizada en el web site de la ESPOCH.
- Implementación de nuevos servicios en el área de la informática y telemática.
- Organizar e implementar programas de capacitación específicos.
- Elaborar los informes técnicos para la adquisición de los recursos informáticos; y,
- Las demás que le señalen las leyes, el Estatuto y los Reglamentos.

Organización

- El director, un profesional con formación y experiencia en el área de la informática, designado por el Rector;
- Los coordinadores de las áreas de: Sistema Académico, Áreas de Investigación, Sistemas y Redes, y, Capacitación y una sub-área de Soporte y

Mantenimiento, el personal responsable es designado de técnicos de la ESPOCH, por el director del DESITEL;

- El personal técnico informático, vinculado a la institución a través de las diferentes facultades, departamentos, otras unidades; y,
- El personal de apoyo.

La estructura organizacional del DESITEL, está integrada por:

i. Nivel directivo:

Dirección.

ii. Nivel operativo:

Área Sistema Académico;

Área de Investigación, Sistemas y Redes; Sub-área de Soporte y Mantenimiento; y,

Área de Capacitación.

iii. Nivel apoyo:

Secretaría;

Bodega; y,

Conserjería.

4.1.4. Planificación específica

Planificación Específica

Entidad: Escuela Superior Politécnica de Chimborazo.

Departamento de Sistemas y Telemática.

Dirección*:* Panamericana Sur Km 1 ½.

Tipo de Trabajo: Auditoría a la Gestión de las Tecnologías de la Información al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH.

Fecha de iniciación: 4 de diciembre del 2013.

1. Objetivos de la Auditoría

Realizar una Auditoría a la Gestión de las Tecnologías de la Información al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012, con el fin de evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.

1. Realizar un diagnóstico situacional del departamento, con el propósito principal de determinar las Fortalezas, Oportunidades, Debilidades y Amenazas, con la aplicación de Normas de la Tecnología de Información.
2. Evaluar el sistema de control interno mediante la aplicación de las normas de control interno emitidas en el grupo 410 acerca de las tecnologías de la información establecidas por la contraloría general del estado, como elemento principal que direccione la investigación.
3. Presentar el Informe de Auditoría Informática al departamento de sistemas y telemática DESITEL.

2. Alcance de la Auditoría

La AGTI, es la revisión y la evaluación del control interno sobre los procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información los cuales sirven para la buena toma de decisiones.

3. Determinación de la Estructura Orgánica

Tabla No 11: Estructura Orgánica

NIVEL	NOMBRE	DESIGNACIÓN	MODALIDAD LABORAL
Nivel directivo			
Dirección.	Ing. Paul Bernal	Director	
Nivel operativo			
• **Área Desarrollo e investigación de aplicaciones informáticas.**			
	Ing. Alex Tacuri	Técnico Informático	Nombramiento
	Ing. Juan Díaz	Técnico Informático	Nombramiento
	Ing. Ana Llalao	Técnico Informático	Contrato
	Ing. Javier Romero	Técnico Informático	Contrato
• **Área de Infraestructura de redes y telecomunicaciones.**			
	Ing. Iván Camacho	Administrador de Red	Nombramiento
	Ing. Roberto Morales	Auxiliar Informático	Nombramiento
• **Área de Soporte y Mantenimiento.**			
	Ing. Marcelo Velasco	Jefe Laboratorio Electrónico	
	Dr. Wilfrido Jarrín	Técnico de Laboratorio	Nombramiento
	Tec. Lenín Merizalde	Técnico de Laboratorio	Nombramiento
	Tec. Eugenio Meléndrez	Técnico de Laboratorio	Nombramiento
Nivel apoyo			
	Tec. Inés Miño Sr. José Eugenio	Secretaría Conserjería	Nombramiento Nombramiento

FUENTE: DESITEL
ELABORADO: Autor

4. Tiempo.

El tiempo que se ha estimado para realizar este trabajo es de 60 días laborables contados desde la fecha de aprobación de la orden de trabajo por el departamento.

5. Recursos a utilizarse.

Los recursos los dividiremos en humanos y materiales los cuales detallaremos a continuación:

Tabla No 12: Recursos Humanos y Económicos

Recursos Humanos		Recursos Económicos
Asesor	Ing. Jimena Viteri	Laptop
Auditor	Enrique Marcelo Beltrán Bravo	Impresora
		Hojas de papel bond
		Carpetas
		Calculadora

FUENTE: DESITEL
ELABORADO: Autor

8. Presentación de resultados

Al término de la auditoría se pretende emitir un informe detallado de las respetivas conclusiones y recomendaciones establecidas al departamento, para que tomen las medidas más adecuadas acerca de los hallazgos encontrados.

Ing. Jimena Viteri — Enrique Marcelo Beltrán Bravo

SUPERVISORA — **AUDITOR**

4.1.5. Programas de trabajo

Primera Fase

Departamento de Sistemas y Telemática "DESITEL"

Auditoría a la Gestión de las Tecnologías de la Información

Programa de Auditoría – Planificación

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	- Determinar los recursos a utilizarse para la realización de la auditoría. - Acordar el pacto de colaboración de parte de las autoridades del departamento. - Adquirir el conocimiento general de las actividades que realiza el departamento.			
PROCEDIMIENTOS				
1	Entrevista con el director y solicite la documentación referente a la base legal interna y externa.			
2	Efectué una visita preliminar			
3	Elabore y aplique cuestionarios al personal operativo para determinar la misión, visión y objetivos.			

Segunda Fase

Departamento de Sistemas y Telemática "DESITEL"

Auditoría a la Gestión de las Tecnologías de la Información

Programa de Auditoría – Ejecución

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	- Determinar el grado de eficiencia y efectividad delos recursos asignados. - Evaluar el grado de cumplimiento de las control interno. - Especificar el nivel cumplimiento de los requerimientos de los usuarios del departamento.			
PROCEDIMIENTOS				
1	Identificación de procesos.			
2	Elaboración de flujogramas.			
3	Elaborar y aplicar encuestas al personal operativo, docentes y estudiantes.			

Tercera Fase

Departamento de Sistemas y Telemática "DESITEL"

Auditoría a la Gestión de las Tecnologías de la Información

Programa de Auditoría – Comunicación de Resultados

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	- Emitir el informe de auditoría con las respectivas conclusiones y recomendaciones.			
PROCEDIMIENTOS				
1	Elaborar y emitir el informe de auditoría			

4.2. Ejecución

4.2.1 Papeles de trabajo

Cuestionario de visita preliminar al Departamento de Sistemas y Telemática DESITEL

Objetivo General: Recopilar información para determinar el grado de cumplimiento de las normas de control interno adoptadas por el departamento.

Razón Social: Departamento de Sistemas y Telemática DESITEL.

Fecha de Creación: En el mes de julio del 2003, se crea estatutariamente el Departamento de Sistemas y Telemática, como consta en los Artículos 59, 60 y 61 de Estatuto Politécnico.

Domicilio: Panamericana Sur Km 1 1/2

Servicios que ofrece el departamento: Proporcionar servicios integrales de calidad en las áreas de desarrollo organizacional y sistemas de información a la ESPOCH y entidades externas, utilizando tecnología de punta, con personal capacitado, estándares de calidad y una participación activa y eficaz del usuario.

Teléfono: 032998-271

Ext: 270 dirección

271 secretaría

Horario de Trabajo: 9:00 am a 1:00 pm y de 14:00pm a 18:00pm.

4.2.2. Archivo permanente

MARCH EBB
Auditores Consultores

ARCHIVO

PERMANENTE

AP

INDÍCE GENERAL

DEPARTAMENTO DE SISTEMAS Y TELEMÁTCA

ARCHIVO PERMANENTE

Elaborado por: EMBB	Fecha: 9-12-2013
Revisado por : JVO	Fecha:

INFORMACIÓN GENERAL

Según Ley 6909 del 18 de abril de 1969, expedida por el Congreso Nacional publicada por el registro Oficial Nº, 173 del 7 de mayo de 1969, se crea el Instituto Superior Tecnológico de Chimborazo, iniciando sus labores académicas el 2 de mayo de 1972. El cambio de denominación a Escuela Superior Politécnica de Chimborazo ESPOCH, se produce mediante Ley No. 1223 del 29 de octubre de 1973 publicada en el Registro Oficial Nº 425 del 6 de noviembre del mismo año. Las Escuelas de Nutrición y Dietética y de Ingeniería Zootécnica convirtieron en facultades conforme lo estipula la Ley de Educación Superior en sus artículos pertinentes.

Que, dentro de la Estructura de la Escuela Superior Politécnica de Chimborazo, se crea estatutariamente el Departamento de Sistemas y Telemática, como consta en los Artículos 59, 60 y 61 de Estatuto Politécnico.

La Escuela Superior Politécnica de Chimborazo, en el mes de julio del 2003 aprobó mediante resolución del H. Consejo Politécnico la reestructuración orgánica funcional de la institución, misma que involucró a las diferentes dependencias administrativas y académicas con la finalidad de lograr una administración moderna y eficiente en sus diferentes ámbitos.

Este cambio determino que las tareas académicas encargadas al Departamento de Cómputo y Sistemas se vinculen directamente a las diferentes facultades y las funciones técnicas de asesoría, desarrollo de soluciones tecnológicas en el área informática se integren en el Departamento de Sistemas y Telemática mismas que se

encontraban divididas en el comité Informático y el Departamento de Cómputo y Sistemas.

Misión

Proporcionar servicios integrales de calidad en las áreas de desarrollo organizacional y sistemas de información a la ESPOCH y entidades externas, utilizando tecnología de punta, con personal capacitado, estándares de calidad y una participación activa y eficaz del usuario.

Visión

Convertirse en un departamento líder en el desarrollo e incorporación de tecnologías de la Información y comunicación, que soporten las demandas de generación, procesamiento y tratamiento de la información a través de redes de comunicación a nivel interno y externo.

Objetivos

- Definir estándares de procesos y documentación de las actividades informáticas de la institución.
- Planificar, dirigir y controlar el procesamiento automático de datos.
- Determinar las prioridades de trabajo.
- Establecer normas y políticas de trabajo para el procesamiento automático de información.
- Establecer programas de capacitación.
- Asesorar a los departamentos y usuarios de los recursos informáticos.

- Desarrollar e implantar sistemas que automaticen el procesamiento de información.

Funciones

- Presentar al H. Consejo Politécnico el Plan Informático Anual.
- Desarrollar y mantener los sistemas informáticos administrativos, académicos y de la organización.
- Apoyar los procesos de modernización administrativa, académica y de gestión institucionales.
- Proporcionar servicios de identificación digital y otras especialidades a la ESPOCH y la sociedad.
- Elaborar los informes técnicos para la adquisición de los recursos informáticos; y,
- Las demás que le señalen las leyes, el Estatuto y los Reglamentos.

ORGANIZACIÓN

- El director, un profesional con formación y experiencia en el área de la informática, designado por el Rector.
- Los coordinadores de las áreas de: Sistema Académico, Áreas de Investigación, Sistemas y Redes, y, Capacitación y una sub-área de Soporte y Mantenimiento, el personal responsable es designado de técnicos de la ESPOCH, por el director del DESITEL.

La estructura organizacional del DESITEL, está integrada por:

- **Nivel directivo**:

  Dirección.

- **Nivel operativo:**

  Área Sistema Académico.

  Área de Investigación, Sistemas y Redes; Sub-área de Soporte y Mantenimiento.

  Área de Capacitación.

- **Nivel apoyo:**

  Secretaría

  Bodega y,

  Conserjería.

ABREVIATURAS

No	DESCRIPCIÓN	ABREVIATURA
1	Marcelo Beltrán	MB
2	Archivo Corriente	AC
3	Archivo Permanente	AP
4	Hoja de Marcas	HM
5	Programa de Auditoría	PA
6	Carta de Requerimiento	CR
7	Entrevista Preliminar	EP
8	Cuestionario de Control Interno	CCI
9	Matriz de Ponderación	MP
10	Hoja de Hallazgos	HH

HOJA DE MARCAS

No	DESCRIPCIÓN	SIMBOLO
1	Positivo	✓
2	Negativo	☒
3	Sumatoria	Σ
4	Hallazgo	®

Elaborado por: EMBB	Fecha: 10-12-2013
Revisado por : JVO	

MARCH EBB
Auditores Consultores

ARCHIVO

CORRIENTE

DS

INDÍCE

DEPARTAMENTO DE SISTEMAS Y TELEMÁTCA

FASE I

DIAGNOSTICO SITUACIONAL

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
FASE: Planificación

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	• Reunir un conocimiento específico de los requerimientos existentes para la aplicación de la auditoría.			
	PROCEDIMIENTOS			
1	Realice una carta compromiso indicando que se iniciara con el desarrollo de la auditoría, a fin de que se brinde las facilidades para el desarrollo de la misma.	CA	EMBB	16/12/2013
2	Realice una entrevista al director del departamento para obtener información general del área.	EA	EMBB	18/12/2013
3	Aplicar entrevista al área desarrollo e investigación de aplicaciones informáticas y área de Soporte y Mantenimiento.	EDM	EMBB	18/12/2013
4	Aplicar entrevista al área Infraestructura de Redes y Telecomunicaciones	EI	EMBB	18/12/2013
5	Solicite el organigrama de la ESPOCH para determinar la ubicación del departamento.	OR	EMBB	18/12/2013
6	Solicite el reglamento del departamento.	RE	EMBB	18/12/2013

Elaborado por: EMBB	Fecha: 13-12-2013
Revisado por : JVO	

Riobamba, 16 de Diciembre del 2013

Ingeniero.

Paul Bernal

DIRECTOR DEL DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA "DESITEL"

Presente.

De mi consideración:

En atención al pedido que se efectuó para la realización de la Auditoría Informática como herramienta para medir el grado de cumplimiento sobre las tecnologías de información.

El señor Enrique Marcelo Beltrán Bravo, realizara la Auditoría de Gestión a las Tecnologías de la Información de acuerdo a las normas emitidas por la Contraloría General del Estado, con lo referente a las tecnologías de información y comunicación

Al mismo tiempo pedirle de la manera más comedida solicitarle la completa colaboración de todo el personal que labora en el departamento, para acceder a la respectiva documentación con el fin de obtener la evidencia que sustente la opinión emitida acerca del funcionamiento del departamento.

Considero propicia la oportunidad para reiterarle mis sinceros agradecimientos.

Atentamente.

Enrique Marcelo Beltrán Bravo

Elaborado por: EMBB	Fecha: 16-12-2013
Revisado por : JVO	

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Entrevista Preliminar

DIRECTOR: Paul Bernal

1. ¿Cuál es la fecha de creación del Departamento de Sistemas y Telemática DESITEL?

La Escuela Superior Politécnica de Chimborazo, en el mes de julio del 2003 aprobó mediante resolución del H. Consejo Politécnico la reestructuración orgánica funcional de la institución, misma que involucró a las diferentes dependencias administrativas y académicas con la finalidad de lograr una administración moderna y eficiente en sus diferentes ámbitos.

2. ¿Quiénes son los responsables y que funciones cumplen el personal operativo de este departamento?

Figura No 13: Responsables y funciones del personal operativo.

• **Área Desarrollo e Investigación de Aplicaciones Informáticas.**		
	Ing. Alex Tacuri	Técnico Informático
	Ing. Juan Díaz	Técnico Informático
	Ing. Ana Llalao	Técnico Informático
	Ing. Javier Romero	Técnico Informático
• **Área de Infraestructura de Redes y Telecomunicaciones.**		
	Ing. Iván Camacho	Administrador de Red
	Ing. Roberto Morales	Auxiliar Informático
• **Área de Soporte y Mantenimiento.**		
	Ing. Marcelo Velasco	Jefe Laboratorio Electrónico
	Dr. Wilfrido Jarrín	Técnico de Laboratorio
	Tec. Lenín Merizalde	Técnico de Laboratorio
	Tec. Eugenio Meléndrez	Técnico de Laboratorio

Elaborado por: EMBB	Fecha: 18-12-2013
Revisado por : JVO	

FUNCIONES QUE CUMPLE EL DEPARTAMENTO

1. Presentar al H. Consejo Politécnico el Plan Informático Anual.
2. Desarrollar y mantener los sistemas informáticos administrativos, académicos y de la organización.
3. Apoyar los procesos de modernización administrativa, académica y de gestión institucionales.
4. Administrar el correo electrónico, redes computacionales y todos los recursos informáticos de hardware y software.
5. Proporcionar servicios de mantenimiento de Hardware y Software a la ESPOCH y la colectividad.

4. ¿Se han realizado Auditoría Informática en períodos anteriores?

SI [X] NO [ ]

5. ¿Existe dentro del departamento Indicadores del uso de los sistemas informáticos?

SI [X] NO [ ]

6. ¿El sistema de Control Interno existente está acorde con las necesidades actuales del departamento?

SI [ ] NO [X]

7. ¿Existen planes preventivos para mitigar los riesgos informáticos tanto internos como externos?

SI [ ] NO [X]

8. ¿La Información se encuentra bien custodiada?

SI [X] NO [ ]

Elaborado por: EMBB	Fecha: 18-12-2013
Revisado por : JVO	

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Entrevista Preliminar

Área Desarrollo e Investigación de Aplicaciones Informáticas y Área de Soporte y Mantenimiento: **Ing. Marcelo Velasco**

1. **¿La infraestructura física existente es la adecuada?**

   SI [ ] **NO** [X]

2. **¿Existe personal con conocimientos suficientes en videoconferencias?**

   SI [X] **NO** [ ]

3. **¿El departamento cuenta con planes de capacitación?**

   SI [ ] **NO** [X]

4. **¿Existen los repuestos para los equipos electrónicos?**

   SI [ ] **NO** [X]

5. **¿Existe el personal necesario para cubrir el Plan Anual Informático?**

   SI [ ] **NO** [X]

Elaborado por: EMBB	Fecha: 18-12-2013
Revisado por : JVO	

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Entrevista Preliminar

Área de Infraestructura de Redes y Telecomunicaciones: **Ing. Iván Camacho**

1. **¿Existen zonas WIFI para los usuarios?**

   SI [X] NO [ ]

2. **¿La planta eléctrica soporta el equipo activo de red y el sistema de climatización del DataCenter?**

   SI [ ] NO [X]

3. **¿La cobertura Wifi cumple con los indicadores de acreditación?**

   SI [ ] NO [X]

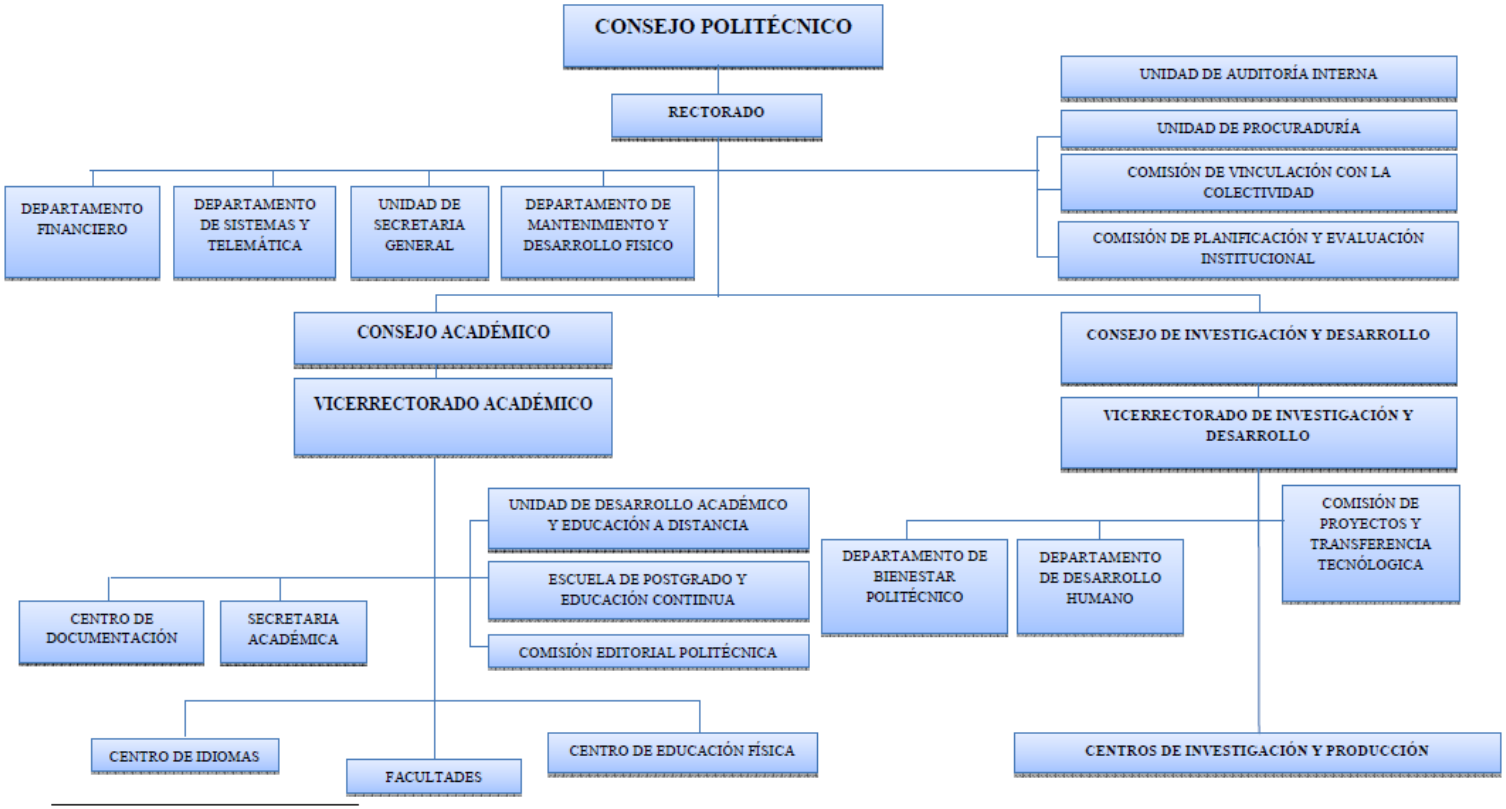
4. **¿El equipo de red DataCenter ha cumplido su tiempo de vida útil?**

   SI [X] NO [ ]

Elaborado por: EMBB	Fecha: 18-12-2013
Revisado por : JVO	

ORGANIGRAMA ESTRUCTURAL

OR



FUENTE: www.espoch.edu.ec
ELABORADO POR: Autor

Elaborado por: EMBB	Fecha: 18-12-2013
Revisado por : JVO	

REGLAMENTO DEL DEPARTAMENTO DEL DESITEL

Dentro de los aspectos más relevantes del reglamento consta la misión, visión, objetivos, organización y funciones para los niveles directivo, operacional y de apoyo.

Dentro de las funciones que cumple la dirección de DESITEL esta desarrollar proyectos encaminados al fortalecimiento tecnológico institucional

Dentro del sistema académico estará integrado por un Coordinador 1 quién preside y un Coordinador 2 que es de apoyo, además por los técnicos informáticos del sistema académico de facultades, los mismos que serán responsables del mantenimiento y desarrollo del sistema en cada facultad.

Dentro de las atribuciones en el área de Investigación, Sistemas y Redes:

Generar proyectos de producción, tecnológicos y de investigación.
Realizar el seguimiento y avances de los proyectos que se estén ejecutando.

En el Área de Capacitación tenemos:

Definir y planificar proyectos de capacitación y soporte continuo a los usuarios.
Generar alternativas de capacitación interna y externa para el personal informático de la institución.

Ver anexo 1

Elaborado por: EMBB	Fecha: 18-12-2013
Revisado por : JVO	

INDÍCE

DEPARTAMENTO DE SISTEMAS Y TELEMÁTCA "DESITEL"

FASE II

CONTROL INTERNO

Evaluación de Control Interno

MEMORÁNDUM DE PLANEACIÓN

1. DATOS

Nombre o Razón Social: Departamento de Sistemas y Telemática "DESITEL"

2. PROGRAMA

Programa de Auditoría: Auditoría a la Gestión a la Tecnologías de la información

Períodos a Auditar: Del 01/01/2012 al 31/12/2012

3. OBJETIVO DEL EXAMEN

Realizar una Auditoría a la Gestión de las Tecnologías de la Información(AGTI) al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012, con el fin de evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.

4. ALCANCE DEL EXAMEN

Se realizará una auditoría bajo el Programa de Auditoría A la Gestión de Tecnologías de la Información, por el período tributario 2012.

Se medirá el grado de cumplimiento de las normas de Control Interno emitidas por la Contraloría General del Estado, referente a las tecnologías de información y comunicación, analizando aspectos relacionados con seguridad lógica, seguridad física, utilización y aprovechamiento de las TICs, gestión de la informática.

5. CONOCIMIENTO GENERAL Y ACTIVIDADES DEL DEPARTAMENTO

La Escuela Superior Politécnica de Chimborazo, en el mes de julio del 2003 aprobó mediante resolución del H. Consejo Politécnico la reestructuración orgánica funcional de la institución, misma que involucró a las diferentes

dependencias administrativas y académicas con la finalidad de lograr una administración moderna y eficiente en sus diferentes ámbitos.
Este cambio determino que las tareas académicas encargadas al Departamento de Cómputo y Sistemas se vinculen directamente a las diferentes facultades y las funciones técnicas de asesoría, desarrollo de soluciones tecnológicas en el área informática se integren en el Departamento de Sistemas y Telemática mismos que se encontraban divididas en el comité Informático y el Departamento de Cómputo y Sistemas.

DESITEL proporciona servicios integrales de calidad en las áreas de desarrollo organizacional y sistemas de información a la ESPOCH y entidades externas, utilizando tecnología de punta, con personal capacitado, estándares de calidad y una participación activa y eficaz del usuario.
Las actividades se a realizarse serán las siguientes:

- Evaluación de la unidad de tecnologías informáticas, comunicaciones y sistemas
- Evaluación de los sistemas
- Evaluación de los Equipos

6. NORMATIVIDAD APLICABLE

- ❖ Normas de la Contraloría General del Estado
- ❖ Ley Orgánica de la Ley de Educación Superior

7. IDENTIFICACIÓN DE ÁREAS CRITICAS

Evaluación de sistemas.- la elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o un bien si existen programas aislados.
Otro factor que no se puede dejar de evaluar es si existe un plan estratégico para la elaboración de los sistemas.

Evaluación del análisis.- se evalúan políticas, procedimientos y normas que se tienen para llevar acabo para realizar el análisis.

8. INFORMES A EMITIR Y FECHAS DE ENTREGA

Se entregarán tres informes parciales, dos de ellos a la culminación del 50 y 75% del trabajo de campo y el otro al culminar el 100% del mismo; se coordinará permanentemente con el supervisor.

Al término del informe se entregaran tres ejemplares en los 30 días siguientes de la siguiente manera:

- 1 ejemplar a la Escuela Superior Politécnica de Chimborazo.
- 1 ejemplar a la Facultad de Administración de Empresas.
- 1 ejemplar al Departamento de Sistemas y Telemática.

9. EQUIPO AUDITOR

EQUIPO AUDITOR

SUPERVISOR	Ing. Jimena Viteri
AUDITOR	Sr. Marcelo Beltrán

10. PERSONAL EXISTENTE

NIVEL DIRECTIVO	NIVEL OPERATIVO	NIVEL DE APOYO
Dirección.	Área Desarrollo de Investigación de Aplicaciones Informáticas	Secretaría
	Área de Infraestructura de Redes y Telecomunicaciones	Conserjería
	Área de Soporte y Mantenimiento.	

11. PRESUPUESTO DEL TIEMPO

Tabla No 14: Presupuesto del Tiempo

DESCRIPCION	TIEMPO	PERSONAS A UTLIZAR
Planificación	9 días hábiles	**1**
Trabajo de campo	9 días hábiles	**1**
Evaluación de Descargos	9 días hábiles	**1**
Redacción del Informe Administrativo	5 días hábiles	**1**
Redacción del Informe	3 días hábiles	**1**
TOTALES	**35 días hábiles**	

FUENTE: DESITEL
ELABORADO: Autor

Cabe resaltar que el tiempo asignado al auditor es de 35 días hábiles, el mismo que no incluye los días para la revisión del Control Interno.

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
FASE: Evaluación del Sistema del Control Interno.

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	❖ Revisar el cumplimiento de las Normas de Control Interno de la Contraloría General del Estado, emitidas para la aplicación de forma obligatoria a las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos. ❖ Reunir un conocimiento general de las funciones específicas del departamento. ❖ Establecer la ponderación de las Matrices de Control Interno con la finalidad que proporcione seguridad razonable acerca de cómo se está manejando los recursos dentro del departamento. ❖ Establecer los hallazgos para determinar los puntos críticos que permitan mejorar el sistema de Control Interno por medio de nuestras conclusiones y recomendaciones.			
	PROCEDIMIENTOS			
1	**Elaborar el Plan de Control Interno**	PCI	EMBB	24/12/2013
2	**Aplicar cuestionarios de Control Interno**			
2.1	Organización informática	CCI 1/17	EMBB	02/01/2014
2.2	Segregación de funciones	CCI 2/17	EMBB	02/01/2014
2.3	Plan informático estratégico de tecnología	CCI 3/17	EMBB	02/01/2014
2.4	Políticas y procedimientos	CCI 4/17	EMBB	03/01/2014
2.5	Modelo de información organizacional	CCI 5/17	EMBB	03/01/2014
2.6	Administración de proyectos tecnológicos	CCI 6/17	EMBB	03/01/2014
2.7	Desarrollo y adquisición de software aplicativo	CCI 7/17	EMBB	06/01/2014
2.8	Adquisiciones de infraestructura tecnológica	CCI 8/17	EMBB	06/01/2014

Elaborado por: EMBB	Fecha: 23-12-2013
Revisado por : JVO	

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
FASE: Evaluación del Sistema del Control Interno.

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
2.9	Mantenimiento y control de la infraestructura tecnológica	CCI 9/17	EMBB	07/01/2014
2.10	Seguridad de tecnología de información	CCI 10/17	EMBB	07/01/2014
2.11	Plan de contingencias	CCI 11/17	EMBB	08/01/2014
2.12	Administración de soporte de tecnología de información	CCI 12/17	EMBB	08/01/2014
2.13	Monitoreo y evaluación de los procesos y servicios	CCI 13/17	EMBB	08/01/2014
2.14	Sitio web, servicios de internet e intranet	CCI 14/17	EMBB	09/01/2014
2.15	Capacitación informática	CCI 15/17	EMBB	09/01/2014
2.16	Comité informático	CCI 16/17	EMBB	10/01/2014
2.17	Firmas electrónicas	CCI 17/17	EMBB	10/01/2014
3	**Evaluación de Riesgo**			
3.1	Tabulación y Ponderación de riesgos	CCI 1/17 - 17/17	EMBB	13/01/2014

Elaborado por: EMBB	Fecha: 23-12-2013
Revisado por : JVO	

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
FASE: Plan de Auditoría de Control Interno

PLAN DE AUDITORIA DE CONTROL INTERNO

a) Motivo

La Evaluación del Sistema de Control Interno enmarcadas en las normas establecidas por la Contraloría General del Estado incluido en el grupo 410 referente a TECNOLOGÍA DE INFORMACIÓN, se realizó de conformidad al oficio Nº 001-AI-01, suscrito por el Director del departamento.

b) Objetivos

Determinar si el control interno existente en el departamento brinda un nivel de confianza acerca del cumplimiento de forma eficiente y eficaz de la gestión en aspectos relacionados con los objetivos y disposiciones legales aplicables.

c) Alcance

La evaluación del Control Interno acerca de las Tecnologías de la Información obtenidas del grupo 410, se lo realizo dentro del período económico del año 2012.

d) Autorización del departamento

Por medio de la autorización del director tenemos la completa colaboración del todo el personal existe en el departamento.

e) Personal encargado

EQUIPO AUDITOR

SUPERVISOR	Ing. Jimena Viteri	JVO
AUDITOR	Sr. Enrique Marcelo Beltrán Bravo	EMBB

Elaborado por: EMBB	Fecha: 24-12-2013
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO Y SU PONDERACIÓN

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Organización Informática.
OBJETIVO: Evaluar la Organización Informática para cumplir con la norma 410-01

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿El departamento cuenta con un modelo de información?	✓	10				
2	¿La capacidad de compartir recursos tecnológicos dentro de la institución es excelente?	✓	10				
3	¿Los servicios web han facilitado la metodología de enseñanza docente - estudiante?	✓	10				
4	¿Las plataformas informáticos satisfacen las necesidades de las autoridades, docentes y estudiantes?	✓	10				
5	¿Mantiene servidores virtuales que permitan el almacenamiento, recuperación y corrección de la información generada por los ordenadores de la institución?	✓	10				
6	¿El departamento es la unidad responsable que se encarga de regular y estandarizar los temas tecnológicos a nivel institucional?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{60}{60} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 -100 **NR**= O

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 02-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Segregación de Funciones.
OBJETIVO: Evaluar la Segregación de Funciones para cumplir con la norma 410-02

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Aplica el departamento la segregación de funciones?	✓	10				
2	¿La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles?	✓	10				
3	¿La posibilidad de reubicación e incorporación de un nuevo personal se da a partir de la supervisión de roles y funciones del personal?	✓	10				
4	¿Los puestos de trabajo para la unidad de tecnologías de información se contemplan de acuerdo a las habilidades y experiencia necesarias en cada área?	✓	10				
5	¿Los sistemas de información que posee el departamento son de fácil manejo para el personal administrativo y técnico?	✓	10				
6	¿Existe una equitativa distribución de responsabilidades en las distintas áreas?			✓	10		

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{50}{60} * 100$ **NC**= 83, 33

NR= NC - 100 **NR**= 100 - 83, 33
NR= 16, 67

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 02-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Plan informático Estratégico de Tecnología.
OBJETIVO: Evaluar el Plan informático Estratégico de Tecnología para cumplir con la norma 410-03

N	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿La unidad de tecnología de la información elabora un plan informático estratégico?	✓	10				
2	¿El departamento elabora planes operativos de tecnología de la información alineados con el plan estratégico informático?	✓	10				
3	¿El plan estratégico y los planes operativos de tecnología de información y el presupuesto son analizados y aprobados por la máxima autoridad?	✓	10				
4	¿Para evitar la obsolescencia en los planes operativos de TI se encuentran consideraciones relacionadas con la incorporación de nuevas TI?	✓	10				
5	¿La unidad de tecnología cuenta con la implementación de un plan informático para administrar y dirigir todos los recursos tecnológicos?	✓	10				
6	¿Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico?	✓	10				

NC= CT * 100 / PT **NC**= 60 * 100 / 60 **NC**= 100

NR= NC - 100 **NR**= 100 -100 **NR**= O

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 02-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Políticas y Procedimientos.
OBJETIVO: Evaluar las Políticas y Procedimientos para cumplir con la norma 410-04

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿La Unidad de Tecnología cuenta con políticas y procedimientos?	✓	10				
2	¿Las atribuciones, actividades, procedimientos o productos del personal están claramente definidos?	✓	10				
3	¿Existen Políticas de Seguridad Industrial?	✓	10				
4	¿El plan estratégico y los planes operativos de tecnología de información, es aprobado por la máxima autoridad?	✓	10				
5	¿La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución?	✓	10				
6	¿Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{60}{60} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 -100 **NR**= 0

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 03-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Modelo de Información Organizacional.
OBJETIVO: Evaluar el Modelo de Información Organizacional para Cumplir Con la Norma 410-05

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿El departamento cuenta con un modelo de información organizacional?	✓	10				
2	¿Se generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad?	✓	10				
3	Se expiden políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en el departamento.	✓	10				
4	Se garantiza disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{40}{40} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 - 100 **NR**= O

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 03-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Administración de Proyectos Tecnológicos.
OBJETIVO: Evaluar la Administración de Proyectos Tecnológicos para cumplir con la Norma 410-06

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Se ha determinado quien se dedique a gestionar, elaborar, ejecutar y emprender proyectos tecnológicos en bien de la institución?	✓	10				.
2	¿Se ejecutaron todos los proyectos tecnológicos establecidos en PAI?			✓	10		® Faltan dos proyectos por cumplir.
3	¿Existen Políticas de Seguridad Industrial?	✓	10				
4	La seguridad con la que cuenta la base de datos es de confianza.	✓	10				
5	Se Busca mayor capacidad en equipos, ya sea hardware y bases de datos más robustas que permitan manejar mayor información	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{40}{50} * 100$ **NC**= 80

NR= NC - 100 **NR**= 100 - 80 **NR**= 20

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 03-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Desarrollo y Adquisición de Software Aplicativo.
OBJETIVO: Evaluar el Desarrollo y Adquisición de Software Aplicativo para cumplir con la Norma 410-07.

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	Se busca soluciones tecnológicas considerando las políticas públicas establecidas por el estado	✓	10				
2	Se cumple con totalidad la adquisición de software de conformidad con el Plan Anual de Adquisiciones.			✓	10		® No cumple con el Plan Anual de Adquisiciones.
3	¿El departamento cuenta con políticas internas?			✓	10		® No aplica políticas internas.
4	¿Por medio de la utilización de políticas públicas se intenta dar soluciones tecnológicas al departamento?	✓	10				
5	¿Se identifica, prioriza y específica los requerimientos funcionales de las unidades usuarias?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{30}{50} * 100$ **NC**= 60

NR= NC - 100 **NR**= 100 - 60
NR= 40

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
	✓	
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 06-01-2014
Revisado por : JOV	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Adquisiciones e Infraestructura Tecnológica.
OBJETIVO: Evaluar las Adquisiciones e Infraestructura Tecnológica para cumplir con la Norma 410-08

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	Se estableció en el plan anual de contrataciones adquirir y dar mantenimiento a la infraestructura tecnológica	✓	10				
2	¿Los procedimientos de adquisiciones de infraestructura tecnológica son calificados y aprobados por la máxima autoridad?	✓	10				
3	¿Se cumplió en su totalidad la adquisición de hardware establecido en el plan anual de contrataciones?			✓	10		® No cumple con el Plan Anual de Adquisiciones.
4	¿La infraestructura tecnológica existente ayuda al desarrollo permanente del departamento?			✓	10		® Falta de infraestructura física.
5	El plan de adquisición tecnológica se alinea con el plan de infraestructura tecnológica	✓	10				
6	¿Las adquisiciones están alineadas a los principios del departamento?	✓	10				
7	¿Las adquisiciones se encuentran dentro de los portafolios de proyectos y servicios?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{50}{70} * 100$ **NC**= 71, 43

NR= NC - 100 **NR**= 100 – 71, 43
NR=28, 57

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
	✓	
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**

Elaborado por: EMBB	Fecha: 06-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Mantenimiento y Control de la Infraestructura Tecnológica.
OBJETIVO: Evaluar el Mantenimiento y Control de la Infraestructura Tecnológica para cumplir con la Norma 410-09

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Se elaborará un plan de mantenimiento preventivo o correctivo de la infraestructura tecnológica?	✓	10				
2	¿Se mantiene el control de los bienes informáticos por medio de un inventario actualizado?	✓	10				
3	¿El plan de mantenimiento preventivo o correctivo es distribuido a los técnicos informáticos de las facultades para su aplicación?			✓	10		® No se distribuye el plan de mantenimiento preventivo o correctivo.
4	¿El mantenimiento de los bienes que se encuentren en garantía es proporcionado por el proveedor, sin costo adicional para la entidad?	✓	10				
5	¿Se implementaron medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura?	✓	10				
6	¿Existe el control y registro de las versiones del software que ingresa a producción?	✓	10				
7	Existe el personal suficiente para cubrir con el plan de mantenimiento anual.			✓	10		® Personal escaso.

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{50}{70} * 100$ **NC**= 71, 43

NR= NC - 100 **NR**= 100 – 71, 43
NR=28, 57

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
	✓	
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 07-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Seguridad de Tecnología de Información
OBJETIVO: Evaluar la Seguridad de Tecnología de Información para cumplir con la Norma 410-10

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Existe el adecuado almacenamiento de respaldos con información crítica y sensible en lugares externos a la organización?	✓	10				
2	¿La obtención de respaldos se realiza periódicamente?			✓	10		® No se realizan los respaldos de la información adecuadamente
3	Conoce si se realiza monitoreo de seguridad a los sistemas de información, en especial al sistema software	✓	10				
4	¿Se mantiene ambiente con temperatura y humedad relativa del aire contralado?	✓	10				
5	¿El departamento mantiene un ambiente con temperatura y humedad relativa del aire contralado, que los equipos informáticos lo requieren?	✓	10				
6	¿El departamento posee un sistema de alarma anti incendios que puedan prevenir la pérdida de recursos tecnológicos?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{50}{60} * 100$ **NC**= 83, 33

NR= NC - 100 **NR**= 100 – 83, 33
NR=16, 67

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 07-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Plan de Contingencias.
OBJETIVO: Evaluar el Plan de Contingencias para cumplir con la Norma 410-11

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿El departamento cuenta con un plan de contingencias?	✓	10				
2	¿Dentro del plan de contingencias se ha contemplado el plan de respuesta a los riesgos?	✓	10				
3	¿El plan de contingencias determina las actividades a seguir en caso de una emergencia en el curso normal de las actividades del departamento?	✓	10				
4	El plan de contingencias ayuda a salvaguardar la integridad y seguridad de la información	✓	10				
5	¿El plan de contingencias comprenderá en actividades previas, durante y después al desastre?	✓	10				
6	¿El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución?			✓	10		® No se ha realizado las gestiones administrativas para su aprobación.
7	¿El plan de contingencias es sujeto a pruebas, entrenamientos y evaluaciones periódicas?			✓	10		® No son sujetos a ningún tipo de pruebas

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{50}{70} * 100$ **NC**= 71, 43

NR= NC - 100 **NR**= 100 – 71, 43
NR= 28, 57

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
	✓	
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 08-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Administración de Soporte de Tecnologías de Información.
OBJETIVO: Evaluar la Administración de Soporte de Tecnologías de Información para cumplir con la Norma 410-12

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Se efectúan revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para satisfacer a los usuarios?	✓	10				
2	Se estandariza la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.	✓	10				
3	¿Como medida de seguridad se emite una identificación a los usuarios internos, externos y temporales que interactúan con los sistemas y servicios de tecnologías de la entidad?	✓	10				
4	¿Se efectúan medidas de prevención, detección y seguridad que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informático?	✓	10				
5	¿Se elabora un proceso de estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas para controlar el uso de los equipos informáticos?	✓	10				
6	¿Existe una administración adecuada de la información, librerías de software, respaldos y recuperación de datos?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{60}{60} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 – 100 **NR**= 0

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 08-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Monitoreo y Evaluación de los Procesos y Servicios.
OBJETIVO: Evaluar la Monitoreo y Evaluación de los Procesos y Servicios para cumplir con la Norma 410-13

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Se define sobre la base de operaciones de la entidad, indicadores de desempeño y meretrices del proceso para monitorear la gestión y acciones correctivas?	✓	10				
2	¿Cree que al efectuar el proceso de monitoreo nos ayudara a salvaguardar y alargar la vida útil de los equipos informáticos?	✓	10				
3	¿Conoce usted si existe un proceso de monitoreo en la institución, o si se aplicado antes alguna herramienta de monitoreo?	✓	10				
4	¿Es necesario establecer el alcance, la metodología y el proceso a seguir para monitorear la tecnología de información?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{40}{40} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 – 100 **NR**= 0

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 08-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: **S**itos Web, servicios de Internet y Extranet.
OBJETIVO: Evaluar los **S**itos Web, servicios de Internet y Extranet para cumplir con la norma 410-14

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Se encuentran formalizados la normas, procedimientos, e instructivos de los servicios de sitios web, internet extranet?			✓	10		® No se encuentran formalizados.
2	¿Los servicios web e internet han facilitado la metodología de aprendizaje entre docente y estudiante?	✓	10				
3	¿La cobertura WIFI cumple satisface las necesidades de los usuarios?			✓	10		® La cobertura WIFI es mínima.
4	¿Los nuevos servicios de Sitios web, servicios de internet e intranet cumplen con lo establecido en esta norma?	✓	10				
5	¿La velocidad del servicio de internet es el adecuado?			✓	10		® Velocidad del servicio deficiente.

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{30}{50} * 100$ **NC**= 60

NR= NC - 100 **NR**= 100 – 50 **NR**= 40

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
	✓	
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 09-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Capacitación Informática.
OBJETIVO: Evaluar la Capacitación Informática para cumplir con la norma 410-15

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿Cuenta con un plan de capacitación y especialización?			✓	10		® Falta elaborar un plan de capacitación.
2	¿Se organizan eventos de capacitación para los estudiantes, docentes y público en general?	✓	10				
3	¿Usted cree que es importante para institución contar con una excelente capacitación tecnológica?	✓	10				
4	¿El conocimiento adquirido por los técnicos informáticos es el más adecuado para el desarrollo del departamento?	✓	10				
5	Se realizan programas de capacitación con la ayuda de los sistemas de educación virtual, tales como aulas virtuales, videos conferencias, servicios web, etc.	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{40}{50} * 100$ **NC**= 80

NR= NC - 100 **NR**= 100 – 80 **NR**= 20

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 09-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información.
ALCANCE: Comité Informático.
OBJETIVO: Evaluar el Comité Informático para cumplir con la norma 410-16

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿El departamento posee un comité informático encardo de realizar las actividades correspondientes al área?	✓	10				
2	¿Se ha formulado normas de control para brindar mayor seguridad dentro de la organización al momento de emitir alguna información?	✓	10				
3	¿Existe jefes de área para potenciar y controlar de mejor manera el desarrollo del departamento?	✓	10				
4	¿El comité informático esta formalizado y claramente definido dentro del departamento?	✓	10				
5	¿Las normas emitidas por la máxima autoridad son evaluadas por el comité informático para que se cumplan con normalidad sin ningún tipo de novedades ajenas al área?	✓	10				
6	¿El comité imparte objetivos en conjunto para que el beneficio sea colectivo y no solo departamental?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{60}{60} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 – 100 **NR**= 0

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 10-01-2014
Revisado por : JVO	

CUESTIONARIO DE CONTROL INTERNO

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
ALCANCE: Firmas Electrónicas.
OBJETIVO: Evaluar las Firmas Electrónicas para cumplir con la norma 410-17

No	Preguntas	Respuesta y Ponderación					Observaciones
		SI		NO		N/A	
1	¿La institución posee el sistema de firmas electrónicas para realizar transacciones, procedimientos y contratos virtuales?	✓	10				
2	¿Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros?	✓	10				
3	¿Los titulares de certificados de firma electrónica y dispositivos portables seguros son los responsables de su buen uso y protección?	✓	10				
4	¿La institución capacita, advierte e informará a los solicitantes y usuarios, respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados?	✓	10				
5	¿Las respectivas claves de acceso no son divulgadas ni compartidas en ningún momento?	✓	10				
6	¿El uso de la firma electrónica en la administración pública está sujeto a las garantías, reconocimiento, efectos y validez señalados en estas disposiciones legales y su normativa secundaria de aplicación?	✓	10				

NC= $\frac{CT}{PT} * 100$ **NC**= $\frac{60}{60} * 100$ **NC**= 100

NR= NC - 100 **NR**= 100 – 100 **NR**= 0

CONFIANZA		
Confianza Alta (95% - 76%)	**Confianza Moderado (75% - 51%)**	**Confianza Baja (50% - 5%)**
✓		
Riesgo Bajo (5% - 24%)	**Riesgo Moderado (25% - 49%)**	**Riesgo Alto (50% - 95%)**
RIESGO		

Elaborado por: EMBB	Fecha: 10-01-2014
Revisado por : JVO	

A continuación se detalla un resumen de los porcentajes encontrados de las matrices de confianza y de riesgo obtenidos de la aplicación de los cuestionarios de control interno.

Tabla No 14: Matriz de Confianza y Riesgo.

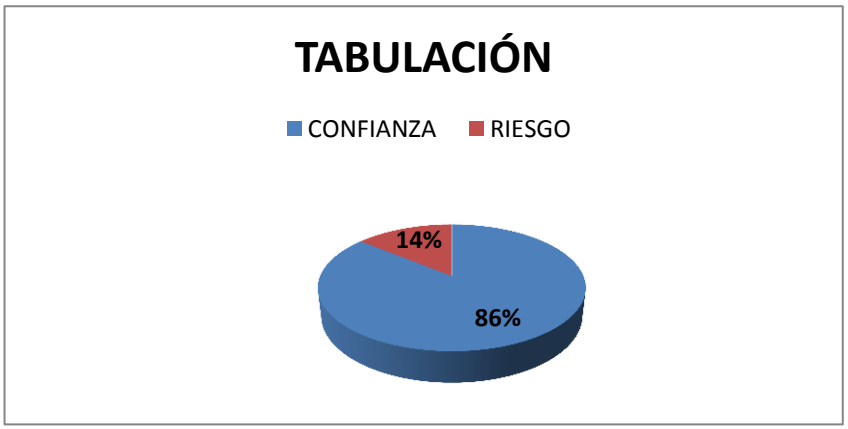
Norma Relacionada	Detalle	Confianza	Riesgo
410 - 01 Organización Informática.	No existe ninguna inconsistencia	100%	0%
410 – 02 Segregación de Funciones	Inequitativa distribución de responsabilidades.	83,33%	16,67%
410 -03 Plan informático Estratégico de Tecnología.	No existe ninguna inconsistencia	100%	0%
410 – 04 Políticas y Procedimientos.	No existe ninguna inconsistencia	100%	0%
410 – 05 Modelo de Información Organizacional.	No existe ninguna inconsistencia	100%	0%
410 – 06 Administración de Proyectos Tecnológicos	Proyectos existentes en el PII incumplidos	80 %	20 %
410 – 07 Desarrollo y Adquisición de Software Aplicativo	El departamento no cuenta con políticas internas.	60%	40%
410 – 08 Adquisiciones e Infraestructura Tecnológica	Falta de infraestructura tecnológica y física básica.	71,43%	28,57%
410 – 09 Mantenimiento y Control de la Infraestructura Tecnológica	Formalización del plan de mantenimiento preventivo o correctivo.	71,43%	28,57%
410 -10 Seguridad Informática	No se realizan la obtención de respaldos periódicamente.	83,33%	16,67%
410 – 11 Plan de Contingencias	Legalización del plan de contingencias.	71,43%	28,57%
410 – 12 Administración de Soporte de Tecnologías de Información	No existe ninguna inconsistencia	100%	0%

410 – 13 Monitoreo y Evaluación de los Procesos y Servicios	No existe ninguna inconsistencia	100%	0%
410 – 14 Sitios Web, servicios de internet y extranet	Cobertura WIFI deficiente. Velocidad del internet mínima.	60%	40%
410 – 15 Capacitación Informática	No cuenta con un plan de capacitación y especialización.	80%	20%
410 – 16 Comité Informático.	No existe ninguna inconsistencia	100%	0%
410 – 17 Firmas Electrónicas.	No existe ninguna inconsistencia	100%	0%
TOTAL		**85,94 %**	**14,06 %**

NC= $\frac{CT}{PT}$ **NC**= $\frac{1461}{17} * 100$ **NC**= 85, 94 %

NR= NC - 100 **NR**= 100 – 85, 94 **NR**= 14, 06

Gráfico No 3: Tabulación de la Matriz de Confianza y Riesgo



FUENTE: **DESITEL**
ELABORADO: **Autor**

Análisis: Del análisis del control interno efectuado al DESITEL se ha determinado que existe una confianza del 85,94% y un riesgo 14,06%, lo que nos demuestra que el porcentaje del riesgo es bajo.

INDÍCE

DEPARTAMENTO DE SISTEMAS Y TELEMÁTCA "DESITEL"

FASE III

DETERMINACIÓN DE HALLAZGOS

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
FASE: Determinación de Hallazgos.

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	❖ Determinar los hallazgos encontrados de la evaluación y ponderación de los cuestionarios de control interno.			
	PROCEDIMIENTOS			
1	Elaboración de hojas de hallazgos.	HH	EMBB	20/01/2014
2	Aplicación de indicadores de las GTI.	IT	EMBB	17/02/2014

DETERMINACION DE HALLAZGOS

1. Inequitativa distribución de responsabilidades.

Condición: El departamento de Sistemas y Telemática "DESITEL" mantiene una inadecuada distribución de responsabilidades, lo que da lugar una incompatibilidad de funciones y responsabilidades del personal existentes en cada una de las distintas áreas.

Criterio: De acuerdo a la norma de control interno 410-02 Segregación de Funciones establecidas por la contraloría general del estado establece que la asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles y que se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas.

Causa: La falta de un manual de funciones en el departamento, lo que provoca una inadecuada organización entre el personal y lo directivos existentes en el área.

Efecto: Por la inequitativa distribución de responsabilidades provoca la pérdida de tiempo y de recursos por no haber la distribución justa del personal para cada área.

Conclusiones: El departamento de Sistemas y Telemática "DESITEL" mantiene una inadecuada distribución de responsabilidades, lo que da lugar una incompatibilidad de funciones y responsabilidades del personal existentes en cada una de las distintas áreas.

Recomendaciones:

- Incluir al menos dos personas del área de desarrollo de investigación a aplicaciones informáticas al área de soporte y mantenimiento en los momentos que se los requiera.

Elaborado por: EMBB	Fecha: 22-01-2014
Revisado por : JVO	

2. Incumplimiento de los proyectos tecnológicos.

Criterio: No se cumple el proyecto de actualización del equipo activo de red del Data Center establecido en el PII 2012.

Condición: En la norma 410-06 Administración de Proyectos Tecnológicos establece la unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad.

Causa: La falta en el cumplimiento de la actualización del equipo activo de red del Data Center se dio por el cambio permanente del director de DESITEL.

Efecto: El no poder prestar los servicios adecuados a todos los usuarios de la ESPOCH y evitar que el sistema institucional quede in-operativo y obsoleto.

Conclusiones: El incumplimiento del proyecto de actualización del equipo activo de red del Data Center establecido en el PII 2012, provocaría que el sistema institucional quede in-operativo y obsoleto.

Recomendaciones:

- Establecer una reestructuración del plan integral informático.
- Realizar la actualización del equipo activo de red del Data Center establecida en el PII 2012, dentro del periodo específico.

Elaborado por: EMBB	Fecha: 24-01-2014
Revisado por : JVO	

3. No se cumple con las adquisiciones de software y hardware

Criterio: No se cumple en su totalidad con la adquisición de software y hardware de conformidad con el Plan Integral Informático del 2012.

Condición: En la norma 410-07 Desarrollo y Adquisición de Software Aplicativo se establece que la adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado

Causa: La falta de políticas internas no se han establecidas los cambios y no han cumplido con las necesidades de implementación de aplicaciones de software, en aspectos de factibilidad, costo-beneficio.

Efecto: El cumplimiento de forma parcial en la adquisición de software hace que exista un desfase en el desarrollo de las actividades ya programadas, lo que provoca que el departamento no se actualice de manera constante en aspectos tecnológicos.

Conclusiones: El incumplimiento en la adquisición de software y hardware establecido en el plan integral informático del año 2012, han provocado que el desarrollo del departamento se haya estancado y no exista un crecimiento constante.

Recomendaciones:

- La elaboración de políticas internas que ayuden al cumplimiento total de adquisiciones de software y hardware conforme lo establece el plan integral informático.
- Realizar las gestiones administrativas que permitan contar con el presupuesto necesario para cumplir con las adquisiciones de software y hardware en su totalidad.

Elaborado por: EMBB	Fecha: 24-01-2014
Revisado por : JVO	

4. El plan de mantenimiento preventivo o correctivo.

Criterio: El departamento no cuenta con un plan de mantenimiento preventivo o correctivo, por ende no es distribuido a los técnicos informáticos de las facultades para su aplicación.

Condición: De acuerdo a la norma de control interno 410-09 Mantenimiento y Control de la Infraestructura Tecnológica Adquisiciones e Infraestructura Tecnológica emitidas en la contraloría general del estado establece que la unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica.

Causa: No existe el personal suficiente para cubrir con el plan de mantenimiento preventivo y correctivo y por esta razón no se ha distribuido a los técnicos informáticos de las facultades para su aplicación.

Efecto: Al no haber la distribución de este plan de mantenimiento a los técnicos informáticos de las facultades de la ESPOCH, pueden provocar la obsolescencia de los equipos informáticos.

Conclusiones: El departamento cuenta con un plan de mantenimiento preventivo o correctivo, que no es legalmente aprobado.

Recomendaciones:

- Aprobar legalmente el plan de mantenimiento de mantenimiento preventivo o correctivo.
- Socializar el plan de mantenimiento preventivo o correctivo
- Incluir verificación de instalaciones eléctricas.
- Incluir verificación y aseguramiento de las instalaciones físicas.

Elaborado por: EMBB	Fecha: 31-01-2014
Revisado por : JVO	

5. La obtención de respaldos.

Criterio: El departamento no realiza la obtención de respaldos de la información periódicamente, lo que provoca la inseguridad en la veracidad de la información.

Condición: De acuerdo a la norma de control interno 410-10 Sistemas de Información emitidas en la contraloría general del estado establece mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

Causa: Por la falta de un cronograma definido y aprobado que servirá como una guía por parte de los directivos del departamento

Efecto: Al no tener una obtención de respaldos periódicamente, provocara la pérdida de información si no se realiza en el momento adecuado.

Conclusiones: El departamento no realiza la obtención de respaldos de la información periódicamente, lo que provoca la inseguridad en la veracidad de la información.

Recomendaciones:

- Determinar un área externa al departamento en el que se ubiquen los respaldos en caso de producirse siniestros en el Desitel.
- Los respaldos se realizan cada 30 días pero se deberá realizarlo cada 7 días para tener la certeza que la información mantenga una adecuada actualización.

Elaborado por: EMBB	Fecha: 03-02-2014
Revisado por : JVO	

6. El plan de contingencias no es aprobado.

Criterio: El plan de contingencias no es aprobado, ni difundido entre el personal responsable de su ejecución.

Condición: De acuerdo a la norma de control interno 410-11 Plan de Contingencias emitidas en la contraloría general del estado establece que le corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Causa: No se han realizado las gestiones administrativas para su aprobación.

Efecto: La falta de un plan de contingencias provoca que no se tenga un manual a seguir en caso de estar al frente de una emergencia y no tener el problema de pérdida de equipos informáticos.

Conclusiones: Existe el plan de contingencias el cual no se encuentra aprobado y por lo tanto ni difundido entre el personal responsable de su ejecución, ni se encuentra en vigencia.

Recomendaciones:

- Realizar las gestiones administrativas necesarias para la aprobación del plan de contingencias, el cual debe ser sometido a pruebas y entrenamientos periódicos, para que en el momento que sea necesario poder utilizarlo.

Elaborado por: EMBB	Fecha: 05-02-2014
Revisado por : JVO	

7. Sitios Web, Servicios de Internet y Extranet.

Criterio: No se culpe con estándares de red inalámbrica en los interiores de edificios del campus principal de la ESPOCH.

Condición: De acuerdo a la norma de control interno 410-14 Sitios Web, Servicios de Internet y Extranet emitidas en la contraloría general del estado establece que es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad.

Causa: No se han cumplido con las especificaciones establecidas en el plan integral informático.

Efecto: El incumplimiento con los estándares establecidos por la CEACES y la inconformidad de los usuarios (autoridades, docentes, estudiantes).

Conclusiones: La cobertura existente de la red inalámbrica en los interiores de edificios del campus principal de la ESPOCH es deficiente, lo que provoca la pérdida de tiempo y la molestia en los usuarios.

Recomendaciones:

- Realizar el cambio del internet comercial de 149 Mbps a la banda ancha comercial de 450Mbps, lo cual permitirá conectar algo más de 500 computadores portátiles y dispositivos móviles a la intranet.

8. No cuenta con un plan de capacitación.

Criterio: El departamento no cuenta con un plan de capacitación y especialización al personal existente en cada una de las áreas del departamento.

Condición: De acuerdo a la norma de control interno 410-15 Capacitación Informática emitidas en la contraloría general del estado establece que las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.

Causa: Por falta de gestión administrativa el departamento no cuenta con un plan de capacitación de capacitación y especialización.

Efecto: La falta de un plan de capacitación y especialización produce que el personal no pueda adquirir conocimientos innovadores y actualizados, los mismos que ayudaran al desenvolvimiento de sus actividades.

Conclusiones: El departamento cuenta con un plan de capacitación y especialización dirigido únicamente a las autoridades, docentes, estudiantes y público en general.

Recomendaciones:

- Elaborar un plan de capacitación y especialización exclusivo para garantizar la capacitación y actualización al personal de Desitel.
- Incluir al menos dos capacitaciones anuales.

Elaborado por: EMBB	Fecha: 07-02-2014
Revisado por : JVO	

ÍNDICE

DEPARTAMENTO DE SISTEMAS Y TELEMÁTCA "DESITEL"

FASE IV

COMUNICACIÓN DE RESULTADOS

ARCHIVO CORRIENTE	
Programa de Auditoría para comunicación de resultados	PAR
Informe Final	IF

ENTIDAD: Escuela Superior Politécnica de Chimborazo
ÁREA: Departamento de Sistemas y Telemática "DESITEL"
TIPO DE AUDITORÍA: Auditoría a la Gestión de las Tecnologías de la Información
FASE: Comunicación de Resultados.

No	DESCRIPCIÓN	REF P/T	REALIZADO POR	FECHA
	OBJETIVOS			
	❖ Exponer las respectivas conclusiones y recomendaciones en el informe de Auditoría.			
	PROCEDIMIENTOS			
1	Elaborar Informe Final.	HH	EMBB	07/03/2014

Riobamba, 10 de Marzo del 2014

Ingeniero.
Paul Bernal
DIRECTOR DEL DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA "DESITEL"
Presente.

De mi consideración:

Hemos realizado la Auditoría a la Gestión de las Tecnologías de la Información (AGTI) al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012.

El examen se efectuó en base a las normas de control interno emitidas por la Contraloría General del Estado en lo referente a las Tecnologías de la Información. Estas Normas requieren que el examen sea planificado y ejecutado para obtener certeza razonable de que la información y la documentación examinada no contienen exposiciones erróneas de carácter significativo, que se haya ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Los resultados encontrados en el examen se encuentran expresados en los comentarios, conclusiones y recomendaciones que consta en el presente informe.

Atentamente

Marcelo Beltrán
Auditor

PARTE I

INFORMACIÓN INTRODUCTORA

Motivo de la Auditoría

Realizar una Auditoría a la Gestión de las Tecnologías de la Información(AGTI) al departamento de Sistemas y Telemática "DESITEL" de la ESPOCH, de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012, con el fin de evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.

Objetivos de la Auditoría

- Evaluar el control interno
- Evaluar y medir el grado de cumplimiento sobre la Gestión de las Tecnologías de la Información.
- Formular comentarios, conclusiones y recomendaciones, dirigidas a mejorar la Gestión de las Tecnologías de la Información

Enfoque

Este examen especial de auditoria está orientado al grado de cumplimiento sobre la Gestión de las Tecnologías de la Información establecidas en el departamento de Sistemas y Telemática "DESITEL".

PARTE II

INFORMACIÓN DE LA INSTITUCIÓN

La Escuela Superior Politécnica de Chimborazo, en el mes de julio del 2003 aprobó mediante resolución del H. Consejo Politécnico la reestructuración orgánica funcional de la institución, misma que involucró a las diferentes dependencias administrativas y académicas con la finalidad de lograr una administración moderna y eficiente en sus diferentes ámbitos.

Este cambio determino que las tareas académicas encargadas al Departamento de Cómputo y Sistemas se vinculen directamente a las diferentes facultades y las funciones técnicas de asesoría, desarrollo de soluciones tecnológicas en el área informática se integren en el Departamento de Sistemas y Telemática mismas que se encontraban divididas en el comité Informático y el Departamento de Cómputo y Sistemas.

Misión

Proporcionar servicios integrales de calidad en las áreas de desarrollo organizacional y sistemas de información a la ESPOCH y entidades externas, utilizando tecnología de punta, con personal capacitado, estándares de calidad y una participación activa y eficaz del usuario.

Visión

Convertirse en un departamento líder en el desarrollo e incorporación de tecnologías de la Información y comunicación, que soporten las demandas de generación, procesamiento y tratamiento de la información a través de redes de comunicación a nivel interno y externo.

Objetivos

- Definir estándares de procesos y documentación de las actividades informáticas de la institución.
- Planificar, dirigir y controlar el procesamiento automático de datos.
- Asesorar a los departamentos y usuarios de los recursos informáticos.
- Desarrollar e implantar sistemas que automaticen el procesamiento de información.
- Requerir la adquisición de HW y SW justificando su necesidad en su área.
- Administrar el personal técnico que se encuentra involucrado en las actividades informáticas

Funciones

- Presentar al H. Consejo Politécnico el Plan Informático Anual.
- Desarrollar y mantener los sistemas informáticos administrativos, académicos y de la organización.
- Apoyar los procesos de modernización administrativa, académica y de gestión institucionales.

- Administrar el correo electrónico, redes computacionales y todos los recursos informáticos de hardware y software.
- Proporcionar servicios de mantenimiento de Hardware y Software a la ESPOCH y la colectividad.
- Proporcionar servicios de identificación digital y otras especialidades a la ESPOCH y la sociedad.
- Mantener la información electrónica actualizada en el web site de la ESPOCH.
- Implementación de nuevos servicios en el área de la informática y telemática.
- Organizar e implementar programas de capacitación específicos.
- Elaborar los informes técnicos para la adquisición de los recursos informáticos; y,
- Las demás que le señalen las leyes, el Estatuto y los Reglamentos.

PARTE III

RESULTADOS ESPECÍFICOS POR COMPONENTES

1. Norma 410-02 Segregación de Funciones

Conclusión:

Inequitativa distribución de responsabilidades.

Análisis:

El departamento de Sistemas y Telemática "DESITEL" mantiene una inadecuada distribución de responsabilidades, lo que da lugar una incompatibilidad de funciones y responsabilidades del personal existentes en cada una de las distintas áreas.

Recomendaciones:

- Incluir al menos dos personas del área de desarrollo de investigación a aplicaciones informáticas al área de soporte y mantenimiento en los momentos que se los requiera.

Áreas involucradas:

- Área de desarrollo e investigación de aplicaciones informáticas.
- Área de soporte y mantenimiento.

2. Norma 410-06 Administración de Proyectos Tecnológicos

Conclusión:

Existe incumplimiento del proyecto de actualización del Data Center**.**

Análisis:

El incumplimiento del proyecto de actualización del equipo activo de red del Data Center establecido en el PII 2012, provocaría que el sistema institucional quede in-operativo y obsoleto. **(Anexo 6; Ficha 4 dentro del PII)**

Recomendaciones:

- Establecer una reestructuración del plan integral informático.
- Realizar la actualización del equipo activo de red del Data Center establecida en el PII 2012, dentro del periodo específico.

Áreas involucradas:

- Área de infraestructura de redes y telecomunicaciones.

3. Norma 410-07 Desarrollo y Adquisición de Software Aplicativo.

Conclusión:

El desarrollo y actualización del software aplicativo se lo desarrollo de acuerdo a lo planificado, sin embargo a pesar de estar establecido en el Plan Integral Informático no se cumple según la programación establecida para el efecto.

Análisis:

El incumplimiento en la adquisición de software establecido en el plan integral informático del año 2012, han provocado que el desarrollo del departamento se haya estancado y no exista un crecimiento constante.

Recomendaciones:

- La elaboración de políticas internas **(Anexo 4 dentro PII)** que ayuden al cumplimiento total de adquisiciones de software y hardware conforme lo establece el plan integral informático.
- Realizar las gestiones administrativas que permitan contar con el presupuesto necesario para cumplir con las adquisiciones de software y hardware en su totalidad.

Áreas involucradas:

- Área de desarrollo e investigación de aplicaciones informáticas.
- Área de infraestructura de redes y telecomunicaciones.

4. Norma 410-08 Adquisiciones e Infraestructura Tecnológica.

Conclusión:

La infraestructura física inadecuada en el departamento

Análisis:

La falta de infraestructura física en el departamento provoca que el desarrollo en las áreas existentes no cumpla con el impacto planteado en el PII. **(Anexo PII 4.3)**

Recomendaciones:

Realizar las gestiones administrativas que permitan contar con el presupuesto necesario obtener la infraestructura física que el departamento lo requiere.

Áreas involucradas:

- Área de infraestructura de redes y telecomunicaciones.

5. Norma 410-09 Mantenimiento y Control de la Infraestructura Tecnológica.

Conclusión:

No se formaliza el plan de mantenimiento preventivo o correctivo.

Análisis:

El departamento cuenta con un plan de mantenimiento preventivo o correctivo, que no es legalmente aprobado. **(Anexo 7 dentro PII).**

Recomendaciones:

- Aprobar legalmente el plan de mantenimiento de mantenimiento preventivo o correctivo.
- Socializar el plan de mantenimiento preventivo o correctivo
- Incluir verificación de instalaciones eléctricas.
- Incluir verificación y aseguramiento de las instalaciones físicas.

Áreas involucradas:

- - Área de soporte y mantenimiento.

6. Norma 410-10 Seguridad de Tecnología de Información.

Conclusión:

La obtención de respaldos no se realiza en los tiempos establecidos.

Análisis:

El departamento no realiza la obtención de respaldos de la información periódicamente, lo que provoca la inseguridad en la veracidad de la información. **(Anexo 3 dentro PII).**

Recomendaciones:

- Determinar un área externa al departamento en el que se ubiquen los respaldos en caso de producirse siniestros en el Desitel.
- Los respaldos se realizan cada 30 días pero se deberá realizarlo cada 7 días para tener la certeza que la información mantenga una adecuada actualización.

Áreas involucradas:

- Área de desarrollo e investigación de aplicaciones informáticas.

7. Norma 410-11 Plan de Contingencias

Conclusión:

El plan de contingencias no está aprobado.

Análisis:

Existe el plan de contingencias el cual no se encuentra aprobado y por lo tanto ni difundido entre el personal responsable de su ejecución, ni se encuentra en vigencia. **(Anexo 2 dentro PII).**

Recomendaciones:

- Realizar las gestiones administrativas necesarias para la aprobación del plan de contingencias, el cual debe ser sometido a pruebas y entrenamientos periódicos, para que en el momento que sea necesario poder utilizarlo.

Áreas involucradas:

- Área de desarrollo e investigación de aplicaciones informáticas.
- Área de infraestructura de redes y telecomunicaciones.
- Área de soporte y mantenimiento.

8. Norma 410-14 Sitios Web, Servicios de Internet y Extranet

Conclusión:

La cobertura de la red inalámbrica no cumple con las necesidades de los usuarios.

Análisis:

La cobertura existente de la red inalámbrica en los interiores de edificios del campus principal de la ESPOCH es deficiente, lo que provoca la pérdida de tiempo y la molestia en los usuarios. **(Anexo 6: Ficha 5 dentro PII).**

Recomendaciones:

- Realizar el cambio del internet comercial de 149 Mbps a la banda ancha comercial de 450Mbps, lo cual permitirá conectar algo más de 500 computadores portátiles y dispositivos móviles a la intranet.

Áreas involucradas:

- Área de desarrollo e investigación de aplicaciones informáticas.
- Área de infraestructura de redes y telecomunicaciones.
- Área de soporte y mantenimiento.

9. Norma 410-15 Capacitación Informática.

Conclusión:

Existe un plan de capacitación insuficiente.

Análisis:

El departamento cuenta con un plan de capacitación y especialización dirigido únicamente a las autoridades, docentes, estudiantes y público en general. **(Anexo PII 4.3).**

Recomendaciones:

- Elaborar un plan de capacitación y especialización exclusivo para garantizar la capacitación y actualización al personal de Desitel.
- Incluir al menos dos capacitaciones anuales.

Áreas involucradas:

- Área de desarrollo e investigación de aplicaciones informáticas.
- Área de infraestructura de redes y telecomunicaciones.
- Área de soporte y mantenimiento.

CAPÍTULO V

5. Conclusiones y recomendaciones

5.1. Conclusiones.

- La tecnología informática cambia permanentemente, lo que demanda de un continuo desarrollo y actualización de aplicaciones informáticas que automaticen los diferentes procesos con la finalidad que la Escuela Superior Politécnica de Chimborazo se mantenga como una institución de vanguardia.

- Las normas de control interno emitidas por la Contraloría General del Estado establecidas en el sub grupo 410, son de aplicación obligatoria para todas las instituciones y organismos del sector público, que sirven como marco de referencia para la evaluación y control de sus procesos.

- En base al análisis de riesgo y confianza se determinó que se tiene un riesgo del 14,06%, lo cual implica una confianza del 85,94%.

- Si bien es cierto que Desitel cuenta con un Plan Integral Informático es inevitable que su desarrollo no se cumple según la programación lo cual provoca un desequilibrio en el crecimiento permanente del departamento.

5.2 Recomendaciones.

- Mantenerse a la vanguardia tecnológica tanto a nivel de hardware como de software lo cual permitirá continuar en el lugar de excelencia dentro de las entidades educativas de nivel superior en el país.

- Incluir en el Plan Integral Informático procesos y mecanismos que nos permitan llegar a un nivel de confianza del ciento por ciento, enmarcados siempre dentro de las normas de control interno emitidas por la Contraloría General del Estado.

- Es necesario establecer calendarios de capacitación y especialización exclusiva al personal del DESITEL, además una ampliación en la cobertura de la red inalámbrica y sobre todo la actualización del Data Center.

- Analizar y considerar las recomendaciones emitidas en el presente informe de auditoría con la finalidad de que se tomen las medidas correctivas necesarias en beneficio del crecimiento institucional.

Bibliografía

Arens Alvin, A. (2007). *Auditoria un enfoque integral.* Mexico: Pearson Educación.

Aumatell, C. (2003). *La auditoría de la información, componente clave de la gestión estratégica de la información.* Mexico: El profesional de la información.

Hernández Sampieri, R. (2004). *Metodología de la investigación.* La Habana: Editorial Felix Varela.

López Hermoso, J. J. (2013). *Informática Aplicada a la gestion de las empresas* . México: ESIC Editorial, 2000 ISBN.

OLACEFs, X. C. (2011). *"Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones".*

Ortiz Frida, G. M. (2005). *Metodología de la Investigación.* México: Editoral Limosa.

Rivas, G. A. (1998). *Auditoría Informática.* Colombia: ediciones ISBN.

Tamayo Alzate, A. (2010). *Sistemas de Información.* Colombia: Univ. Naccional de Colombia.

Linkografía

Alfaro, E. (21 de enero de 2008). *Auditoría sobre TIC`s.* Obtenido de http://oscarvasan21.wordpress.com/2010/06/02/concepto-de-auditoria-de-tecnologia-de-informacion-2/

Aymara, Hernaandez, & Arias. (25 de julio-diciembre de 2010). *Auditoría Información y Gestion de Tecnologias de la Información y Comunicación.* Obtenido de http://www.redalyc.org/articulo

Figeroa, J. L. (10 de Agosto de 2005). *Gobierno de TICs desde las perspectivas de auditoría.* Obtenido de http://www.ruv.itesm.mx/pce

Herrera, I. B. (21 de diciembre de 2010). *Planififcación Estrategica*. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/952/6/Capitulo_2.pdf

Contraloría General del Estado, E. (01 de Diciembre de 2009). *410 Tecnologías de la Información* . Obtenido de http://www.contraloria.gob.ec/normatividad_vigente.asp

McGraw, H. (23 de 2 de 2000). *Auditoria un enfoque integral*. Obtenido de http://www.casadellibro.com/libro-auditoria-un-enfoque-integral-12-ed/9789584100399/706812

Glosario de Términos

Alcance.- Selección de aquellas áreas o actividades que serán revisados a profundidad en la fase de ejecución; esta decisión debe ser tomada en función de la materialidad, sensibilidad, riesgo y costo de la auditoría, así como al efecto de los posibles resultados a obtener.

Ambiente de control interno.- Se refiere al establecimiento de un entorno que estimule e influencie, las tareas de las personas con respecto al control de sus actividades.

Áreas críticas.- Actividades que inciden de manera directa y determinante en los procesos medulares de la organización, actividad, sector o unidad auditada, es importante su control, para mantener la calidad de la auditoría de gestión.

Auditoría.- Examen objetivo, sistemático, profesional y posterior de las operaciones financieras, administrativas y de gestión, practicado con la finalidad de verificar y evaluar dichas operaciones y de formular observaciones y recomendaciones pertinentes.

Calidad.- Adecuación de un producto o servicio a especificaciones o estándares establecidos por autoridades competentes, o de aceptación general, con aptitud para satisfacer las necesidades del cliente o usuario.

Causa.- Motivo que origina el incumplimiento de las normas legales y administrativas, reguladoras del ejercicio de la función pública; es la razón que explica, el hecho o situación irregular.

Condición.- Descripción objetiva e imparcial de las observaciones o deficiencia encontrada, en los documentos, procesos, actividades u operaciones analizadas.

Criterio.- Constituye la norma legal o técnica, o los principios generalmente aceptados, que regulan la ejecución de una actividad; es la referencia para efectuar la comparación con los hechos y determinar cumplimientos o desviaciones.

Entorno.- Ambiente o comunidad, a la que va dirigido el bien generado o el servicio prestado por la organización.

Estructura de control interno.- es el conjunto de planes, métodos, procedimientos y otras medidas, incluyendo la actitud de la dirección de una entidad, para ofrecer seguridad razonable respecto a que están lográndose los objetivos planificados por el organismo auditado.

Estructura organizacional.- Proporciona el marco dentro del cual se planean, ejecutan, controlan y supervisan sus actividades, a fin de lograr los objetivos y metas establecidos.

Evidencia.- Pruebas que respaldan el contenido del informe del auditor, y que son obtenidas a través de los diversos medios empleados en el proceso de auditoría.

Evidencia suficiente.- Evidencia objetiva y competente, obtenida a través de las pruebas de control y de los procedimientos propios de la auditoría, para sustentar los hallazgos, conclusiones y recomendaciones del auditor.

Gestión.- Las actividades, tareas y acciones expresadas en programas, proyectos u operaciones, a cargo de una organización, dirigida a la producción de bienes o servicios, para satisfacer propósitos, metas u objetivos previamente determinados.

Hallazgo de auditoría.- Es toda información que a juicio del auditor, permite identificar hechos o circunstancias importantes que inciden en forma significativa, en la gestión de la entidad o programa que merecen ser comunicados en el informe; sus elementos son: condición, criterio, causa y efecto.

Impacto.- Nivel de repercusión a mediano o largo plazo en el entorno social, económico o ambiental, de los productos o servicios prestados.

Integridad.- Constituye una calidad de la persona que mantiene principios morales sólidos y vive en un marco de valores.

Metas.- Resumen cuantitativo, específico y cronológico de las acciones y actividades a realizar, para el cumplimiento de los objetivos planteados por la organización.

Monitoreo.- Evalúa la calidad del control interno en el tiempo y permite al sistema reaccionar en forma dinámica; se orienta a la identificación de controles débiles, insuficientes o innecesarios y, promueve su reforzamiento.

Muestreo.- Técnica empleada en el análisis de un grupo de hechos o eventos, para obtener cierta probabilidad o certidumbre, en relación con las características del universo analizado.

Observación.- Hechos o circunstancias significativas, identificadas durante el examen, susceptibles de mejoras.

Organización.- Puede conceptualizarse de diferentes formas, pero en la mayoría de los casos, significa la suma de personas, estructuras y procesos que se proponen lograr determinados objetivos.

Papeles de Trabajo.- Documentos que contienen la evidencia que respalda los hallazgos, observaciones, opiniones, conclusiones y recomendaciones.

Planeamiento.- Fase de la auditoría durante la cual el auditor identificará el que, cómo, cuándo y con qué recursos, ejecutará el examen, así como determinará el enfoque de la auditoría, los objetivos y el alcance.

Población.- Es cualquier grupo de elementos individuales o unidades del universo, de los cuales va a seleccionarse una muestra.

Políticas.- Decisiones de alto nivel, que buscan unificar conductas y orientar procesos hacia el logro de un estándar objetivo.

Procedimiento de control.- Elementos establecidos por la administración, para asegurarse que los objetivos específicos de la organización, sean alcanzados.

Proceso.- Serie de pasos, actividades o tareas secuenciales y lógicas, que en combinación con el personal, la infraestructura y la tecnología, permite a la organización, agregar valor a los insumos y transformarlos en el producto o en el servicio deseado.

Programa de auditoría.-Es el documento final de la fase de planeamiento, en el cual se resumen las decisiones más importantes, relativas a la estrategia para el desarrollo de la auditoría de gestión.

Prueba selectiva.- Procedimiento que consiste en examinar una muestra representativa de la población, para derivar del resultado obtenido, una opinión general sobre esta última.

Usuario.- Individuo o persona a quien va dirigido el bien producido o el servicio prestado por la organización.

Valor agregado.- Contribución que cada tarea o actividad adiciona al bien o servicio intermedio o final, que produce o presta la organización; el valor que agrega todo el proceso productivo se denomina, valor agregado total, y su análisis se realiza a través del estudio de la cadena de valor.

Anexos

Anexo 1

EL CONSEJO POLITÉCNICO DE LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CONSIDERANDO

Que, la Escuela Superior Politécnica de Chimborazo es una institución de educación Universitaria, persona jurídica de Derecho Público, autónoma, con domicilio principal en la ciudad de Riobamba, provincia de Chimborazo; se rige por la constitución política de la República del Ecuador, la Ley de Educación Superior y Reglamento General, su Ley Constitutiva No. 6909, publicada en el Registro Oficial No. 425 del 6 de Noviembre de 1973, mediante el cual obtuvo la actual nominación; y otras leyes conexas su estatuto politécnico y sus reglamentos.

Que, dentro de la Estructura de la Escuela Superior Politécnica de Chimborazo, se crea estatutariamente el Departamento de Sistemas y Telemática, como consta en los Artículos 59, 60 y 61 de Estatuto Politécnico; donde se define su Misión y sus Funciones.

En uso de las atribuciones que le confiere el Artículo 11 literal h) del Estatuto Politécnico y conforme a lo estipulado en la Ley Orgánica de Educación Superior,

RESUELVE:

Expedir el presente;

REGLAMENTO DEL DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA DE LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CAPITULO II

DE LA MISIÓN Y VISIÓN

Art. 1.- La visión del DESITEL es: convertirse en un departamento líder en el desarrollo e incorporación de tecnologías de la Información y comunicación, que soporten las demandas de generación, procesamiento y tratamiento de la información a través de redes de comunicación a nivel interno y externo.

Art. 2.- La misión del DESITEL es: proporcionar servicios integrales de calidad en el área de sistemas e informática para el desarrollo institucional.

El Departamento de Sistemas y Telemática usará las siglas DESITEL.

CAPITULO III

DE SUS FUNCIONES

Art. 3.- Las funciones del Departamento de Sistemas y Telemática son:

Presentar al Consejo Politécnico el plan informático anual;

Desarrollar sistemas informáticos administrativos, académicos y de organización;

Apoyar los procesos de modernización administrativa y de gestión;

Administrar los servicios informáticos, redes computacionales y los recursos informáticos de hardware y software;

Proporcionar servicios de mantenimiento de hardware y software;

Proporcionar servicios de identificación digital y otras especialidades;

Implementar nuevos servicios en el área de la informática y la telemática;

Organizar e implementar programas de capacitación específicos;

Elaborar informes técnicos para la adquisición de los recursos informáticos para administración central y unidades de apoyo;

Asesorar, regular, orientar, coordinar y supervisar actividades del desarrollo informático de la ESPOCH;

Optimizar los recursos informáticos de la institución; y,

Participar en los convenios nacionales e internacionales en materia de desarrollo tecnológico y científico en el campo de la informática a favor de la ESPOCH.

CAPITULO IV

DE LA ORGANIZACIÓN

Art. 4.- El DESITEL, para el cumplimiento de sus funciones se regirá por el presente reglamento, y estará integrado por:

El director, un profesional con formación y experiencia en el área de la informática, designado por el Rector;

Los coordinadores de las áreas de: Sistema Académico, Áreas de Investigación, Sistemas y Redes, y, Capacitación y una sub-área de Soporte y Mantenimiento, el personal responsable es designado de técnicos de la ESPOCH, por el director del DESITEL;

El personal técnico informático, vinculado a la institución a través de las diferentes facultades, departamentos, otras unidades; y,

El personal de apoyo.

Art. 5.- La estructura organizacional del DESITEL, está integrada por:

Nivel directivo:

Dirección.

Nivel operativo:

Área Sistema Académico;

Área de Investigación, Sistemas y Redes; Sub-área de Soporte y Mantenimiento; y,

Área de Capacitación.

Nivel apoyo:

Secretaría;

Bodega; y,

Conserjería.

CAPITULO V

DEFINICIÓN DE PERFILES, OBJETIVOS Y FUNCIONES DE LA ESTRUCTURA ORGANIZACIONAL DEL DESITEL DE LA DIRECCIÓN DEL DESITEL

Art. 6.- La dirección del DESITEL, dependerá directamente del Rectorado.

Art. 7.- Bajo la coordinación y liderazgo de la dirección se encontrarán los niveles asesor, operativo y de apoyo.

Art. 8.- Para la dirección del DESITEL, se deberá considerar la experiencia y conocimientos en Procesos Administrativos, Ciencias de la computación, Desarrollo de Proyectos Informáticos, Desarrollo de Software, Administración de Redes.

Art. 9.- Son atribuciones y funciones de la dirección del DESITEL:

Desarrollar proyectos encaminados al fortalecimiento tecnológico institucional;

Gestionar los recursos informáticos como el talento humano y los recursos hardware y software;

Presentar el plan operativo informático anual al Consejo Politécnico;

Apoyar a los técnicos responsables de las facultades, escuelas, departamentos y unidades;

Administrar los proyectos que harán posible el cumplimiento de la misión y de la visión del DESITEL;

Analizar, evaluar y dirigir el desempeño y productividad del personal;

Autorizar la utilización de los recursos necesarios para el cumplimiento de los programas y el desarrollo de tareas específicas del DESITEL;

Coordinar con los diferentes estamentos internos y externos con la finalidad de determinar las necesidades y establecer los planes de soluciones;

Convocar a reuniones periódicas al personal informático de la institución, para coordinar, planificar y dar el cumplimiento de metas y objetivos establecidos en el plan informático anual; y,

Efectuar actividades inherentes encomendadas al DESITEL.

CAPITULO VI

DEL SISTEMA ACADÉMICO Y DE LAS ÁREAS DE INVESTIGACIÓN, SISTEMAS Y REDES DEL SISTEMA ACADÉMICO

Art. 10.- Estará integrado por un Coordinador 1 quién preside y un Coordinador 2 que es de apoyo, además por los técnicos informáticos del sistema académico de facultades, los mismos que serán responsables del mantenimiento y desarrollo del sistema en cada facultad.

DEL ÁREA DE INVESTIGACIÓN, SISTEMAS Y REDES

Art. 11.- Para la coordinación del área se deberá considerar experiencia y conocimientos en la generación de proyectos productivos, tecnológicos y de investigación, la coordinación de cada área dependerá directamente de la dirección del DESITEL.

Art. 12.- Son atribuciones y funciones de la coordinación:

Generar proyectos de producción, tecnológicos y de investigación;

Realizar el seguimiento y avances de los proyectos que se estén ejecutando;

Involucrar pasantes, tesistas para que apoyen el desarrollo de proyectos tecnológicos;

Gestionar los recursos informáticos disponibles en el laboratorio de Investigación y Desarrollo para el cumplimiento de las metas y objetivos;

Presentar el plan operativo informático anual de su área a la dirección del DESITEL;

Administrar los proyectos que harán posible el cumplimiento de la misión y de la visión del DESITEL;

Definir la Metodología, procesos y estándares de desarrollo y documentación de los procesos de desarrollo de aplicaciones informáticas;

Convocar a reuniones periódicas quincenales para analizar el avance de los proyectos;

Definir proyectos de desarrollo de sistemas informáticos orientados a la automatización de procesos y servicios;

Brindar soporte y mantenimiento de las aplicaciones informáticas implantadas en la institución;

Realizar el seguimiento y avances de los proyectos de desarrollo que se estén ejecutando;

Involucrar pasantes, tesistas para que apoyen la automatización de procesos y servicios;

Gestionar los recursos informáticos disponibles en el laboratorio de Investigación y Desarrollo para el cumplimiento de las metas y objetivos;

Presentar el plan operativo informático anual de su área a la dirección del DESITEL;

Administrar los proyectos que harán posible el cumplimiento de la misión y de la visión del DESITEL;

Definir la Metodología, procesos y estándares de desarrollo y documentación de los procesos de desarrollo de aplicaciones informáticas;

Convocar a reuniones periódicas para analizar el avance de actividades;

Definir proyectos de implantación de redes informáticas orientadas a incrementar la accesibilidad de los usuarios de la ESPOCH;

Dar mantenimiento a los servidores y enlaces que soportan los servicios de la intranet;

Dar soporte técnico a los usuarios institucionales con la finalidad de garantizar su integración al uso de las tecnologías de red disponibles en la institución;

Realizar el seguimiento y avances de los proyectos de desarrollo tecnológico en el área de redes;

Gestionar los recursos informáticos disponibles en el laboratorio de Investigación y Desarrollo para el cumplimiento de las metas y objetivos; y,

Definir las metodologías, procesos y estándares para la implementación de tecnologías de redes en la institución.

DEL ÁREA DE CAPACITACIÓN

Art. 13.- La coordinación del área dependerá directamente de la dirección del DESITEL.

Art. 14.- Son atribuciones y funciones de la coordinación del Área de Capacitación:

Definir y planificar proyectos de capacitación y soporte continuo a los usuarios;

Generar alternativas de capacitación interna y externa para el personal informático de la institución;

Establecer vínculos con la sociedad a través de proyectos de capacitación orientados a segmentos como empresas e instituciones públicas y privadas; orientado a la generación de recursos para invertir en desarrollo de tecnología;

Desarrollar planes de capacitación continua para los servidores politécnicos y estudiantes, a través del uso de las nuevas tecnologías de la Información y comunicación (e-virtual, mail, video conferencias, otros);

Dar soporte técnico a los usuarios institucionales con la finalidad de garantizar su integración al uso eficiente y eficaz de las tecnologías disponibles en la institución;

Realizar el seguimiento y avances de los proyectos de capacitación y soporte;

Involucrar pasantes, tesistas para que apoyen los procesos de capacitación y soporte;

Gestionar los recursos informáticos disponibles en el laboratorio de Capacitación y Video Conferencias para el cumplimiento de las metas y objetivos;

Brindar soporte al desarrollo de objetos de aprendizaje con fines pedagógicos de las distintas facultades y de capacitación;

Presentar el plan operativo informático anual de su área a la dirección del DESITEL;

Administrar los proyectos que harán posible el cumplimiento de la misión y de la visión del DESITEL;

Definir las metodologías, procesos y estándares para el desarrollo de cursos y materiales para la generación de contenidos; y,

Convocar a reuniones periódicas para analizar el avance de los proyectos.

DE LA SUB-AREA DE MANTENIMIENTO Y SOPORTE.

Art. 15.- La coordinación del área dependerá directamente del área de investigación, Sistemas y Redes y se apoyará en el Manual de mantenimiento de equipos y sus anexos.

Art. 16.- Para el mantenimiento de equipos se debe aplicar el respectivo Manual de Mantenimiento de Equipos.

DEL PERSONAL DE APOYO DEL DESITEL.

Art. 17.- El personal de apoyo estará constituido por Secretaría y Consejería; personal que será designado por el departamento de recursos humanos considerando el área y las funciones del DESITEL.

DEL PERSONAL DE APOYO DE LABORATORIOS INFORMÁTICOS

Art. 18.- Las Facultades contarán con personal de apoyo para los laboratorios informáticos quienes controlarán su buen uso en coordinación con los técnicos informáticos.

El presente Reglamento fue discutido y aprobado por los miembros del Consejo Politécnico en sesión ordinaria realizada el 24 de junio de 2008, mediante Resolución No.279.CP.2008.

Dr. Silvio Álvarez Luna Dr. Julio Falconí Mejía

RECTOR DE LA ESPOCH SECRETARIO GENERAL

nexo 2

ENCUESTAS

MARCH EBB
Auditores Consultores

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Entrevista Preliminar

Área Desarrollo e Investigación de Aplicaciones Informáticas y Área de Soporte y Mantenimiento: **Ing. Alex Tacuri**

7. **¿La infraestructura física existente es la adecuada?**

   SI ☐ **NO** ☐

8. **¿Existe personal con conocimientos suficientes en videoconferencias?**

   SI ☐ **NO** ☐

9. **¿El departamento cuenta con planes de capacitación?**

   SI ☐ **NO** ☐

10. **¿Existen los repuestos para los equipos electrónicos?**

    SI ☐ **NO** ☐

11. **¿Existe el personal necesario para cubrir el Plan Anual Informático?**

    SI ☐ **NO** ☐

Anexo 3

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Entrevista Preliminar

Área de Infraestructura de Redes y Telecomunicaciones: **Ing. Alex Tacuri**

12. ¿Existen zonas WIFI para los usuarios?

SI ☐ NO ☐

13. ¿La planta eléctrica soporta el equipo activo de red y el sistema de climatización del DataCenter?

SI ☐ NO ☐

14. ¿La cobertura Wifi cumple con los indicadores de acreditación?

SI ☐ NO ☐

15. ¿El equipo de red DataCenter ha cumplido su tiempo de vida útil?

SI ☐ NO ☐

PLAN INTEGRAL INFORMÁTICO

ESCUELA SUPERIOR POLITÉCNICA
DE CHIMBORAZO

2012

PLAN INFORMÁTICO ESPOCH 2012

I. PROPOSITO

Presentar un plan informático acorde con la misión, visión, objetivos institucionales y sujeto al Plan de Mejoras Institucional 2012-2014, aprobado por el Consejo Politécnico.

II. APLICACIÓN

La metodología, procedimientos y actividades definidos en este documento deberán ser aplicados en su totalidad por la Dirección de Tecnologías de la Información y Comunicación (DTIC), de la Escuela Superior Politécnica de Chimborazo.

III. ALCANCE

El contenido y definición del Plan Informático involucra tanto a los miembros del área de Tecnologías de la Información y Comunicación (DTIC y Técnicos de Facultades), como también la Unidad Técnica de Planificación Institucional, y deberá ser aprobado en conjunto con los Planes y Proyectos de desarrollo institucional.

IV. RESPONSABILIDADES

Serán responsables de la aplicación de este plan, directivos y responsables técnicos del área DTIC, en coordinación con la Unidad Técnica de Planificación Institucional.

V. USO

Se utilizará como elemento normativo y procedural para su uso en la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH y formará parte de los Proyectos Institucionales.

VI. REFERENCIAS

- Plan Operativo DESITEL 2012
- Informes Ejecutivos Comité de Plan de Mejoras 2012-2014
- MEMORIA TECNICA – DOCUMENTACION DE IMPLEMENTACION DE INFRAESTRUCTURA PARA EQUIPAMIENTO DE DATA CENTER ESPOCH.2010 COMPUEQUIP DOS.

VII. DEFINICION DEL PLAN INFORMÁTICO

1) INTRUDUCCION

Con la finalidad de proyectar el desarrollo informático institucional, se definirá el plan informático, donde se plasmarán estrategias y proyectos encaminados a incorporar las Nuevas Tecnologías de la Información y Comunicación al proceso de Gestión Académica y Administrativa en la institución. Como resultado de la ejecución del plan se pretende incorporar y desarrollar tecnología enmarcada en el desarrollo de redes de voz y datos, servidores de aplicaciones, y desarrollo de aplicaciones informáticas, así como el mantenimiento de los servicios y equipo informático institucional.

Este documento, resume la formulación del Plan para el desarrollo de las Tecnologías de Información en el presente año. Su estructura se establece a partir de un diagnóstico de la situación actual, para luego desarrollar las líneas estratégicas y los proyectos específicos a través de los cuales se pueda aportar a la re categorización institucional.

Cabe mencionar que un plan informático, no es un método para resolver problemas corrientes en cortos períodos, puesto que no permite competir con cambios inesperados, esto no es un indicador de error de concepto, pero prueba el riesgo adquirido en las actividades del plan.

2) OBJETIVOS

El plan Informático de la Escuela Superior Politécnica de Chimborazo, se enmarca dentro de lo que es la definición de la misión y visión de la Dirección de Tecnologías de Información y Comunicación:

MISION: Proporcionar servicios integrales de calidad en el área de sistemas e información para el desarrollo institucional.

VISION: Integrar Tecnologías de la Información y Comunicación, que satisfagan las demandas de gestión documental, de información con la finalidad de aportar al desarrollo de conocimiento en el área académica, de investigación, administrativa y vinculación de nuestra institución.

2.1. OBJETIVO ESTRATEGICO

Consolidar la modernización de la gestión institucional, apoyando las funciones y procesos académico-administrativos institucionales, proporcionando servicios integrales en el área de las tecnologías de información y comunicación, teniendo como base el plan de Mejoras Institucional 2012-2014.

2.2. OBJETIVOS OPERATIVOS

a) Actualizar la infraestructura científica tecnológica institucional.

b) Elaborar, aprobar y ejecutar el plan de mantenimiento de hardware y software institucional.

c) Desarrollar y gestionar aplicaciones informáticas institucionales que automaticen los procesos académicos, administrativos y de organización de la institución, garantizando su integridad y seguridad;

d) Desarrollar y mantener las aplicaciones informáticas que apoyen la ejecución y gestión de proyectos institucionales para brindar un excelente servicio y satisfacer las necesidades de nuestros clientes politécnicos.

e) Administrar, gestionar, brindar soporte y generar proyectos de infraestructura de redes y comunicaciones de la institución con la finalidad de garantizar el acceso, uso y seguridad de los diferentes servicios informáticos institucionales;

3. METAS

3.1. Elaborar un Diagnóstico de la Situación Informática de la ESPOCH

3.2. Proponer alternativas de mejoramiento institucional (Planes y Proyectos)

3.3. Identificar los recursos y los responsables para desarrollar un Plan Informático de la ESPOCH a mediano y largo plazo.

4. DIAGNÓSTICO DE LA SITUACION ACTUAL

4.1. ESTRUCTURA DTIC

En respuesta al Nuevo Manual de Procesos y Funciones para los servidores politécnicos aprobado mediante resolución de Consejo Politécnico en el mes de febrero de 2012 la Dirección de Tecnologías de la Información y Comunicación está estructurada por la Dirección, el área de Investigación y Desarrollo de Aplicaciones Informáticas, área de Infraestructura de Redes y Telecomunicaciones y Área de Soporte y Mantenimiento tal como se presenta en la *figura 1:*

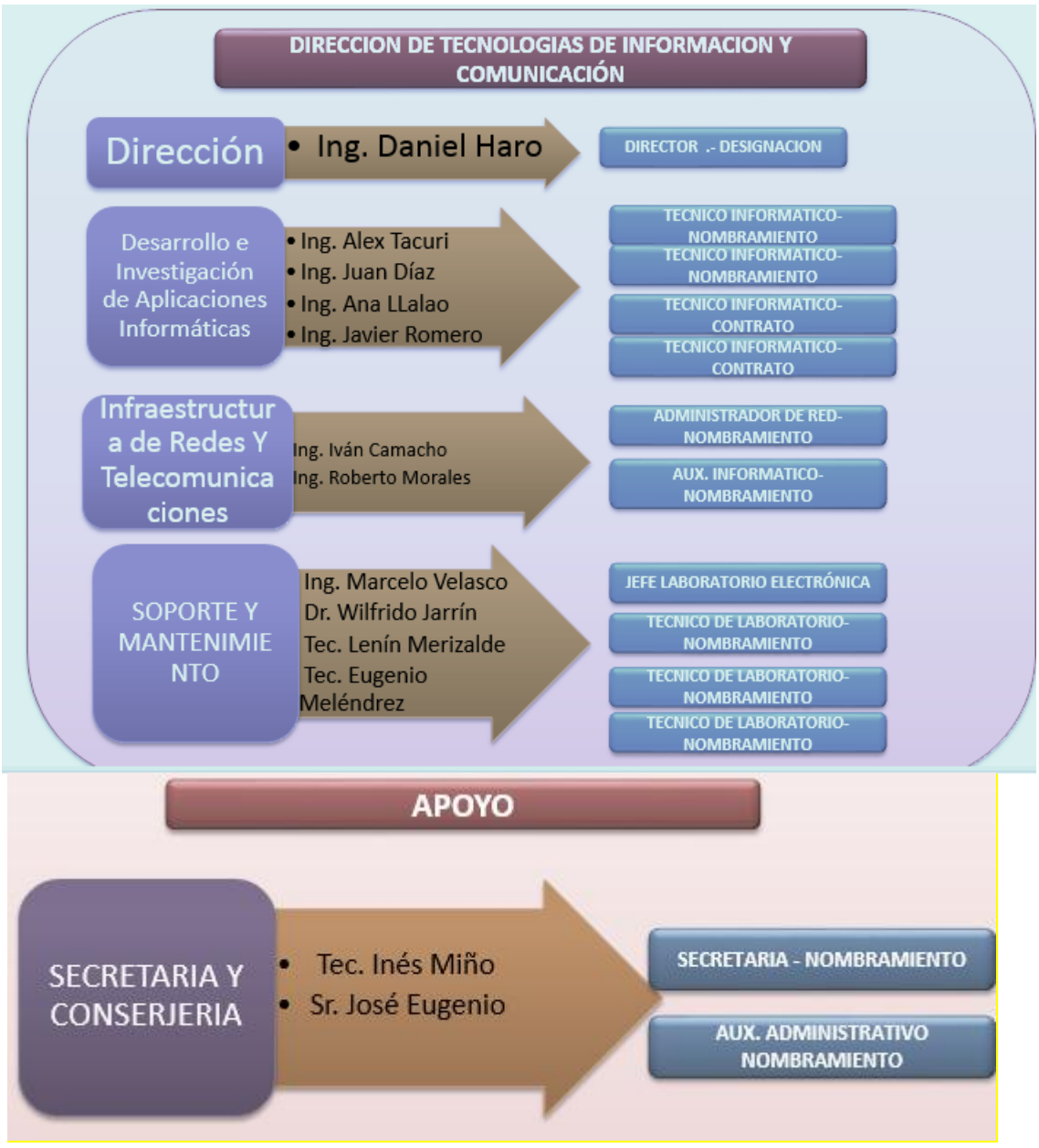


Figura 1. Estructura del DTIC

4.2. PROCESOS DE LA DTIC

Con esta estructura la Dirección maneja los procesos que se detallan a continuación con los respectivos responsables:

PROCESO	ATRIBUCIONES Y RESPONSABILIDADES	SUBPROCESOS	PRODUCTOS	PERSONAL	PUESTO
DIRECCION DE TECNOLOGIAS DE INFORMACION Y COMUNICACIÓN	Proponer al Consejo Politécnico, para su aprobación, las políticas institucionales de gestión de las Tecnologías de la Información y Comunicación, en concordancia a la misión, visión, fines y objetivos institucionales	Planificación	Políticas Institucionales de gestión de las TIC	Ing. Paul Bernal.	Director de Tecnologías de Información y Comunicación
	Desarrollar el Plan de Tecnologías de Información y Comunicaciones; y, coordinar los procesos de diseño e implementación, en el marco de los objetivos del plan Estratégico Institucional;	Coordinación	Plan Informático Institucional		
	Mantener una coordinación permanente con organismos públicos y privados en asuntos relacionados al área de informática a fin de realizar actividades conjuntas		Participar como parte del Directorio y Asambleas de CEDIA		
	Planificar, organizar y coordinar la administración y actividades relacionadas a la Dirección TIC's con la implementación de mejores prácticas tecnológicas, permitiendo mejorar el rendimiento, valor y control sobre las inversiones en tecnología de la información;	Gestión	Renovación tecnológica de la DTIC		
	Monitorear el cumplimiento de los productos y servicios asignados a los equipos bajo su dependencia, en el marco del Sistema de Control de Gestión Interna		Informes de avances y cumplimiento		
	Elaborar, proponer, ejecutar y evaluar los planes, programas y proyectos de su gestión, así como efectuar las reformas que permitan retroalimentar y mejorar los	Evaluación	Proyectos Informáticos en base al PEDI		

	procesos críticos				

PROCESO	SUBPROCESOS	PRODUCTOS	PERSONAL	PUESTO
Desarrollo e Investigación de Aplicaciones Telemáticas	Planificación	Plan Informático de software	Ing. Alex Tacuri	Técnico Informático
		Informe de ejecución del plan informático de software		
	Ingeniería de software	Especificaciones de los requerimientos de software		
		Estudios e informes de factibilidad		
		Informes de análisis y diseño de arquitectura de software		
		Manual de Usuario	Ing. Diego Palacios	Técnico Informático
		Manual Técnico		
		Aplicaciones Informáticas		
		Informe de Prueba		
	Mantenimiento de software	Sistema de control de Aplicaciones Informáticas	Ing. Javier Romero	Técnico Informático
		Respaldos de Aplicaciones		
		Actualizaciones de Aplicaciones Informáticas		
	Administración de base de datos	Respaldos de Datos		
		Estudios e informes de factibilidad	Ing. Juan Carlos Diaz	Técnico Informático
		Informe de mantenimiento y monitoreo de la base de datos		
		Informe de Seguridad de datos		

		Informe de diseño lógico y físico de base de datos para aplicaciones		
PROCESO	**SUBPROCESOS**	**PRODUCTOS**	**PERSONAL**	**PUESTO**
INFRAESTRUCTURA DE REDES Y TELECOMUNICACIONES	Planificación de Infraestructura de Redes y Telecomunicaciones	Plan de Infraestructura de Redes y Telecomunicaciones	Ing. Iván Camacho	Auxiliar Informático
		Informe de Ejecución del plan de Infraestructura de Redes y Telecomunicaciones		
		Informe de Utilización de los Recursos Tecnológicos		
		Informe de Proyección de Requerimientos Futuros		
	Configuración de Infraestructura de Redes y Telecomunicaciones	Diseño de la Red		
		Manual de Configuraciones		
		Informe de Instalación/Configuración		
		Inventario Lógico y Físico de la red		
		SLA (Service Level Agreement)		
		HelpDesk		
		Bitácora de Cambios/Configuraciones		
		Informes de estado de la Red		
	Control de Fallas	Informes de monitoreo y supervisión del estado de la infraestructura y la red	Ing. Roberto Morales	Administrador de Red
		Informe de reporte, determinación y corrección de problemas.		
		Informe de respaldo, reemplazo/reconfiguración y pruebas.		
		Reporte de actualización equipos/dispositivos		
	Monitoreo y	Informe de Indicadores de Rendimiento		

	Rendimiento de Infraestructura de Redes y Telecomunicaciones	Informe de indicadores de uso de red, dispositivos, enlaces y monitoreo del rendimiento.		
		Informe de análisis y afinamiento		
	Gestión de Seguridades	Informe de Análisis de Riesgos y Evaluación de los servicios de seguridad		
		Informe de evaluación de soluciones de gestión de seguridad		
		Manual de políticas de uso aceptable		

PROCESO	SUBPROCESOS	PRODUCTOS	PERSONAL	PUESTO
SOPORTE Y MANTENIMIENTO	Planificación	Plan de Mantenimiento	Ing. Marcelo Velasco	Jefe Laboratorio Electrónica ESPOCH
		Informe de Ejecución del Plan de Mantenimiento		
	Mantenimiento Preventivo / Correctivo	Informes del Estado del Equipo Electrónico	Tec. Eugenio Melendres Paula	Técnico de Laboratorio
		Informes de Mantenimiento Preventivo y Correctivo		
		Informe de requerimientos para mantenimiento correctivo		
	Soporte HW/SW	Informe de incidencias en aplicaciones informáticas	Tec. Eugenio Melendres Paula	Técnico de Laboratorio
		Informe de asesoramiento en el manejo de equipos electrónicos y de telecomunicaciones		
		Informe de instalación de equipos y redes		
	Especificaciones Técnicas de Requerimientos de equipos electrónicos	Informe técnico de caracterización de equipos electrónicos y de telecomunicaciones	Dr. Wilfrido Jarrin Moreira	Técnico de Laboratorio
		Informe de fiscalización de compra de equipos electrónicos y de telecomunicaciones		
		Informe para reingreso de equipos electrónicos a bodega		

4.3. ANÁLISIS FODA

FORTALEZAS	**DEBILIDADES**
Experiencia en mantenimiento software y hardware de equipos electrónicos y de Telecomunicaciones.	Falta de infraestructura Física.
Dominio de sistemas de videoconferencias.	Falta de personal para cubrir con el plan de mantenimiento anual en la Espoch.
Dominio de varias aplicaciones informáticas para el soporte institucional	Falta de plan de capacitación y especialización
Trabajo en Equipo	Falta de herramientas adecuadas para realizar el mantenimiento.
Experiencia en instalación de redes informáticas. (Hardware).	Falta de recursos económicos y materiales para cubrir imprevistos de último momento en las diferentes dependencias de la ESPOCH.
Personal identificado con la institución	Falta de accesorios de cómputo, en la bodega institucional.
	No existen repuestos para los equipos electrónicos ni de telecomunicaciones en la bodega
	Políticas de seguridad industrial.
	Inequitativa distribución de responsabilidades en las distintas áreas.
	Poca comunicación entre el área y las dependencias.
OPORTUNIDADES	**AMENAZAS**
Brindar capacitación externa e interna	Disminución en el apoyo financiero.
Personal con motivación	Empresas de desarrollo.
Personal con experiencia	Desprestigio departamental
Producir servicios para clientes internos y externos	

4.4. DESCRIPCION DE LAS POLITICAS INFORMATICAS ACTUALES

INTRANET INSTITUCIONAL

Soporte y Mantenimiento a:

- Backbone de Fibra Óptica Mono modo y Multimodo que integra todos los edificios.
- Equipos activos de Red que permiten conectar a equipos (PCs y Laptos) de forma inalámbrica a la intranet institucional.
- Servidores BLADE, mismos que contienen aplicativos institucionales, permitiendo reducir espacio, con un bajo consumo de energía.
- Servicios TCP/IP (base del funcionamiento aplicaciones TICs) funcionando con tecnología IPV6.
- Internet Comercial que cuenta con una conexión de 149 Mbps; e Internet Avanzado con una conexión de 45 Mbps. Cabe resaltar que desde este mes se han realizado las gestiones para el aumento del ancho de banda Comercial a 450 Mbps.
- Redes Privadas Virtuales Institucionales (VPNs), mismas que permiten integrar a la red local (Campus Principal), los centros asociados y las extensiones.
- Telefonía IP con alrededor de 250 extensiones habilitadas.
- LA red inalámbrica que permite conectar algo más de 500 computadores portátiles y dispositivos móviles a la intranet e internet.
- Sistema de videoconferencias Punto a Punto, Punto Multipunto de contexto local, nacional o internacional.

SISTEMAS INFORMATICOS

Los sistemas informáticos del área de Desarrollo de la DTIC se muestran en la siguiente tabla, con la descripción de los sistemas que actualmente están en producción, es decir están siendo utilizados por la comunidad politécnica:

5. PROYECTOS PROPUESTOS

5.1. AREA DE INVESTIGACION Y DESARROLLO DE APLICACIONES INFORMÁTICAS

En el Anexo 10, se pueden revisar las fichas técnicas de estos proyectos a realizarse en el área de Investigación y Desarrollo de Aplicaciones Informáticas durante el 2012.

Objetivo 1. *Desarrollar y mantener las aplicaciones informáticas que apoyen la ejecución y gestión de proyectos institucionales para brindar un excelente servicio y satisfacer las necesidades de nuestros clientes politécnicos.*		
Proyecto	***Responsable***	***Tiempo Estimado***
Mantenimiento del sistema OASIS – Secretarias Académicas	Ing. Alex Tacuri.	12 meses

Mantenimiento del sistema OASIS – Docentes	Ing. Alex Tacuri.	12 meses
Mantenimiento del sistema OASIS – Estudiantes	Ing. Alex Tacuri.	12 meses
Mantenimiento del sistema Passport	Ing. Alex Tacuri.	12 meses
Mantenimiento del sistema de Recaudaciones y Retenciones	Ing. Juan Carlos Díaz	12 meses
Mantenimiento del sistema SAWE	Ing. Javier Romero	12 meses
Mantenimiento del módulo SISREC – SISEPEC	Ing. Ana LLalao	12 meses
Mantenimiento del Sistema SIGATH	Ing. Javier Romero	12 meses
Mantenimiento de Base de Datos Centralizada V2	Ing. Juan Carlos Díaz	12 meses
Consulta del estado de Matriculas	Ing. Juan Carlos Díaz	12 meses
Sistema de Pago de Matricula	Ing. Juan Carlos Díaz	12 meses

5.2. AREA DE REDES E INFRAESTRUCTURA

En el Anexo 7, se pueden revisar las fichas técnicas de estos proyectos a realizarse en el área de Investigación y Desarrollo de Aplicaciones Informáticas durante el 2012.

Objetivo 1. Actualizar la infraestructura científica tecnológica institucional.		
Proyecto	***Responsable***	***Tiempo Estimado***
Actualización del equipo activo de red del DataCenter	Área de Redes e Infraestructura	12 meses

Objetivo 2. Administrar, gestionar, brindar soporte y generar proyectos de infraestructura de redes y comunicaciones de la institución con la finalidad de garantizar el acceso, uso y seguridad de los diferentes servicios informáticos institucionales.		
Proyecto	***Responsable***	***Tiempo Estimado***
Ampliación de la Cobertura inalámbrica a todos los edificios académicos de la Instituciones 410-14	Director DTIC	12 meses

5.3. AREA DE SOPORTE Y MANTENIMIENTO

Objetivo 1. Elaborar, aprobar y ejecutar el plan de mantenimiento de hardware y software institucional.		
Proyecto	***Responsable***	***Tiempo Estimado***
Mantenimiento Preventivo Equipos informáticos, electrónicos y de telecomunicaciones	Dr. Wilfrido Jarrín Tec. Lenin Merizalde	6 meses.
Mantenimiento Correctivo de Equipos informáticos, electrónicos y de telecomunicaciones	Ing. Marcelo Velasco Tec. Eugenio Meléndrez	6 meses.
Elaboración y ejecución de ser necesario del plan de contingencia informático	Ing. Marcelo Velasco	12 meses

1.1. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

De lo expuesto anteriormente se puede concluir que:

- La tecnología informática cambia permanentemente, lo que demanda de investigación científica con la finalidad de desarrollar los proyectos necesarios que vinculen el desarrollo institucional con el adecuado respaldo tecnológico.

- El sistema organizacional de las instituciones y de la nuestra en particular es dinámico, lo que demanda del continuo desarrollo de aplicaciones informáticas que automaticen los diferentes procesos con la finalidad de convertirnos en una institución más competitiva.

- En la era digital, basada en la gestión de la información y generación de conocimiento donde las redes de datos y el internet han creado nuevos paradigmas comunicacionales, de comportamiento, compartimiento y colaboración, se vuelve necesario administrar y alcanzar niveles de disponibilidad y accesibilidad deseados a los diferentes servicios ofertados a través de la intranet institucional.

- El adecuado manejo de las diferentes aplicaciones informáticas y acceso a los diferentes servicios disponibles a través de la intranet de la ESPOCH, será posible a través de los diferentes programas de capacitación y soporte a los usuarios.

- La prolongación del ciclo de vida de los diferentes equipos electrónicos será siempre posible con un adecuado mantenimiento preventivo y correctivo de ser el caso.

RECOMENDACIONES

- Se recomienda que las autoridades institucionales brinden todo el apoyo para que el desarrollo tecnológico de la ESPOCH, vaya de la mano con el crecimiento institucional.

ANEXO 1

PLAN DE ADMINISTRACION DE REDES, INTRANETS, INTERNET, EXTRANET. (ADMINISTRACION DE SITIOS WEB, CUENTAS DE INTERNET, PROVEEDORES DE SITIOS)

CONFIGURACIÓN E INSTALACIÓN DE EQUIPOS ACTIVOS DE RED

- Seleccionar equipo activo de red a ser adquirido, con base a las necesidades (cantidad de puertos, capacidad de memoria, sistema operativo).
- Enviar la solicitud a la unidad de Adquisiciones, para que gestionen la compra según el procedimiento de contratación pública.
- Una vez que llegue el equipo activo de red, definir y aplicar los parámetros básicos de configuración, asegurando que el acceso al equipo quede restringido al personal autorizado.
- Instalar físicamente el equipo activo de red.

ADICIÓN DE SUBREDES

- Definir la necesidad de creación de una subred, dependiendo de diferentes factores como construcción de un nuevo edificio, solución a conflictos de direcciones IP, separación de tráfico entre estudiantes y funcionarios, etc.

    - Definir el esquema de direccionamiento IP para la Subred.
    - Crear listas de acceso de los equipos que se van a activar en la Subred.
    - Habilitar los puertos que necesitan activarse en la Subred.

ELIMINACIÓN DE SUBREDES

- Definir la necesidad de eliminación de una subred, dependiendo de diferentes factores como traslados o cambios de usuarios y/o dependencias a otros edificios.
- Borrar las listas de acceso a la Subred.
- Deshabilitar puertos asociados a la Subred.

ADMINISTRACIÓN DEL ANCHO DE BANDA

Definición de reglas para manejo de ancho de banda

- Determinar las necesidades de ancho de banda de los diferentes servicios de la red (web, transferencia de archivos, correos electrónicos, videoconferencias, etc.), así como las garantías a ofrecer.
- Crear reglas en el manejador de ancho de banda (servidor especializado), para cumplir con las necesidades establecidas.
- Actualizar en el manejador de ancho de banda, las reglas creadas para que las active.
- Verificar que el servicio quede operando.

Monitoreo del ancho de banda

- Monitorear las herramientas gráficas del ancho de banda, tanto de entrada como de salida hacia Internet.
- Si se detecta degradación en la calidad del ancho de banda (no se puede entrar a todos los sitios web o se presentan largos tiempos de respuesta), acceder remotamente al manejador de ancho de banda y a los servidores básicos para Internet, revisar también el punto de conexión física con el proveedor.
- Si no se puede acceder remotamente al manejador de ancho de banda y/o a los servidores básicos, revisar físicamente la conexión, si se detectan problemas o si solo algunos servicios no están en funcionamiento, realizar diagnóstico y reparar; si no responden, reiniciar la máquina.
- Si el manejador de ancho de banda, los servidores básicos para Internet y los Switchs se encuentran operando normalmente, contactar al proveedor del servicio, informar la anomalía y solicitar tiempo de solución.

Definición de reglas de entrada y salida en Firewall

- Determinar las necesidades de seguridad de los diferentes servicios de la red (web, transferencia de archivos, correos electrónicos, videoconferencias, etc.), así como las garantías a ofrecer.
- Crear reglas en el Firewall, para cumplir con las necesidades establecidas.
- Actualizar en el Firewall, las reglas creadas para que las active.
- Verificar que el servicio quede operando.

Monitoreo de temperatura en el Centro de Datos de la ESPOCH

- Revisar los reportes gráficos de temperatura en el Centro de Datos de la ESPOCH.
- Si se detectan subidas de temperatura, identificar la falla y, si es posible corregirla inmediatamente.
- Si la solución toma mucho tiempo, desconectar todos los equipos.
- Contactar al contratista especializado para reparar la falla.
- Hacer seguimiento al proveedor hasta que solucione el problema.

PLAN DE ADMINISTRACIÓN DE SERVIDORES

INSTALACIÓN, CONFIGURACIÓN Y CONTROL DE ACCESO DE SERVIDORES

- Instalar físicamente el servidor, en el Datacenter (ubicarlo en el gabinete, instalar herrajes, conectarlo a la red, verificar alimentación regulada de energía).
- Instalar el Sistema Operativo, teniendo en cuenta la capacidad requerida.
- Determinar la posición del servidor dentro de la red, según su utilidad.

- Configurar la dirección IP del servidor, según la información suministrada por el Profesional del DTIC, encargado de administrar la Red.
- Configurar Firewalls para delimitar funciones y alcance del servidor en la red, así como los usuarios que pueden acceder a él.

MONITOREO DE SERVIDORES Y APLICACIONES, INCLUIDAS MOTORES DE BASES DE DATOS

- Verificar paneles de alarmas para detectar anomalías o fallas.
- Verificar la conectividad del servidor (que esté en red).
- Si no hay conectividad, revisar elementos de Hardware y reemplazar los que se encuentren dañados.
- Si hay daño en la aplicación, revisar los registros que arroja en el sistema y buscar la causa del daño; si es por agentes externos como falta de fluido eléctrico o refrigeración, esperar que vuelva a la normalidad y revisar si ocasionaron daños en Hardware o Software; si es de Hardware, reemplazar la parte; si es software, cambiar la configuración.

ACTUALIZACIÓN DE SERVIDORES

- Determinar las necesidades de actualización (capacidad, procesamiento, memoria o conectividad).
- Instalar componentes (disco duro, procesador, tarjeta de memoria o tarjeta de red).
- Instalar el controlador del nuevo Hardware.
- Iniciar el funcionamiento del servidor.

PLAN DE ADMINISTRACIÓN DE EQUIPOS (HARDWARE) DEL DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

- Controlar el inventario y manejo de compras menores.
- Instalar, configurar y brindar mantenimiento a los equipos del Departamento de Sistemas y Telemática (hardware y periféricos) si es necesario escalar, se coordina con el proveedor respectivo.
- Monitorear el correcto funcionamiento de dispositivos internos de los equipos (procesador, memorias, disco duro, tarjetas).

ANEXO 2

PLAN DE RIESGOS Y CONTINGENCIAS EN LA UTILIZACIÓN DEL SOFTWARE Y HARDWARE

ANÁLISIS DE RIESGO

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad que suceda cada uno de los problemas posibles, de esta forma se puede priorizar los problemas y coste potencial desarrollando un plan de acción adecuado.

El Análisis de riesgo supone responder preguntas del tipo:

¿Qué puede ir mal?
¿Con que frecuencia puede ocurrir?
¿Cuáles serían sus consecuencias?
¿Qué fiabilidad tendrá las respuestas a la tres primeras preguntas?

En la evaluación de riesgos que se ha de llevar a cabo hay que contestar con la mayor fiabilidad posible a las siguientes preguntas:

¿Qué se intenta proteger?
¿Cuál es su valor para uno o para la organización?
¿Frente a que se intenta proteger?
¿Cuál es la probabilidad de ataque?

IDENTIFICACIÓN DE RIESGOS

¿A qué riesgos en seguridad informática se enfrenta la institución?

- Al fuego que puede destruir los equipos y archivos
- Al robo común, llevándose los equipos y los archivos
- Al vandalismo, que dañen los equipos y archivos
- A fallas en los equipos, que dañen los archivos
- A equivocaciones, que dañen los archivos
- A la acción de virus, que dañen los equipos y archivos
- A terremotos que dañen los equipos y archivos
- A acceso no autorizados, filtrándose datos no autorizados
- Al robo de datos, difundiendo los datos sin autorización
- Al fraude, desviando fondos a merced de la computadora

Para cada riesgo se determinará la probabilidad del factor de riesgo, de la siguiente manera:

Tipos de riesgo	Factor de riesgo
Robo	Alto
Vandalismo	Medio
Fallas en los equipos	Bajo
Acciones de virus	Medio
Equivocaciones	Medio
Terremotos	Bajo
Accesos no autorizados	Medio
Robo de datos	bajo
Fuego	Medio
Fraude	Muy bajo
Fuga de agua	Alto

ANÁLISIS DE FALLAS DE SEGURIDAD

Será el de estudiar las computadoras, su software, localización y utilización con el objeto de identificar los requisitos que pudieran suponer un peligro.

PROTECCIONES ACTUALES

Generales.- Se hace una copia casi diaria de los archivos que son vitales para la institución.

Robo común.- Se cierran las puertas de entrada y ventanas, del Departamento de Sistemas y Telemática y en su conjunto el área de Administración es responsable de los activos de la institución.

Vandalismo.- Se cierra la puerta de entrada.

Falla de equipos.- Se tratan con cuidado y se realiza el mantenimiento en forma regular, no se permite fumar.

Daño por virus.- Todo el software que llega se analiza en el sistema utilizado el software de antivirus, los programas de dominio público y de uso compartido.

Equivocaciones.- Los empleados deben tener buena formación. Cuando son necesarios se intenta conseguir buenos trabajadores temporales.

Terremoto.- La empresa deberá contar con los stickers de ZONA SEGURA, los mismos que deben estar ubicados, en cada piso, EN CASOS DE SISMO en lugares estratégicos designados por Defensa Civil.

Acceso no autorizado.- Cada usuario tiene una clave de acceso única para el acceso al computador y a la red, así como un perfil personal por equipo asignado.

Robo de datos.- Se cuenta con claves de acceso personales.

Fuego.- En la actualidad se cuenta con extinguidores instalados en sitios estratégicos y se ha brindado entrenamiento al personal en forma periódica en el manejo de los mismos.

RECUPERACIÓN DE DESASTRES

Cuando ocurre una contingencia es esencial que se conozca al detalle el motivo que la origino y el daño producido lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia deben de ser planteados y probados fehacientemente, en estos procedimientos está involucrados todo el personal de la institución. Los procedimientos de planes de recuperación de desastres deben de emanar de la misma autoridad institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un plan de recuperación de desastres se pueden clasificar en tres etapas:

- Actividades previas al desastre
- Actividades durante el desastre
- Actividades después del desastre

ACTIVIDADES PREVIAS AL DESASTRE.-

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de recuperación con el menor costo posible para el DTIC.

Se puede detallar las siguientes actividades generales:

Establecimiento del Plan de Acción

En esta fase de planeamiento se debe establecer los procedimientos relativos a:

a) Sistemas de Información
b) Equipos de Cómputo
c) Obtención y almacenamiento de los respaldos de información (Backups)
d) Políticas (Norma y Políticas de Backups)

a) Sistema de Información.- La persona encargada debe dar a conocer a la persona cualquier tipo de actualización realizada a los sistemas.

Esta relación debe contar con los siguientes datos:

- Nombre del Sistema
- Lenguaje o paquete con el que fue creado el sistema, detallando los programas fuente, objetos, rutinas, macros, etc.
- El nombre de la persona que generó la actualización de la información base.
- Las unidades o departamentos (internos / externos) que usan la información del sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del sistema, las fechas en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este sistema, para la institución (medido en horas o días que la empresa puede funcionar adecuadamente sin disponer de la información del sistema). Equipamiento mínimo necesario para que el sistema siga funcionando.
- Actividades a realizar para volver a contar con el sistema de información (actividades de restauración).

Con toda esta información se deberá de realizar una lista de prioridad (ranking) de los sistemas de información necesarios para que la institución pueda recuperar su operatividad perdida en el desastre. (Contingencia).

b) Equipos de cómputo.- En este aspecto se tendrá en cuenta lo siguiente, inventario actualizado de los equipos de manejo de información (computadoras, lectoras, impresoras, etc.), especificando su contenido y condición, (software que usa, principales archivos que contiene), su ubicación y nivel de uso en la empresa.

Pólizas de seguros comerciales. Como parte de los activos institucionales, pero haciendo la salvedad en el contrato, que en caso de siniestros, la restitución del computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando este dentro de los montos asegurados.

Formación de equipos operativos

En cada unidad operativa del DTIC que almacena información y sirva para la operatividad de la institución, se deberá designar un responsable de la seguridad de la información de su unidad, pudiendo ser el jefe de dicha área operativa, sus labores serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos para los archivos, bibliotecas, utilitarios, etc.; para los principales sistemas o subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivo de datos de las aplicaciones y la creación de los respaldos adicionales.

Formación de equipos de evaluación (Auditoria de cumplimiento de seguridad).

Esta función debe ser realizada de preferencia por personal de inspectoría, de no ser posible la realizara el personal del área de informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar que las normas y procedimientos con respecto a BACKUPS, seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los BACKUPS por parte de los equipos operativos, comprobando físicamente su relación, adecuando registro y almacenamiento.
- Informar de los cumplimientos e incumplimientos de las normas para las acciones de corrección respectiva.

ACTIVIDADES DURANTE EL DESASTRE.-

Plan de emergencia

En este plan se establecen las acciones que deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del siniestro:

- Durante el día
- Durante la noche o madrugada

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presente en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida y de escape.
- Plan de evacuación del personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de información) de la empresa (si las circunstancias del siniestro lo posibilitan).
- Ubicación y señalización de los elementos contra el siniestro, (extinguidores, cobertores contra agua, etc.).

- Relación o lista de teléfonos de bomberos, ambulancia, jefatura de seguridad, y de nuestro personal nombrados para este caso.

Formación de equipos

Establecer claramente cada equipo (nombres, puertos, ubicación, etc), con funciones claramente definidas a ejecutar durante el siniestro.

Deberán existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos informáticos de acuerdo a los lineamentos para salvar los equipos señalados en establecimiento del plan de acción. (Equipos de cómputo).

Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros de acuerdo a los roles que se les haya asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Actividades después del siniestro

Después de ocurrido el siniestro es conveniente realizar lo siguiente:

Evaluación de los daños

Inmediatamente después que el siniestro ha ocurrido se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar y en cuanto tiempo, etc.

Terminada la evaluación de resultados se deberá de optimizar el plan de acción original mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente y evaluar el costo que habría causado la contingencia de no haber contado con el plan de contingencias y el entrenamiento adecuado.

Priorización de actividades del plan de acción

Toda vez que el plan de acción contempla una pérdida total, la evaluación de daños reales y su comparación contra un plan determinado nos dará la lista de las actividades que se deben realizar siempre priorizándola en vista a las actividades estratégicas y urgentes de la institución.

ANEXO 3

PLAN DE SEGURIDAD INFORMÁTICA

SEGURIDAD INTEGRAL DE LA INFORMACIÓN

La función de procesamiento de datos es un servicio de toda la institución, que apoya no solo a los sistemas de información administrativa sino también a las operaciones funcionales.

Las medidas de seguridad están basadas en definición de controles físicos, funciones, procedimientos y programas que conlleven no solo a la protección de la integridad de los datos sino también a la seguridad física de los equipos y de los ambientes en que estos se encuentran.

La seguridad de la información tiene dos aspectos: El primero consiste en negar el acceso a datos a aquellas personas que no tengan derechos a ellos, el cual también se le puede llamar protección de la privacidad si se trata de datos personales, mantenimiento de la seguridad en el caso de datos de la empresa.

Un segundo aspecto de la protección; es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.
En general la protección de datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, y el mantenimiento de la privacidad.

ACCESOS NO AUTORIZADOS

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- A los sistemas
- Computadoras personales y/o terminales de la red
- Información confidencial.

CONTROL DE ACCESO A LOS SISTEMAS

La libertad de acceso al área de sistemas crea un significativo problema de seguridad.

El acceso normal debe ser dado a la gente que regularmente trabaja en esta área. Cualquier otra persona de otro modo puede tener acceso únicamente bajo control.
Mantener la seguridad física de su área es una primera línea de defensa. Para ello deberá tomar en consideración el valor de los datos, el costo de protección, el impacto que su pérdida podría tener en la empresa y la motivación.

ACCESO LIMITADO A LOS TERMINALES

Cualquier terminal que puede ser utilizado como acceso a los datos de un sistema controlado, debe ser encerrado en un área segura o guardado de tal manera que no sean usados excepto por aquellos que tengan autorización para ello.

Igualmente se deberá considerar la mejor manera de identificar a los operadores de las terminales del sistema, y el uso de contraseñas cuando un terminal no sea usado pasado un tiempo predeterminado (5 a 10 minutos).

- Restricciones que pueden ser aplicadas.
- Determinación de los periodos de tiempo para los usuarios o las terminales
- Designación del usuario por el terminal o del terminal por usuario
- Limitación del uso de programas para usuario o terminales
- Tiempo de validez de las señas o contraseñas.

CONTROL DE ACCESO A LA INFORMACIÓN

Se deberá considerar la existencia de:

- **Programa de Control:** Deben de existir programas protegidos que mantengan y controlen a los usuarios y derechos de acceso ya sea por grupos o individualmente.

- **Palabra de Acceso (password):** Es una palabra especial o código que debe digitarse cuando el sistema lo solicite. El password constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados.

A fin de proteger el proceso de obtención de una llave de sistema cuando el usuario realiza la entrada, solicita una clave de acceso con el nombre del usuario, la cual consiste de unas cuantas letras elegidas por el usuario.

El sistema de computación debe cerrase. Después que el individuo no autorizado falle dos veces al intentar reingresar una clave de acceso. Las claves de acceso no deben ser largas puesto que son más difíciles de recordar.

- **Niveles de Acceso:** Los programas de control de acceso deberán identificar a los usuarios autorizados a usar los sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso esta referidos a la lectura modificación de las diferentes formas.

De acuerdo a ello se consideran los siguientes niveles de acceso a la información:

- Nivel de consultas de información no restringida o reservada. (Se le permite leer mas no modificar datos).

- Nivel de mantenimiento de la información no restringida o reservada (permite el ingreso de nuevos datos, la modificación o borrado de los ya existentes o una combinación de ellos).
- Nivel de consulta de información incluyendo la restringida o la reservada.
- Nivel de mantenimiento de la información incluyendo la restringida.

DESTRUCCIÓN

Sin adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de su equipo informático.

La destrucción del equipo puede darse por una serie de desastres como incendios, inundaciones, sismos o posibles fallas eléctricas, etc.

Cuando se pierden datos y no hay disponibles copias de seguridad se ha de volver a crear los datos o trabajar sin ellos. Los archivos de contabilidad suponen una situación diferente, ya que volver a crear puede necesitar de mucho tiempo y costo.
Para evitar la destrucción de información debe realizarse BACKUPS de la información vital de la empresa y almacenarse en lugares adecuados y de preferencia aparte de los equipos que se encuentran en el uso de este tipo de información.

REVELACIÓN O INFIDENCIA

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio. La información que es de carácter confidencial es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

- Control del uso de información en paquetes abiertos o cintas con otros datos residuales.
- La información puede ser conocida por personas no autorizadas, cuando se deja en paquetes abiertos o cintas que otras personas pueden usar.
- Mantener datos sensitivos fuera del trayecto de la basura.
- El material de papel en la plataforma de la descarga de la basura puede ser una fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Esta información sensitiva debe ser separada para la mejor seguridad de protección de la información. Estos deben ser separados y destruidos debiendo recurrirse a las destructoras o picadores de papel.
- Preparar procedimientos de control para la distribución de información.
- Una manera de controlar la distribución y posible diversificación de información es mantener un rastro de copias múltiples indicarlos confidencialmente o usando numeración como Pág. 1 de 9. Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de las oficinas y relativamente disponibles a gran número de personas.

MODIFICACIONES

El personal estará entrenado y concientizado de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados, profundizarse con una serie de seminarios y reforzarse con una serie de carteles y circulares relacionados al tema.

Nuestra mejor protección contra las pérdidas de datos consiste en realizar copias de seguridad almacenando copias actualizadas de todos los archivos valiosos en un lugar seguro.

La empresa debe tener muy en cuenta los siguientes puntos para la protección de los datos de una posible contingencia.

- Hacer de la copia de seguridad una política, no una opción.
- Hacer que la copia de seguridad resulte deseable.

ANEXO 4

PLAN DE PROCEDIMIENTOS DE ADMINISTRACIÓN

DESARROLLO DE POLÍTICAS Y PROCEDIMIENTOS

La cultura de institucional debe centrarse en que todos sus empleados entiendan el valor del software comercial, conozcan la diferencia entre el uso legal e ilegal, y se comprometan a utilizar adecuadamente el software.

Para lograrlo, la ESPOCH debe tener una declaración de política clara que exprese los objetivos de la institución en cuanto al uso de los programas de software, la utilización exclusiva de software legal y el detalle del procedimiento para adquirir software legal. Un proceso eficaz de adquisición de programas de software debe incluir los siguientes lineamientos:

- Centralizar todas las compras a través del departamento de adquisiciones de la ESPOCH.
- Exigir que todas las solicitudes de compra de software se efectúen por escrito y cuenten con la aprobación del director de departamento;
- Verificar que los programas solicitados integren la lista de software utilizado en la empresa;
- Comprar programas únicamente a vendedores autorizados, de buena reputación;
- Trabajar solamente con Proveedores de Servicios de Aplicación (ASP)
- de buena reputación y garantizar el mantenimiento de toda la documentación y licencias importantes con dicho ASP;

- Obtener materiales de usuario (por ejemplo: manuales, tarjetas de registro, etc.), licencias y recibos originales por cada compra de software;
- No permitir que los empleados compren programas de software en forma directa ni los carguen a sus cuentas de gastos;
- Garantizar que los empleados no puedan bajar los programas de software legales de Internet sin una aprobación especial; y
- No permitir que los empleados descarguen aplicaciones de software para operar sistemas de peer-to-peer (P2P) que puedan utilizarse para comercializar trabajos protegidos por el derecho de autor.

Es necesario además contar con una declaración de política institucional, para que la ESPOCH, considere su adopción. Cualquiera sea la política, debe asegúrese de que esté incluida en el paquete de información que reciben los nuevos empleados, y además de ser distribuida a todos los empleados, la misma se encuentre disponible en las carteleras de anuncios y las redes informáticas de la institución. Es necesario que todos los empleados conozcan la declaración de política y las consecuencias de infringir sus normas.

A la hora de desarrollar procedimientos internos para la administración de los programas de software, la institución debe hacerse la siguiente pregunta: "¿Qué software se necesita?" La respuesta siempre será valiosa para garantizar que tanto los procesos de compra como de utilización de software sean efectivos y eficientes, y para guiar sus esfuerzos en relación al establecimiento y mantenimiento de las políticas de administración de software.

Como regla general, su análisis debe responder a las siguientes preguntas:

- ¿Se está utilizando los programas de software adecuados en términos de eficacia y efectividad?
- ¿El personal está satisfecho con las actuales aplicaciones de software?
- ¿Existen otros programas de software que permitirían al personal operar de forma más eficiente y eficaz?
- ¿Tiene la institución algún software en su poder que ya no necesita?

Los procedimientos institucionales deberían incluir la identificación del perfil de programa informático adecuado para cada computadora, evaluando si los miembros del departamento/personal necesitan aplicaciones de software alternativas o adicionales. Además, los programas de software que no se estén utilizando deberían identificarse para determinar si se conservan o no.

AUDITORÍA DE SOFTWARE

Una vez que se cuenta con una política y un conjunto de procedimientos, el próximo paso consiste en realizar un inventario del activo en software. Sólo sabiendo cuáles son los programas que se encuentran instalados en todas las computadoras de la ESPOCH, se puede determinar cómo proceder.

Un inventario preciso puede responder a las siguientes preguntas:

- ¿Se está utilizando las versiones más recientes o convenientes de los programas que se necesitan?
- ¿Se está utilizando programas desactualizados o innecesarios que puedan eliminarse?
- ¿Existen otros programas que se debería obtener para ser más productivos o eficientes?
- ¿Tiene cada miembro institucional el conjunto adecuado de programas disponibles?
- Están los miembros institucionales adecuadamente capacitados para utilizar los programas de software?
- ¿Se tiene programas o copias ilegales, no autorizadas o sin licencia en la institución?

Para completar el inventario puede utilizar alguna de las diversas herramientas disponibles o hacerlo en forma manual. Independientemente de las herramientas que utilice, asegúrese de obtener la siguiente información para cada copia de programa informático instalada en cada computadora:

- Nombre del producto
- Número de la versión
- Número de serie

Además, se debería realizar un inventario de los materiales vinculados a los programas de software en las computadoras, incluidos:

- Todos los disquetes, CD, u otros medios de almacenamiento de información, utilizados para instalar los programas en las computadoras;
- Todos los manuales originales y la documentación de referencia;
- Toda la documentación vinculada a la licencia; y
- Todas las facturas, pruebas de compra y otros documentos que prueben la legitimidad de sus programas de software. Esto incluye las facturas por la compra de computadoras que se adquirieron con los programas ya instalados.
- Una vez finalizado el inventario, se deberá guardar cuidadosamente la documentación, las copias originales del software y otros materiales, en un lugar seguro. De esta forma, se pueden aprovechar los servicios, las ofertas de actualización y otros beneficios que ofrecen los editores de programas, y reinstalar los programas de software de forma más sencilla.

DETERMINACIÓN DE QUÉ ES LEGAL Y QUÉ NO LO ES

Al identificar copias ilegales de software en la institución, estas deberían ser eliminadas de las computadoras. Este es también el momento ideal para recordar a los miembros institucionales la política de software de la empresa y los peligros vinculados al uso de programas de software no autorizados.

En este momento puede comparar las copias legítimas de software que permanecen en las computadoras con las necesidades institucionales identificadas al realizar el inventario. Se puede con esto tomar decisiones informadas sobre qué software legal se tiene y cuál se quiere mantener, actualizar o eliminar. Los programas se pueden mover, no copiarse, de una computadora en la que ya no son necesarios a otra que sí los necesita. De ser necesario, los programas se pueden actualizar de forma que todos utilicen la versión del programa más adecuada para la ESPOCH.

Sobre la base del inventario, las actualizaciones, y las nuevas adquisiciones, se puede realizar una lista formal de los programas de software que la institución autorizará a utilizar. La lista debería incluir:

- Los nombres de los programas,
- Los números de serie,
- Los números de versión,
- La cantidad de copias o usuarios permitidos por la licencia,
- Las computadoras en las que se encuentran instaladas las copias y;
- Los planes para agregar, actualizar o eliminar software en el futuro.

ELABORACIÓN DE PROCEDIMIENTOS DE CALIDAD

Plan de aseguramiento de la calidad de un proyecto

Los planes de este nivel son los más detallados y se incorporan a los planes de trabajo y descripciones de proyecto. Para cada uno de los productos informativos planeados se deberá completar un informe con detalles de:

- Procedimientos de supervisión y evaluación, incluidas revisiones internas y externas;
- Procedimientos de participación temprana de grupos de interés;
- Resultados esperados de los procesos de revisión.

Corresponde al personal investigador del DTIC, elaborar un informe en coincidencia con la planeación de trabajo anual del proyecto, y se deberá incorporan a un sistema de rastreo automatizado (dotproject).

- Políticas y procedimientos de mantenimiento y archivo.

Se elaborará un informe para todos los casos en los que se planee:

- Integrar o crear una base de datos que se empleará para apoyar resultados de programas;
- Proporcionar un servicio en línea, tal como una base de datos o un recurso informativo para consulta, o bien

.

ANEXO 5
FICHAS DE PROGRAMACION DE PROYECTOS DEL AREA DE INVESTIGACION Y DESARROLLO DE LA DTIC

FICHA 1. IMPLEMENTACION DE LA NUEVA PLATAFORMA VIRTUAL MOODLE V.2.6 INSTITUCIONAL

I. Denominación de la actividad/proyecto:
Implementación de la Nueva Plataforma de Aulas Virtuales "Moodle" para las actividades académicas de la institución.

II. Datos Generales:

Unidad Ejecutora	**:**	Área de Investigación y Desarrollo DTIC
Duración	**:**	Abril 2012 – Octubre 2012
Costo Total	**:**	No definido

III. Del Proyecto:

a. Descripción

Debido a los problemas presentados en las aulas virtuales para docentes y estudiantes de la ESPOCH, el área de Investigación y Desarrollo de la DTIC ha planificado la implementación de la Nueva Plataforma Moodle para Aulas Virtuales, para lo cual se configurará un servidor con la última versión Moodle 2.6.

b. Objetivos

Brindar al personal académico y estudiantes de la institución una nueva plataforma de aulas virtuales con nuevas actividades y recursos, que contribuyan a mejorar el proceso de enseñanza – aprendizaje.

IV. Meta Anual:

- Nuevas Actividades y Recursos virtuales utilizados por la comunidad académica politécnica.

V. Cobertura de Acción:

- Campus Principal y Extensiones

VI. Instituciones / Área Involucrada:

- Dirección de Tecnologías de la Información y Comunicación.
- Facultades y Unidades Académicas
- Unidad de Nivelación y Admisión.

VII. Productos Finales:

- Plataforma Virtual con nuevos recursos y actividades para la creación de Aulas Virtuales.

VIII. Usuarios de Productos Finales:

- Estudiantes y Docentes Politécnicos.

FICHA 2. DESARROLLO DEL SISTEMA DE SEGUIMIENTO A GRADUADOS

FASE I

I. Denominación de la actividad/proyecto:

Desarrollo e Implementación del Sistema de Seguimiento a Graduados en su primera Fase (Fichas de Graduados, Encuestas y Certificaciones).

II. Datos Generales:

Unidad Ejecutora	**:**	Área de Investigación y Desarrollo DTIC
Duración	**:**	Abril 2012 – Agosto 2012
Costo Total	**:**	No definido

III. Del Proyecto:

a. Descripción

Atendiendo la solicitud de la Comisión de Vinculación Institucional de acuerdo al Plan de Mejoras Institucional 2012-2014 se hace imprescindible el desarrollo de un Sistema de Seguimiento a los Graduados de la Institución: en el cual se pueda tener la ficha de los profesionales, bolsa de empleos, manejo de estadísticas y reportes.

b. Objetivos

Obtener información válida, confiable y oportuna sobre el proceso de inserción laboral, tanto de su desempeño en el empleo como de su trayectoria profesional, con la finalidad de valorar el grado de impacto de la Institución en el sector productivo y social.

IV. Meta Anual:

- Contar con información sobre áreas de oportunidad e implementar estrategias de mejora durante la permanencia de los estudiantes y en su egreso.

V. Cobertura de Acción:

- Campus Principal y Extensiones

VI. Instituciones / Área Involucrada:

- Dirección de Tecnologías de la Información y Comunicación.
- Comisión de Vinculación con la Colectividad
- Graduados de la ESPOCH

VII. Productos Finales:

El seguimiento de egresados nos permite tener un mayor acercamiento y comunicación con nuestros egresados para conocer su situación laboral y desempeño profesional, fortaleciendo el modelo de acuerdo a las necesidades del mercado laboral mediante una base de datos actualizada y confidencial.

VIII. Usuarios de Productos Finales:

- Miembros de la Comisión de Vinculación con la Colectividad y graduados de la ESPOCH.

ANEXO 6

FICHAS DE PROGRAMACION DE PROYECTOS DEL AREA DE INFRAESTRUCTURA DE REDES Y TELECOMUNICACIONES DE LA DTIC

FICHA 4. ACTUALIZACIÓN DEL EQUIPO ACTIVO DE RED DEL DATA CENTER

I. Denominación de la actividad/proyecto:

Actualización del equipo activo de red del Data Center Institucional.

II. Datos Generales:

Unidad Ejecutora	**:**	Área de Infraestructura de Redes y Telecomunicaciones
Duración	**:**	Abril 2012 – Octubre 2012
Costo Total	**:**	$ 472.477,25

III. Del Proyecto:

a. Descripción

Dentro del análisis de la situación actual del área de Redes e Infraestructura se debe mencionar que en el DataCenter Institucional se encuentra el equipo activo de red principal, sin el cual no se podría brindar los servicios que proporciona el BackBone Institucional entre los que cuentan los servicios de: Red Interna, Internet, Telefonía, Sistema Académico, Virtualización de Servidores (alojados en la Infraestructura EVA HP y 4 servidores KVM Linux) entre otros, que permiten el desarrollo normal de las actividades tanto académicas como administrativas que dependen de las Tecnologías de la Información y Comunicación.

En la actualidad los equipos principales como: Switch de Core, Infraestructura HP EVA, FortiGate, entre otros; ya han sobrepasado el tiempo de vida útil considerado para los equipos informáticos/electrónicos. El Switch de Core, equipo medular de la infraestructura de red, está ya presentando problemas, lo que causa que en ocasiones los servicios del BackBone Institucional no estén funcionando de forma adecuada. Cabe mencionar que en el momento que este equipo sufra daños graves, todos los servicios institucionales dejaran de funcionar.

Por lo expuesto se hace imperativa la actualización del equipo activo del DataCenter Institucional con la finalidad de brindar servicios adecuados a todos los usuarios de la

ESPOCH, poder atender la demanda de nuevos servicios, adaptarse a los avances tecnológicos en el corto plazo y evitar que el BackBone de la institución quede in-operativo y obsoleto .

b. Objetivos

Tener una infraestructura de red sólida que soporte y permita la implementación de nuevos servicios que estén acorde con los avances tecnológicos y a la demanda de los usuarios internos (estudiante, docentes empleados y trabajadores) como externos.

IV. Meta Anual:

- Brindar la infraestructura necesaria para los actuales y nuevos servicios que brinda la Institución a estudiantes, docentes, empleados y trabajadores.
- Mejorar los servicios de Internet tanto cableada como inalámbrica.
- Evitar que el DataCenter quede inutilizable por el daño del equipo activo, y esto cause que los servicios institucionales no se puedan utilizar.

V. Cobertura de Acción:

- Campus Principal y Extensiones

VI. Instituciones / Área Involucrada:

- Dirección de Tecnologías de la Información y Comunicación.
- Unidad de Adquisiciones

VII. Productos Finales:

- Actualización del equipo activo de red del DataCenter.

VIII. Usuarios de Productos Finales:

- Estudiantes, docentes, empleados, trabajadores Politécnicos y usuarios externos.

FICHA 5. AUMENTO DE COBERTURA DE RED INALAMBRICA INTERIOR EN EDIFICIOS ACADEMICOS DEL CAMPUS PRINCIPAL DE LA ESPOCH

I. Denominación de la actividad/proyecto:

AUMENTO DE COBERTURA DE RED INALAMBRICA INTERIOR EN EDIFICIOS DEL CAMPUS PRINCIPAL DE LA ESPOCH

II. Datos Generales:

Unidad Ejecutora: DTIC	Área de Infraestructura de Redes y Telecomunicaciones
Duración:	Abril 2012 – Octubre 2012
Costo Total:	2000 USD

III. Del Proyecto:

a. Descripción

Acorde al siempre creciente número de usuarios de la infraestructura de red y ante la no existencia de suficientes puntos de acceso a red inalámbrica en los interiores de edificios administrativos y académicos en el campus se ha planificado la adquisición de Access points para aumentar la cobertura.

b. Objetivos

Aumentar la cobertura de red inalámbrica en los interiores de edificios del campus principal de la ESPOCH.

IV. Meta Anual:

- Aumentar la cobertura de red inalámbrica en los interiores de edificios del campus principal de la ESPOCH.

V. Cobertura de Acción:

- Campus Principal Riobamba

VI. Instituciones / Área Involucrada:

- Dirección de Tecnologías de la Información y Comunicación.
- Área de Infraestructura de Redes y Telecomunicaciones
- Unidad de Adquisiciones

- Dependencias Académicas y Administrativas del Campus

VII. Productos Finales:

- Puntos de acceso a red inalámbrica instalados y operativos.

VIII. Usuarios de Productos Finales:

- Comunidad Politécnica.

ANEXO 7

FICHAS DE PROGRAMACION DE PROYECTOS DEL AREA SOPORTE Y MANTENIMIENTO DE LA DTIC

FICHA 6. MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS ELECTRONICOS Y DE TELECOMUNICACIONES

I. Denominación de la actividad/proyecto:

Ejecutar un Plan de Mantenimiento Preventivo y Correctivo de los Equipos Electrónicos y de Telecomunicaciones de la ESPOCH en el año 2012

II. Datos Generales:

Unidad Ejecutora	**:**	Área de Soporte y Mantenimiento DTIC
Duración	**:**	Mayo 2012 – Enero 2013
Costo Total	**:**	No definido

III. Del Proyecto:

a. Descripción

Las operaciones de mantenimiento preventivo y correctivo son destinadas a la conservación de equipos o instalaciones de todos los equipos eléctricos, electrónicos y de telecomunicaciones de la ESPOCH, mediante realización de revisión y reparación que garanticen su buen funcionamiento y fiabilidad, así como reparar o poner en condiciones de funcionamiento aquellos que dejaron de funcionar o están dañados.

b. Objetivos

Evitar o mitigar las consecuencias de los fallos del equipo, logrando prevenir las incidencias antes de que estas ocurran, o corregirlas cuando estas ya han sucedido.

IV. Meta Anual:

Mantener en perfectas condiciones de operatividad y ampliar la vida útil de los equipos eléctricos, electrónicos y de telecomunicaciones de nuestra Institución.

V. Cobertura de Acción:

- Campus Principal.

VI. Instituciones / Área Involucrada:

- Dirección de Tecnologías de la Información y Comunicación.
- Administración Central
- Facultades y Unidades Académicas y Producción.

VII. Productos Finales:

Disminuir costos de operación, aumento de eficiencia en el soporte tecnológico de los equipos.