UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

SEMINARIO DE GRADUACIÓN "SEGURIDAD INFORMATICA"

TEMA:

"AUDITORIA INFORMÁTICA PARA OPTIMIZAR EL MANEJO DE LA INFORMACIÓN Y EQUIPAMIENTO INFORMÁTICO EN EL MIES INFA TUNGURAHUA"

Trabajo de Graduación Modalidad: SEMINARIO, Presentado previo la obtención del título de Ingeniera en Sistemas Computacionales e Informáticos

AUTOR: Castro Núñez Diana Margoth

PROFESOR REVISOR: Ing. Jaime Bolívar Ruiz Banda

Ambato – Ecuador
Noviembre - 2012

APROBACION DEL TUTOR

En mi calidad de tutor del trabajo de graduación sobre el tema: **"AUDITORIA INFORMÁTICA PARA OPTIMIZAR EL MANEJO DE LA INFORMACIÓN Y EQUIPAMIENTO INFORMÁTICO EN EL MIES INFA TUNGURAHUA",** de la señorita Diana Margoth Castro Núñez, estudiante de la carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que le informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato Septiembre 14, 2012.

TUTOR

_____

Ing. Jaime B. Ruiz B

AUTORIA

El presente trabajo de graduación titulado**: "AUDITORIA INFORMÁTICA PARA LOS DEPARTAMENTOS DE INFORMÁTICA, COMUNICACIÓN SOCIAL, PLANIFICACIÓN, SECRETARIA, TALENTO HUMANO, TÉCNICOS TERRITORIALES Y UNIDAD ADMINISTRATIVA DEL MIES INFA TUNGURAHUA".** Es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Septiembre 14, 2012

Diana Margoth Castro Núñez
C.I. 180415530-5

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La comisión calificadora del presente trabajo conformada por los señores docentes Ing. David Omar Guevara Aulestia e Ing. Francisco Xavier López Andrade, revisó y aprobó el informe final del trabajo de graduación titulado **"AUDITORIA INFORMÁTICA PARA LOS DEPARTAMENTOS DE INFORMÁTICA, COMUNICACIÓN SOCIAL, PLANIFICACIÓN, SECRETARIA, TALENTO HUMANO, TÉCNICOS TERRITORIALES Y UNIDAD ADMINISTRATIVA DEL MIES INFA TUNGURAHUA",** presentado por la señorita Diana Margoth Castro Núñez de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Oswaldo Eduardo Paredes Ochoa
PRESIDENTE DEL TRIBUNAL

Ing. David Omar Guevara Aulestia
DOCENTE CALIFICADOR

Ing. Francisco Xavier López Andrade
DOCENTE CALIFICADOR

DEDICATORIA:

Dedico la presente tesis a los seres que Más amo en este mundo: mi esposo Fernando Mayorga y mis hijos Josué y David Mayorga Por ser la fuente de mi inspiración y motivación para superarme cada día y así luchar para que la vida nos depare un futuro mejor

Diana Margoth Castro Núñez

AGRADECIMIENTO:

En primer lugar a Dios por ser la piedra angular de mi hogar y por haberme guiado hasta el camino final de mi carrera

Un Profundo agradecimiento a mis padres Ángel y Fabiola, mis hermanos que me brindaron el apoyo necesario para continuar.

A mi esposo Fernando y mis hijos Josué y David que son mi fuerza y mi aliento incondicional en mi vida y carrera.

A la Universidad Técnica de Ambato, de manera especial a la Facultad de ingeniería en Sistemas, Electrónica e Industrial por ser el organismo que ha permitido mi formación profesional, a todos y cada uno de los docentes que la conforman, que impartieron sus conocimientos y sobre todo su calidad humana.

A MIES INFA por darme la apertura y colaboración necesaria para la realización de la presente investigación.

A mi tutor Ing. Jaime Ruiz por el tiempo dedicado a la asesoría de este proyecto y sus conocimientos impartidos.

A todos y cada uno de ellos que aportaron con su granito de arena para el logro de este Trabajo de Grado.

Diana Margoth Castro Núñez

INDICE GENERAL DE CONTENIDOS

CAPITULO II

MARCO TEORICO

CAPITULO III

MARCO METODOLOGICO

CAPITULO IV

ANÁLISIS E INTERPRETACION DE RESULTADOS

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO VI

PROPUESTA

INDICE DE GRAFICOS

INDICE DE TABLAS

RESUMEN EJECUTIVO

Presente trabajo denominado **"AUDITORIA INFORMÁTICA PARA OPTIMIZAR EL MANEJO DE LA INFORMACIÓN Y EQUIPAMIENTO INFORMÁTICO EN EL MIES INFA TUNGURAHUA",** se realizara una Auditoria Informática para ayudar a la Institución en la búsqueda de fallas con el fin de mejorar la calidad de servicio de la misma.

La investigación realizada surge de las diferentes falencias que posee la institución a nivel informático donde hoy en día se maneja la información ya que en cada momento los avances del desarrollo de nuevas ideas especializadas en el área de informática van en un constante aumento en el mundo.

La lentitud en sus ordenadores, la proliferación de virus, el innecesario software instalado y no utilizados por parte de los funcionarios ha sido un detonante para tomar una medida a través de la aplicación de una auditoria Informática de esta manera conocer que es lo que está sucediendo en la institución como evitar y qué medidas tomar.

La auditoria Informática tiene como fin recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo de una entidad, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recurso en pos de la seguridad Informática.

INTRODUCCION

Capítulo I: El Problema de Investigación

En el Capítulo I se detalla el tema del proyecto investigativo, planteamiento del Problema, Contextualización, Análisis Crítico, Prognosis, Fundamentación del Problema, delimitación, Justificación, Objetivo General y Específicos.

Capítulo II: Marco Teórico

Contiene Antecedentes Investigativos, Fundamentación Legal, Fundamentación Teórica, Categorías Fundamentales, Hipótesis, Señalamiento de Variables.

Capítulo III: Metodología

Contiene Enfoque, Modalidades Básicas de la Investigación, Tipos de Investigación, Población y Muestra, Operalizacion De La Variables, Recolección y Análisis de la Información, Procesamiento y Análisis.

Capítulo IV: Análisis E Interpretación De Resultados

Análisis De Los Resultados, Análisis de los resultados de las encuestas.

Capitulo V: Conclusiones Y Recomendaciones

Conclusiones, Recomendaciones.

Capítulo VI: Propuesta

Datos Informativos, Antecedentes De La Propuesta, Justificación, Objetivos, Análisis De Factibilidad, Informe Técnico, Fase I, Fase II, Fase III, Fase IV, Fase V, Documentación Final ,Carta a la Gerencia, Informe Final, Bibliografía, Anexos.

CAPÍTULO I

EL PROBLEMA

1.1. TEMA

Auditoria Informática para Optimizar el Manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua.

1.2. Planteamiento del Problema

1.2.1. Contextualización

A nivel mundial la auditoria informática ha constituido un pilar fundamental en las organizaciones, tanto los sistemas como la estructura física deben estar sometidos a controles de calidad ya que los ordenadores como procesamiento de datos son blanco fácil para la delincuencia, terrorismo o espionaje.

La Auditoria informática permite la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad de la organización que está inmersa en el procesamiento de la información con el fin de lograr una utilización más eficiente y segura de la misma que servirá para una adecuada toma de decisiones.

En el país, en pos de salvaguardar la información, eficacia de las auditorias informáticas para el buen desempeño de los sistemas de información en las organizaciones públicas o privadas en su gran mayoría no se realizan por dos factores; el primero el alto costo resultante de este proceso y el segundo y de mayor peso es el desconocimiento ya que se piensa "*es el método para evaluar al personal y por ende el removimiento del cargo"* lo cual no es de agrado para los empleados de cualquier organización.

Considerando que la ciudad de Ambato es una zona de crecimiento empresarial, razón por la cual sería recomendable realizar Auditorías informáticas tanto a organizaciones públicas y privadas con el fin de mejorar el desenvolvimiento de las mismas, lamentablemente en la práctica no se aplican pues no es un ámbito muy conocido.

En el MIES – INFA como institución pública busca conseguir logros de servicio en todos los aspectos: social, cultural, y otros, buscando siempre el propósito de servir a la sociedad en las diferentes situaciones de riesgo y sobre todo ofreciendo por parte del servidor público, la calidad, compromiso, eficiencia, eficacia y efectividad en los procesos que realiza.

MIES INFA es consciente que los procesos que se llevan a cabo son de vital importancia para la institución, por ende el realizar un examen crítico y detección de errores con el objetivo de evaluar la eficiencia y eficacia tanto del manejo de la

información como también del equipo informático es esencial, por medio de la información brindada por los funcionarios y la observación del auditor.

ÁRBOL DE PROBLEMAS

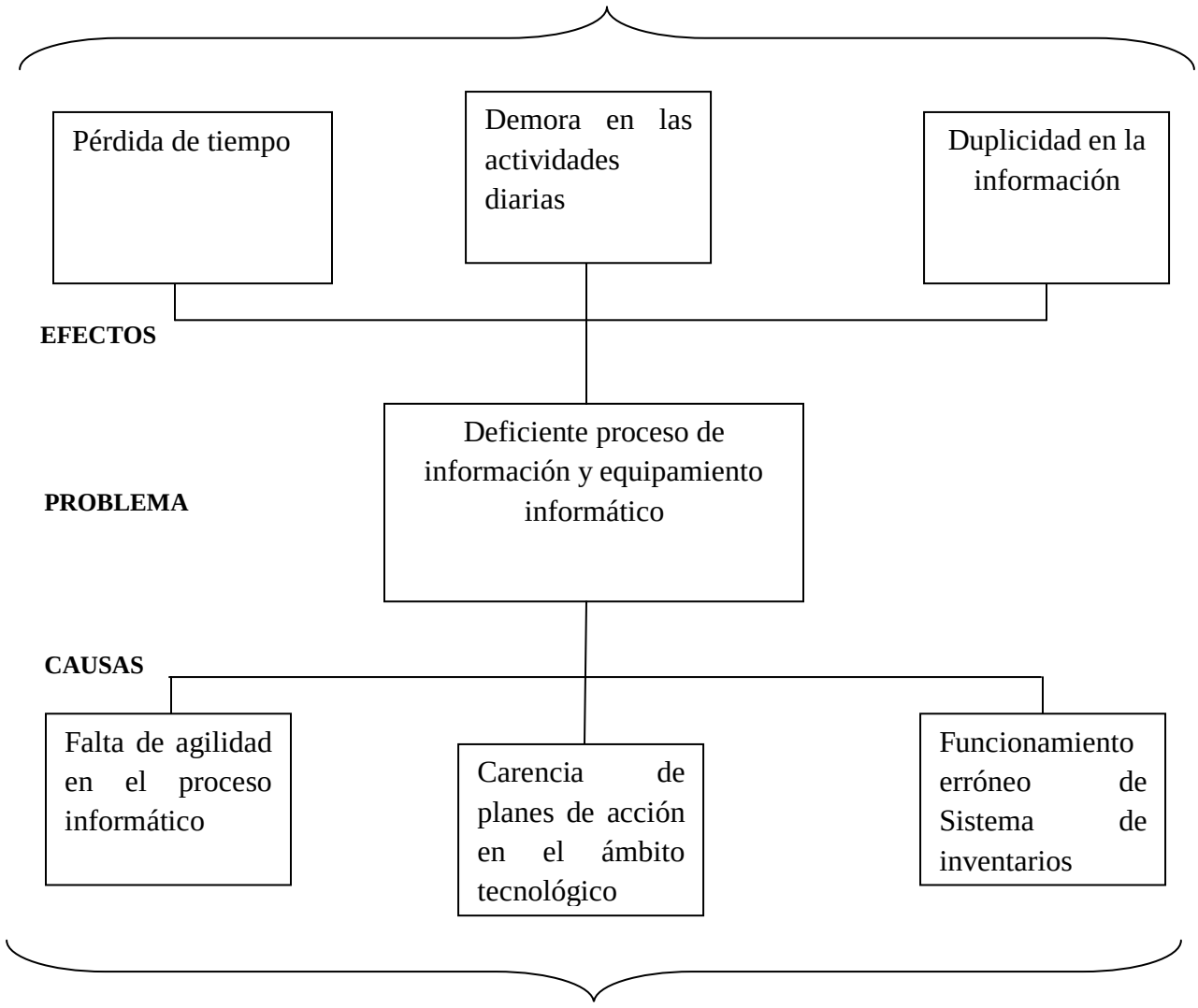


Grafico #1 Árbol de Problemas

1.2.2. Análisis Crítico

Los cambios trascendentales que vive el mundo moderno, caracterizados por su incesante desarrollo, el aumento de la información, los sistemas que la proveen, las amenazas cibernéticas, la seguridad de la información y los futuras transformaciones tecnológicas permite cambios en las organizaciones para su mejor desenvolvimiento tanto en prácticas de negocio como en la prestación de servicios, creando oportunidades en el ejercicio de la Auditoria Informática.

La labor desempeñada por el MIES INFA tiene como fin ayudar proteger y garantizar los derechos de niños/as y adolescentes víctimas de violencia, permitir la participación de los mismo en un espacio donde se brinde la atención necesaria, trabajo que realizan los técnicos de campo que se trasladan a los distintos Centros de Desarrollo Infantil de la provincia de Tungurahua para supervisar a cada establecimiento posteriormente se realiza un informe de actividades realizadas por el funcionario, cabe mencionar que los equipos informáticos que están en custodia de los mismos son demasiado lentos y no procesan con agilidad la información ocasionando pérdida de tiempo a los funcionarios.

Es importante en toda institución sea pública o privada el de poseer planes de acción tanto preventivos como de contingencias ante cualquier eventualidad, cabe destacar que no existe ningún plan que permita solucionar problemas esporádicos que pueden surgir en el ámbito tecnológico lo que origina demora en las actividades diarias que realizan los funcionarios.

Llevar un control de activos fijos en cualquier institución es primordial ya de esa manera se puede tener un registro de los bienes que se los realiza mediante una codificación de cada elemento físico existente, el inconveniente se origina cuando se desea realizar una modificación de custodio en el sistema Olympo (Sistema de inventarios utilizado por la institución) por parte de la persona encargada se produce

duplicidad en la información ya que el sistema no hace una actualización de los datos, almacenando en la base de datos el mismo activo fijo a dos personas diferentes.

Del análisis Crítico realizado en el MIES-INFA Tungurahua, es necesario que se realice una auditoría informática para los departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y Unidad Administrativa para permitir una solución viable con miras a mejor el funcionamiento y servicio de la institución.

1.2.3. Prognosis

De no dar solución al problema, corre el riesgo de que los procesos tengan demora en el tratamiento de la información ocasionando molestias tanto a los funcionarios como beneficiarios del servicio social que presta el MIES INFA TUNGURAHUA.

1.2.4. Formulación del Problema

¿Cómo la Auditoria Informática optimiza el manejo de la información y equipamiento Informático en el MIES INFA Tungurahua?

1.2.5. Preguntas Directrices

- ¿Mediante que técnicas se obtendrá información necesaria de cada área en el ámbito Informático?
- ¿De qué manera se detectará errores y deficiencias en los procesos manejados por los sistemas informáticos?

- ¿Cómo Controlar la fiabilidad del software que maneja la institución y el uso que se le da al mismo?
- ¿Cómo Verificar la seguridad Física de los diversos ambientes de procesamiento de información?
- ¿De qué manera se Establecerá el grado de satisfacción de las necesidades y requerimientos en relación a la calidad, oportunidad, integridad, confidencialidad de la información?

1.2.6. Delimitación

Campo: Seguridad Informática

Área: Departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y Unidad Administrativa

Aspecto: Auditoria Informática

Tiempo: Información será tomada desde el año 2011

Lugar: La presente investigación se realizara en el MIES – INFA Tungurahua, ubicado en la calle Av. José Peralta y Pareja Diez Canseco, Teléfono: 032587680

1.3. Justificación

Las tendencias en la utilización de herramientas tecnológicas para el mejor desenvolvimiento laboral han generado gran interés en la sociedad. El hombre ha hecho del uso de la tecnología parte de su diario vivir.

Por ello es de gran interés realizar una auditoría informática que permita proporcionar un reporte donde se detalle los puntos críticos de la institución en el ámbito

tecnológico y permita tomar medidas correctivas, asegurando confiabilidad, confidencialidad y disponibilidad de la información encaminando a guiar al buen desarrollo y correcto funcionamiento de los departamentos Auditados de la institución, cabe recalcar que la información está disponible tanto en la red como en libros.

Es de gran interés y de importancia para los funcionarios realizar dicha investigación ya que invierten gran parte de su tiempo en el uso de la tecnología como herramienta de trabajo, y que servirá como aporte en la correcta utilización de los equipos que permitirá en el futuro el mejor desenvolvimiento de la institución.

1.4. Objetivos

1.4.1. Objetivo General

- Desarrollar una Auditoria Informática para la optimización el manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua.

1.4.2. Objetivos Específicos

- Detectar deficiencias en los procesos manejados por los sistemas informáticos.
- Realizar un análisis del software legal e ilegal de cada área.
- Verificar la seguridad Física, lógica de los diversos ambientes de procesamiento de información.

CAPITULO II

MARCO TEORICO

2.1. Antecedentes Investigativos

En la biblioteca de la Universidad Técnica De Ambato, en la Facultad de Ingeniería en Sistemas Electrónica e Industrial reposa la tesis "Auditoria Informática para los departamentos Financiero, Tesorería, Proveeduría, Agencia Norte y agencia Sur de la Empresa municipal de agua potable y Alcantarillado de Ambato" del Autora Maritza Andrea Espinoza Apráez donde afirma haber realizado una Auditoria Informática con el fin de solucionar los problemas ocurridos por averías tanto de Hardware como de Software, la intromisión de usuarios no autorizados en la institución donde se realizó la auditoria.

También existe una tesis en la Universidad Iberoamericana en la Ciudad de México D.F. para obtener el grado de Maestro en Ingeniería en Sistemas Empresariales con el título "Seguridad Informática Auditoria de Sistemas" del Autor Luis Daniel Álvarez Basaldúa donde menciona que se realizo una Auditoria Informática donde Abarca un análisis de los recursos lógicos y físicos que puedan sufrir riesgo de violación de la seguridad y donde plantea paso a paso las fases que realizadas en la auditoria evaluando la infraestructura lógica y física y la entrega de un reporte de las actividades realizadas las conclusiones y recomendaciones del Autor .

De los estudios anteriormente mencionados serán tomados en cuenta tanto en las recomendaciones como en las conclusiones.

2.2. Fundamentación Legal

La Constitución de la República del Ecuador, en los artículos siguientes señala:

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

2. El acceso universal a las tecnologías de información y comunicación.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 19.- La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, elaboren en cualquier actividad de comunicación.

Tomado de la página www.infa.gov.ec (2008, Folio Nº 01405) menciona los puntos más relevantes:

ART. 52 De la misión de la Dirección Tecnológica

Administrar con la mística del INFA los servicios informáticos institucionales y asegurar el óptimo funcionamiento de los sistemas y equipos.

Formular ejecutar y evaluar planes, programas y proyectos con el fin de proveer de nuevas tecnologías de comunicación e información TIC, que permita brindar servicios de calidad, optimizar la gestión institucional, la atención al cliente y la toma de decisiones, garantizando la seguridad, la oportunidad y confidencialidad de los datos y de la información.

Responsable: Director de Gestión Tecnológica

ART. 52 De los objetivos operativos, productos y servicios de la Dirección Tecnológica

Para el logro de los objetivos estratégicos e institucionales de la Dirección de Gestión Tecnológica, establecerá sus objetivos operativos y metas, los que serán gestionados a través de planes programas y proyectos.

Para el cumplimiento de la misión de la dirección de Gestión de tecnología, se definen los siguientes productos y servicios, los que serán gestionados bajo un enfoque de procesos, para lo cual deberá elaborar el manual de procesos, estableciendo los correspondientes indicadores de gestión:

1. Plan anual de requerimientos tecnológicos;
2. Sistemas informáticos analizados, desarrollados e implementados
3. Aplicaciones institucionales implementadas;
4. Plan de mantenimiento de Hardware y Software;
5. Informes de administración de Hosting;
6. Información de respaldo almacenada en un sitio de alta seguridad;
7. Actas de entrega de recepción de aplicaciones y equipos informáticos;
8. Políticas de Hardware y Software;
9. Soporte Tecnológico frente a problemas y

10. Administrar, orientar y capacitar el uso de Sistemas de Información automatizado (hardware y software), proporcionando el apoyo técnico necesario a los operadores y usuarios

2.3. Fundamentación Teórica

2.3.1. Red de Ideas Conceptuales

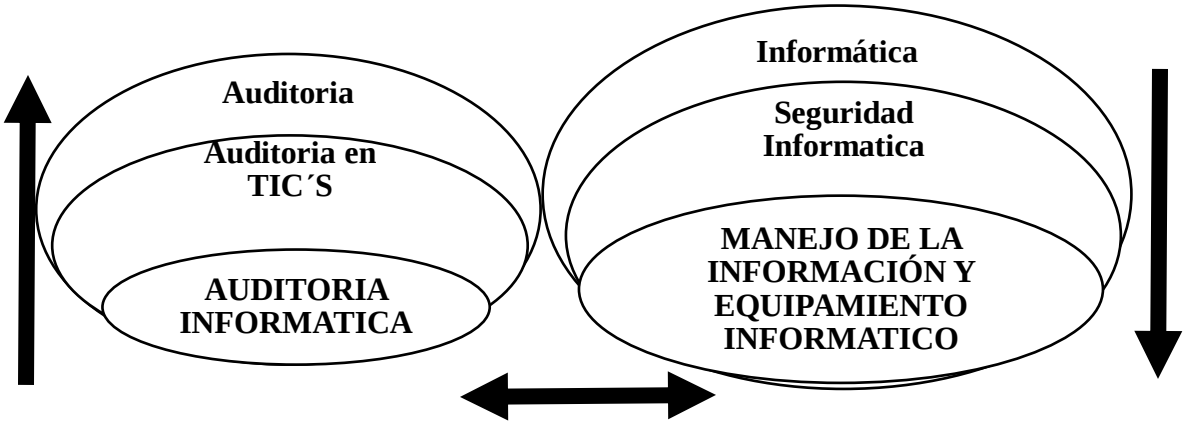


Grafico #2 Red de Inclusiones conceptuales

Ideas de Variable Independiente y Dependiente

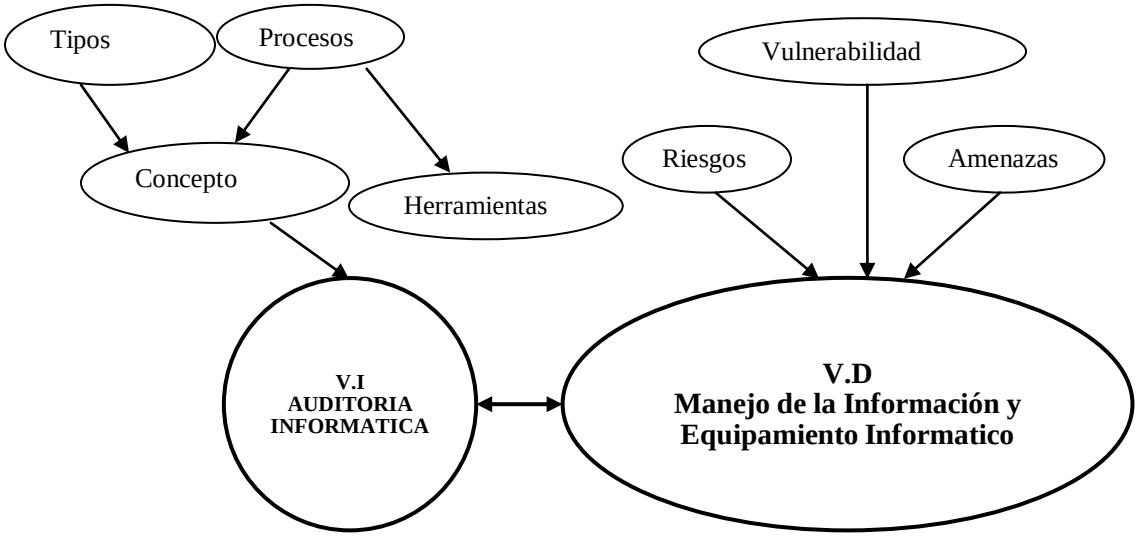


Grafico #3 Red de Inclusiones conceptuales

CATEGORÍA I

VARIABLE INDEPENDIENTE

2.3.1.1. AUDITORIA

La competitividad que existe en las empresas a nivel mundial, la gestión y control de la actividad económica-financiera de cualquier instituto, ya sea de carácter público o privado; se desarrolla a través de la Auditoría, que se basa en el examen y evaluación de la actividad financiera, económica y administrativa de una institución, realizada generalmente por especialistas ajenos a la misma.

2.3.1.1.1. CONCEPTO

Es un examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, con frecuencia este término ha sido utilizado incorrectamente ya que se ha considerado como una evaluación donde el fin es detectar errores y señalar fallas, pero el concepto de auditoría va mas allá de la detección de errores sino el un examen crítico donde el objetivo es evaluar la eficiencia y la eficacia de un área u organismo.

Etimológicamente, la palabra auditoria proviene del latín **Auditorius,** de donde procede **auditor** que tiene la **Virtud de oír**, y Auditor es la persona que revisa, examina y evalúa los resultados de una dependencia o entidad donde su objetivo está encaminado a evaluar la eficacia y la eficiencia con que se está operando a través de normas de acción donde se tomen decisiones que permitan corregir los errores en caso de existirlos o mejorar la forma de actuación.

Si tomamos en cuenta los términos eficiencia y eficacia no son similares pero las dos forman un papel muy importante ya que **Eficiencia** es poder lograr lo planeado con los menores recursos posibles y **Eficacia** es lograr los objetivos. Según **El Boletín "C" de Normas de Auditoría del Instituto Mexicano de Contadores nos dice:** ***"****La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos para arrojar resultados, sino también requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos".*

Segun Kell Zeigler, Walter, (1998, Pag 22) afirma "*Es un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados".*

ZAMARRIPA, 2002, "*Define como la acumulación y la evaluación de las evidencias sobre la información cuantificable de una entidad económica para determinar y opinar sobre el grado de correspondencia que hay entre la información y el criterio establecido"*

Tomando los criterios anteriores podemos decir que auditoria es un proceso ordenado para obtener y evaluar información cuantificable de una entidad para la toma de decisiones en pro de mejorar.

2.3.1.2. AUDITORIA EN TIC´S (Tecnologías de Información y Comunicación)

La introducción de nuevas tecnologías mediante el uso de equipos como sistemas informáticos tanto en empresas como instituciones públicas o privadas es una herramienta fundamental para el desarrollo de las actividades diarias, para ello se

utilizan tecnologías de información para gestionar sus funciones de forma rápida y eficiente, con el fin de obtener beneficios económicos y de costos, su correcta utilización facilita al usuario y directivos la realización de sus tareas en el menor tiempo posible, aumentando así la productividad notablemente.

En toda actividad hay riesgos, que deben ser minimizados o más bien ser previstos, de ahí se llevan a la práctica las auditorias a las TICs, las cuales es importante que existan y se realicen periódicamente, dado que la información es uno de los activos más importantes de las empresas e instituciones, es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología, frente a esta realidad se hace posible llevar a cabo auditorias en TICs,

La Auditoria en TIC´S son un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, telecomunicaciones, redes o equipamiento, con el fin de proteger actividades y recursos, verificar si las actividades se desarrollan eficientemente y de acuerdo con la normatividad informática y general en cada empresa o institución, para conseguir la eficacia exigida por la organización.

Es muy importante recalcar que la función de la auditoria en TIC´S es prevenir desvíos, modificaciones o manipulaciones a la información, analiza el control de la función informática, el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normatividad general, la revisión de la gestión de los recursos materiales, humanos e informáticos, los niveles de seguridad, etc.

2.3.1.3. AUDITORIA INFORMATICA

Desde que la informática se enfoco en la sistematización de las distintas aéreas de una organización incrementándose el número de computadoras en red y de componentes tecnológicos se vio en la necesidad de evaluar, controlar y salvaguardar la información que se maneja en las organizaciones es así donde aparece la auditoria informática.

Para determinar de mejor manera el concepto de Auditoria Informática en primera instancia se tomara el concepto de Auditoria anteriormente mencionado.

AUDITORIA, Verifica si la información financiera, operacional y administrativa que se presenta es confiable, veraz y oportuna, revisando los hechos, fenómenos y operaciones se den en la forma como fueron planeados a través de las políticas y lineamientos establecidos y que se cumplen con obligaciones fiscales, jurídicas y reglamentarias en general.

INFORMATICA, Proviene del vocablo francés *automatique d'informations* (información automática) es decir es la ciencia que estudia el tratamiento automático de la información utilizando técnicas, procesos y máquinas (ordenadores) para apoyar y potenciar su capacidad de memoria, de pensamiento y de comunicación.

Teniendo los conceptos de auditoría e informática podemos concluir que:

AUDITORIA INFORMATICA, Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo de una entidad, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

2.3.1.3.1. TIPOS DE AUDITORIA INFORMATICA

Auditoria Física: abarca el activo informático registrado en el inventario de la entidad auditada, se proporciona evidencia del nivel de la seguridad física en el ámbito en el que se va a desarrollar la actividad, no limitándose a comprobar que existen los medios físicos, sino también su funcionalidad, racionalidad y seguridad.

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales en un centro de procesamiento de información.

Auditoria Ofimática: Comprende los programas o aplicaciones que en conjunto sirven de herramienta para generar, procesar, almacenar, recuperar, comunicar y presentar la información en un lugar de trabajo, así como de forma doméstica.

El software de ofimática comprende una serie de aplicaciones que se distribuyen de forma conjunta para así mismo ser empleadas simultáneamente en diversos sistemas como por ejemplo:

- Hojas de cálculo
- Procesadores de Textos
- Presentadores de ideas
- Gráficos

Existen dos características a analizar de los entornos ofimáticos: la distribución de las aplicaciones por los diferentes departamentos de la organización en lugar de centralizarse en una única ubicación, y el traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios finales no dedicados

profesionalmente a la informática, quienes pueden no comprender de un modo adecuado la importancia de éstos y la forma de realizarlos.

Como consecuencia de esto, se ha generado la siguiente problemática: adquisiciones poco planeadas, desarrollos ineficaces e ineficientes, falta de conciencia de los usuarios acerca de la seguridad de los sistemas de Información, utilización de copias ilegales de aplicaciones, procedimientos de copias de seguridad deficientes, escasa formación del personal, falta de documentación suficiente, etc.

Auditoria de Base de Datos: La gran difusión de los Sistemas Administradores de Bases de Datos (DBMS – Database Management Systems) y la identificación de los datos como uno de los recursos fundamentales de las empresas, ha hecho que la auditoría y control interno de esta área cobre mayor interés.

Algunos de los objetivos y técnicas de control están basados en el ciclo de vida de una BD son los siguientes:

- **Estudio previo y plan de trabajo**

Se debe verificar que: se ha realizado un estudio tecnológico de viabilidad en el cual se contemplen varias alternativas para alcanzar los objetivos.

- **Diseño y carga**

Los diseños lógicos y físicos se realicen correctamente donde se contemple restricciones oportunas, especificaciones de almacenamiento y cuestiones relativas a la seguridad.

- **Explotación y mantenimiento**

Donde se establecen procedimientos de explotación y mantenimiento que aseguran que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas se modifica sólo con la autorización adecuada.

- **Revisión post-implantación**

Donde los resultados esperados satisfacen las necesidades del usuario tanto los costos y beneficios coinciden con los previstos.

Auditoria de Redes: Se encarga de una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información. En primer instancia hay iniciar una gestión responsable de la seguridad es identificar la estructura física (hardware, topología) y lógica (software, aplicaciones) del sistema (sea un equipo, red, intranet, extranet), y hacerle un Análisis de Vulnerabilidad para saber en qué grado de exposición se encuentra la entidad de esta manera estudiada la "radiografía" de la red, se procede a localizar sus falencias más críticas, para proponer una Estrategia de Saneamiento de los mismos; un Plan de Contención ante posibles incidentes y un seguimiento Continuo del desempeño del sistema.

Auditoría de la Seguridad: La seguridad es el área principal a auditar, hasta el punto de que en algunas entidades se creó inicialmente la función de auditoría informática para revisar la seguridad, la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnología de información y comunicaciones, por lo que el impacto de las fallas, los accesos no autorizados, la revelación de la información, entre otros problemas, tienen un impacto mucho mayor.

2.3.1.3.2. Procesos de la Auditoria Informática

El objetivo que sigue el proceso de una auditoria informática es salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos

gerenciales, y la utilización de los recursos con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias que debe seguir un orden como son:

- Planificación de la Auditoria Informática
- Ejecución de la Auditoria Informática
- Finalización de la Auditoria Informática

2.3.1.3.2.1. Planificación de la Auditoria Informática

Este inicia con una fase de planeación donde se encuentren involucradas los departamentos a ser auditadas para identificar los recursos necesarios que permitirán que se lleve a cabo, planteando objetivos como son:

* Evaluación de los sistemas y procedimientos
* Evaluación de los equipos de cómputo
* Evaluación del proceso de Datos

Obteniendo el conocimiento inicial de la entidad se establecerán metas, programas de trabajo de auditoría, personal que intervendrá en el proyecto, presupuesto financiero, y las fechas y la manera como se presentarán los informes de las actividades de cumplimiento del proyecto.

2.3.1.3.2.2. Ejecución de la Auditoria Informática

Consiste en la recolección de la información y de los elementos suficientes para fundamentar los comentarios, conclusiones y recomendaciones respecto a las TI por medio de la utilización de técnicas y herramientas:

- Entrevistas
- Encuestas
- Cuestionarios
- Análisis de la Información Documentada
- Revisión y Análisis de Estándares

Toda la información recabada debe ser completa y detallada para que pueda ser comprendida y permita la obtención de comentarios, conclusiones y recomendaciones, mediante su revisión.

2.3.1.3.2.3. Finalización de la Auditoria Informática

El resultado de la auditoría Informática, se materializa en un informe de conclusiones que se debe redactar y entregar a la administración de la organización para su evaluación, por lo que antes de la emisión del informe final se debe realizar varios borradores, para descubrir fallos en la evaluación de auditoría debido a la incorrecta comprensión de la organización por parte del auditor.

2.3.1.3.3. Técnicas y Herramientas

Para detectar falencias de información como de equipo tecnológico se debe recurrir a la recolección de la información observada y documentada donde se analiza las situaciones de debilidad o fortalezas de los diferentes entornos es por ello que se debe utilizar una técnica para recabar la información relevante que pueden ser:

2.3.1.3.3.1. Cuestionario

Es un instrumento de investigación que se basa a través de listas escritas de preguntas que se distribuyen entre los usuarios que nos permiten obtener información útil y eficaz en un tiempo breve.

2.3.1.3.3.2. Entrevista

Se utiliza para recabar información en forma verbal, a través de preguntas que propone el interesado, quienes responden pueden ser gerentes o empleados, los cuales son usuarios actuales del sistema existente, usuarios potenciales del sistema propuesto o aquellos que proporcionarán datos o serán afectados por la aplicación propuesta.

2.3.1.3.3.3. Checklist

Es una herramienta útil para definir un problema y organizar ideas, se encuentra dentro de las fases de definición, medición y análisis del ciclo de un proceso donde se identifica información específica para la descripción de un problema.

CATEGORÍA II

VARIABLE DEPENDIENTE

2.3.2. INFORMATICA

La informática reúne muchas técnicas que el hombre ha desarrollado con el objetivo de potenciar sus capacidades de pensamiento, memoria y comunicación. Su área de aplicación no tiene límites: la informática se utiliza en la gestión de negocios, en el almacenamiento de información, en el control de procesos, en las comunicaciones, en los transportes, en la medicina y en muchos otros sectores.

La informática abarca también los principales fundamentos de las ciencias de la computación, como la programación para el desarrollo de software, la arquitectura de las computadoras y del hardware, las redes como Internet y la inteligencia artificial.

Según PAREJA Cristóbal, ANDEYRO Ángel, OJEDA Manuel (1994, Pag.17), define la Informática como *"la ciencia que estudia el procesamiento automático de la información y que solo se produce con el desarrollo de los computadores".*

GALLARDO, Miguel A.(Internet:14/Dic/2009;05/Nov/2011;3:15 am), afirma que la informática es "*El conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores puede ser muy básico, o inacabable e hipercomplejo".*

Tomando en cuenta los puntos de vista de los dos autores la informática es la ciencia encargada del estudio del procesamiento automático de la información y que este abarca técnicas y conocimientos científicos a través de ordenadores.

Las herramientas tecnológicas y los ordenadores hoy en día son esenciales para enfrentar el reto de la competencia global, donde los negocios deben ser eficientes y sensibles a las necesidades y producir bienes y servicios de alta calidad. Los computadores proveen la información necesaria precisa y actualizada para tomar decisiones estratégicas y administrar procesos en las empresas.

2.3.2.1. SEGURIDAD INFORMATICA

Actualmente la información constituye un activo fundamental para el progreso y mantenimiento en el mercado de cualquier organización, resulta por tanto lógico el que uno de los objetivos prioritarios de cualquier empresa sea el aseguramiento de dicha información y de los sistemas que la procesan.

La experiencia muestra que el nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo por lo que cualquier organización debería tomar parte activa para conseguir una gestión efectiva de la seguridad.

La seguridad informática se refiere a la protección de la infraestructura computacional que estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática. Entendiéndose como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo

La Revista RED, La comunidad de expertos en redes, **(**Internet: 01/Nov./2002;06/ Nov./2011;17:00**)** Puntualiza que la **Seguridad Informática** consiste en "*Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos.*

Según expertos hoy en día todavía no se ha creado un sistema que sea 100% seguro y explican que un sistema se puede definir como seguro cuando tiene las tres características principales como son: Integridad (Autorización para que la información sea modificada), Confidencialidad (Información asequible para autorizados), Disponibilidad (Disponible solo cuando se necesite).

La seguridad informática de una empresa es primordial debido a la existencia de personas ajenas a la información (hackers), quienes buscan la mínima oportunidad para acceder a la red, modificar, borrar datos o tomar información que puede ser de vital importancia para la empresa.

Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70% de las violaciones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías o tiene acceso a la información sensible de la empresa que puede afectar el buen funcionamiento de la organización, pudiendo representar un daño con valor de miles o millones de dólares.

Se debe establecer políticas de seguridad como un factor importante para la empresa, pudiendo ser el monitoreo de la red, los enlaces de telecomunicaciones, respaldar datos, para establecer los niveles de protección de los recursos.

Es recomendable que las políticas se basen en los siguientes puntos:

- Identificar y seleccionar la información sensible (que se debe proteger).
- Establecer niveles de importancia en la información.
- Dar a conocer los resultados que traería a la organización, si se llegase a perder la información importante. Referente a costos y productividad.
- Identificar los niveles de vulnerabilidad de la red y las amenazas que tiene al tener una red mal estructurada.
- Realizar un análisis de los costos para prevenir y recuperar la información en el caso de sufrir un ataque.

- Implementar respuesta a incidentes y recuperación para disminuir el impacto.

Las políticas detalladas permitirán desplegar un diseño de la seguridad basada en soluciones técnicas, así como el desarrollo de un plan de contingencias para manejar los incidentes y disminuir el impacto que estas causarían.

La seguridad informática básicamente abarca la protección de recursos informáticos y la información contenida en ellos, estando disponibles para su utilización Tomando en cuenta dos factores importantes:

- Seguridad Física
- Seguridad Lógica

2.3.2.1.1. SEGURIDAD FÍSICA

La importancia de ser consciente ya que por más segura que sea una empresa o institución sea desde el punto de vista de ataques externos como Hackers, virus, etc. La seguridad de la misma será nula si no se ha previsto como combatir diversas eventualidades como desastres naturales, Sabotajes internos, imprudencias de los propios usuarios etc. Se puede mencionar que la seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

La **Seguridad Física** según *HUERTA, Antonio Villalón (**Internet: 2/Oct./2000;11, Nov. /2011; 04:00am**)* consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*" Se refiere a los controles y mecanismos de seguridad dentro y alrededor dentro de una empresa o institución así también los medios de acceso, implementados para proteger el hardware y medios de almacenamiento de datos.

Pues bien se puede decir que de la seguridad informática física es la prevención de acceso de personas no están autorizadas, pues si cualquiera puede entrar en una sala de computadoras, sentarse delante de una y comenzar a trabajar sin que nadie le diga nada, entonces el problema radica en el control de acceso de esa manera alguien robe o que dañe los datos o el equipo.

2.3.2.1.2 SEGURIDAD LÓGICA

Dentro de la seguridad informática, la seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático complementándose con la seguridad Física.

La seguridad lógica se puede salvaguardar mediante técnicas de seguridad que deben ser tomadas muy en cuenta por las instituciones como por ejemplo:

- Restringir el acceso a los programas y archivos.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.

Controles de Acceso

- Identificación y Autentificación
- Roles
- Limitaciones a los Servicios
- Administración

Día a día, las nuevas tecnologías se han ido introduciendo en las actividades diarias de cualquier empresa que permite mejorar aspectos tan importantes como la gestión,

la planificación y la mejora de las relaciones con los clientes. Por otro lado, la dependencia existente de la información digitalizada y de los sistemas informáticos es tan alta, que un desastre podría ocasionar elevadas pérdidas e incluso el cese de la actividad económica.

De esta problemática, se deriva la necesidad de estar preparados ante cualquier eventualidad y así, minimizar los trastornos que éste pudiera ocasionar. Por lo tanto, toda empresa debería preparar y desarrollar un plan de contingencias para prevenir y recuperar información importante para la misma.

2.3.2.2. DELITOS INFORMÁTICOS

Es una amenaza producida por mano humana, ya sea intencional, por accidente, o por fallas producidas en sistemas o máquinas producidas por el hombre tales como:

- **Robo Informático**.- utilización de sistemas de computadoras para *robar* información clasificada.
- **Fraude Informático.-** Son operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.
- **Sabotaje Informático.-** no solo afecta el bien jurídico intermedio de la información, sino que lesiona directamente el patrimonio económico destinado a actividades laborales.

  Dentro de los Sabotajes informáticos mencionaremos:
- **Virus.-** Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.
- **Gusanos.** - Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

- **Bomba lógica o cronológica.** - Requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

2.3.2.3. MANEJO DE LA INFORMACION Y EQUIPAMIENTO INFORMATICO

(Peralta, 2008) La información es el activo más importa para toda empresa o institución al igual que el equipo informático es un factor primordial que facilita la tarea diaria de los usuarios que manejan sistemas de información realizando cuatro actividades básicas:

2.3.2.3.1. ENTRADA DE INFORMACIÓN

Es el proceso manual o automático donde los datos son ingresados al computador a través de las unidades de entrada de datos como son las terminales, las cintas magnéticas, las unidades de diskette, los códigos de barras, los escáners, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras.

2.3.2.3.2. ALMACENAMIENTO DE INFORMACIÓN

Es el proceso más importante que tiene una computadora, ya que el sistema puede recordar la información guardada en estructuras de información denominadas archivos; La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM).

2.3.2.3.3. PROCESAMIENTO DE INFORMACIÓN

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida, estos cálculos pueden efectuarse con

datos introducidos recientemente en el sistema o bien con datos que están almacenados.

La característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene.

2.3.2.3.4. SALIDA DE INFORMACIÓN

Se basa en sacar la información procesada o bien datos de entrada al exterior mediante unidades de salida como son las impresoras, terminales, la voz, los graficadores y los plotters, entre otros.

Dentro de equipo tecnológico y la información que se maneja se puede mencionar que existen riesgos, amenazas y vulnerabilidades que afectan a ambas partes para la cual se debe tomar las medidas correspondientes y necesarias para el mejor desempeño de las actividades para ello se debe conocer el concepto de cada término.

2.3.2.4. AMENAZA

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el tema de seguridad es necesario la garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Generalmente se distingue y divide tres grupos

- **Criminalidad**: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- **Sucesos de origen físico**: son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

- **Negligencia y decisiones institucionales**: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

También hay que tomar en cuenta las siguientes amenazas que son alarmantes en toda institución:

- Falta de respaldo de datos
- Perdida de información por rotación, salida de personal
- Abuso de conocimientos
- Mal manejo de equipos y programas
- Acceso no-autorizado

2.3.2.5. VULNERABILIDAD

Es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos, dentro de ellos se puede mencionar:

a) **Hardware,** Representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

b) **Software,** Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.). Ambos factores hacen susceptible al sistema a las amenazas de software.

c) **Red,** Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio. Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

2.3.2.6. Riesgo

Es la incertidumbre de que ocurra un acontecimiento que pudiera afectar el logro de los objetivos:

a) **Riesgos de Integridad,** Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes

en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones.

b) **Riesgos de Acceso,** Inapropiado acceso a información clasificada que puede ser alterada por terceros.

c) **Riesgos de Infraestructura,** En organizaciones no existe una estructura información tecnológica efectiva (*hardware, software, redes, personas y procesos)* para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan entorno de procesamiento de información y las aplicaciones asociadas (*servicio al cliente, pago de cuentas, etc.)*.

2.4. Hipótesis

Auditoria Informática en el MIES INFA Tungurahua optimizará el manejo de la información y equipamiento informático.

Unidades de Observación: Departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y Unidad Administrativa.

2.5. Señalamiento de Variables

2.5.1. Variable Independiente

Auditoria Informática

2.5.2. Variable Dependiente

Manejo de la Información y Equipamiento Informático

CAPITULO III

3.- MARCO METODOLOGICO

3.1. Enfoque

Según MARTINEZ, Miguel.(2006: 6)Dice: "Investigación Cualitativa trata de identificar la naturaleza profunda de las realidades, su estructura dinámica aquella que da razón plena de su comportamiento y manifestaciones ".

Tomando en cuenta el criterio anterior se puede decir que el presente trabajo investigativo tomara un enfoque cuali-cuantitativo por las siguientes consideraciones:

Participativo.- ya que es un proceso de interacción donde se une la perspectiva comunitaria y científica tomando en cuenta las opiniones de las personas que intervienen en nuestro estudio.

Humanista.- ya que se intentara llegar a las personas de una manera clara, para crear una cultura de conocimiento.

Considerando una realidad dinámica, pero al mismo tiempo está orientada a la comprobación de hipótesis y con énfasis en los resultados.

3.2. Modalidades Básicas de la Investigación

La presente investigación tiene las siguientes modalidades:

Modalidad Bibliográfica o Documentada: se ha considerado esta modalidad por que se ha tomado información de fuentes como: libros virtuales, revistas periódicos, e internet.

Modalidad Experimental: se ha considerado la relación de la variable independiente Auditoria Informática y su influencia y relación en la variable dependiente Manejo de la Información y Equipamiento Informático para considerar sus causas y sus efectos.

Modalidad de Campo: se ha considerado esta modalidad ya que el investigador ira a recoger la investigación primaria directamente de los usuarios involucrados a través de una encuesta.

3.3. Tipos de Investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de investigación ¿Cómo la Auditoria Informática optimiza el manejo de la información y equipamiento Informático en el MIES INFA Tungurahua?, como de la misma manera ayudo a plantear la hipótesis.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente Auditoria Informática y la variable dependiente Manejo de la Información y Equipamiento Informático.

3.4. Población y Muestra

La población que se va a considerar para la presente investigación es alrededor de 10 funcionarios que laboran en cada departamento.

Departamento	Funcionarios
Departamentos de Informática,	Tecnóloga Catherine Analuisa
Comunicación Social	Lic. Francisco Vaca
Planificación	Ing. Luis Auz
Secretaria	Laura Barrera
Talento Humano	Grisca Terán Verónica Tamayo
Técnicos Territoriales	Rosita Freire Víctor Escobar Luis Barreno
Unidad Administrativa	Gerardo Sánchez
TOTAL	**10**

Tabla # 1. Población y Muestra

3.5. OPERALIZACION DE LAS VARIABLES

3.5.1. VARIABLE INDEPENDIENTE: Auditoria Informática

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Es el proceso de recoger y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo de una entidad y utiliza eficientemente los recursos.	Proceso	Plan Contingencia	1.-¿La institución posee planes de contingencia ante cualquier eventualidad ?	Se aplicara cuestionario a los funcionarios de la institución
	Evidencias	Control de acceso	2.- ¿Existe control de acceso a los computadores para usuarios no autorizados? 3.- ¿Las claves de acceso al computador son visibles a otros usuarios?	
	Sistema de Información	Fallos Tecnológicos	4.- ¿Cuándo se produjo alguna falla en la parte tecnología usted soluciona el problema por si solo? 5.-¿Se realizan respaldos habitualmente de la información de la institución ?	
	Recurso	Humano	6.- ¿El Depto. De Tecnología cuenta con el personal suficiente para cubrir las necesidades de la institución? 7.- ¿Se capacita al personal entorno al ámbito tecnológico?	

Tabla # 2. Operalizacion de la Variable Independiente

3.5.2. VARIABLE DEPENDIENTE: Manejo de la Información y Equipamiento Informático

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Es el proceso que se le da a la información de una institución a través del equipo informático y el factor humano que lo manipula	Proceso Información Equipo Informático Factor humano	Agilidad Software de protección Chequeos Periódicos	1.-¿Al realizar las actividades diarias, los equipos de computo responde con agilidad en el proceso? 2.-¿Tiene conocimiento del todo el software instalado en su computador? 3.-¿El software de protección de virus es eficaz para detectar los mismos ? 4.- ¿Se realiza chequeos habituales de mantenimiento del equipo de cómputo en la institución? 5.- ¿Se efectúan actualizaciones de software periódicamente? 6.- ¿Los programas que utiliza habitualmente poseen las respectivas licencias?	Se aplicara cuestionario a los funcionarios de la institución

Tabla # 3. Operalizacion de la Variable Dependiente

3.6. Recolección y Análisis de la Información

SECUNDARIA	PRIMARIA
• Se recolecta de estudios realizados anteriormente. • Se encuentra registrada en documentos y material impreso libros y revistas, tesis, monografías. • Las fuentes de la información son: Bibliotecas, archivos. Internet.	• Se recolecta directamente a través del contacto directo entre el sujeto investigador y los usuarios que forman parte del estudio, es decir con la realidad

Técnicas De Investigación

BIBLIOGRAFICAS	DE CAMPO
• La información se encuentra registrada en: • Libros, archivos	• Se llevara a cabo la investigación a través de: • Encuestas • Observación

Recolección de la Información

PREGUNTAS	**EXPLICACION**
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis
2. ¿A qué personas o sujetos?	Funcionarios de los Departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y

	Unidad Administrativa del MIES – INFA Tungurahua
3. ¿Sobre qué aspectos?	**V.I.** Auditoria Informática **V.D.** Manejo de la Información y Equipamiento Informático
4. ¿Quién?	Diana Castro
5. ¿Cuándo?	De acuerdo al cronograma
6. ¿Lugar de recolección de la información?	Departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y Unidad Administrativa del MIES INFA Tungurahua
7.-¿Cuántas veces?	1 sola vez
8. ¿Qué técnicas?	Encuesta
9. ¿Con que?	Cuestionario
10. ¿en qué situación?	Situación Normal y Cotidiana

Tabla # 4. Plan para Recolección de información

3.7. Procesamiento y Análisis

Revisión y codificación de la información

Categorización y tabulación de la información

1. Tabulación Manual.
2. Tabulación Computarizada (SPSS).

Análisis de los datos

1. La presentación de los datos se realizara a través de los datos para analizarlos e interpretarlos.

Interpretación de los resultados

1. Describir los resultados.
2. Analizar la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla.
3. Estudiar cada uno de los resultados por separado.
4. Redactar una síntesis general de los resultados.

CAPITULO IV

ANÁLISIS E INTERPRETACION DE RESULTADOS

4.1. ANÁLISIS DE LOS RESULTADOS

Para la recopilación y análisis de información se ha considerado una muestra de 10 funcionarios, los mismos que laboran dentro de los departamentos que son parte de la Auditoria en el MIES INFATUNGURAHUA.

4.1.1. Análisis de los resultados de la encuesta

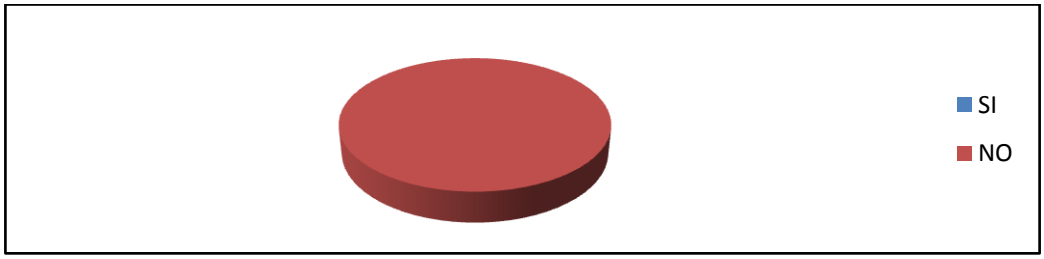
1.- ¿La institución posee planes de contingencia ante cualquier eventualidad?

Tabla # 5. Frecuencia Pregunta # 1

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 4. Existencia de Plan de Contingencia



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, 100 % correspondiente a 10 personas indican que no existe algún plan de contingencia.

Cualitativo: Por lo tanto ante cualquier eventualidad que pudiese suscitarse en el MIES-INFA Tungurahua no se cuenta con plan de contingencia que pudiera solucionar los inconvenientes.

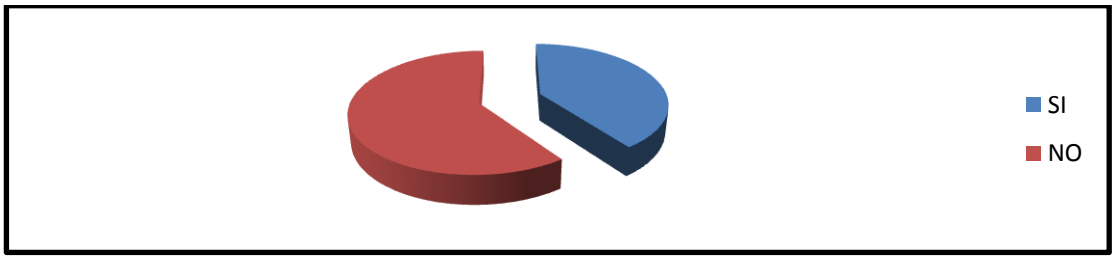
2.- ¿Existe control de acceso a los computadores para usuarios no autorizados?

Tabla # 6. Frecuencia Pregunta # 2

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	4	0 %
NO	6	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 5. Control de Acceso de Usuarios no Autorizados



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 60 % correspondiente a 6 personas indican no poseer algún control para acceso de usuarios a los computadores de la institución, mientras 40% correspondiente a 4 personas que aseguran sus maquinas para que no sean manipuladas por terceros.

Cualitativo: Por lo tanto se considera que cada funcionario debe llevar un control de sus computadores para evitar el acceso al mismo.

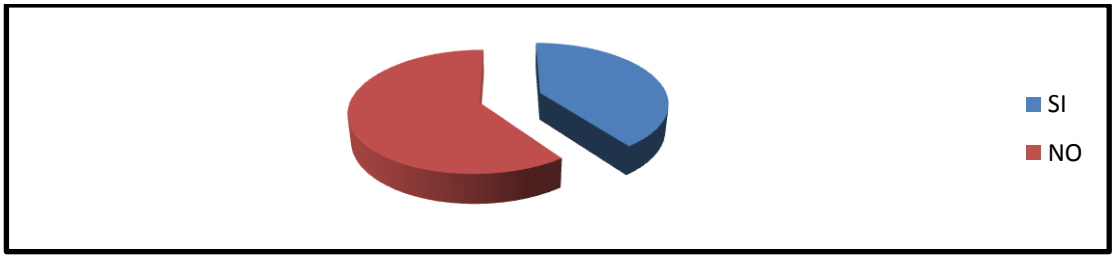
3.- ¿Las claves de acceso al computador son visibles a otros usuarios?

Tabla # 7. Frecuencia Pregunta # 3

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	4	0 %
NO	6	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 6. Claves de acceso Visibles a Terceros



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 60 % correspondiente a 6 personas aseguran que sus claves son visibles a otros usuarios, 40% correspondiente a 4 personas que afirman que sus claves son personales.

Cualitativo: Por lo tanto se considera que los funcionarios muestran sus claves lo que facilita la infiltración de usuarios.

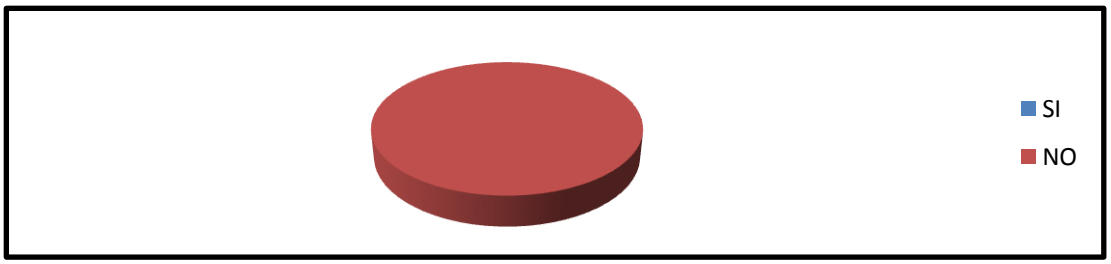
4.- ¿Cuándo se produjo alguna falla en la parte tecnología usted solucionó el problema por si solo?

Tabla # 8. Frecuencia Pregunta # 4

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 7. Solución a fallas en el área tecnológica



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 100 % correspondiente a 10 personas afirman que necesitan la ayuda del encargado del departamento de Tecnología para solucionar fallas en el área tecnológica.

Cualitativo: Por lo tanto se considera que la intervención del encargado del Departamento de Tecnología es primordial.

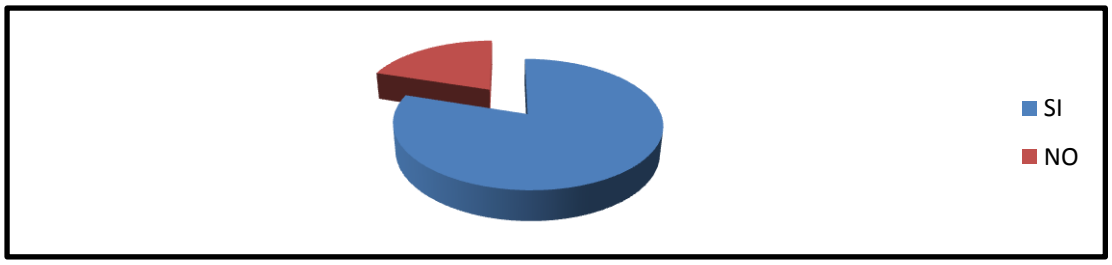
5.- ¿Se realizan respaldos habitualmente de la información de la institución?

Tabla # 9. Frecuencia Pregunta # 5

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	8	80 %
NO	2	20 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 8. Respaldo de Información



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 80 % correspondiente a 8 dicen respaldar la información que poseen, 20% correspondiente a 2 personas que afirman no respaldar la información.

Cualitativo: por lo tanto se considera que no existe un hábito de respaldo de la información ante posibles amenazas.

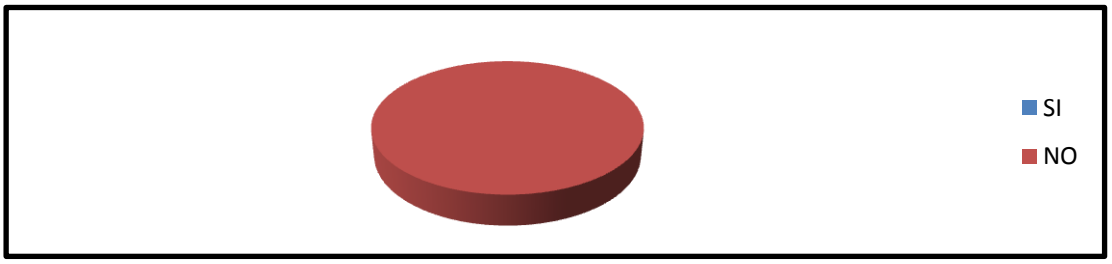
6.- ¿El Departamento de Tecnología cuenta con el personal suficiente para cubrir las necesidades de la institución?

Tabla # 10. Frecuencia Pregunta # 6

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 9. Personal del área Tecnológica cubre necesidades



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 100 % correspondiente a aseguran se necesitan al menos 2 personas en el Departamento de Tecnología para cubrir las necesidades de la institución.

Cualitativo: Por lo tanto se debe considerar que el personal del Departamento de Tecnología no es suficiente para cubrir las necesidades que se suscitan.

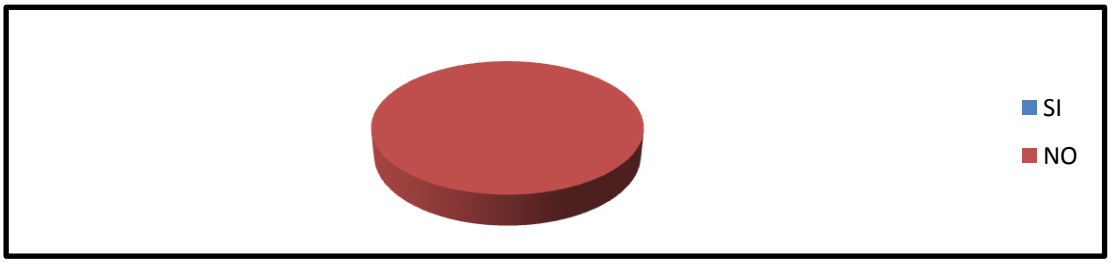
7.- ¿Se capacita al personal entorno al ámbito tecnológico?

Tabla # 11. Frecuencia Pregunta # 7

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 10. Capacitación del personal ámbito tecnológico



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 100 % correspondiente a afirman no recibir capacitación en el área tecnológica.

Cualitativo: Por lo tanto se considera como base primordial la capacitación de los funcionarios del MIES-INFA Tungurahua para mejor desenvolvimiento de sus funciones.

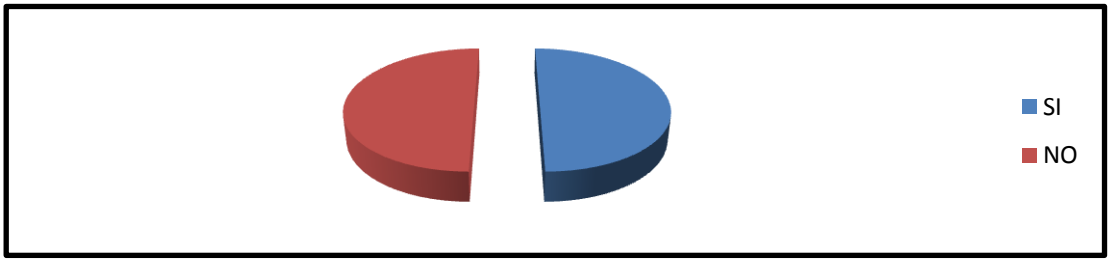
8.- ¿Al realizar las actividades diarias, los equipos de cómputo responde con agilidad en el proceso?

Tabla # 12. Frecuencia Pregunta # 8

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	5	50 %
NO	5	50 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 11. Funcionalidad de los Equipos



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 50 % correspondiente a 5 aseveran que los equipos si responden con agilidad en los procesos, 50% correspondiente a 5 personas afirman que sus equipos son obsoletos para trabajar con velocidad.

Cualitativo: Por lo tanto que la institución posee equipos que no desempeñan sus funciones a cabalidad por ser antiguos.

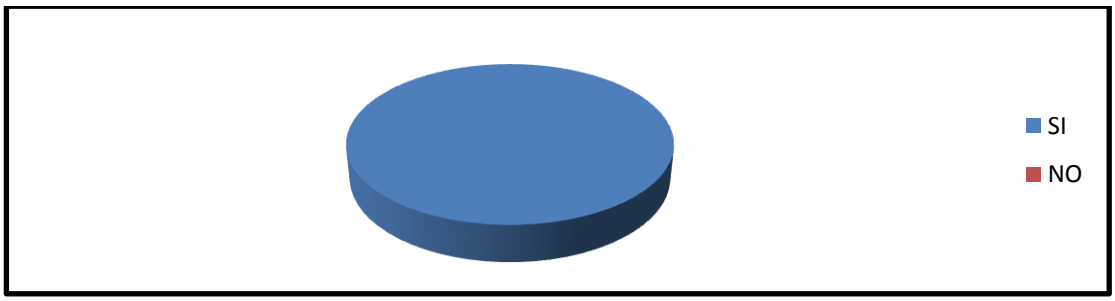
9. -¿Tiene conocimiento de todo el software instalado en su computador?

Tabla # 13. Frecuencia Pregunta # 9

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	10	100%
NO	0	0 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 12. Software instalado



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 100 % responde que si tienen conocimiento de los programas instalados pero que en su mayoría no son utilizados.

Cualitativo: Por lo tanto tiene presente el software que se encuentra instalado más se crea precedente que en su mayoría no se utiliza.

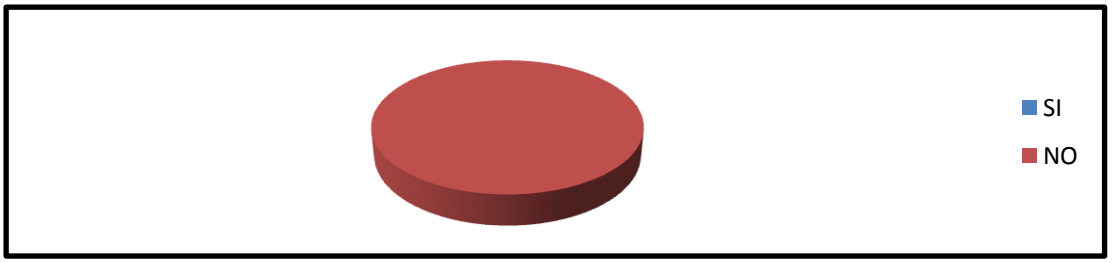
10.- ¿El software de protección de virus es eficaz para detectar los mismos?

Tabla # 14. Frecuencia Pregunta # 10

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 13. Protección de Virus



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 100 % correspondiente a afirman que el software para protección de virus es obsoleto.

Cualitativo: Por lo tanto la institución no se encuentra inmune ante la aparición de virus en sus ordenadores.

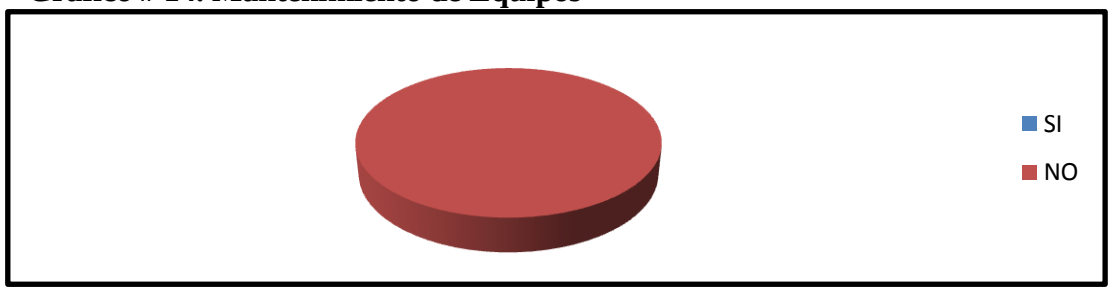
11.- ¿Se realiza chequeos habituales de mantenimiento del equipo de cómputo en la institución?

Tabla # 15. Frecuencia Pregunta # 11

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 14. Mantenimiento de Equipos



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 100 % afirma que no se realiza mantenimiento del equipo informático de la institución.

Cualitativo: Por lo tanto se manifiesta que no existe mantenimiento de los equipos en el MIES - INFA Tungurahua.

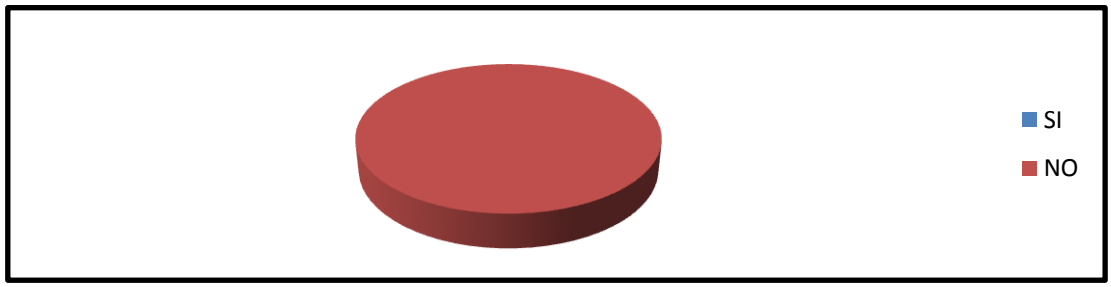
12.- ¿Se efectúan actualizaciones de software periódicamente?

Tabla # 16. Frecuencia Pregunta # 12

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0 %
NO	10	100 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 15. Actualizaciones de Software



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativa: De los 10 encuestados, el 100 % aseguran que no se realiza actualizaciones frecuentes del software en los equipos informáticos de la institución.

Cualitativa: Por lo tanto las actualizaciones en los ordenadores de la institución no se realizan con frecuencia.

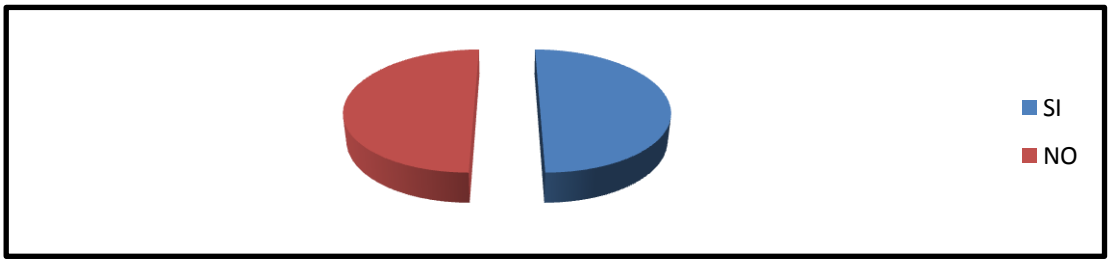
13.- ¿Los programas que utiliza habitualmente poseen las respectivas licencias?

Tabla # 17. Frecuencia Pregunta # 13

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	5	50 %
NO	5	50 %
TOTAL	10	100 %

Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Gráfico # 17. Licencia de Software



Fuente: Personal MIES – INFA Tungurahua
Autor: Diana Castro

Interpretación

Cuantitativo: De los 10 encuestados, el 50 % correspondiente a 5 aseveran que el software utilizado es legal, 50% correspondiente a 5 personas afirman que el software que poseen no tiene licencias.

Cualitativo: Por lo tanto se considera que el software que posee la institución en 50% no es legal.

4.2. INTERPRETACION DE LOS RESULTADOS

Se ha tomado en cuenta las preguntas discriminantes 10, 11 de la encuesta aplicada, con los siguientes resultados.

Pregunta #1. (Pregunta 10) ¿El software de protección de virus es eficaz para detectar los mismos?

Resumen: Symantec es el software de protección utilizado por la institución lamentablemente a pesar de poseer licencias no actúa de manera eficaz para la detección de virus por lo que los computadores se infestan de virus constantemente.

Pregunta #2. (Pregunta 11) ¿Se realiza chequeos habituales de mantenimiento del equipo de cómputo en la institución?

Resumen: El no realizar chequeos en los equipos de cómputo es motivo de muchos inconvenientes para los funcionarios, lo que ocasiona retardo en el desempeño de sus funciones.

4.3. COMPROBACION DE HIPOTESIS

Tomando en cuenta las encuestas realizadas a los funcionarios del MIES–INFA Tungurahua, se puede evidenciar el descuido al sector informático por parte de la institución, siendo este una herramienta que facilita la labor desempeñada por los miembros que integran cada departamento, por ende el área tecnológica debe ser uno de los puntos más importantes, por lo que se sugiere realizar una Auditoria Informática que permita tomar planes de acción para corregir falencias que afronta la institución a nivel informático.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- De la investigación se concluye que los funcionarios del MIES – INFA en su mayoría deja a visibilidad las contraseñas de sus ordenadores bajo teclados, en hojas adhesivas en los monitores lo que hace posible que terceros puedan ingresar libremente y tomar información importante.

- No existe un plan de contingencia en la institución en el ámbito informático ante cualquier eventualidad que puede suscitarse la cual puede afectar de manera significativa el desempeño de la institución.

- Los funcionarios del MIES – INFA poseen en sus computadores software que en gran parte no es utilizado, lo cual ocupa espacio de memoria y lentitud en sus equipos.

- El antivirus utilizado por la institución es deficiente por lo que la proliferación de virus en los computadores es frecuente.

- No existe mantenimiento periódico de los equipos de cómputo de la institución lo que evitaría fallos recurrentes en los ordenadores y molestias en los funcionarios.

5.2. RECOMENDACIONES

- Se recomienda realizar una Auditoria Informática en fin de proponer soluciones viables que permitan un mejor desenvolvimiento de la institución.

- Se recomienda a los funcionarios proteger sus contraseñas y cambiarlas periódicamente para evitar que usuarios externos accedan a la información.

- Se sugiere implementar un plan de contingencias para que la institución se encuentre preparada ante cualquier imprevisto ocurrido sea por el factor humano o por la naturaleza.

- Se recomienda eliminar aplicaciones innecesarias de los computadores para prevenir saturación de memoria y beneficiar el cumplimiento de las labores diarias.

- Se recomienda a la institución en lo posible adquiera un antivirus con licencia para que los problemas provocados por virus no sea frecuente.

- Se recomienda al departamento de Tecnología se realicen chequeos periódicos de los equipos de computo para un mejor desempeño de las actividades diarias y evitar fallos.

CAPITULO VI

PROPUESTA

6.1. DATOS INFORMATIVOS

- **Titulo**

"Auditoria Informática para Optimizar el Manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua"

- **Institución Ejecutora**

MIES INFA

- **Director de Tesis**

Ing. Jaime Ruiz

- **Beneficiarios**

Funcionarios de la Institución MIES INFA

- **Ubicación**

Av. José Peralta y pareja Diez Canseco.

- **Tiempo Estimado**

Fecha de Inicio: Junio del 2012

Fecha Fin: Noviembre del 2012

- **Equipo Técnico Responsable**
  - **Investigadora:** Diana Castro
  - **Responsable del Depto. De Tecnología:** Catherine Analuisa
  - **Tutor:** Ing. Jaime Ruiz

6.2. ANTECEDENTES DE LA PROPUESTA

Los cambios trascendentales que vive el mundo moderno, caracterizados por su incesante desarrollo, el aumento de la información, los sistemas que la proveen, las amenazas cibernéticas y los futuras transformaciones tecnológicas permitiendo cambios en las organizaciones para su mejor desenvolvimiento tanto en prácticas de negocio como en el de prestar sus servicios, creando oportunidades en el ejercicio de la Auditoria Informática.

La auditoria informática ha constituido un pilar fundamental en las organizaciones, tanto los sistemas como la estructura física deben estar sometidos a controles de calidad ya que los ordenadores como procesamiento de datos son blanco fácil para la delincuencia, terrorismo o espionaje.

La Auditoria informática permite la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que está inmersa en el procesamiento de la

información con el fin de lograr una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Con el fin beneficiar a la institución como a los funcionarios es necesario que se realice una Auditoría Informática para recoger, evaluar posibles falencias y proponer soluciones con el objetivo de mejorar la calidad de servicio para sus beneficiarios.

6.3. JUSTIFICACIÓN

La auditoria Informática nos permite detectar falencias, de la estructura física de la institución, estructura de hardware y software por medio de la recopilación de la información a través de técnicas y herramientas con el fin de dar solución a dichas fallas y mejorar la calidad de servicio.

6.4. Objetivos

6.4.1. Objetivo General

- Desarrollar una Auditoria Informática para la optimización en el manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua.

6.4.2. Objetivo Específico

- Analizar e Interpretar la información Recopilada.
- Definir las aéreas críticas de la Institución.
- Determinar las falencias tanto Físicas como Lógicas de la institución.
- Proporcionar un Reporte a la institución de las actividades realizadas a través de una Carta e Informe Final dirigida a la Dirección, detallado las aéreas críticas de los Departamentos Auditados con sus respectivas conclusiones y recomendaciones.

6.5. ANALISIS DE FACTIBILIDAD

Político.- Es política del Estado Ecuatoriano mantener seguridad de la información difundida a través del internet para proteger ante ataques cibernéticos.

Socio Cultural.- Desde el punto de vista socio cultural el proyecto brindará las medidas correctivas necesarias para salvaguardar la información contenida en los ordenadores de la institución.

Tecnológico.- Se utilizará software que permita constatar las falencias e informar sobre ellas.

Equidad de Género.- Tanto hombre como mujeres de cualquier edad utilizan herramientas tecnológicas para desempeñar sus funciones de la mejor manera posible.

Ambiental.- La utilización de los equipos informáticos que forman parte de la institución se asegura que no existirá contaminación o daño al medio ambiente.

Económico – Financiero.- El proyecto de investigación es factible de realizarlo debido a que los equipos tecnológicos de la institución se encuentran a disposición del investigador y las herramientas que se utilizarán son de fácil acceso.

Legal.- Es factible por que cumple con todos los requerimiento necesarios y establecidos por la ley.

6.6. FUNDAMENTACIÓN TEÓRICA (PROCESO DE LA AUDITORIA)

6.6.1. Fase I Tema

Auditoria Informática para Optimizar el Manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua.

6.6.2. Fase II

6.6.2.1. ANTECEDENTES Y EVOLUCIÓN DE MIES INFA

El Ministerio de Inclusión Económica y Social (MIES) promueve y fomenta activamente la inclusión económica y social de la población, para asegurar una adecuada calidad de vida de todos y todas. En esta línea, el MIES, a través del Instituto de la Niñez y la Familia - INFA, garantiza los derechos de niños, niñas y adolescentes en el Ecuador, poniendo en ejecución planes, normas y medidas que imparte el Gobierno Nacional en materia de protección integral a los niños, niñas y sus familias. Su gestión se desarrolla en cuatro líneas de acción: Desarrollo Infantil, Protección Especial, Participación, Atención en Riesgos y Emergencias.

En Desarrollo Infantil, el MIES INFA atiende a cerca de 500 mil niños y niñas, de entre 0 y 5 años, en cuidado diario, alimentación, estimulación, formación y capacitación familiar.

Niños, niñas y adolescentes son atendidos por Protección Especial, cuando se encuentran en situación de: maltrato, abuso, explotación sexual y laboral, víctimas de trata y tráfico, migración, perdidos, con padres privados de la libertad, con discapacidad, embarazo adolescente, mendicidad. Lo hace con acciones de prevención, exigibilidad y restitución de derechos.

La participación ciudadana de los niños, niñas y adolescentes del Ecuador es también una de las prioridades del MIES INFA, por lo que se promueve espacios para que éstos participen y opinen sobre los temas que les afectan. También genera movilización social para mantener y fortalecerla. Para ello, desarrolla una serie de mecanismos vinculados al desarrollo de capacidades de los actores sociales: familias, comunidades, niños, niñas y adolescentes, instituciones y otros actores sociales.

Así también, el MIES INFA a través de su línea de Riesgos y Emergencias implementa estrategias para reducir la amenaza de niños, niñas, adolescentes y sus familias afectadas por desastres naturales, además de mecanismos de protección ante

catástrofes individuales, situación de refugio y ayudas médicas emergentes a las personas que necesitan de algún tipo de servicio, insumo, medicamento o bien, que no pueda ser entregada por ninguna otra institución pública de salud.

Es así como el MIES a través del INFA, es el ejecutor de servicios de modo directo y a través de terceros, mediante el establecimiento de reglas transparentes, recursos de asignación competitiva y con base en acuerdos de co-inversión, de tal manera que se ha constituido en la institución líder en la ejecución de políticas de protección integral de la niñez y la adolescencia.

6.6.2.2. FUNDAMENTACION LEGAL

Tomado de la página www.infa.gov.ec (2008, Folio Nº 01405) menciona los puntos más relevantes:

ART. 52 De la misión de la Dirección Tecnológica

Administrar con la mística del INFA los servicios informáticos institucionales y asegurar el óptimo funcionamiento de los sistemas y equipos.

Formular ejecutar y evaluar planes, programas y proyectos con el fin de proveer de nuevas tecnologías de comunicación e información TIC, que permita brindar servicios de calidad, optimizar la gestión institucional, la atención al cliente y la toma de decisiones, garantizando la seguridad, la oportunidad y confidencialidad de los datos y de la información.

Responsable: Director de Gestión Tecnológica

ART. 52 De los objetivos operativos, productos y servicios de la Dirección Tecnológica

Para el logro de los objetivos estratégicos e institucionales de la Dirección de Gestión Tecnológica, establecerá sus objetivos operativos y metas, los que serán gestionados a través de planes programas y proyectos.

Para el cumplimiento de la misión de la dirección de Gestión de tecnología, se definen los siguientes productos y servicios, los que serán gestionados bajo un enfoque de procesos, para lo cual deberá elaborar el manual de procesos, estableciendo los correspondientes indicadores de gestión:

- Plan anual de requerimientos tecnológicos;
- Sistemas informáticos analizados, desarrollados e implementados
- Aplicaciones institucionales implementadas;
- Plan de mantenimiento de Hardware y Software;
- Informes de administración de Hosting;
- Información de respaldo almacenada en un sitio de alta seguridad;
- Actas de entrega de recepción de aplicaciones y equipos informáticos;
- Políticas de Hardware y Software;
- Soporte Tecnológico frente a problemas y
- Administrar, orientar y capacitar el uso de Sistemas de Información automatizado (hardware y software), proporcionando el apoyo técnico necesario a los operadores y usuarios.

6.6.3. FASE III

6.6.3.1. ALCANCE Y OBJETIVOS DE LA AUDITORÍA INFORMÁTICA

6.6.3.1.1. ALCANCE DE LA AUDITORÍA

AREAS AUDITABLES

Las aéreas auditables de la institución MIES – INFA son:

- Departamento de Planificación
- Coordinación Territorial (Técnicos de Campo)
- Departamento de Talento Humanos
- Departamento de Comunicación Social
- Secretaría

- Departamento de Tecnología
- Unidad Administrativa

AREAS NO AUDITABLES

Las aéreas al cual no tenemos acceso para realizar una auditoría son:

- Departamento Financiero
- Departamento Jurídico

Dichas áreas mantienen información confidencial crítica propia del normal funcionamiento de la institución la cual tiene acceso solo personal autorizado.

EXCEPCIONES DEL ALCANCE DE AUDITORIA

Se considera fuera del alcance de la auditoria, los sistemas de información ya que estos provienen de la matriz Quito en donde está el edificio principal del MIES - INFA, y allí se centraliza la información que es distribuida a las distinta dependencias de cada provincia y que se encuentra únicamente controlado desde Quito recibiendo soporte técnico desde una empresa de software ubicada en la misma ciudad, tiene restricciones de acceso y por lo tanto consideramos como una excepción del alcance de la auditoria que a de efectuarse en la institución.

6.6.3.2. OBJETIVOS DE LA AUDITORIA INFORMÁTICA

6.6.3.2.1 Objetivo General

- Desarrollar una Auditoria Informática para la optimización en el manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua.

6.6.6.3.2.2. Objetivos Específicos

- Analizar e Interpretar la información Recopilada.
- Definir las aéreas críticas de la Institución.
- Determinar las falencias tanto Físicas como Lógicas de la institución.
- Proporcionar un Reporte a la institución de las actividades realizadas a través de una Carta e Informe Final dirigida a la Dirección, detallado las aéreas críticas de los Departamentos Auditados con sus respectivas conclusiones y recomendaciones a fin de solucionar en lo posible las deficiencias.

6.6.4. FASE IV

6.6.4.1. PLANIFICACION DEL TRABAJO DE AUDITORIA

6.6.4.1.1. PERSONAL INVOLUCRADO

6.6.4.1.1.1. Auditor

Está conformado por la Srta.: Diana Castro la misma que tiene conocimientos en lo que respecta a seguridad informática, mantenimiento y reparación de computadores, redes, diseño de páginas Web.

6.6.4.1.1.2. Supervisor

El responsable de supervisar y revisar esta Auditoría es la Tecnóloga. Catherine Analuisa, quien se encargará de dirigir las diferentes actividades del auditor en las direcciones y secciones, y discutirá los informes emitidos.

6.6.4.1.1.3. Interlocutor

El interlocutor de la Auditoría es la Tecnóloga. Catherine Analuisa, que es la encargada de la sección de procesamiento de datos, además posee buenas relaciones con todo el personal de la institución. El mismo que ayudará y colaborará en el desenvolvimiento de las actividades correspondientes a la Auditoría.

6.6.4.2. CRONOGRAMA DE ACTIVIDADES

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Auditoria Informatica**	**63 días**	**lun 18/06/12**	**mié 12/09/12**	
2	Conformacion del Equipo Auditor	1 día	lun 18/06/12	lun 18/06/12	
3	Definicion del Alcance y Objetivos	2 días	mar 19/06/12	mié 20/06/12	2
4	Tramites en la Institucion	8 días	jue 21/06/12	lun 02/07/12	3
5	Formalizacion de la Auditoria en la Institucion	3 días	mar 03/07/12	jue 05/07/12	4
6	Elaboracion del Cronograma de Actividades	5 días	vie 06/07/12	jue 12/07/12	5
7	**Evaluacion del Control Interno Informatico**	**6 días**	**vie 13/07/12**	**vie 20/07/12**	
8	Recopilacion de la informacion de la Institucion	1 día	vie 13/07/12	vie 13/07/12	6
9	Analisis del Informe de la Institucion	1 día	lun 16/07/12	lun 16/07/12	8
10	Recopilacion de la Informacion Operacional	2 días	mar 17/07/12	mié 18/07/12	9
11	Analisis de la Informacion Operacional	2 días	jue 19/07/12	vie 20/07/12	10
12	Recopilacion de Informacion Detallada	2 días	jue 26/07/12	vie 27/07/12	11
13	Analisis de la Informacion Detallada	2 días	lun 30/07/12	mar 31/07/12	12
14	Definicion de Areas Criticas	3 días	mié 01/08/12	vie 03/08/12	13
15	Elaboracion de la Carta a la Gerencia	2 días	jue 23/08/12	vie 24/08/12	14
16	Elaboracion del Informe Final	2 días	lun 27/08/12	mar 28/08/12	15
17	Revision del Borrador del Proyecto	5 días	mié 29/08/12	mar 04/09/12	16
18	Correccion del Borrador del Proyecto	3 días	mié 05/09/12	vie 07/09/12	17
19	Revision del Proyecto	3 días	lun 10/09/12	mié 12/09/12	18
20	Presentacion del Proyecto	1 día	lun 17/09/12	lun 17/09/12	19

Gráfico # 18. Cronograma de Actividades Correspondiente a la Auditoria Informática

6.6.5. FASE V

6.6.5.1. ESTUDIO INICIAL DEL ENTORNO AUDITABLE

El estudio inicial se realiza para obtener un análisis en el entorno en el cual se va a trabajar, con el objetivo de que una vez, finalizada la Auditoría, se pueda realizar un balance de los resultados obtenidos por la misma.

6.6.5.2. ENTORNO ORGANIZACIONAL

6.6.5.2.1. Organigrama Estructural de la institución Vigente

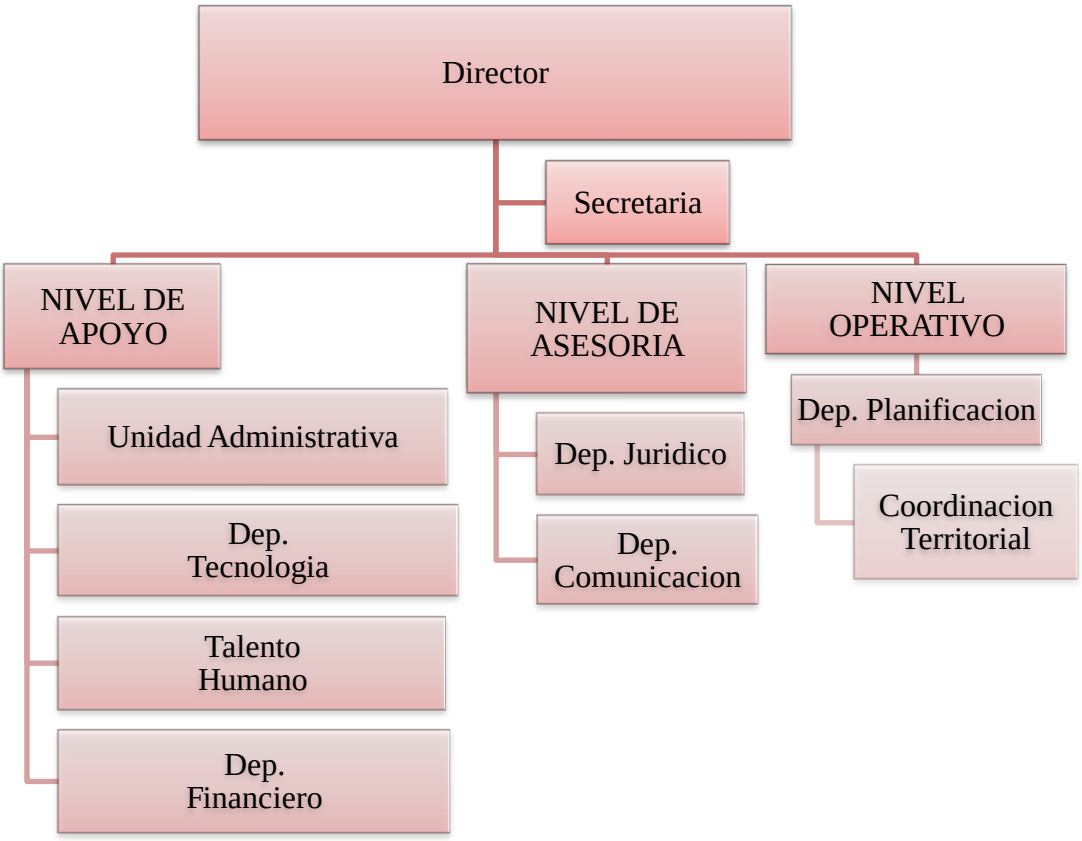


Gráfico # 19. Organigrama Estructural de la Institución

6.6.5.2.2. Descripción de Funciones de acuerdo Organigrama Funcional Vigente

En esta fase de la Auditoria el análisis manejado es general ya que la mayor parte de los departamentos auditados no corresponden al área informática.

6.6.5.2.2.1. SECRETARIA

El objetivo es brindar apoyo a la dirección MIES INFA con las tareas establecida, además de acompañar en la vigilancia de los procesos a seguir en el área de institucional.

6.6.5.2.2.2. UNIDAD ADMINISTRATIVA

Esta encargada de las adquisiciones de bienes inmuebles como de su conservación, además, es el responsable de llevar un control de los activos fijos y su correspondiente custodio y mantener actualizado el inventario de los mismos.

6.6.5.2.2.3. TALENTO HUMANO

Se encarga de la selección, inducción y capacitación institucional del personal, lleva un seguimiento de resultados en las contrataciones realizadas, como también se encarga de cumplir y hacer cumplir el reglamento interno de la institución.

6.6.5.2.2.4. COMUNICACIÓN SOCIAL

Permite que a través de la comunicación el tema de la niñez y la adolescencia sea asumido por la sociedad en general desde la perspectiva de derechos en particular las personas involucradas; niñas, niños, familias, funcionarios públicos y privados en lo que corresponde al desarrollo infantil, protección especial, participación y ejercicio de ciudadanía y apoyo a las familias en situaciones de riesgo y emergencia fortaleciendo la identidad institucional.

6.6.5.2.2.5. PLANIFICACION

Establece, integra, evalúa, monitorea los planes, herramientas, metodologías, mecanismos, protocolos que el INFA necesita para dar cumplimiento a sus objetivos.

6.6.5.2.2.6. TECNICOS TERRITORIALES

Se encarga de la promoción de las acciones de participación así como articulación de los planes de desarrollo comunitario y agendas de niños, niñas y adolescentes será parte del nivel técnico y administrativo más próximo a las comunidades, es responsable de incidir para que los planes de desarrollo comunitario de niños, niñas y adolescentes fortalezcan redes, foros, movimientos y formas de organización de nivel seguro y que tenga como incidencia política y exigibilidad.

6.6.5.2.2.7. TECNOLOGIA

Administra los servicios informáticos institucionales y asegura el óptimo funcionamiento de los sistemas y equipos, formula, evalúa y ejecuta programas y proyectos con el fin de proveer nuevas tecnologías de comunicación e información TIC, que permita brindar servicios de calidad, optimizar la gestión institucional, la atención al cliente, toma de decisiones garantizando la seguridad, oportunidad y confidencialidad de los datos y de la información.

6.6.5.2.3. TALENTO HUMANO

SECRETARÍA

Puesto: Secretaria

Nombre: Laura Barrera

Objetivo:

Ejecutar actividades pertinentes al área y asistir a su jefe inmediato, aplicando técnicas secretariales, a fin de lograr un eficaz y eficiente desempeño acorde con los objetivos de la institución.

Funciones:

- Redacta correspondencia, actas, oficios, memorándums y otros documentos encargados
- Recibe y envía correspondencia
- Da seguimiento a los procesos de documentación
- Lleva agenda de su superior

Escolaridad:

Título de profesional en Administración de Empresas o aéreas afines.

Experiencia: 2 años de experiencia en área secretarial y de oficina

Conocimientos:

- El manejo de equipo común de oficina (computadora, fax, fotocopiadora, máquina de escribir electrónica y otros).
- Métodos y procedimientos de oficina.
- Técnicas de archivo, ortografía, redacción y mecanografía.
- Computación básica.
- Relaciones humanas.
- Normas de cortesía.

Habilidades:

- Relacionarse con público en general.
- Expresarse claramente en forma verbal y escrita.
- Seguir instrucciones orales y escritas.
- Tratar en forma cortés y efectiva al público.
- Redactar correspondencia de rutina, actas e informe de cierta complejidad.
- Comprender situaciones de diversa índole.
- Organizar el trabajo de la oficina.

UNIDAD ADMINISTRATIVA

Puesto: Unidad Administrativa

Nombre: Gerardo Sánchez

Objetivo:

Organización, ejecución y custodia de los bienes inmuebles, equipos y materiales de la institución.

Funciones:

- Plan anuales de adquisiciones
- Plan de mantenimiento de bienes inmuebles, vehículos en carpeta de control
- Actas de cambio de custodio y transferencia
- Actas de inventarios y bienes inmuebles existentes y faltantes
- Informe de administración de bodegas
- Informe de administración y control de activos fijos.

Escolaridad:

Título de profesional en Comunicación Social y/o Periodista profesional.

Experiencia: Experiencia de dos años en labores de administración y control de Bodegas.

Conocimientos:

Conocimiento de paquetes computacionales utilizados en el área. Haber realizado un curso de control de bienes o similares.

Habilidades:

Apto para organizar, supervisar, coordinar, control y reserva de los bienes de la Institución y ejerce supervisión los mismos.

TALENTO HUMANO

Puesto: Talento Humano

Nombre: Grisca Terán – Verónica Tamayo

Objetivo:

Cumplir y hacer cumplir el reglamento interno de la institución, evaluar permanentemente al personal.

Funciones:

- Informe de selección de personal
- Plan de evaluación de desempleo
- Plan de inducción y capacitación institucional
- Plan de evaluación de capacidades y potenciales del recurso humano para profesionalizar y especializar la personal.
- Informe de auditorías de trabajo
- Informe de seguimiento y evaluación de los resultados de las contrataciones
- Reglamento interno de administración de recursos humanos
- Plan de incentivos.

Escolaridad:

Título de profesional en Administración de Empresas.

Experiencia:

Tres años en labores de Administración de Personal.

Conocimientos:

Legislación Laboral, Ley de Servicio Civil y Carrera Administrativa y otras leyes y reglamentos relacionados con el área. Paquetes computarizados para el área.

Habilidades:

Responsabilidad de prevenir conflictos de trabajo y ejerce amplia supervisión sobre el personal de la Institución.

COMUNICACIÓN SOCIAL

Puesto: Comunicación Social

Nombre: Francisco Vaca

Objetivo:

Permitir la comunicación desde la perspectiva de derechos en particular las personas involucradas; niñas, niños, familias, funcionarios públicos y privados en lo que corresponde al desarrollo infantil, protección especial, participación y ejercicio de ciudadanía y apoyo a las familias en situaciones de riesgo y emergencia fortaleciendo la identidad institucional.

Funciones:

- Asesoría en campañas de difusión masiva dirigida a grupos focales.
- Material comunicacional publicado
- Secciones informativas de la pagina web actualizada.
- Estrategias de comunicación por cada línea de acción
- Monitoreo de la imagen institucional.
- Boletines y ruedas de prensa.

Escolaridad:

Título de profesional en Comunicación Social y/o Periodista profesional.

Experiencia:

Dos años en labores profesionales afines.

Conocimientos:

Cursos de office básico, manejo de equipos de comunicación.

Habilidades:

Apto para la difusión e información de las actividades y actos de la Institución.

Requiere de conocimientos profesionales y de gran creatividad e iniciativa.

PLANIFICACION

Puesto: Jefe de Planificación

Nombre: Luis Auz

Objetivo:

Establece, integra, evalúa, monitorea los planes, herramientas, metodologías, mecanismos, protocolos que el INFA necesita para dar cumplimiento a sus objetivos

Funciones:

- Dirigir y coordinar la elaboración de políticas, planes, programas y proyectos institucionales.
- Orientar y acompañar la elaboración e implementación de estudios metodologías. Modelos y protocolos en materia de atención de niños/as y adolescentes.
- Detectar diseñar y proponer políticas públicas y sectoriales con procesos de planificación y desarrollo territorial.
- Realizar seguimiento y monitoreo de programas estipulados.
- Realizar informes de su gestión y realizar rendición de cuentas.

Escolaridad:

Título de profesional en Ingeniería en Sistemas

Experiencia:

Dos años en labores profesionales afines.

Conocimientos:

Manejo de office Básico.

Habilidades:

Apto para trabajar en equipo.

TECNICOS TERRITORIALES

Puesto: Técnicos Territoriales

Nombre: Rosita Freire - Víctor Escobar - Luis Barreno

Objetivo:

Promover las acciones de participación así como articulación de los planes de desarrollo comunitario y agendas de niños, niñas y adolescentes.

Funciones:

- Garantizar los derechos de los niños/as y adolescentes
- Diseñar y apoyar la ejecución de planes, programas, proyectos y presupuestos de acuerdo al territorio.
- Asistencia técnica y apoyo en la implementación de procesos de fortalecimiento de las capacidades de los niños/as y adolescentes.

Escolaridad:

Título de profesional en Trabajo Social, Psicología industrial o infantil, parvulario, Docencia, licenciatura.

Experiencia:

Dos años en labores profesionales afines.

Conocimientos:

Básicos de programas de computación como office y relaciones Humanas.

Habilidades:

Apto para la difusión e información de las actividades y actos de la Institución.

Requiere de conocimientos profesionales y de gran creatividad e iniciativa.

TECNOLOGIA

Puesto: Asistente de la Información

Nombre: Catherine Analuisa

Objetivo:

Administra los servicios informáticos institucionales y asegura el óptimo funcionamiento de los sistemas y equipos**.**

Funciones:

- Plan anual de requerimientos tecnológicos;
- Sistemas informáticos analizados, desarrollados e implementados
- Aplicaciones institucionales implementadas;
- Plan de mantenimiento de Hardware y Software;

- Informes de administración de Hosting;
- Información de respaldo almacenada en un sitio de alta seguridad;
- Actas de entrega de recepción de aplicaciones y equipos informáticos;
- Políticas de Hardware y Software;
- Soporte Tecnológico frente a problemas y
- Administrar, orientar y capacitar el uso de Sistemas de Información automatizado (hardware y software), proporcionando el apoyo técnico necesario a los operadores y usuarios

Escolaridad:

Título de profesional en Tecnología Informática

Experiencia:

Dos años en labores profesionales afines.

Conocimientos:

Office avanzado, amplio conocimiento en Redes, Base de Datos, mantenimiento y Reparación de Computadores, programación.

Habilidades:

Requiere de conocimientos profesionales y de gran creatividad e iniciativa.

FUENTE: Estatuto Orgánico por Proceso del MIES INFA

6.6.5.2.4. ANALISIS DEL ENTORNO ORGANIZACIONAL

6.6.5.2.4.1. RELACIONES JERARQUICAS Y FUNCIONALES

MIES – INFA cuenta con 4 niveles jerárquicos que están distribuidos de la siguiente manera:

PRIMER NIVEL

Conformado por los siguientes departamentos:

- Director
- Secretaria

SEGUNDO NIVEL

Conformado por los siguientes Departamentos:

- Unidad Administrativa
- Depto. Tecnología
- Depto. Talento Humano
- Depto. Financiero

TERCER NIVEL

Constituido por:

- Depto. Jurídico
- Depto. Comunicación Social

CUARTO NIVEL

- Conformado por:
- Depto. Planificación
- Depto. Coordinación Territorial

Según el organigrama del MIES-INFA cada departamento se rige a las órdenes de la Directora de la institución quien toda las decisiones.

6.6.5.2.4.2. PUESTOS DE TRABAJO

PUESTO	# de PERSONAS
Secretaria	1
Unidad administrativa	1
Depto. Talento Humano	2
Depto. Tecnología	1
Depto. Planificación	1
Depto. Comunicación Social	1
Técnicos Territoriales	3

Tabla # 18 Puestos de Trabajo

El personal de los Deptos. Recursos Humanos, Secretaria, Comunicación Social, Técnicos Territoriales, Unidad Administrativa no se encuentra debidamente capacitado para resolver algún tipo de problema informático (virus en el computador, sistema operativo inestable, etc.), sin embargo algunas personas solamente manejan el sistema perteneciente al área que le corresponde.

6.6.5.3. ENTORNO OPERACIONAL

6.6.5.3.1. UBICACIÓN FÍSICA DE LA EMPRESA

MIES-INFA Tungurahua se encuentra ubicado en las Calles Av. José Peralta y Pareja Diez Canseco, Vía a Santa Rosa la cual tiene una puerta de acceso para la entrada

tanto de los funcionarios de la institución, personal de los Centros de Desarrollo Infantil y beneficiarios del servicio.

La institución consta de 4 pisos, en el primer piso está ubicado los técnicos territoriales, donde se realizan la entrega de informes por parte del personal de los Centros de Desarrollo Infantil a su respectivo Técnico encargado, el mismo que también realiza un chequeo periódico de los establecimientos ubicados en los distintos cantones de la provincia.

En el segundo piso se encuentra distribuidos los departamentos de Secretaria a mano izquierda, seguido de la Dirección, a mano derecha encontramos el departamento de Talento Humano, junto a él se encuentra el departamento Financiero.

En el tercer piso está ubicado a mano izquierda la Unidad Administrativa, seguidamente se encuentra el cuarto de servidores de la institución, adyacente a el encontramos el departamento de Planificación, a continuación el Departamento de Comunicación Social y a mano derecha al fondo se encuentra el departamento Jurídico y por último en el cuarto piso se encuentra el departamento de Tecnología.

OBSERVACION

En el área de los técnicos territoriales por encontrarse en el primer piso, y que es frecuentemente visitado por el personal de los CDI y los beneficiarios de los servicios que presta la institución, se encuentra vulnerable ante el acceso de personas que pueden sustraerse objetos valiosos para la misma ocasionando pérdidas tanto económicas como retraso en las actividades diarias.

El departamento de tecnología que se encuentra en el último piso posee un espacio pequeño donde se encuentra almacenado los equipos dañados, equipos con que se encuentran en reparación, anaqueles con suministros para los distintos departamentos lo que dificulta el acceso del encargado provocando algún accidente y a la vez dichos equipos al no encontrarse ordenados pueden también ser víctimas de robos de los implementos.

RECOMENDACIÓN

Con respecto al departamento de Tecnología adecuar un espacio donde se pudiese almacenar los equipos que se encuentren dañados para en lo posterior ser dados de baja y a la vez ubicar allí los equipos que se encuentren en reparación, tomar en cuenta que el llevar un orden es importante por lo que se sugiere al encargado del departamento se dé tiempo para organizar cada material par evitar posibles robos.

Con respecto a los Técnicos Territoriales se sugiere mas control de las personal que ingresan y salen de la institución con el fin de que objetos que se encuentren dentro de la institución no sean sustraídos por agente externos evitando pérdidas.

ESTUDIO DEL CABLEADO ESTRUCTURADO EN LOS DEPARTAMENTOS DEL MIES-INFA TUNGURAHUA SEGÚN EL ESTÁNDAR "ISO/TIA/EIA -568-A"

CABLEADO ESTRUCTURADO NORMA ISO/TIA/EIA-568-A							
DEPTO	**CP**	**UPS**	**SWITCH**	**CIELORAZO**	**CONECCION A TIERRA**	**TOMAS DE DATOS**	**CANALETAS**
TECNOLOGIA	2	2	2	x	x	x	x
PLANIFICACION	1	1	---	x	x	x	x
COMUNICACIÓN SOCIAL	1	1	---	x	x	x	x
SECRETARIA	1	1	1	x	x	x	x
TALENTO HUMANO	2	2	---	x	x	x	x
TECNICOS TERRITORIALES	3	3	---	x	x	x	x
UNIDAD ADMINISTRATIVA	1	1	---	x	x	x	x
CONCLUSION Se puede mencionar que los departamentos cumplen con los requisitos mínimos de la norma.							

Tabla # 19. Cableado Estructurado por departamentos

ANÁLISIS DE LAS SEGURIDAD FÍSICAS DEPARTAMENTOS DEL MIES-INFA TUNGURAHUA

SEGÚN LA NORMA "ISO 27001/27002"

SEGURIDAD FISICA						
DEPTO	**EXTINTORES**	**ALARMAS**	**VIGILANCIA**	**ILUMINACION**	**VENTILADORES**	**HUMEDAD**
TECNOLOGIA	---	---	----	x	---	x
PLANIFICACION	---	---	---	x	----	----
COMUNICACIÓN SOCIAL	---	---	---	x	----	----
SECRETARIA	---	---	---	x	----	----
TALENTO HUMANO	---	---	---	x	----	----
TEC.TERRITORIALES	---	---	---	x	----	----
U. ADMINISTRATIVA	---	---	---	x	----	----
CONCLUSION en el depto. De Tecnología existe humedad para lo cual se deben tomar las medidas correspondientes de manera urgente ya que allí se encuentran los equipos de computo y herramientas que ayudan al mantenimiento de otros equipos; la institución no posee alarma pues cuenta con servicio de guardianía pero para mayor seguridad se recomienda la adquisición de alarmas.						

Tabla # 20. Seguridad Física

6.6.5.4. ARQUITECTURA Y CONFIGURACION HARDWARE Y SOFWARE

6.6.5.4.1. INVENTARIO

Se realizo un inventario tanto de hardware como de software a los departamentos auditados con el uso de la Herramienta WINAUDIT ya que es de fácil manejo y rápido.

6.6.5.4.1.1. INVENTARIO DE HARDWARE Y SOFTWARE VIGENTE

SECRETARIA

HARDWARE			
RESPONSABLE	**LAURA BARRERA**		
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
MOUSE	SIN CODIGO	COMPAQ	---
TECLADO	01-06-024-0171	COMPAQ	B21B50F6AJY85
MONITOR	01-06-018-0143	COMPAQ	039BB65NKR95
IMPRESORA	05-01-004-1319	XEROX PE 120I	VKC271881
REGULADOR	01-03-081-0041	TDE	21072544
UPS	01-06-002-3450	DATALINE	PCM081479
SCANNER	SIN CODIGO	GENIUS	ZP6491MO2783
SWITCH	01-06-023-0140	ENCORE	---

COMPONENTES LOGICOS				
#	**Equipo**	**Pentium 4**		**IP: 192.168.9.106**
	COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
1	ProcesS Pentium3GHz	INTEL	6Y1AFXHZZ0DX	
1	MAINBOARD	INTEL	MXJ634075G	

1	Disco Duro(3 GHZ)	CLON		
1	Floppy Disk			
1	Tarjeta Memoria 256MB	INTEL		
1	Tarjeta de Video	INTEL		
1	Tarjeta de Red	INTEL		
1	Tarjeta de Sonido	INTEL		

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Ahead - Nero Fast CD -Burning Plug-in		1A20-020E-0000-1349-1210-6697
Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674
Adobe Acrobat Reader	5.0.0.0	
Microsoft – Windows XP Professional		76460-OEM-0061914-63674
Ahead Software AG – Nero Burning ROM	6, 3, 1, 18	
Intel Audio Studio 2.00.0059	2.00.0059	
Intel® Common User Interface	7.0.0.4363	
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	
Microsoft Corporation – Messenger	4.7.3000	
Microsoft ® Windows Script Host	5.6.0.8820	
Microsoft Corporation - Zone.com	1.2.626.1	
Symantec Antivirus	10.1.4.4000	
Symantec Corporation LiveUpdate	3.0.0.160	
Microsoft Office Outlook	11.0.5510	
Power DvD	6.0.8820	

Reproductor de Windows Media de Microsoft®	9.00.00.3250	
Servicios Internet de Microsoft®	6.1.33.0	
Microsoft Office Picture Manager	11.0.5510	
Microsoft Office InfoPath	11.0.5510	
Microsoft Office Outlook	11.0.5531	

Tabla # 21. Inventario Hardware, Componentes Lógicos y Software de Secretaria

TALENTO HUMANO

HARDWARE			
RESPONSABLE	**GRISCA TERAN**		
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
MOUSE	SIN CODIGO	HP	---
TECLADO	01-06-024-0169	GENERICO	BN1B50F6AJY
MONITOR	01-06-018-0144	COMPAQ	143BM28HB361
IMPRESORA	07-01-013-1196	HP 3050	CNRK260672
UPS	01-06-002-3449	DATALINE	PCM081478
SCANNER	SIN CODIGO	GENIUS	ZP6491MO1476
MOUSE	SIN CODIGO	HP	---
TECLADO	01-06-024-0169	GENERICO	BN1B50F6AJY
RESPONSABLE	**VERONICA TAMAYO**		
MOUSE	SIN CODIGO	GENERICO	NFA20-0612
TECLADO	SIN CODIGO	GENERICO	KX-17030X
MONITOR	SN	SAMSUNG	LE1HCD629OA
IMPRESORA	5111533163	LEXMARK Z715	BETA580600018
UPS	X1131402	DATALINE	KK1688MR29

COMPONENTES LOGICOS			
RESPONSABLE: Grisca Terán			
Equipo	**Pentium 4**		**IP: 192.168.9.61**
COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
ProcesPentium4-.5GHz	INTEL	8Y1FXHZF0DX	
MAINBOARD	INTEL	MXJ634075G	
Disco Duro(19GHZ)	CLON		
Floppy Disk			
Tarjeta Memoria 256MB	INTEL		
Tarjeta de Video	INTEL		
Tarjeta de Red	INTEL	537EP	

Tarjeta de Sonido	Realtek	0019D151A7C2	
RESPONSABLE: Verónica Tamayo			
Equipo	**Pentium 4**		**IP: 192.168.9.62**
ProcesPentium4-1.7GHz	Intel	KX-17030X	
MAINBOARD	Company u8668		
Disco Duro(40GHZ)	Maxtor	4R060J0	
Floppy Disk			
Tarjeta Memoria 45MB			
Tarjeta de Video	Graphics ProsavageDDR		
Tarjeta de Red	Fast ethernet		
Tarjeta de Sonido	AC97		

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Ahead - Nero Fast CD-Burning Plug-in		
Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674
Adobe Acrobat Reader	5.0.0.0	
Microsoft - Windows XP Professional		76460-OEM-0061914-63674
Ahead Software AG - Nero Burning ROM	6, 3, 1, 18	
Intel Audio Studio 2.00.0059	2.00.0059	
Intel® Common User Interface	7.0.0.4363	
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	
Microsoft Corporation – Messenger	4.7.3000	
Microsoft ® Windows Script Host	5.6.0.8820	
Symantec Antivirus	10.1.4.4000	
Symantec Corporation LiveUpdate	3.0.0.160	
Microsoft Office Outlook	11.0.5510	
Power DvD	6.0.8820	

Reproductor de Windows Media de Microsoft®	9.00.00.3250	
Servicios Internet de Microsoft®	6.1.33.0	
Microsoft Office Picture Manager	11.0.5510	
Microsoft Office InfoPath	11.0.5510	
Microsoft Office Outlook	11.0.5531	

Tabla #22. Inventario Hardware, Componentes Lógicos y Software Talento Humano

PLANIFICACIÓN

HARDWARE			
RESPONSABLE		**ING. LUIS AUZ**	
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
MOUSE		COMPAQ	
TECLADO	01-06-024-0170	COMPAQ	B21B50F6AJY20
MONITOR		LCD HP L1506	CNC625RHKF
IMPRESORA	07-01-013-0068	CANNON	
REGULADOR	01-03-081-0040	TDE	21073983
UPS	01-06-002-3448	DATALINE	PCM08552

COMPONENTES LOGICOS				
#	**Equipo**	**Pentium III**		**IP: 192.168.9.4**
	COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
1	Process Pentium3GHz	Intel	MXJ82606RH	
1	MAINBOARD	Intel		
1	Disco Duro(40 GHZ)	Clon		
1	Floppy Disk			
1	Tarjeta Memoria512MB	Intel		

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Ahead - Nero Fast CD-Burning Plug-in		
Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674
Adobe Acrobat Reader	5.0.0.0	
Microsoft – Windows XP Professional		76460-OEM-0061914-63674
Ahead Software AG - Nero Burning ROM	6, 3, 1, 18	
Intel Audio Studio 2.00.0059	2.00.0059	

Intel® Common User Interface	7.0.0.4363	
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	
Microsoft Corporation Messenger	4.7.3000	
Microsoft ® Windows Script Host	5.6.0.8820	
Microsoft Corporation - Zone.com	1.2.626.1	
Symantec Antivirus	10.1.4.4000	
Symantec Corporation LiveUpdate	3.0.0.160	
Microsoft Office Outlook	11.0.5510	
Power DvD	6.0.8820	
Reproductor de Windows Media de Microsoft®	9.00.00.3250	
Servicios Internet de Microsoft®	6.1.33.0	
Microsoft Office Picture Manager	11.0.5510	
Microsoft Office InfoPath	11.0.5510	
Microsoft Office Outlook	11.0.5531	

Tabla #23. Inventario Hardware, Componentes Lógicos y Software Planificación

TECNICOS TERRITORIALES

HARDWARE			
RESPONSABLE	**LIC. ROSITA FREIRE**		
COMPONENTE	**CÓDIGO**	**MARCA**	**SERIE**
MOUSE	SIN CODIGO	COMPAQ	143BM2BHA315
TECLADO	SIN CODIGO	OMEGA	20169797
MONITOR	07-01-018-0071	COMPAQ Z510	KX-TS500LXV
IMPRESORA	01-06-022-0159	EPSON	BD1V24C000702
UPS	07-01-001-0045	TRIPP LINE	025BB285E835
RESPONSABLE	**LIC.VÍCTOR ESCOBAR**		
MOUSE	SN	TAIRUS	025BB285E835
TECLADO	SN	GENIUS	ZM8612003629
MONITOR	SN	SAMSUNG	B93AB0ACPSTN0
IMPRESORA	07-01-013-0061	HP LASER JET 1200	CNBRB24494
UPS	AF50203068	TRIPP LINE	
RESPONSABLE	**LIC. LUIS BARRENO**		
MOUSE	SN	COMPAQ	
TECLADO	01-06-024-0173	COMPAQ	B21B50FGAJY3D
MONITOR	01-06-018-0146	COMPAQ	023BB28SA138
IMPRESORA	07-01-013-0064	EPSON FX1180	ARSYOG1060
UPS	01-03-081-0034	TDE	21072545

COMPONENTES LOGICOS			
RESPONSABLE LIC. ROSITA FREIRE			
Equipo	**Pentium II**		**IP: 192.168.9.121**
COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
Process Pentium333GHz	OEM PRIMA		
MAINBOARD	INTEL		
Disco Duro(4.0GB)	INTEL	G112FZ4ZB3	
Floppy Disk		106BB285B95	
Tarjeta Memoria 256MB	INTEL		
Tarjeta de Video	INTEL	STSI298847	
Tarjeta de Red	INTEL	BOA090MGA	
Tarjeta de Sonido	INTEL		
RESPONSABLE LIC. VICTOR ESCOBAR			
Equipo	**Pentium II**		**IP: 192.168.9.67**
COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
Process Pentium333MHz	INTEL	CNBRB24494	
MAINBOARD	INTEL	3BE2600019	
Disco Duro(4.01GB)	INTEL		
Floppy Disk		9500517	
Tarjeta Memoria 256MB	INTEL		
Tarjeta de Video	INTEL		
Tarjeta de Red	INTEL		
Tarjeta de Sonido	INTEL		
RESPONSABLE LIC. LUIS BARRENO			
Equipo	**Pentium II**		**IP: 192.168.9.109**
COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
ProcesS Pentium3GHz	INTEL	GY1BKGMZ0JJ	
MAINBOARD	INTEL		
Disco Duro(3 GHZ)	CLON	FX890	
Floppy Disk			

Tarjeta Memoria 256MB	INTEL	143BM28HB405	
Tarjeta de Video	INTEL	21073469	
Tarjeta de Red	INTEL		
Tarjeta de Sonido	INTEL		

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Adobe Acrobat Reader	5.0.0.0	
Microsoft – Windows XP Professional		76460-OEM-0061914-63674
Ahead Software AG - Nero Burning ROM	6, 3, 1, 18	
Intel Audio Studio 2.00.0059	2.00.0059	
Intel® Common User Interface	7.0.0.4363	
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	

Tabla #24. Inventario Hardware, Componentes Lógicos y Software Tec. Territoriales

COMUNICACIÓN SOCIAL

HARDWARE			
RESPONSABLE	**FRANCISCO VACA**		
COMPONENTE	CODIGO	MARCA	SERIE
MOUSE	01-06-024-0175	COMPAQ	ZM8612003629
TECLADO	01-06-024-0167	GENIUS	ZM8612003629
MONITOR	01-06-018-0154	COMPAQ	143BM2BHA315
IMPRESORA	07-01-010-0058	LEXMARK	13231262134
REGULADOR	07-01-005-0037	COMPAQ	GB1BJKW28069

COMPONENTES LOGICOS				
#	Equipo	**Pentium 4**	**IP: 192.168.9.2**	
	COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
1	ProcesS Pentium3GHz	INTEL		
1	MAINBOARD	INTEL	6107FZ4ZB734	
1	Disco Duro(3 GHZ)	CLON		
1	Floppy Disk		023BB28SA138	
1	Tarjeta Memoria 256MB	INTEL	21072545	
1	Tarjeta de Video	INTEL	B21B50FGAJY3D	
1	Tarjeta de Red	INTEL	107F4ZB73	
1	Tarjeta de Sonido	INTEL		

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Corel CAPTURE ™	11.633	
Corel PHOTO-PAINT®	11.633	
Corel R.A.V.E. ™	2.0	
CorelDRAW®	11.633	

Globalink - Conversation	1, 0, 0, 1	
Ahead - Nero Fast CD -Burning Plug-in		1A20-020E-0000-1349-1210-6697
Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674
Adobe Acrobat Reader	5.0.0.0	
Microsoft – Windows XP Professional		76460-OEM-0061914-63674
Ahead Software AG – Nero Burning ROM	6, 3, 1, 18	
Intel Audio Studio 2.00.0059	2.00.0059	
Intel® Common User Interface	7.0.0.4363	
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	
Microsoft Corporation – Messenger	4.7.3000	
Microsoft ® Windows Script Host	5.6.0.8820	
Microsoft Corporation - Zone.com	1.2.626.1	
Symantec Antivirus	10.1.4.4000	
Symantec Corporation LiveUpdate	3.0.0.160	
Microsoft Office Outlook	11.0.5510	
Power DvD	6.0.8820	
Reproductor de Windows Media de Microsoft®	9.00.00.3250	

Tabla #25. Inventario Hardware, Componentes Lógicos y Software Comunic. Social

UNIDAD ADMINISTRATIVA

HARDWARE			
RESPONSABLE	**GERARDO SANCHEZ**		
MOUSE	SIN CODIGO	GENIUS	
TECLADO	01-06-024-0590	HP	B93CBOACPTDE
MONITOR	SIN CODIGO	HP	CNC625RGZW
IMPRESORA	07-01-013-0060	HP LASER JET 1100	USRJ0529SI
REGULADOR	01-06-002-3447	DATALINE	
MOUSE	SIN CODIGO	GENIUS	

COMPONENTES LOGICOS				
#	**Equipo**	**Pentium 4**	**IP: 192.168.9.54**	
	COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
1	ProcesS Pentium3GHz	INTEL		
1	MAINBOARD	INTEL	SP-F203	
1	Disco Duro(3 GHZ)			
1	Floppy Disk			
1	Tarjeta Memoria 256MB	INTEL		
1	Tarjeta de Video	INTEL	PCM081480	
1	Tarjeta de Red	INTEL	B93AB0ACPSTN	
1	Tarjeta de Sonido	INTEL	025BB285E835	

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Olympo	2.0	
Windows XP Professional		55690-640-0421043
Apple Computer, Inc. QuickTime QuickTime	6.0	
Microsoft Windows Media Player	6.4.09.1120	

Ahead - Nero Fast CD -Burning Plug-in		1A20-020E-0000-1349-1210-6697
Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674
Adobe Acrobat Reader	5.0.0.0	
Microsoft – Windows XP Professional		76460-OEM-0061914-63674
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	
Microsoft Corporation – Messenger	4.7.3000	
Microsoft ® Windows Script Host	5.6.0.8820	
Symantec Antivirus	10.1.4.4000	
Symantec Corporation LiveUpdate	3.0.0.160	
Microsoft Office Outlook	11.0.5510	
Power DvD	6.0.8820	
Reproductor de Windows Media de Microsoft®	9.00.00.3250	
Servicios Internet de Microsoft®	6.1.33.0	
Microsoft Office Picture Manager	11.0.5510	
Microsoft Office InfoPath	11.0.5510	
Microsoft Office Outlook	11.0.5531	

Tabla #26. Inventario Hardware, Componentes Lógicos y Software Unidad Adminis.

DEPTO. TECNOLOGÍA

HARDWARE			
RESPONSABLE	**TECNGA. CATHERINE ANALUISA**		
MONITOR	01-06-018-0149	COMPAQ	V570
	01-06-018-0147	ADC	MDS72101535
TECLADO	SIN CODIGO	COMPAQ	KK1688MR29
	SIN CODIGO	HACER	20662
IMPRESORA	07-01-013-0062	LEXMARK Z51	9330401159
	07-01-013-0063	EPSON	31LDY097554
UPS	01-06-002-0135	THOR UPS	8200
	07-01-001-0082	TRIPP LINE	KXTA308
MOUSE	SIN CODIGO	GENIUS	
	SIN CODIGO	LCD HP L1506	CNC625RHPC
DIFUSORES DE SEÑAL DE RED	07-01-008-0055	D-LINK	P1F1178005673
	01-06-009-0138	D-LINK	D1F1178005667
	07-01-008-0057	ADVANTEK	0529A3A00840
ROUTTER	07-01-019-0072	SYSTEMS	CI500
SWITCH	01-06-023-0134	3COM	3C17300A
	01-06-023-0156	3COM	3C16441A
	01-06-023-0157	SWITCH	CLON
SERVIDOR DE IMPRESORA	01-06-022-0162	D-LINK	F40W167500745
	01-06-022-0161	ADVANTTEK	412AP2716
	01-06-022-0160	D-LINK	F40W167600742
PROYECTOR	05-02-014-0083	LG	2500
	05-02-014-0014	SONY	CPS 200
MULTIMETRO	01-02-019-0005	DT 832	

COMPONENTES LOGICOS				
#	**Equipo**	**Pentium 4**		**IP: 192.168.9.205**
	COMPONENTE	**MARCA**	**SERIE**	**OBSERVACION**
1	ProcesS Pentium3GHz	INTEL		

1	MAINBOARD	INTEL	6107FZ4ZB734	
1	Disco Duro(3 GHZ)	CLON		
1	Floppy Disk		023BB28SA138	
1	Tarjeta Memoria 256MB	INTEL	21072545	
1	Tarjeta de Video	INTEL	B21B50FGAJY3D	
1	Tarjeta de Red	INTEL	107F4ZB73	
1	Tarjeta de Sonido	INTEL		
1	Disco Duro(3 GHZ)	CLON		

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Adobe Acrobat	7.0.0.0	
WinRAR archiver	3.51.0.0	
Mozilla	3.5	
Adobe Acrobat	7.0.0.0	
Adobe Acrobat	7.0.0.0	
WinRAR archiver	3.51.0.0	
Mozilla	3.5	
Symantec Corporation - Client and Host SecurityPlatform	104.0.8.3	
Microsoft ® .NET Framework	1.1.4322.573	
Microsoft ® Windows Script Host	5.6.0.8820	
Microsoft Application Error Reporting	11.0.5515	
Microsoft Clip Organizer	11.0.5510	
Microsoft Corporation - Encarta	15.0.0.0603	
Microsoft Open Database Connectivity	3.520.7713.0	

Microsoft - Windows XP Professional		55690-640-0000356-23286
Corel CAPTURE ™	11.633	
Corel PHOTO-PAINT®	11.633	
Corel R.A.V.E. ™	2.0	
CorelDRAW®	11.633	
Globalink - Conversation	1, 0, 0, 1	
Ahead - Nero Fast CD -Burning Plug-in		1A20-020E-0000-1349-1210-6697
Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674
Adobe Acrobat Reader	5.0.0.0	
Microsoft – Windows XP Professional		76460-OEM-0061914-63674
Ahead Software AG – Nero Burning ROM	6, 3, 1, 18	
Intel Audio Studio 2.00.0059	2.00.0059	
Intel® Common User Interface	7.0.0.4363	
Microsoft Corporation - Windows Movie Maker	2.1.4026.0	
Symantec Corporation - Client and Host Security Platform	104.0.8.3	
Microsoft ® .NET Framework	1.1.4322.573	
Microsoft ® Windows Script Host	5.6.0.8820	
Microsoft Application Error Reporting	11.0.5515	
Symantec Antivirus	10.1.4.4000	
Symantec Corporation LiveUpdate	3.0.0.160	
Microsoft Office Outlook	11.0.5510	
Power DvD	6.0.8820	
Reproductor de Windows Media de Microsoft®	9.00.00.3250	

Tabla #27. Inventario Hardware, Componentes Lógicos y Software Depto. Tecnología.

EQUIPOS DAÑADOS

DESCRIPCIÓN	CÓDIGO	DESCRIPCION	SERIE
DEPTO. TECNOLOGIA			
COMPUTADOR DE ESCRITORIO	07-01-005-0035	COMPAQ	6132FZ4ZC324
COMPUTADOR DE	07-01-005-0027	CLON	
COMPUTADOR DE ESCRITORIO	07-01-005-0038	SUNSHINE	
DIFUSOR DE SEÑAALES DE RED	01-06-009-0136	ALLIED TELESY	AT-AR250E
TELEFONO.- TELEFONO PANASONIC NEGRO	01-03-087-0052	PANASONIC	
REGULADOR DE VOLTAJE	01-03-081-0033	NIVELINE 440	15A-04-3757
COORDINACION TERRITORIAL			
CPU DTK CREMA	SIN CODIGO	DTK	9500517
DEPTO. COMUNICACION			
TECLADO.- TECLADO COMPAQ NEGRO	01-06-024-0175	COMPAQ	ZM8612003629

Tabla #28. Equipos Dañados de los Deptos. Tecnología, Comunicación Social Y Técnico Territorial.

6.6.5.4.1.2. REAL

Se ha verificado que el inventario de hardware vigente con relación al inventario realizado anteriormente existen variantes las cuales se describen a continuación

UNIDAD ADMINISTRATIVA

La unidad administrativa es la encargada de llevar el inventario de todos y cada uno de los muebles y enseres de la institución, mediante un sistema llamado OLYMPO, este sistema se encarga de recabar hasta el mínimo detalle de cada bien, el problema por el cual surge los errores es digitación de la información, pues se transcribieron algunos de los códigos erróneamente, a la vez al realizarse un cambio de custodio se realiza la duplicidad de la información, es decir un bien puede aparecer asignado a dos personas a la vez.

Básicamente se suscita este problema por la falta de capacitación acerca del sistema pues la persona que antes manejaba el mismo ya no se encuentra trabajando en la institución.

DEPARTAMENTO DE TECNOLOGIA

En este departamento existen algunos errores de codificación en algunos de los componentes informáticos y a la vez uno de los teclados que se encuentran en custodia de la Tecnog. Analuisa se encuentra en el Departamento Financiero ya que el teclado de dicho departamento sufrió un desperfecto pero no se han realizado los respectivos cambios de custodio.

DEPARTAMENTO TECNICOS TERRITORALES

En este departamento, el error más común como en todas las aéreas son los errores de codificación ya que algunos de los parámetros no coinciden con el inventario real.

6.6.5.5. SOFTWARE

6.6.5.5.1. LEGAL

En la institución se ha adquirido licencia para el software Windows 2003 Server, este se encuentra instalado y configurado en el servidor principal para otorgar servicios de correo, dhcp, dns. Se debe mencionar que a pesar de que el gobierno actual a impulsadas campañas sobre la utilización de software libre sobre todo en las instituciones públicas aun la institución no ha tomado la decisión de migrar a software libre.

SOFTWARE LEGAL			
SECRETARIA			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
Laura Barrera	Windows XP	Service pack 2	V2C47-MK7JD-3R89-D2KXW-VPK3J
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
	Nero Burning ROM	0, 8, 5, 0	
TALENTO HUMANO			
Grisca Terán Verónica Tamayo	Windows XP	Service pack 2	6F2D7-2PCG6-YQQTB-FWK9V-932CC
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
	Nero Burning ROM	0, 8, 5, 0	
	Converter		
PLANIFICACION			
Luis Auz	Windows XP	Service pack 2	6F2D7-2PCG6-YQQTB-

			FWK9V-932CC
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
	Nero Burning ROM	0, 8, 5, 0	
	Converter		
UNIDAD ADMINISTRATIVA			
Gerardo Sánchez	Windows XP	Service pack 2	6F2D7-2PCG6-YQQTB-FWK9V-932CC
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
	Nero Burning ROM	0, 8, 5, 0	
	Converter		
	Olympo	2.0	
COMUNICACIÓN SOCIAL			
Francisco Vaca	Windows XP	Service pack 2	6F2D7-2PCG6-YQQTB-FWK9V-932CC
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
	Nero Burning ROM	0, 8, 5, 0	
	Converter		
	Corel PHOTO-PAINT®	11.633	
	Corel R.A.V.E. ™	2.0	
	CorelDRAW®	11.633	
TECNICOS TERRITORIALES			
Rosa Freire Víctor Escobar Luis Barreno	Windows XP	Service pack 2	V2C47-MK7JD-3R89-D2KXW-VPK3J
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
TECNOLOGIA			
Catherine Analuisa	Windows XP	Service pack 2	6F2D7-2PCG6-YQQTB-FWK9V-932CC
	Microsoft Office	2007	YFKBB-PQJJV-G996G-VWGXY-2V3X8

	Adobe Reader	5.0.0.0	7.0.8.2006051600
	Symantec antivirus	10.0.0.0	
	Nero Burning ROM	0, 8, 5, 0	
	Converter		
	Corel PHOTO-PAINT®	11.633	
	Corel R.A.V.E. ™	2.0	
	CorelDRAW®	11.633	
	Microsoft - Internet Explorer	6.00.2900.2180	76460-OEM-0061914-63674

Tabla #29. Software Legal en los Departamentos Auditados

6.6.5.5.2. ILEGAL

Hay que recalcar que en la mayoría de los departamentos el software instalado en las maquinas en su mayoría es descargado del internet con su respectivo crack para que no surjan inconvenientes en el desempeño del computador, a continuación se detallan los mismos.

SOFTWARE ILEGAL		
SECRETARIA		
RESPONSABLE	**NOMBRE**	**VERSION**
Laura Barrera	Intel® Common User Interface	6.0.8820
	Microsoft Corporation - Windows Movie Maker	9.00.00.3250
	Microsoft Corporation – Messenger	11.0.5510
	Microsoft ® Windows Script Host	11.0.5531
	Microsoft Corporation - Zone.com	5.6.0.8820
	Power DvD	1.2.626.1
	Reproductor de Windows Media de Microsoft®	6.1.33.0
	Servicios Internet de Microsoft®	11.0.5510
	Microsoft Office Picture Manager	10.1.4.4000

	Microsoft Office InfoPath	3.0.0.160
TALENTO HUMANO		
Grisca Terán Veronica Tamayo	Microsoft Corporation - Windows Movie Maker	2.1.4026.0
	Microsoft Corporation – Messenger	4.7.3000
	Microsoft ® Windows Script Host	5.6.0.8820
	Microsoft Office Outlook	11.0.5510
	Power DvD	6.0.8820
PLANIFICACION		
Luis Auz	Microsoft Corporation - Windows Movie Maker	2.1.4026.0
	Microsoft Corporation – Messenger	4.7.3000
	Microsoft ® Windows Script Host	5.6.0.8820
	Microsoft Office Outlook	11.0.5510
	Power DvD	6.0.8820
UNIDAD ADMINISTRATIVA		
Gerardo Sánchez	Microsoft Corporation - Windows Movie Maker	2.1.4026.0
	Microsoft Corporation – Messenger	4.7.3000
	Microsoft ® Windows Script Host	5.6.0.8820
	Microsoft Office Outlook	11.0.5510
	Power DvD	6.0.8820
COMUNICACIÓN SOCIAL		
Francisco Vaca	Servicios Internet de Microsoft®	6.1.33.0
	Microsoft Office Picture Manager	11.0.5510
	Microsoft Office InfoPath	11.0.5510
	Microsoft Office Outlook	11.0.5531
TECNICOS TERRITORIALES		
Rosa Freire Víctor Escobar Luis Barreno	Ahead Software	6, 3, 1, 18
	AG - Nero Burning ROM	
	Intel Audio Studio 2.00.0059	2.00.0059
	Intel® Common User Interface	7.0.0.4363
	Microsoft Corporation	2.1.4026.0
	- Windows Movie Maker	
TECNOLOGIA		
Catherine Analuisa		
	Intel® Common User Interface	7.0.0.4363
	Microsoft Corporation - Windows Movie Maker	2.1.4026.0
	Symantec Corporation - Client and Host Security Platform	104.0.8.3

	Microsoft ® .NET Framework	1.1.4322.573
	Microsoft ® Windows Script Host	5.6.0.8820
	Microsoft Application Error Reporting	11.0.5515
	Power DvD	
	Reproductor de Windows Media de Microsoft®	

Tabla #30. Software Ilegal en los Departamentos Auditados

6.6.5.5.3. POR ADQUIRIR

Symatec Antivirus es el software que utiliza el MIES- INFA para la protección de virus, sería factible para la institución adquirir otro antivirus tomando en cuenta las características de los computadores ya que el utilizado actualmente ocupa demasiado espacio ocasionando que los equipos se tornen lentos.

6.6.5.5.4. POR ELIMINAR

Los programas que utiliza la mayoría de funcionarios de la institución son los básicos, como procesadores de textos, hojas de cálculo, lectores pdf, presentaciones power point, etc. que son necesarios para el desempeño de sus labores cotidianas lo que se debería eliminar son las aplicaciones descargadas vía internet que en muchos de los casos son para uso personal.

6.6.5.5.5. GRAFICA COMPARATIVA DE SOFTWARE LEGAL E ILEGAL

Las graficas que se muestran a continuación representan el número total de software instalado en cada departamento incluyéndose allí software que ha sido instalado sin autorización del departamento de tecnología.

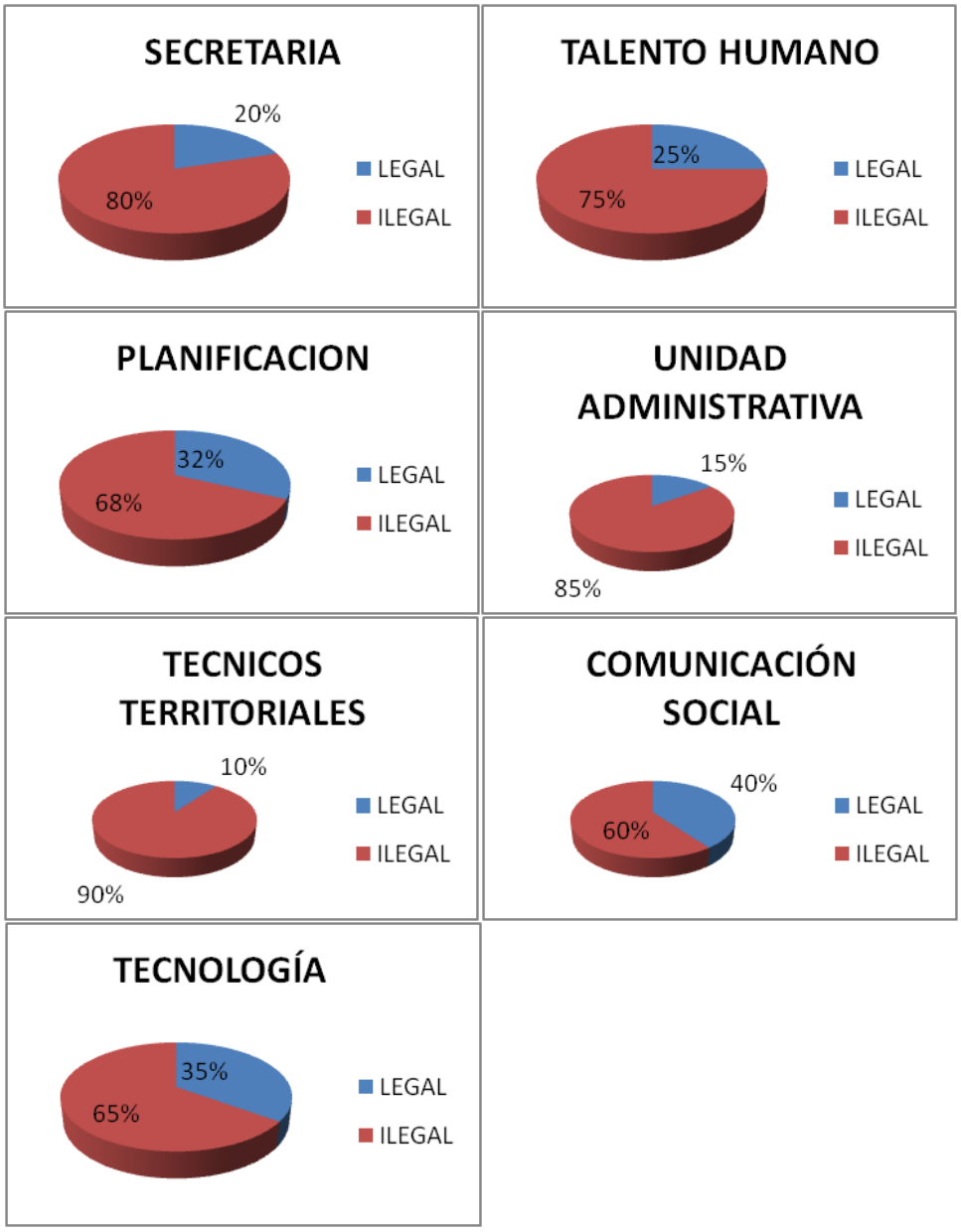
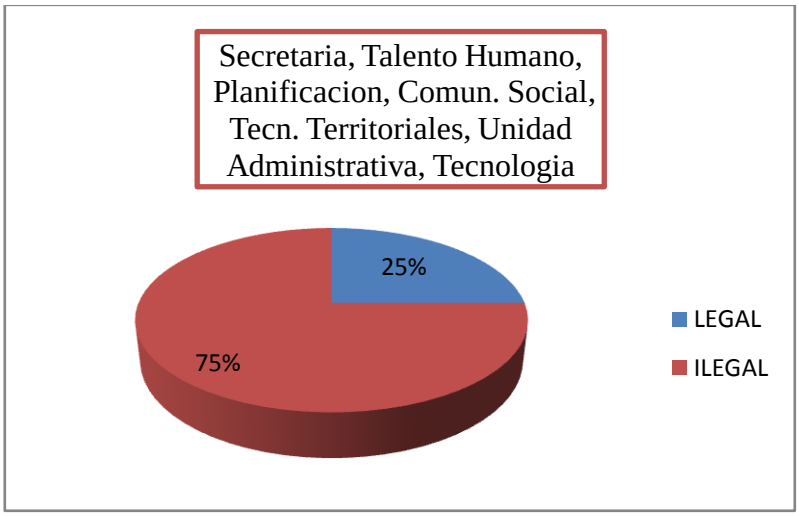


Grafico # 20. Grafica comparativa Software legal e Ilegal de los Departamentos Auditados**.**

6.6.5.5.5.1. ESQUEMA GENERAL DE SOFTWARE LEGAL E ILEGAL



Grafica # 21. Esquema general de Software Legal e Ilegal de los Deptos. Auditados

ANALISIS DEL SOFTWARE LEGAL E ILEGAL

En el gráfico anterior podemos observar que él 25% de software utilizado por la institución es legal, y que la parte restante que corresponde al 75% está constituido por software ilegal, cabe recalcar que existe software instalado sin autorización que en su mayoría es de uso personal lo que ha contribuido el aumento de software no legal.

Conclusión

El software es una herramienta indispensable de trabajo para cualquier empresa o institución, sea ésta grande o pequeña, facilitando el trabajo a los usuarios por lo que es necesario administrarlo de la mejor manera, ya que instalar o usar copias no autorizadas de programas puede acarrear consecuencias muy costosas como por ejemplo:

- No poseer soporte Técnico

- No tener garantías del programa
- No contar con un software confiable
- Riesgos de perder información importante
- no contar con manuales de usuario, etc.

6.6.5.5.6. COMUNICACIONES

6.6.5.5.6.1. INVENTARIO HARDWARE

SERVIDORES				
DESCRIPCIÓN		**CÓDIGO**	**MARCA**	**SERIE**
COMP PROLIANT M1370 G2 MODULO COMP 256MG		07-01-004-0023	COMPAQ	D221RF51DO17
COMPUTADOR CENTRAL		07-01-004-0022	COMPAQ	D105FRY1LO86
COMPUTADOR CENTRAL		07-01-004-0024	HP	USMG3702NT
FIREWALL.- FIREWALL		07-01-012-0059	SYMANTEC 320	
ROUTER.- ROUTER		07-01-019-0072	SYSTEMS	CI500
SECRETARIA				
Laura Barrera	Difusor De Señãles De Red	07-01-008-0055	D-LINK	P1F1178005673
TALENTO HUMANO				
Grisca Terán	Difusor De Señãles De Red	01-06-009-0138	D-LINK	D1F1178005667
Verónica Tamayo	Difusor De Señales De Red	07-01-008-0057	ADVANTEK	0529A3A00840
	SERVIDOR DE IMPRESORA.- OTROS	01-06-022-0162	D-LINK	F40W167500745
PLANIFICACION				

Luis Auz	Difusor De Señãles De Red	07-01-008-0056	BUT	GRO601017339
UNIDAD ADMINISTRATIVA				
DIFUSOR DE SEÑÃLES DE RED		01-06-009-0139	D-LINK	D1F1178005654
TECNICOS TERRITORIALES				
Rosa Freire Víctor Escobar Luis Barrera	SWITCH.-DISPOSITIVO ACTIVO (8 PUERTOS)	01-06-023-0134	3COM	3C17300A
TECNOLOGÍA				
Catherine Analuisa	SWITCH.-DISPOSITIVO ACTIVO (8 PUERTOS)	01-06-023-0156	SWITCH	CLON

Tabla # 31. Inventario de Hardware con respecto a Comunicaciones

6.6.5.5.6.2. INVENTARO DE SOFTWARE (SISTEMAS OPERATIVOS)

Los sistemas operativos utilizados en los departamentos auditados son: Windows 2003 Server en los servidores y Windows XP como clientes.

6.6.5.5.6.3. DIAGRAMA DE DISPOSITIVOS FÍSICOS DE LA RED

DISTRIBUCION DE IPs EN MIES-INFA TUNGURAHUA	
IPS	**ASIGNACION**
192.168.9.4	infa-innfatung.org.ec
192.168.9.25	Portatil-juanjo
192.168.9.24	home-5224364e5e

192.168.9.28	vistare2.innfatung.org.ec
192.168.9.2	aplserver9.innfatung.org.ec
192.168.9.60	administrativo.innfatung.org.ec
192.168.9.54	juridico.innfatung.org.ec
192.168.9.67	
192.168.9.62	infamb2.innfatung.org.ec
192.168.9.101	portatil_hp.innfatung.org.ec
192.168.9.106	computadora.innfatung.org.ec
192.168.9.109	prov-pi-di-003.innfatung.org.ec
192.168.9.121	usuario.innfatung.org.ec
192.168.9.123	cla-pi-di-03.innfatung.org.ec
192.168.9.124	tecnico-p-i.innfatung.org.ec
192.168.9.127	tecprovaem.innfatung.org.ec
192.168.9.150	financiero4.innfatung.org.ec
192.168.9.202	asis-direcion.innfatung.org.ec
192.168.9.203	asis-direcion.innfatung.org.ec
192.168.9.200	ori-9e8ba851ded.innfatung.org.ec
192.168.9.205	des-infantilut.innfatung.org.ec
192.168.9.209	ori-tb11.innfatung.org.ec

192.168.9.207	coloso.innfatung.org.ec
192.168.9.211	ori-tb58.innfatung.org.ec
192.168.9.215	infajuridico1.innfatung.org.ec
192.168.9.222	cla-pi-pe-05.innfatung.org.ec
192.168.9.233	dpt-infatun02.innfatung.org.ec
192.168.9.254	
192.168.9.250	

Tabla # 32. Asignaciones IP de la Institución.

6.6.5.5.7. SEGURIDADES

En cuanto a seguridades se dispone de Firewall Synmatec actualizando automáticamente el Antivirus a todos los Equipos de la institución.

Con respecto al manejo de usuarios y contraseñas se los realiza vía servidor de dominio en Windows Server 2003 con Active Directory dhcp y dns.

6.6.5.5.8. GESTION Y ADMINISTRACION

El mantenimiento y soporte técnico de los ordenadores a los funcionarios lo realiza el asistente de la información Tecnóloga. Catherine Analuisa quien es la persona que brinda el apoyo necesario al personal de la institución con el fin de permitirle a los mismos el mejor desempeño en las labores que se realizan.

La creación de usuarios y contraseñas por medio de dominios Windows Server 2003, estaba a cargo del analista de Tecnología de la Información Ing. Juan José Ninahualpa quien ya no se encuentra laborando en la institución hace 1 año y medio quien era responsable de permitir la utilización de los servicios como Internet, Correo electrónico y otros programas propios de la institución así como manejo de roles,

permisos y monitoreo y de igual manera brindaba apoyo técnico a los funcionarios mediante capacitaciones sobre programas adquiridos, actualizaciones en los sistemas provenientes desde la matriz Quito.

6.6.5.6. SISTEMAS INFORMACIÓN

6.6.5.6.1. SISTEMAS

En cuanto a las aplicaciones informáticas que maneja la institución son cuatro se detallara brevemente ya que estos sistemas son centralizados desde la matriz ubicada en Quito y parte del área no auditable:

SIPI (Sistema de Información de Protección Integral).- básicamente es un aplicativo Web que permite el manejo de información de los centros controlados por el MIES-INFA Tungurahua como por ejemplo:

- Seguimientos de los niños beneficiados en Guarderías MIES- INFA
- Asistencia de Niños/as que son atendidos en las guarderías MIES- INFA
- Ingreso e impresión de niños al sistema según la ubicación del centro a nivel provincial.
- Ingresos e impresión de Pesos y Tallas (niños/as que son atendidos y realizar controles mensuales)
- Ingresos Test de Nelson (controla el nivel de motricidad de los Niños/as)
- Convenios (registra convenios realizados con otras instituciones)
- Creación de Unidades (crea las nuevas unidades para atención de los niños presentando la respectiva documentación requerida para ello)
- Realiza reportes mensuales de asistencias que luego son registradas en departamento financiero para que cada centro reciba mensualmente los recursos económicos dotados por el estado.

SINDI.- es un sistema vía Web en el cual se registra y permite la autorización de centros privados Guarderías para cuidado de los niños.

QUIPUX.-es el sistema de gestión de documentos que es manejado por la mayoría de instituciones públicas que permite el envió y recepción de documentos tales como: memos, solicitudes, oficios a través de la web siendo utilizado dentro y fuera de la institución.

OLYMPO.- este sistema registra los activos fijos de la institución, este a la vez realiza el inventario donde se especifica a detalle el bien inmueble de cada funcionario, hay que mencionar que este sistema estaba a cargo del anterior analista de tecnología quien realiza los ingresos a partir de su salida paso el sistema a manos de la unidad administrativa donde nos indicaron que al hacer el cambio de custodio a los bienes inmuebles en el sistema este duplica los datos en la Base de Datos dando como reportes erróneos.

6.6.5.6.1.1. ANTIGÜEDAD

APLICACION	AÑO INSTALACION	HERRAMIENTA QUE FUE DESARROLLADA
SIPI	JUNIO 2009	PHP
SINDI	OCUBRE 2009	JAVA
QUIPUX	ABRIL 2010	PHP
OLYMPO	FEBRERO 2010	VISUAL BASIC Y SQL SERVER

Tabla # 33. Antigüedad de las aplicaciones adquiridas

6.6.5.6.1.2. COMPLEJIDAD

SIPI, SINDI, QUIPUX, OLYMPO.- Estos sistemas no son complejos para los usuarios que lo manejan, consiste en logearse con un nombre de usuario y contraseña dependiendo del rol que desempeñen cada funcionario aparecerán menús diferentes para cada uno.

ANÁLISIS DE LOS SISTEMAS DE INFORMACIÓN

Los sistemas de información SIPI y SINDI utilizados por la institución a través de la web están centralizados en la matriz que se encuentra en Quito de donde se realizan actualizaciones periódicas a medida de la necesidad de la institución central, el problema surge cuando se produce algún fallo en la matriz o alguna actualización la pagina donde se encuentran dichos sistemas se tornan lentos o en el peor de los casos se cae el sistema la cual imposibilita el trabajo que realizan los técnicos de campo.

Por otra parte dichos sistemas de información poseen un usuario y una contraseña para poder logearse e ingresar donde se puede observar que los funcionarios:

- Poseen contraseñas no complejas.
- No realizan cambio de contraseñas de manera constante.

De tal manera que el acceso a los sistemas no son complejos y se puede suscitar la infiltración de terceros y tomar información importante.

Con respecto al programa de inventarios OLYMPO manejado por la unidad administrativa de la institución posee errores tanto de ingreso como también de procesos internos, como por ejemplo se puede mencionar que la digitación de los códigos de cada activo se lo transcribió erróneamente por la persona encargada y no se ha corregido todavía, y al realizar el cambio de custodio del bien inmueble este se registra dos veces en la base la cual muestra el mismo activo a dos personas al mismo tiempo.

RECOMENDACION

- Las contraseñas al menos deben posee caracteres tanto alfanuméricos con especiales.
- Las claves deben ser cambiadas al menos cada mes para evitar accesos de personas ajenas.

- Corregir errores de digitación en los activos fijos para evitar confusiones.
- Informar a la matriz acerca de la duplicidad de los datos en la base para que se tomen las medidas correspondientes en el sistema de inventarios.
- Capacitar al personal a cargo del sistema de inventarios para que la información se registre de manera correcta.

6.6.5.6.2. DOCUMENTACIÓN

Se puede mencionar que si existen manuales de usuario para manejo de los sistemas informáticos estos se hallan en la página de la institución www.infa.gov.ec/micasa en donde se detalla paso a paso con utilizar las herramientas que posee la entidad.

6.6.6. FASE VI

FRECUENCIA DE LA AUDITORIA

Durante la trayectoria de la organización, no se ha planificado la realización de una auditoria informática, ya que por falta de recursos económicos y tiempo no se ha podido realizar los estudios para una auditoria profunda.

6.6.7. FASE VII

PLANES Y PROGRAMAS DE TRABAJO

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Auditoria Informatica**	**63 días**	**lun 18/06/12**	**mié 12/09/12**	
2	Conformacion del Equipo Auditor	1 día	lun 18/06/12	lun 18/06/12	
3	Definicion del Alcance y Objetivos	2 días	mar 19/06/12	mié 20/06/12	2
4	Tramites en la Institucion	8 días	jue 21/06/12	lun 02/07/12	3
5	Formalizacion de la Auditoria en la Institucion	3 días	mar 03/07/12	jue 05/07/12	4
6	Elaboracion del Cronograma de Actividades	5 días	vie 06/07/12	jue 12/07/12	5
7	**Evaluacion del Control Interno Informatico**	**6 días**	**vie 13/07/12**	**vie 20/07/12**	
8	Recopilacion de la informacion de la Institucion	1 día	vie 13/07/12	vie 13/07/12	6
9	Analisis del Informe de la Institucion	1 día	lun 16/07/12	lun 16/07/12	8
10	Recopilacion de la Informacion Operacional	2 días	mar 17/07/12	mié 18/07/12	9
11	Analisis de la Informacion Operacional	2 días	jue 19/07/12	vie 20/07/12	10
12	Recopilacion de Informacion Detallada	2 días	jue 26/07/12	vie 27/07/12	11
13	Analisis de la Informacion Detallada	2 días	lun 30/07/12	mar 31/07/12	12
14	Definicion de Areas Criticas	3 días	mié 01/08/12	vie 03/08/12	13
15	Elaboracion de la Carta a la Gerencia	2 días	jue 23/08/12	vie 24/08/12	14
16	Elaboracion del Informe Final	2 días	lun 27/08/12	mar 28/08/12	15
17	Revision del Borrador del Proyecto	5 días	mié 29/08/12	mar 04/09/12	16
18	Correccion del Borrador del Proyecto	3 días	mié 05/09/12	vie 07/09/12	17
19	Revision del Proyecto	3 días	lun 10/09/12	mié 12/09/12	18
20	Presentacion del Proyecto	1 día	lun 17/09/12	lun 17/09/12	19

Grafico # 22. Diagrama de Gantt

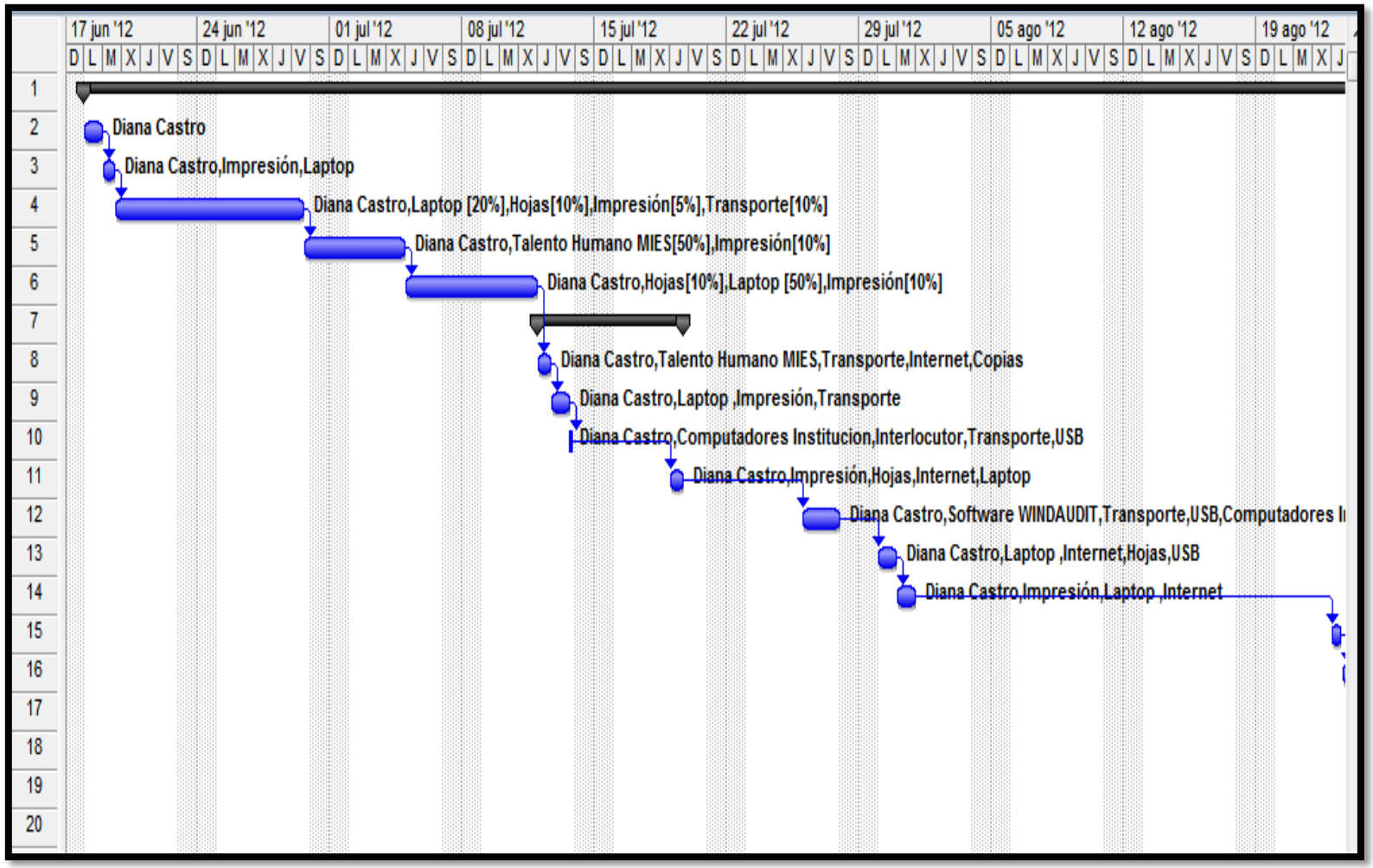


Grafico # 23. Diagrama de Gantt seguimiento

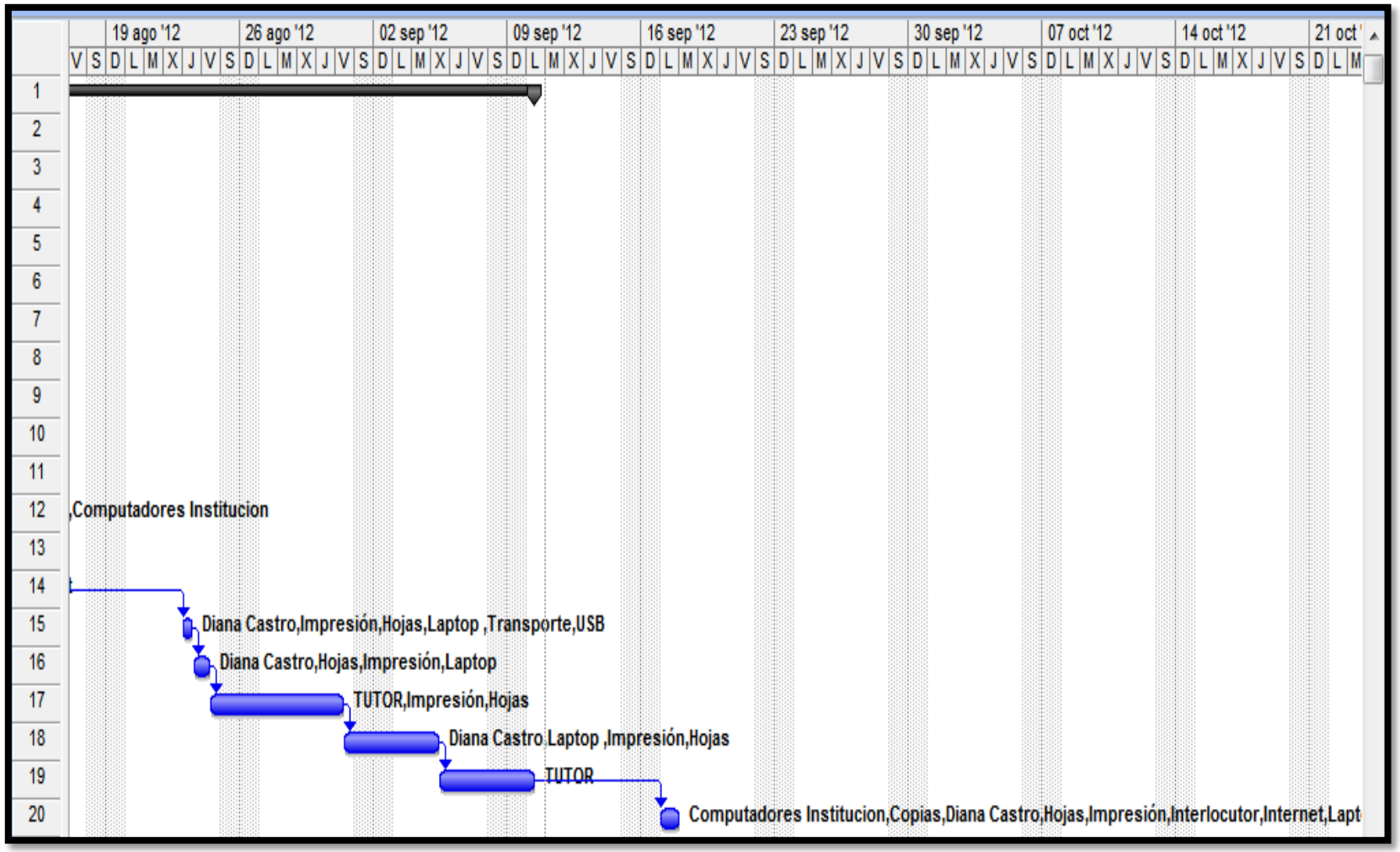


Grafico # 24. Diagrama de Gantt de seguimiento continuación

CRONOGRAMA MIES-INFA TUNGURAHUA

	17/06/12	24/06/12	01/07/12	08/07/12	15/07/12	22/07/12	29/07/12	05/08/12
Auditoria Informatica	$ 40,00	$ 40,00	$ 40,00	$ 40,00	$ 40,00	$ 40,00	$ 40,00	$ 40,00
Conformacion del Equipo Auditor	$ 8,00							
Definicion del Alcance y Objetivos	$ 10,72							
Tramites en la Institucion	$ 6,43							
Formalizacion de la Auditoria en la Institucion		$ 2,67						
Elaboracion del Cronograma de Actividades			$ 8,01					
Evaluacion del Control Interno Informatico								
Recopilacion de la informacion de la Institucion				$ 6,67				
Analisis del Informe de la Institucion				$ 16,30				
Recopilacion de la Informacion Operacional				$ 1,32				
Analisis de la Informacion Operacional					$ 12,87			
Recopilacion de Informacion Detallada						$ 32,25		
Analisis de la Informacion Detallada							$ 16,02	
Definicion de Areas Criticas							$ 16,05	
Elaboracion de la Carta a la Gerencia								
Elaboracion del Informe Final								
Revision del Borrador del Proyecto								
Correccion del Borrador del Proyecto								
Revision del Proyecto								
Presentacion del Proyecto								
Total	$ 65,15	$ 42,67	$ 48,01	$ 64,29	$ 52,87	$ 72,25	$ 72,07	$ 40,00

Grafico # 25. Flujo de caja

CRONOGRAMA MIES-INFA TUNGURAHUA

	12/08/12	19/08/12	26/08/12	02/09/12	09/09/12	16/09/12	23/09/12	**Total**
Auditoria Informatica	$ 40,00	$ 40,00	$ 40,00	$ 40,00	$ 2,00			$ 482,00
Conformacion del Equipo Auditor								$ 8,00
Definicion del Alcance y Objetivos								$ 10,72
Tramites en la Institucion								$ 6,43
Formalizacion de la Auditoria en la Institucion								$ 2,67
Elaboracion del Cronograma de Actividades								$ 8,01
Evaluacion del Control Interno Informatico								
Recopilacion de la informacion de la Institucion								$ 6,67
Analisis del Informe de la Institucion								$ 16,30
Recopilacion de la Informacion Operacional								$ 1,32
Analisis de la Informacion Operacional								$ 12,87
Recopilacion de Informacion Detallada								$ 32,25
Analisis de la Informacion Detallada								$ 16,02
Definicion de Areas Criticas								$ 16,05
Elaboracion de la Carta a la Gerencia		$ 8,32						$ 8,32
Elaboracion del Informe Final		$ 12,07						$ 12,07
Revision del Borrador del Proyecto		$ 0,07						$ 0,07
Correccion del Borrador del Proyecto			$ 12,07	$ 36,00				$ 48,07
Revision del Proyecto								
Presentacion del Proyecto						$ 24,34		$ 24,34
Total	$ 40,00	$ 60,46	$ 52,07	$ 76,00	$ 2,00	$ 24,34		$ 712,17

Grafico # 26. Flujo de caja

RESUMEN DEL PROYECTO

Fechas			
Comienzo:	lun 18/06/12	Fin:	lun 17/09/12
Comienzo previsto:	NOD	Fin previsto:	NOD
Comienzo real:	NOD	Fin real:	NOD
Variación de comienzo:	0 días	Variación de fin:	0 días

Duración			
Programada:	66 días?	Restante:	66 días?
Prevista:	0 días?	Real:	0 días
Variación:	66 días?	Porcentaje completado:	0%

Trabajo			
Programado:	1.188,67 horas	Restante:	1.188,67 horas
Previsto:	0 horas	Real:	0 horas
Variación:	1.188,67 horas	Porcentaje completado:	0%

Costos			
Programados:	$ 712,17	Restantes:	$ 712,17
Previstos:	$ 0,00	Reales:	$ 0,00
Variación:	$ 712,17		

Estado de las tareas		Estado de los recursos	
Tareas aún no comenzadas:	20	Recursos de trabajo:	12
Tareas en curso:	0	Recursos de trabajo sobreasignados:	1
Tareas finalizadas:	0	Recursos materiales:	0
Total de tareas:	20	Total de recursos:	13

Gráfico #23. Resumen del Proyecto

6.6.8. FASE VIII

REVISIÓN DE CONTROLES Y EVALUACION DE SEGURIDADES

6.6.8.1. TECNICA Y HERRAMIENTAS DE AUDITORIA INFORMATICA

La encuesta para Controles y seguridades de los Departamentos Auditados en el MIES –INFA Tungurahua es la herramienta utilizada para recolectar la información necesaria en el proceso de Auditoria Informática.

Además tanto para seguridades lógicas como Físicas se utilizó la observación para su verificación en los distintos departamentos y a través del uso de la herramienta WINDAUDIT se realizó el levantamiento del Inventario tanto de Hardware como de Software.

6.6.8.2. RECOPILACION DE INFORMACION DETALLADA

6.6.8.2.1. CONTROL Y SEGURIDADES DE LA ESTRUCTURA ORGANIZACIONAL DE LOS DEPARTAMENTOS

6.6.8.2.1.1. OBJETIVO

Para lograr el objetivo de evaluar los controles y seguridades de la estructura organizacional, facilitando los documentos, manuales y la estructura de cada departamento del MIES – INFA Tungurahua.

Este cuestionario contendrá información esencial sobre la estructura orgánica, funciones, objetivos y políticas administrativas.

6.6.8.2.1.2. CUESTIONARIO Y TABULACION

1. ¿La estructura actual es óptima para que se realicen con eficiencia las funciones encomendadas?

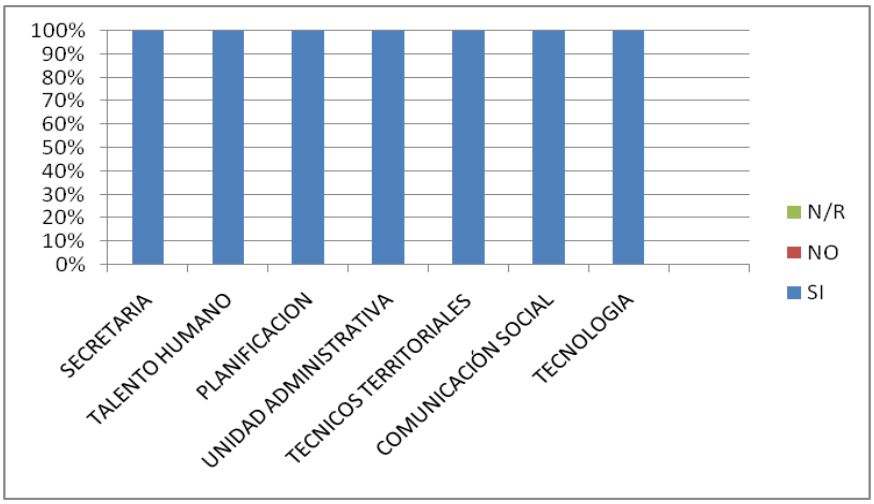


Grafico # 24. Estructura optima para realizar funciones.

2. ¿De acuerdo a la estructura jerárquica de la institución se tiene una adecuada comunicación entre los diferentes departamentos?

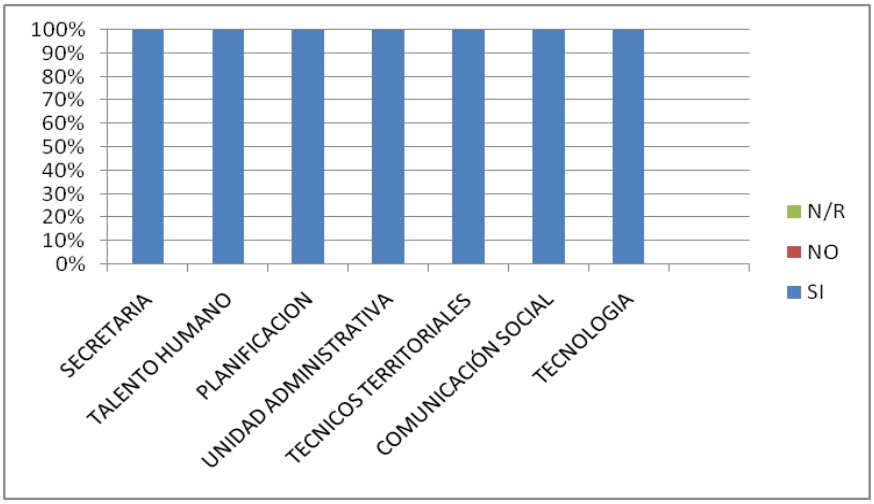


Grafico # 25. Comunicación entre departamentos.

3. ¿Cada departamento tiene establecidas sus responsabilidades?

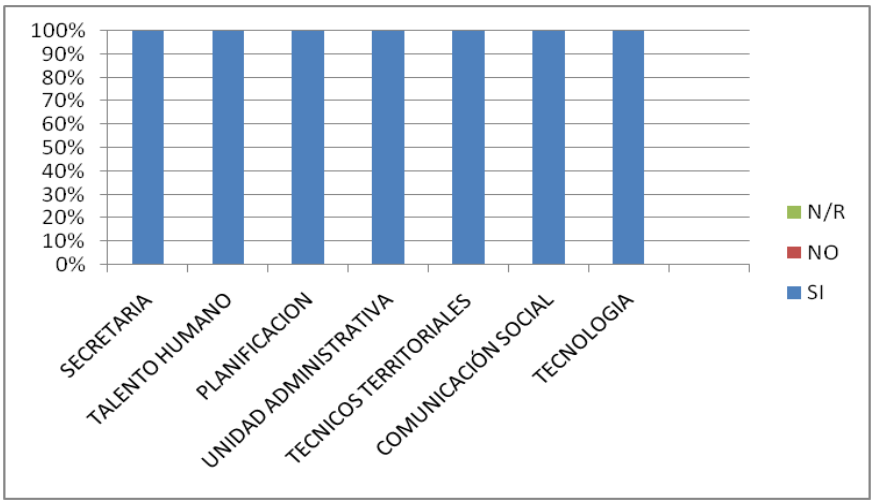


Grafico # 26. Responsabilidades Establecidas

4. ¿Los puestos de trabajo van acorde a los departamentos para realizar sus funciones?

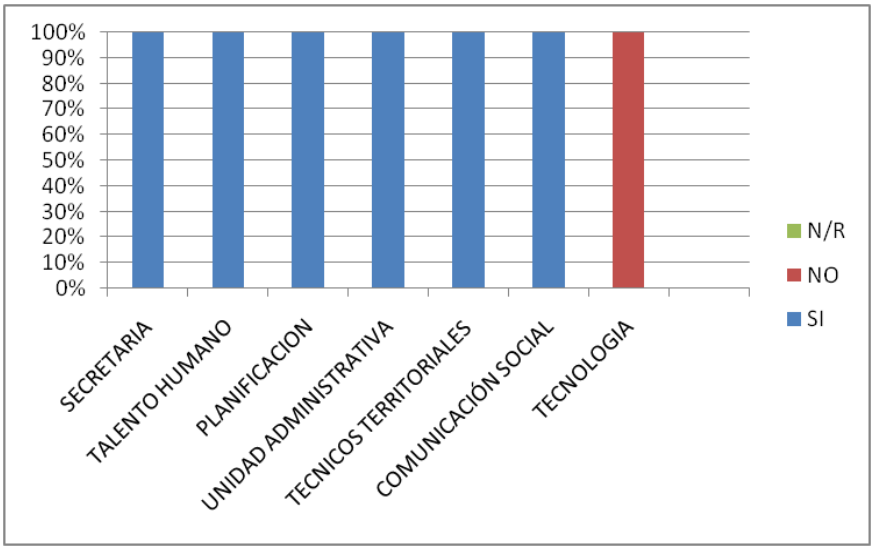


Grafico # 27. Puestos acorde a los departamentos.

5. ¿Se encuentran establecidas en algún documento funciones de cada departamento?

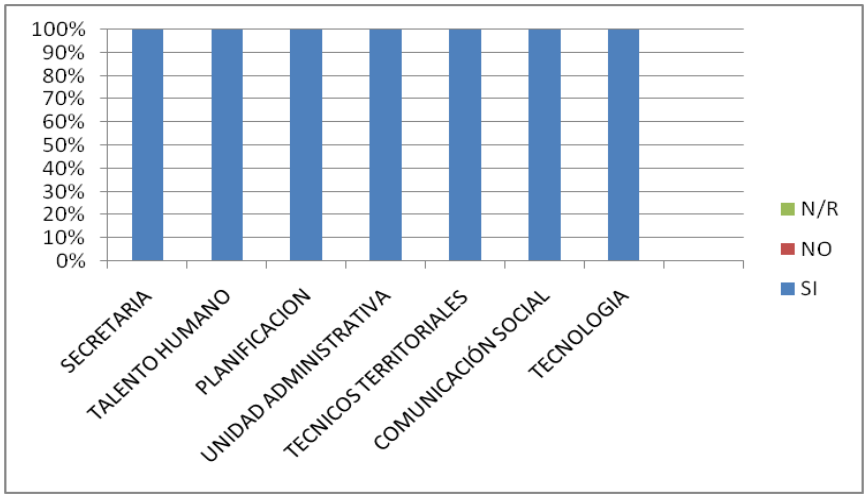


Grafico # 28. Funciones establecidas en documentos.

6. ¿El personal de cada departamento participa en la elaboración de funciones?

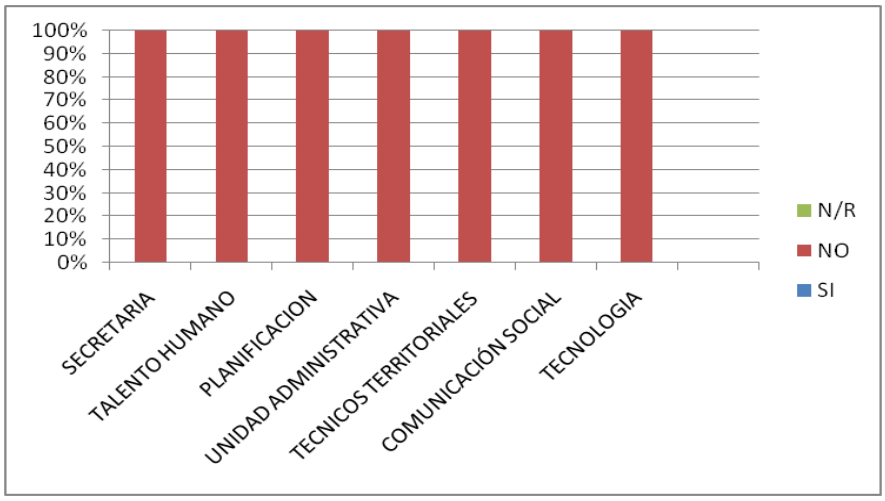


Grafico # 29. Participación del Personal en creación de funciones

7. ¿En caso de no encontrarse el jefe, un miembro inmediato puede realizar sus funciones?

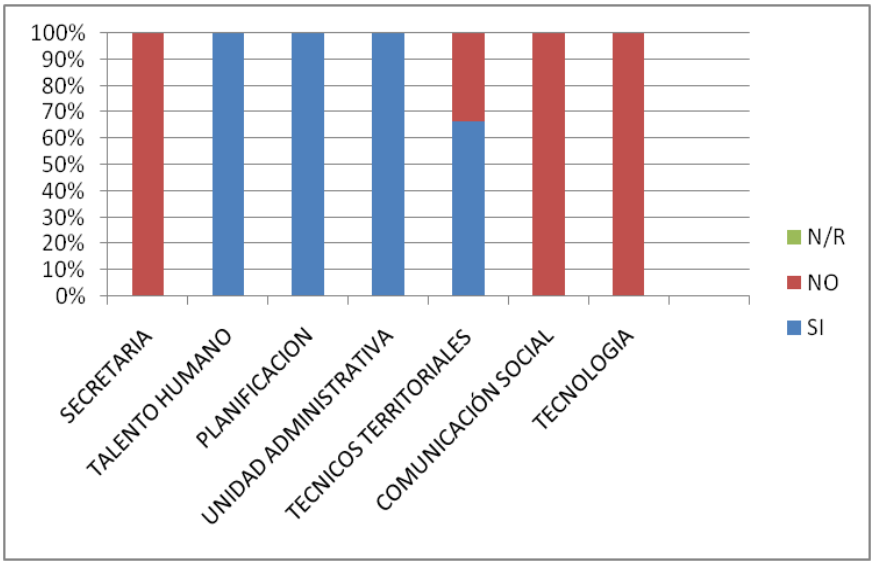


Grafico # 30. Pregunta #7

8. ¿Para cumplir sus funciones se requiere apoyo de otras aéreas?

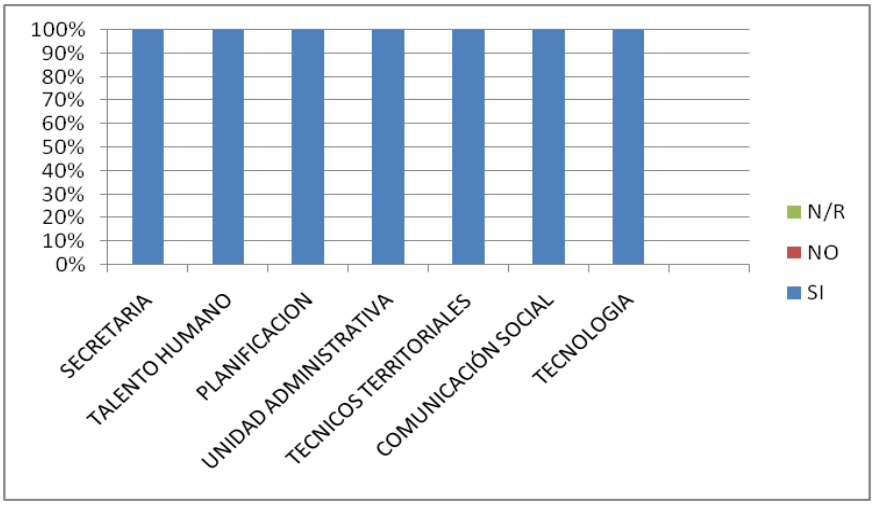


Grafico # 28. Apoyo de otras aéreas para cumplir funciones

9. ¿Se deja de realizar alguna actividad por falta de personal del departamento?

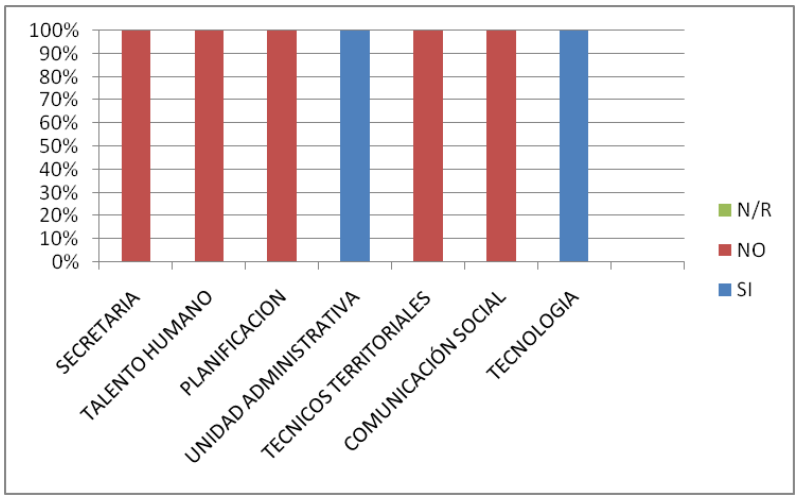


Grafico # 31. Actividades no realizadas por falta de personal.

10. ¿Se da cumplimiento por parte del personal con las políticas, normas y procedimientos establecidos en los departamentos?

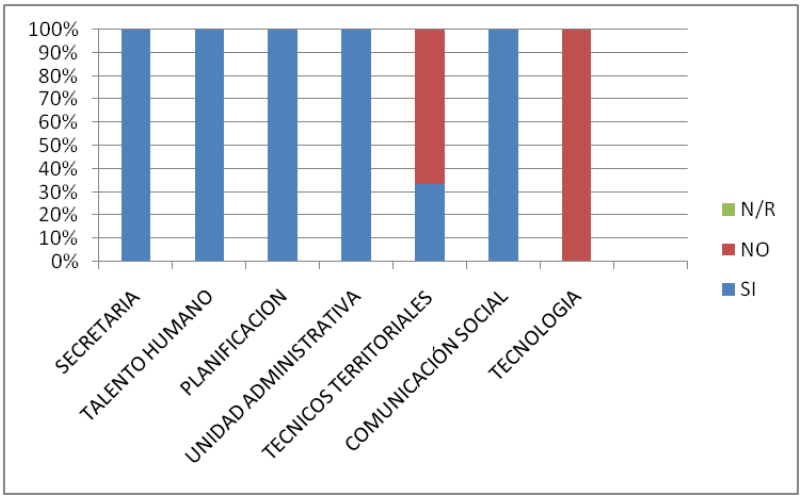


Gráfico # 32. Cumplimiento de normas por parte del personal en cada área.

11. ¿Existen políticas de seguridad cuando se termina la relación laboral con el funcionario?

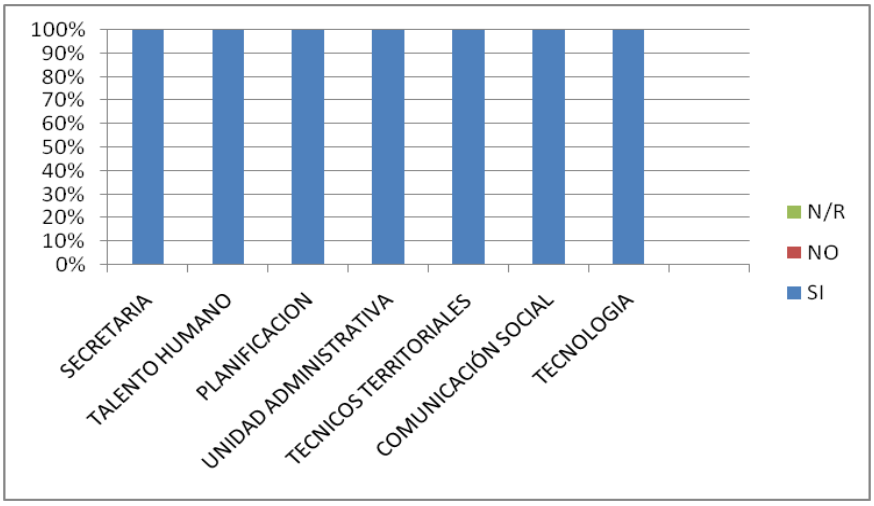


Grafico # 33. Políticas de seguridad cuando termina relación laboral.

12. ¿Se adapta el personal al mejoramiento administrativo del Área?

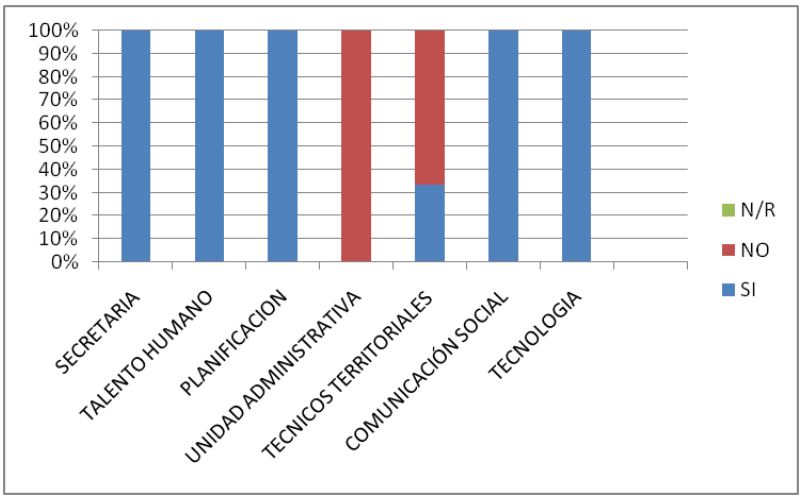


Gráfico # 34. Adaptabilidad ante mejoras administrativas.

13. ¿Conoce el personal el reglamento interno de trabajo del área?

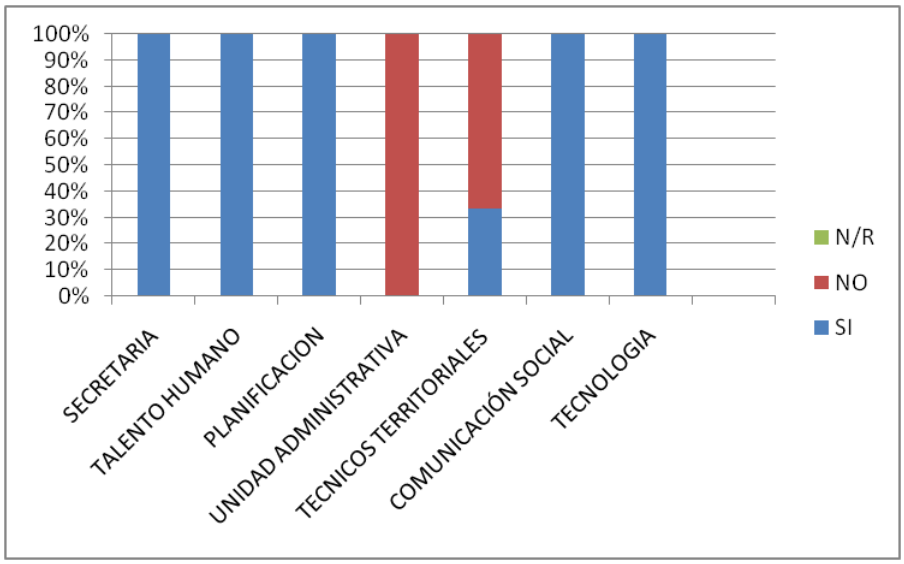


Grafico # 35. Conocimiento del reglamento.

14. ¿Posee el departamento algún plan de selección de personal?

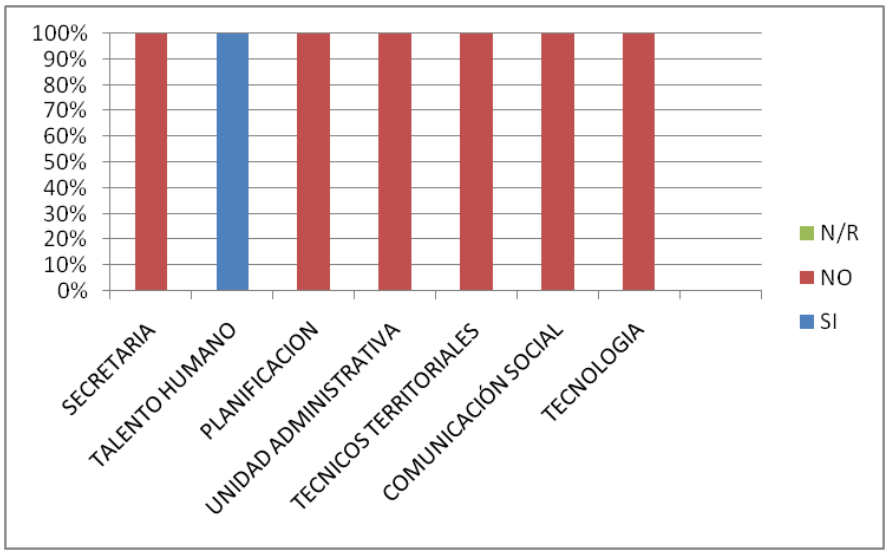


Grafico # 36. Plan para selección de personal

CONCLUSION

- Cada departamento tiene establecidas sus responsabilidades que están basados en el Estatuto Orgánico por Proceso del MIES - INFA Nacional matriz Quito, sin embargo, en ocasiones alguna responsabilidades no son acatadas y son destinadas a otras aéreas acumulando trabajo y retrasándolo.
- El personal no participa en la elaboración de funciones debido a que las normas son enviadas del MIES – INFA de la matriz Quito.
- Se deja de realizar actividades por falta de personal sobre todo en el departamento de tecnología, debido a que solo hay una persona del área y debe prestar asesoría a otras dependencias de la institución ubicadas en otras zonas.
- La adaptabilidad con respecto a mejoras implementadas sobre todo a nivel informático no es de mucho agrado ya que es difícil sobre todo en el área de los técnicos territoriales acoplarse a nuevas herramientas.

RECOMENDACIONES

- Tanto funciones con responsabilidades son normas que ayudan al buen desempeño laboral en toda institución, por lo que se recomienda que sean acatados a cabalidad con el fin de brindar un mejor servicio y cumplir las metas de la institución.
- Si bien las normas son enviadas desde la matriz Quito, se debería elaborar funciones dentro de la institución con el fin de llevar un compromiso no solo con los compañeros de trabajo sino también con la gente que se beneficia de la labor social que brinda el MIES – INFA Tungurahua.
- En el caso del departamento de tecnología se recomienda plantear a la dirección la contratación de personal para que las funciones sean repartidas y no se acumule el trabajo a una sola persona.

- Las mejoras son necesarias y esenciales en toda institución sobre todo si es para facilitar el trabajo para los funcionarios se recomienda que se realicen capacitaciones al personal y la vez que tome iniciativa para auto prepararse en pro de mejor su nivel de conocimientos.

6.6.8.2.2. CONTROL Y SEGURIDADES FISICAS

6.6.8.2.2.1. OBJETIVO

Tomando en cuenta la norma internacional para la seguridad de información ISO/27001 / 27002 ayuda a gestionar la seguridad de la información dentro de la institución.

El objetivo es evaluar el control interno de las seguridades físicas de los departamentos auditados incluyendo el procedimiento ante desastres.

6.6.8.2.2.2. CUESTIONARIO Y TABULACION

1. **¿El departamento en el que usted trabaja tiene seguridades contra desastres?**

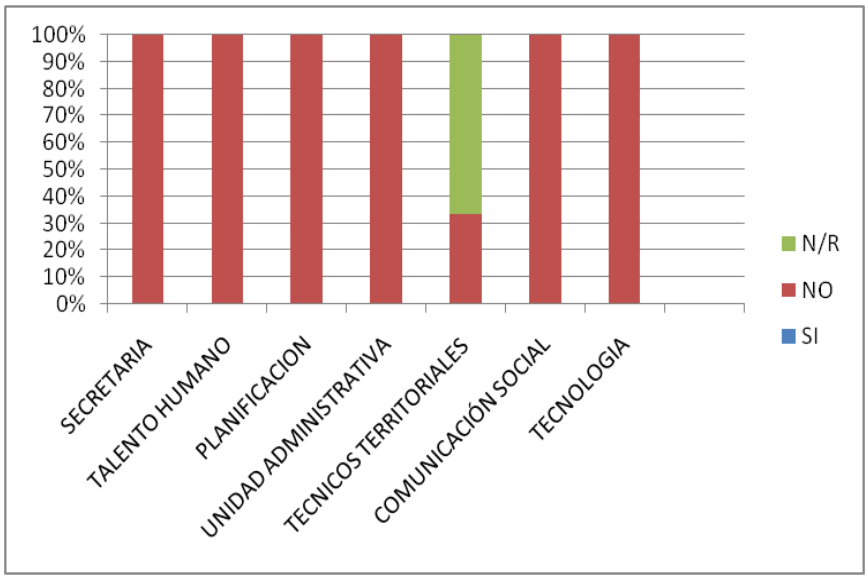


Gráfico # 37. Seguridades contra desastres

2. **¿Existe un plan de evacuación para el departamento?**

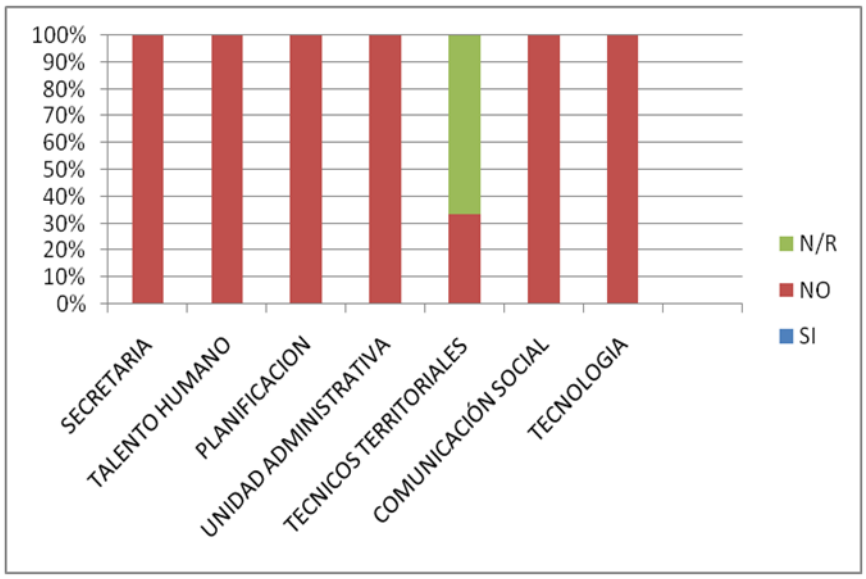


Gráfico # 38. Plan de Evacuación.

3. **¿Cuenta con Horarios fijos de entrada y de salida?**

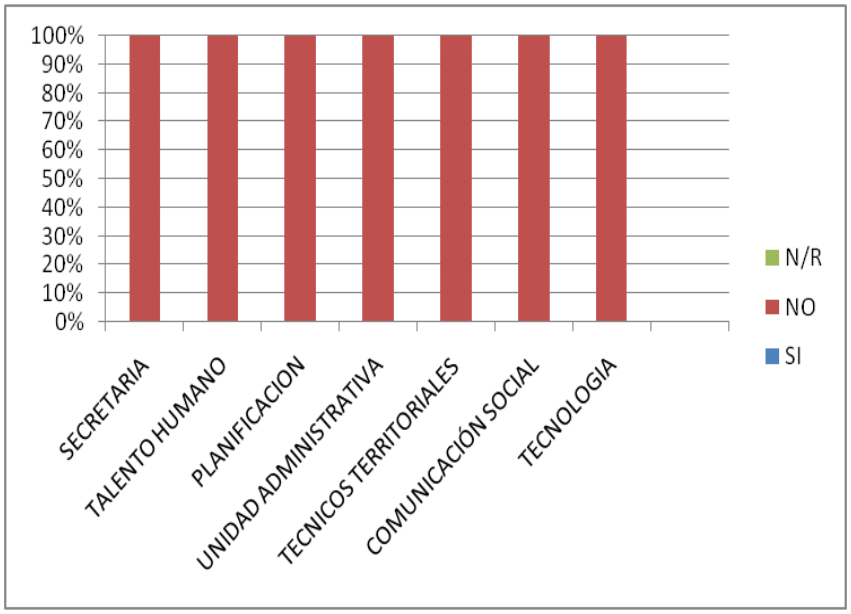


Gráfico # 39. Horarios E/S

4. **¿Se registra el acceso de personas ajenas a cada departamento?**

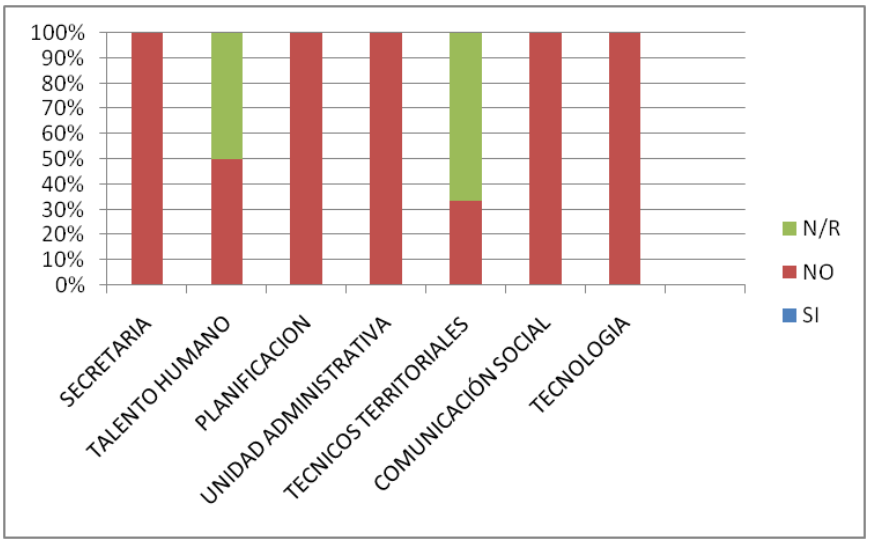


Gráfico # 40. Control de acceso.

5. **¿Existen alarmas para detectar el fuego, agua, calor o humo en forma automática?**

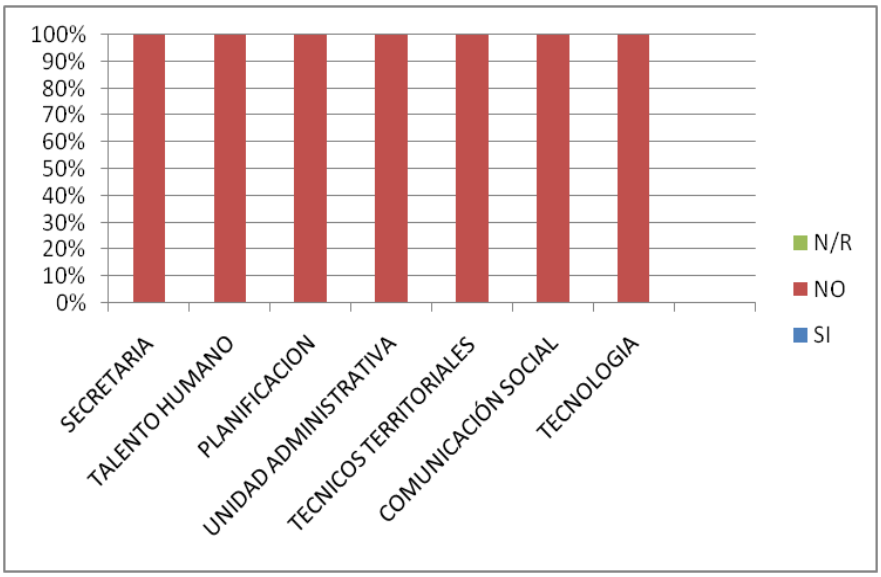


Gráfico # 41. Detección de Percances.

6. **¿Existen en el departamento extintores de fuego?**

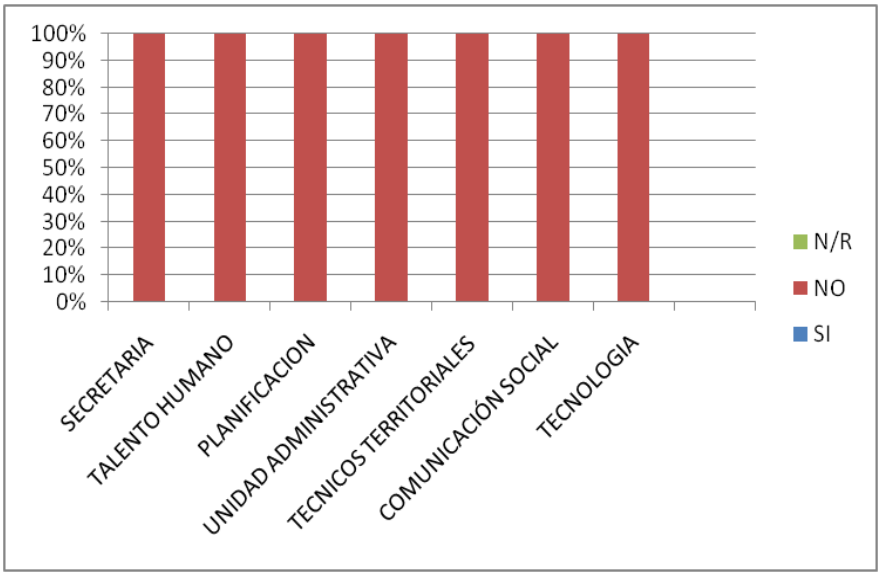


Gráfico # 42. Existencia de extintores.

7. **¿Se ha adiestrado al personal para el manejo de extintores?**

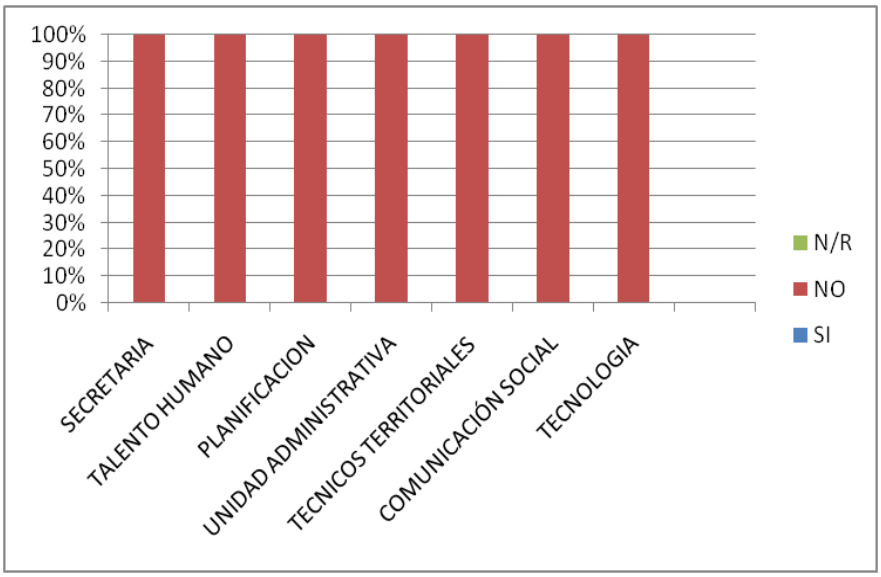


Gráfico # 43. Capacitación de Personal en el uso de Extintores.

8. **¿Los interruptores de energía eléctrica están debidamente protegidos, etiquetados, sin obstáculos para alcanzarlos?**

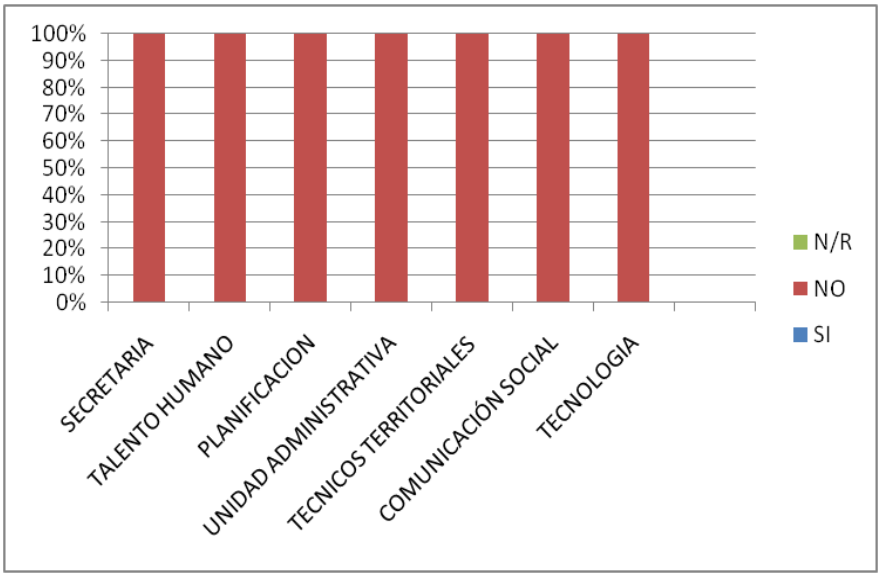


Gráfico # 44. Protección de interruptores de energía.

9. **¿Saben que hacer los funcionarios del departamento en caso de que ocurra una emergencia ocasionada por fuego?**

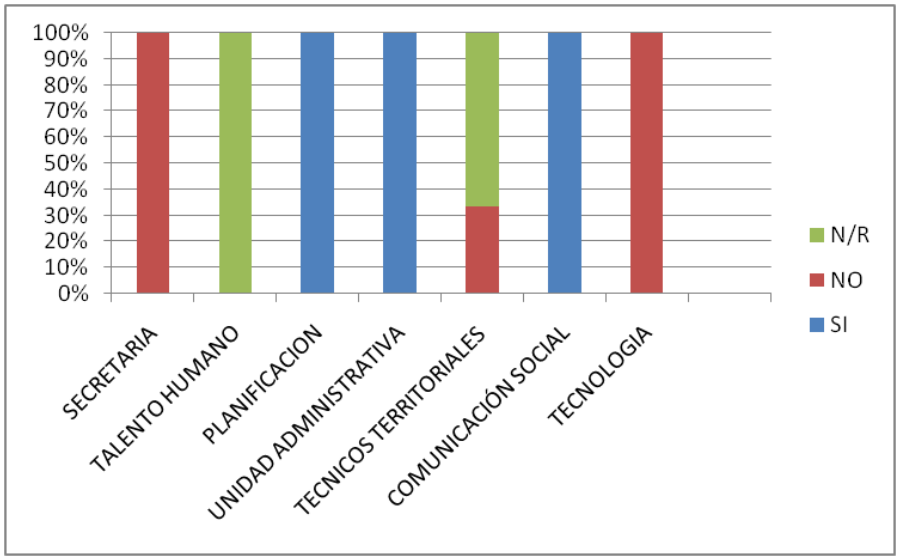


Gráfico # 45. Como actuar ante siniestros.

10. **¿Se ha adiestrado a todo el personal en la forma en que se debe desalojar las instalaciones en caso de emergencia?**

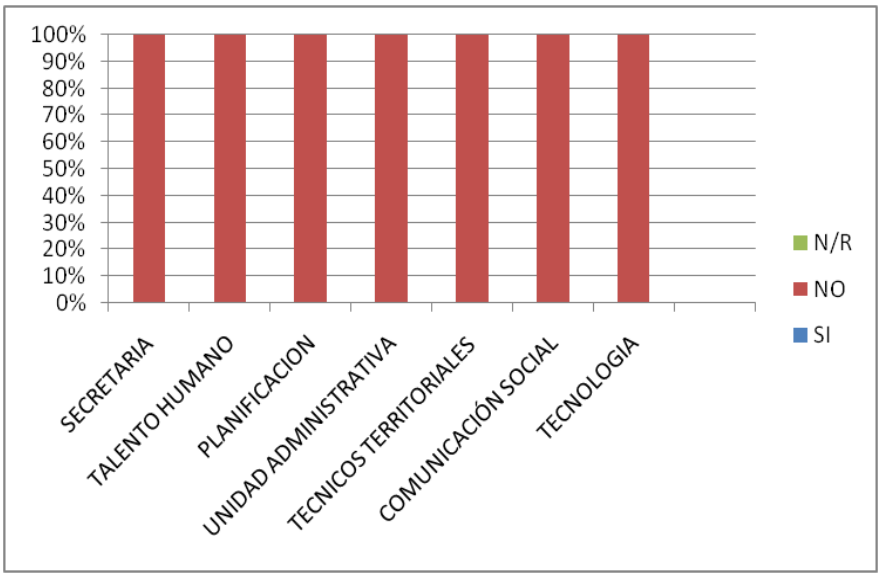


Gráfico # 46. Adiestramiento del personal ante siniestros.

11. ¿**Se hace mantenimiento periódico a los computadores?**

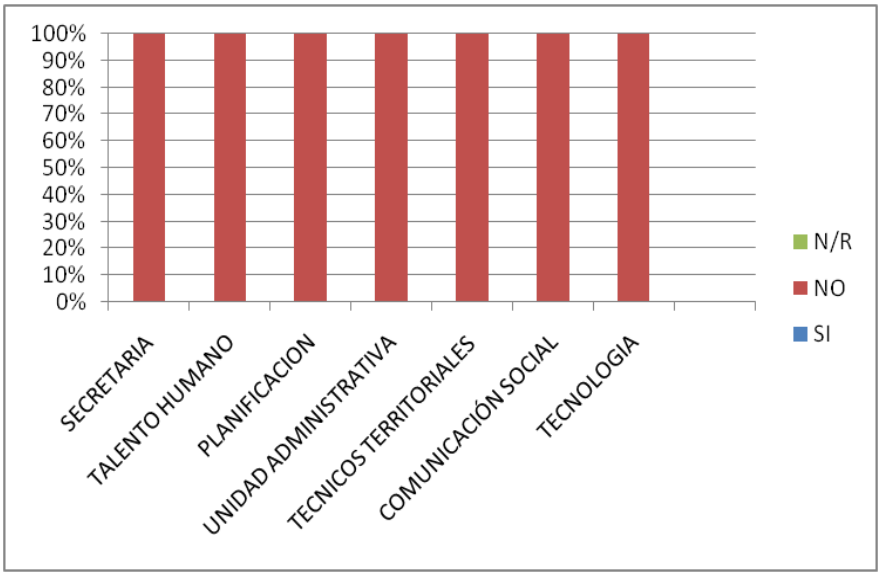


Gráfico # 47. Mantenimiento de Computadores.

12. **¿Tiene conocimiento de la existencia de un plan de contingencias?**

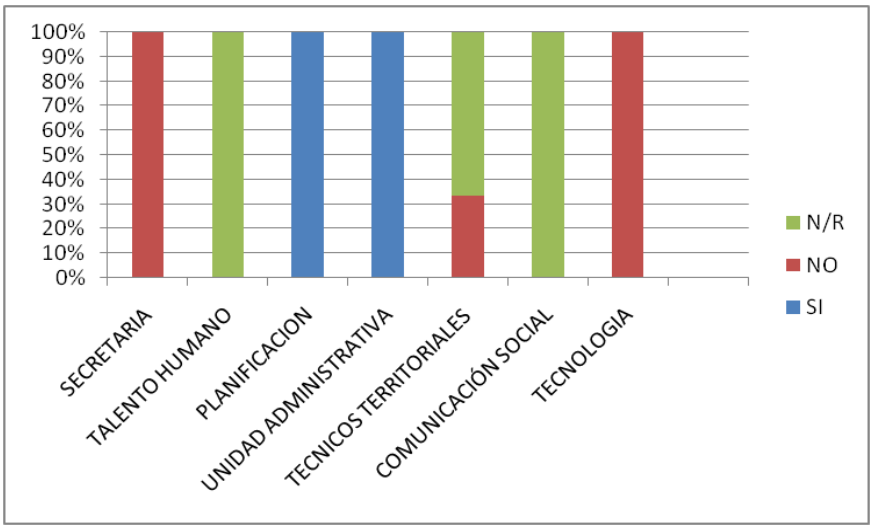


Gráfico # 48. Conocimiento de planes de contingencia.

13. **¿Los cables de red, switch, hubs, etc. se encuentran debidamente etiquetados?**

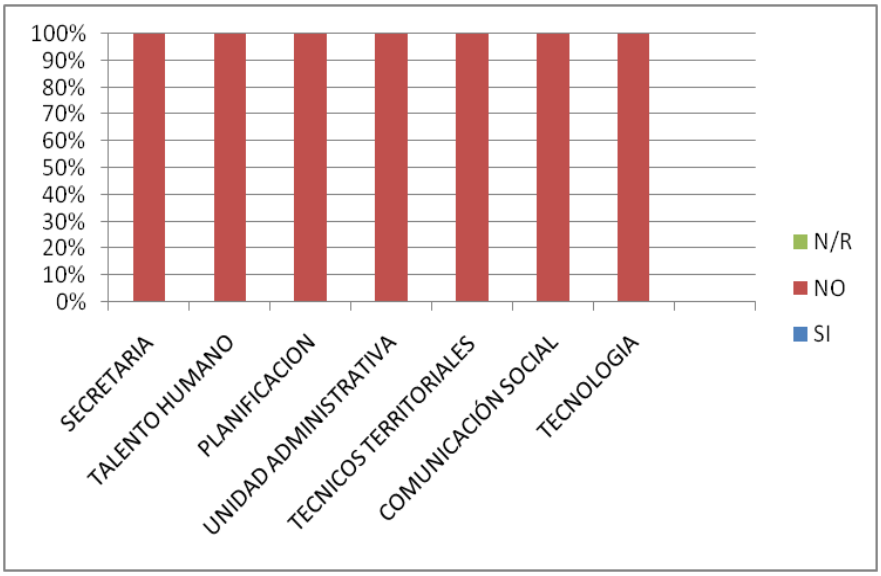


Gráfico # 49. Cableado debidamente etiquetado.

14. **¿El personal de limpieza está preparado para manipular los dispositivos informáticos?**

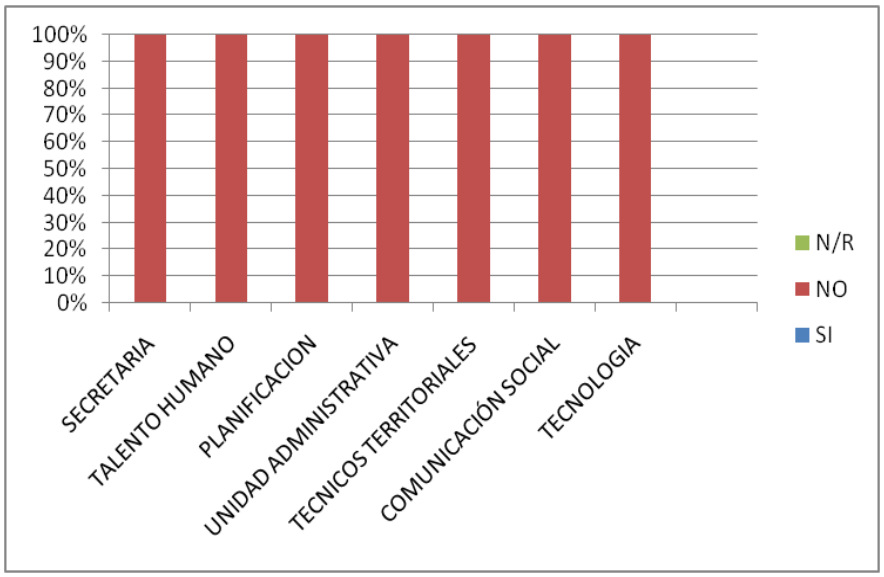


Gráfico # 50. Manipulación de dispositivos informáticos por personal de limpieza.

15. **¿Existe una persona responsable de la seguridad informática en su departamento?**

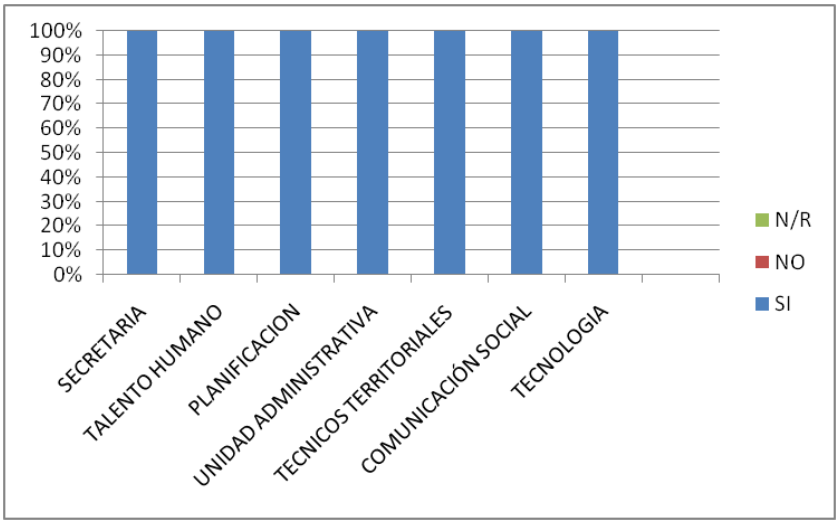


Gráfico # 51. Existencia de personal a cargo de la seguridad de la información.

CONCLUSIONES

- No existe en la institución plan de evacuación ante desastres, manejo de extintores etc. Pues no se ha presentado algún precedente todavía como para tomar medidas preventivas.
- No existe extintores en cada departamento, sino que los extintores se encuentran ubicados en cada pasillo de la institución.
- A pesar de poseer servicio de guardianía no se lleva un control de acceso de personas ajenas a cada departamento.
- El mantenimiento de computadoras no se realiza ya que el personal no abastece para realizar dicha labor.
- No existe planes de contingencia para ante cualquier eventualidad ocurrente.

RECOMENDACIONES

- Aunque no se haya suscitado en la institución algún desastre se recomienda tomar en cuenta planes de evacuación, seguridad ante desastres, capacitación a los funcionarios tanto hombres como a mujeres en manejo de extintores con el fin de salvaguardar la vida del personal y la información de la institución.
- El acceso de personas ajenas es primordial, por lo que se recomienda tomar en cuenta medidas de seguridad en cuanto al acceso de personas para evitar el robo de objetos, sabotajes informáticos e inclusive desastres provocados.
- Poseer un plan de contingencia en toda institución es un pilar fundamental por lo que se recomienda la creación del mismo con la colaboración de todo el personal que aporte con ideas que ayuden a salvaguardar la información.
- El buen funcionamiento de los equipos informáticos, se basa también en un plan de mantenimiento periódico de los mismos se recomienda elaborar dicho plan para realizar esta actividad primordial y contar con el personal suficiente para ejecutar dicha actividad para el mejor desempeño de las labores diarias de la institución.

6.6.8.2.3. SEGURIDADES LÓGICAS

6.6.8.2.3.1. OBJETIVO

El objetivo principal del Cuestionario de Seguridades Lógicas es obtener un mayor conocimiento acerca de la seguridad lógica que los usuarios utilizan para proteger a los sistemas y computadores que están a su cargo en cada departamento Auditado del MIES – INFA Tungurahua.

6.6.8.2.3.2. CUESTIONARIO Y TABULACION

1. **Si tiene algún problema informático**
   a. Usted comunica al Depto. Tecnología

   b. Lo soluciona solo.

   c. Ambos

   d. Ninguno

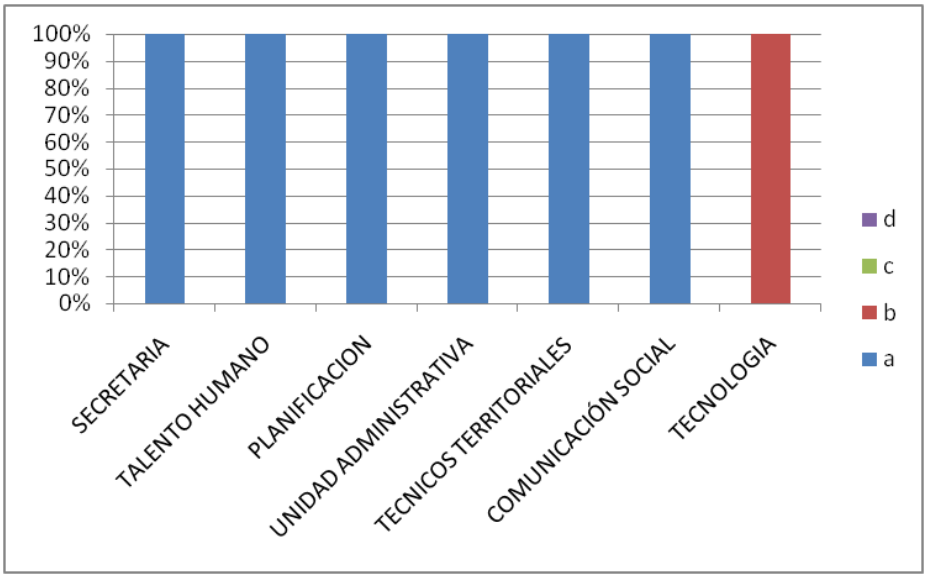


Gráfico # 52. Solución a problemas informáticos.

2. **Cuando usted abandona su lugar de trabajo**

a. Apaga el computador.

b. Coloca un ingreso de contraseña para reiniciar las actividades

c. Ninguna de las dos alternativas

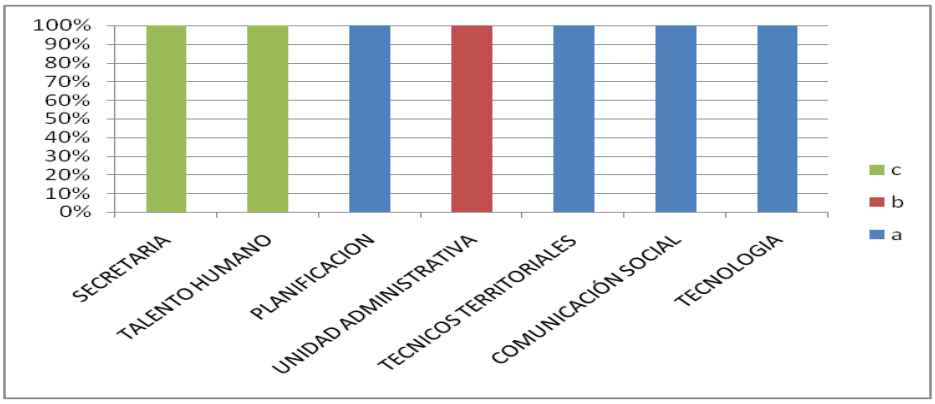


Gráfico # 53. Pregunta 2.

3. **Cada cuanto tiempo modifica la contraseña de su computador**

a. Cada semana

b. Cada mes

c. Nunca

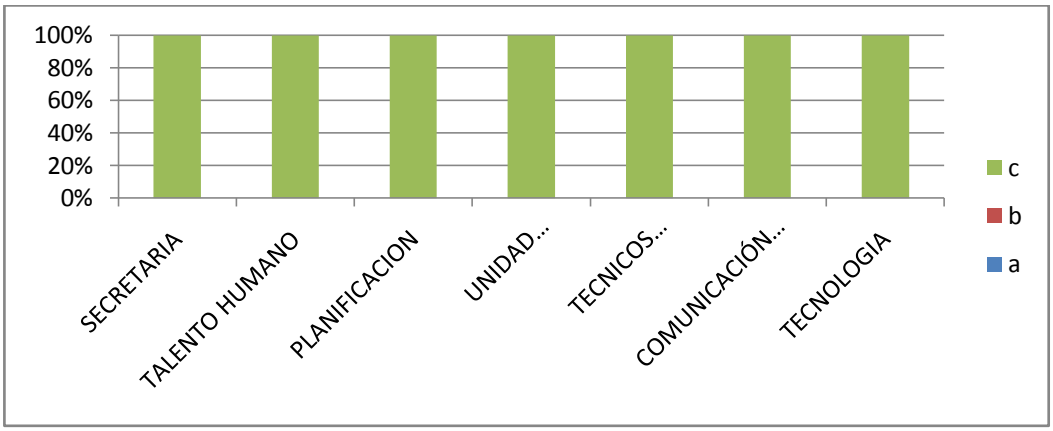


Gráfico # 54. Modificación de Contraseña.

4. **¿Su computador tiene un UPS?**

a. Si

b. No

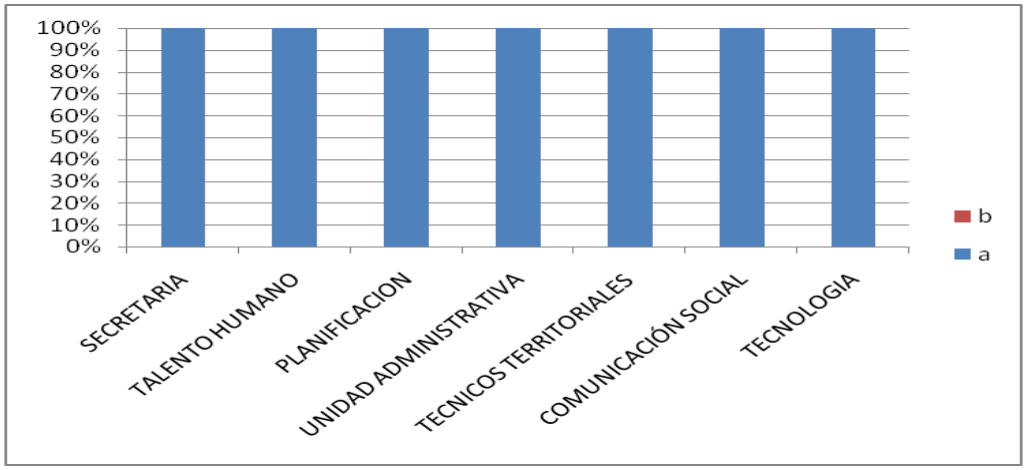


Gráfico # 55. Pregunta 4

5. **¿Cómo apaga su computador?**

a. Botón inicio, y opción apagar

b. Presiona el botón del CPU

c. Otro

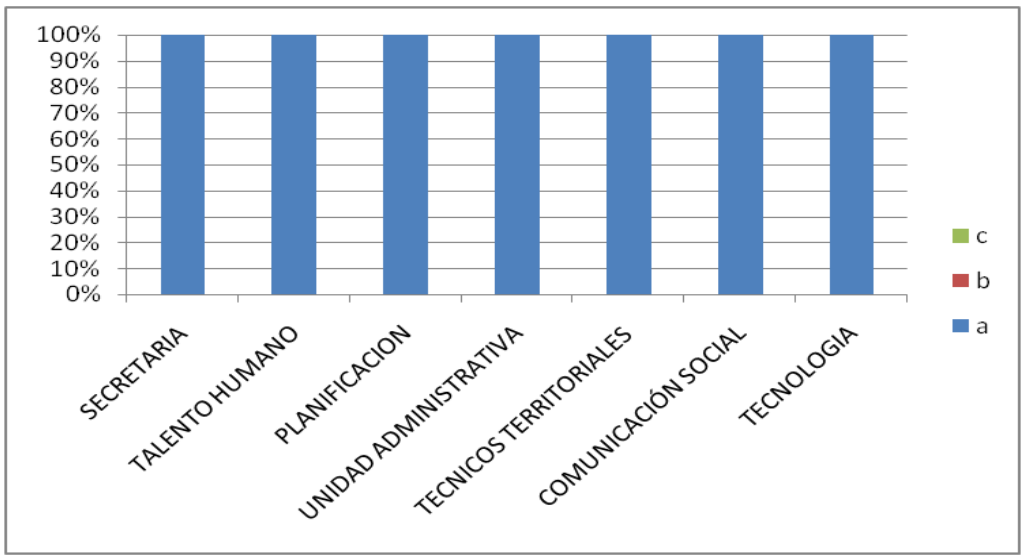


Gráfico # 56. Pregunta 5.

6. **¿Posee una contraseña personal para el uso del sistema de la institución?**

   a. Si

   b. No

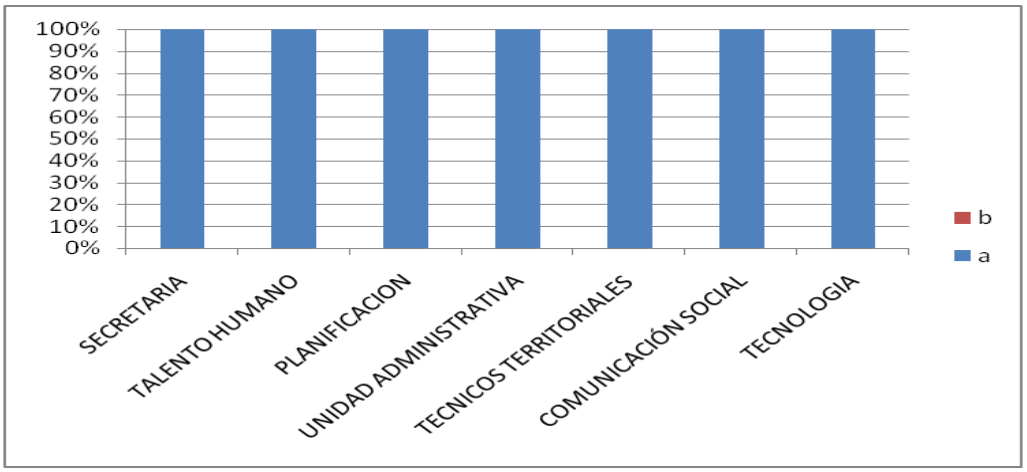


Gráfico # 57. Pregunta 6

7. **Para el uso del Internet usted necesita**

   a. Pedir acceso Al Depto. Tecnología

   b. Simplemente ingresa

   c. Otro

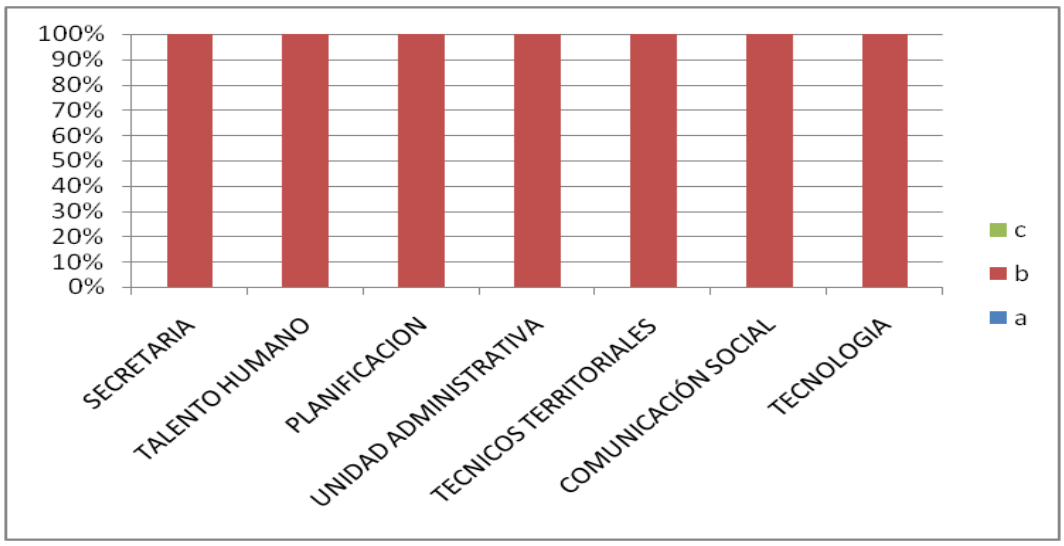


Gráfico # 58. Pregunta 7

8. **Tiene conocimiento de todo el software instalado en su computador**

a. Poco

b. Mucho

c. Nada

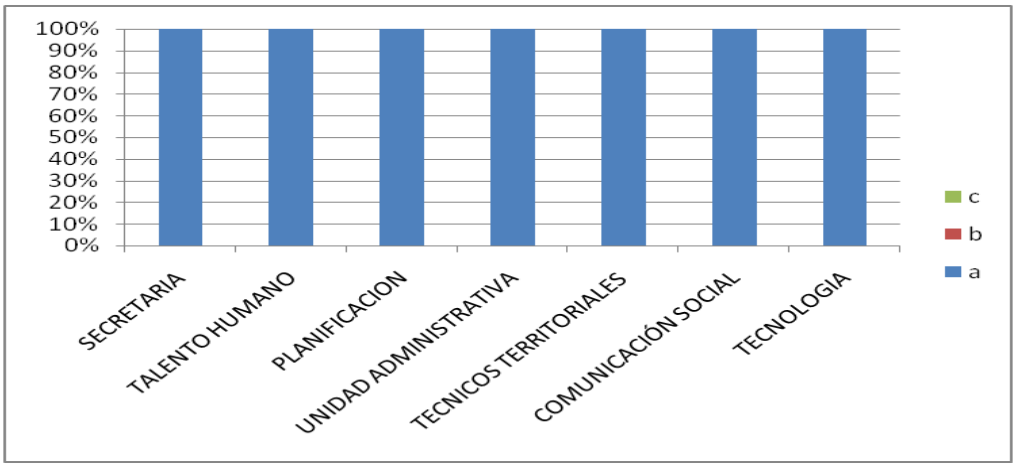


Gráfico # 59. Pregunta 8

9. **Cree que necesita una capacitación para el uso de sistemas nuevos en la empresa.**

a. Si

b. No

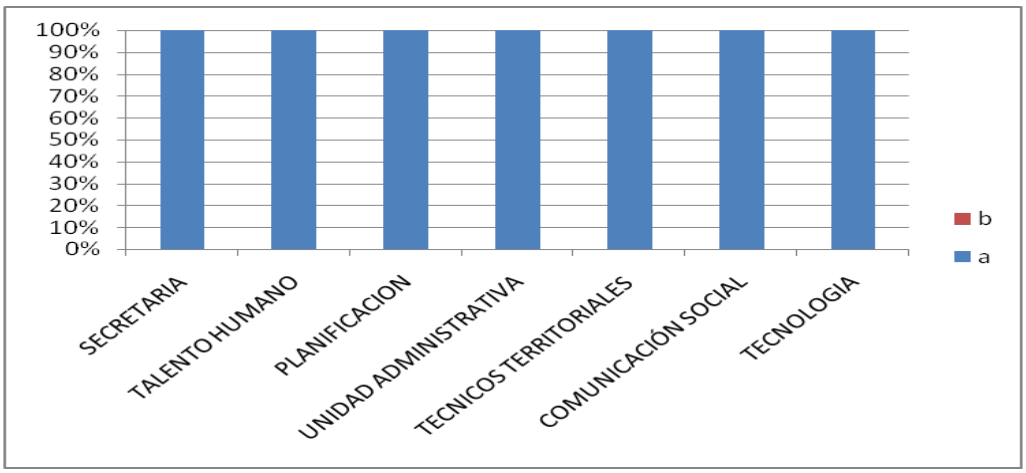


Gráfico # 60. Pregunta 9

10. **Para instalar nuevos software en su computador**

a. Solicita permiso Al Depto. Tecnología

b. Lo Instala usted y lo comunica Al Depto. Tecnología

c. Simplemente lo instala

d. No instala

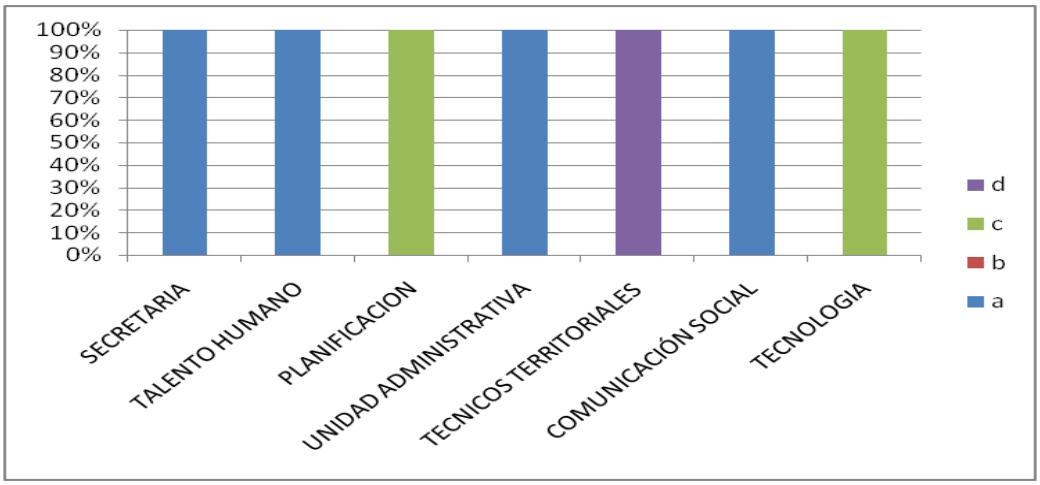


Gráfico # 61. Pregunta 10

CONCLUSIONES

- Cuando el funcionario necesita dejar su puesto de trabajo para realizar alguna actividad tanto dentro como fuera de la institución, en su mayoría sus computadores permanecen prendidos y sin tener un bloqueo automático.
- Los funcionarios no cambian de contraseña por estar acostumbrados o porque esperan a que el cambio sea hecho por parte del técnico en informática.
- Como el acceso a internet es abierto para los funcionarios con restricciones únicamente a páginas de entretenimiento como redes sociales, algunos empleados descargan aplicaciones que luego son instaladas en los ordenadores sin autorización.

- La mayoría de funcionarios desconocen acerca del software que tienen en su ordenador.

RECOMENDACIONES

- Se recomienda a los funcionarios que cuando tengan que dejar sus funciones por un momento bloquen sus maquinas para evitar el acceso de personas no autorizadas a sus computadores.
- Se recomienda cambiar por seguridad al menos 1 vez al mes las contraseñas.
- Para el mejor funcionamiento del su computador se recomienda no instalar software sin autorización pues este puede ocupar espacio necesario para otras aplicaciones y en muchos casos no se lo utiliza.

6.6.8.3. ESTUDIO Y EXAMEN DETALLADO DE LAS AREAS CRÍTICAS

- Manejo del Inventario de Hardware.
- Software innecesario en los computadores.
- Software ilegal.
- Capacitación de personal.
- Mantenimiento de los computadores.

6.6.8.3.1. INFORME DETALLADO DE AREAS CRÍTICAS

NOMBRE: Manejo del Inventario

Condición

Cada departamento maneja una codificación de cada mueble y enseres que están a cargo de cada funcionario, dicho manejo está a cargo de la unidad administrativa a través del sistema OLYMPO.

Criterio

Cada activo debe estar correctamente identificado sin errores para el mejor manejo de los departamentos de la institución y capacitación acerca del funcionamiento del sistema OLYMPO utilizado para el manejo de inventario.

Causas:

- La falta de cuidado al transcribir la información en cuanto a codificación.
- Sistema estaba a cargo de otra persona que ya no labora en la institución.

Efectos:

- La codificación es errónea
- Perdida de dispositivos
- Duplicidad de información

Conclusión

El personal actual encargado de esta actividad debe estar lo suficientemente capacitado en el funcionamiento del sistema para el mejor manejo del mismo como.

Recomendaciones

Se recomienda capacitarse en materia del sistema OLYMPO, acudiendo a los manuales que existe en la página de la institución www.infa.gob,ec/micasa a la vez darse el tiempo necesario para verificar la codificación de cada activo fijo y de corregir de ser necesario.

NOMBRE: Software Innecesario en computadores

Condición

En los departamentos de Comunicación Social, Unidad Administrativa, Tecnología, Secretaria software de uso personal como por ejemplo (software de telefonía celular. Juegos, protectores de pantalla, reproductores de música, entre otros) que ocupa espacio y recursos en el computador.

Criterio

Cada departamento debe tener el software necesario y requerido para cada funcionario para desempeñar sus funciones, ya que le software innecesario puede ser una fuente de distracción ocasionando pérdida de tiempo en otras actividades.

Causas:

- Falta de control Informático

Efectos

- Consumo tanto de espacio como de recursos.
- Pérdida de tiempo en actividades que no van acorde a sus funciones.

Conclusión

El escaso control informático ha provocado que funcionarios instalen software que no corresponde a las actividades que deben realizar en la institución.

Recomendaciones

Por parte del depto, de Tecnología debería llevar un control periódico a los ordenadores de los demás departamentos o la instalación de software que permita congelar el disco para que al apagar el computador se borren las aplicaciones instaladas ese día.

NOMBRE: Software Ilegal

Condición

Tomando en cuenta el análisis realizado encontramos que el 75% de software es ilegal y un 25% es legal en la institución, existiendo también aplicaciones no necesarias y que es de uso personal.

Criterio

Según la Sección V, Articulo 28 de la Ley de Propiedad Intelectual se dice que "los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos". (LEY DE PROPIEDAD INTELECTUAL, Ley No. 83. RO/ 320 de 19 de Mayo de 1998).

Causas:

- Recursos económicos insuficientes
- Falta de conocimiento del personal de la Institución
- Falta de control por el Depto. De Tecnología

Efectos

- Problemas legales
- Sanciones a la Institución

Conclusión

El software ilegal es descargado del internet e instalado por iniciativa propia de los funcionarios, sin control alguno.

Recomendaciones

- La institución debe adquirir licencias necesarias para los programas indispensables o la utilización de software libre como la exige hoy en día el Estado Ecuatoriano.
- Realizar controles a los ordenadores con el fin de desechar el software ilegal y no tener problemas legales.

Nombre

Capacitación el Personal

Condición

El personal no se encuentra debidamente capacitado en materia tecnológica que al presentarse algún tipo de problema no saben cómo actuar de tal manera que esperan a que el técnico vaya a revisar el imprevisto.

Criterio

El personal debe estar capacitado en la solución de pequeños problemas informáticos de manera que no tengan dependencia de una tercera personal.

Causas:

- Falta de interés por parte del personal
- Mal manejo del software
- Manipulación errónea del computador

Efectos

- Pérdida de Tiempo
- Perdida de Información necesaria
- Daño de Equipos informáticos

Conclusión

La falta de capacitación en los empleados y el uso inadecuado de su maquinas hace que estén en riesgo de causar daños a los bienes, perdida de información y a la vez perder tiempo en sus labores cotidianas.

Recomendaciones

- Realizar un plan donde se pueda dar capacitación la personal de manera permanente.
- Cada funcionario de la institución ponga interés en aprender, auto educarse en materia informática para no crear dependencia y evitar el deterioro del bien inmueble que este a su cargo.

Nombre

Mantenimiento de computadores

Condición

Al surgir algún problema en los computadores el técnico encargado no soluciona inmediatamente el problema o simplemente no se acerca a solucionar el inconveniente.

Criterio

El funcionario trata de solucionar el problema que se ha presentado debido a la falta de asistencia del personal.

Causas:

- Falta de Personal

Efectos

- Retardo en el trabajo a realizarse.

- Carencia de mantenimiento en los computadores.

Conclusión

La falta de personal en el área de tecnología es un factor predominante que produce un retardo en realizar actividades como es el mantenimiento preventivo y correctivo de los computadores en la institución.

Recomendaciones

- Elaborar un plan periódico de mantenimiento tanto preventivo como correctivo de los computadores de la institución.
- Comunicar a la dirección que existe una carencia de personal en el departamento de tecnología para que se tomen decisiones inmediatas.

6.6.9. FASE IX

DOCUMENTACION FINAL

6.6.9.1. CARTA A LA GERENCIA

Ambato, 12 de Septiembre 2012

Doctora
Marcela Naranjo
DIRECTORA PROVICIAL MIES – INFA TUNGURAHUA

De mis consideraciones:
Reciba un cordial saludo de parte de la egresada Diana Castro investigador auditor, por medio de la presente le entrego a usted los resultados de la auditoría realizada a los Departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y Unidad Administrativa del MIES INFA Tungurahua que Ud. Acertadamente dirige, la misma que se realizó desde el 15 de junio de 2012 al 30 de Agosto de 2012, a continuación redactamos los puntos más importantes de la auditoria.

El equipo auditor estuvo conformado por Diana Castro estudiante de seminario de Graduación en Seguridad Informática de la Universidad Técnica De Ambato, Facultad de Ingeniería en Sistemas Electrónica e industrial, carrera de Ingeniería en Sistemas Computacionales e Informáticos.

Además como coordinador e interlocutor fue asignado a Tecno. Catherine Analuisa, quien estuvo presente para colaborar con la documentación necesaria para llevar a cabo nuestro cometido.

El proceso de auditoría se realizo en los departamentos antes mencionados sin restricción alguna, tomando en cuenta los datos referentes a control y seguridades de los departamentos a si como los controles y seguridades Físicas y Lógicas.

El objetivo general de la auditoria fue realizar un análisis minucioso de los departamentos, determinar posibles falencias y proporcionar alternativas de solución, con la finalidad que esta información se convierta en una herramienta fundamental para mejorar el desenvolvimiento de sus actividades, disminuyendo las vulnerabilidades, riesgos y errores que podría causar pérdidas irreparables con la utilización de herramientas y técnicas de auditoría informática.

Los puntos analizados en los diferentes departamentos se detallan a continuación con sus respectivos aspectos observados:

- **Controles y Seguridades Físicas**

Los departamentos de la empresa no cuentan con seguridades y planes de evacuación en caso de un desastre, además el personal no conoce de la existencia de un plan de contingencias.
Además a pesar de que se cuenta con servicio de guardianía no se realiza un control de acceso para evitar la pérdida de objetos valiosos para la institución.

- **Seguridades Lógicas**

Un alto porcentaje del personal nunca ha cambiado sus contraseñas en su ordenador, lo que es un punto muy importante ya que cada usuario puede tener información que puede ser vulnerada, manipulada, y sustraída.

La descarga de software a través de la web es otro factor vulnerado ya que se instala aplicaciones que ocupan espacio pueden contener virus ocupando recursos dado como resultado inestabilidad en los ordenadores haciéndolos más lentos.

La falta de personal en el are de informática no permite que se realicen actividades primordiales en la institución en el área tecnológica como por ejemplo: mantenimiento y reparación de computadores, plan preventivo, correctivo y de contingencias ante cualquier eventualidad que se suscitase en la institución.

Conclusión

Se debe tomar en cuenta las aéreas críticas como son:

- Manejo del Inventario de Hardware.
- Software innecesario en los computadores.
- Software ilegal.
- Capacitación de personal.
- Mantenimiento de los computadores

En pos de mejorar entorno al desempeño de la institución, equipos informáticos, prestación de servicio social.

El presente proyecto investigativo de Auditoría Informática se ha logrado finalizar con la total satisfacción siendo de gran beneficio para la institución.

Atentamente.

Diana Castro

Auditora

6.6.9.2. INFORME FINAL

Ambato 12 de Septiembre de 2012

La Auditoria Informática realizada en MIES INFA de la Provincia de Tungurahua tuvo su inicio en la fecha 15 de Junio de 2012. Teniendo como auditor a Srta. Diana Castro estudiante de seminario de Graduación en Seguridad Informática de la Universidad Técnica De Ambato, Facultad de Ingeniería en Sistemas Electrónica e industrial, carrera de Ingeniería en Sistemas Computacionales e Informáticos y la colaboración de Tecno. Catherine Analuisa como supervisor e interlocutor en este proyecto de investigación y el apoyo de cada funcionario.

El proyecto de investigación fue acorde la función informática y se utilizó herramientas y técnicas actualizadas de auditoría informática, para determinar las posibles falencias y proporcionar alternativas de solución.

El alcance de la auditoría estuvo orientado a evaluar los Departamentos de Informática, Comunicación Social, Planificación, Secretaria, Talento Humano, Técnicos Territoriales y Unidad Administrativa del MIES INFA Tungurahua que lo conforman pero restringiendo esta actividad a los Departamentos Jurídico y Financiero.

La tarea realizada en la auditoría comprendió lo que a continuación se detallan:

- Obtener información necesaria de las áreas en el ámbito informático.
- Adquirir un inventario de hardware y software mediante el uso de herramientas y técnicas de auditoría informática.
- Hacer un análisis del software legal e ilegal de los departamentos, detectando los posibles errores que podrían encontrarse.

- Determinar las posibles falencias de la red a nivel físico.
- Plantear alternativas de solución a los problemas que se encuentren en el transcurso del proceso de auditoría.

ÁREAS, ACTIVIDADES O PROCESOS AUDITADOS

- **Seguridades físicas**

Durante el proceso investigativo se ha verificado la falta de control en el ingreso de personal a las diferentes aéreas para evitar robos de objetos valiosos ocasionados por terceros.

Contar con planes de evacuación capacitación el manejo de extintores ante cualquier siniestro o eventualidad que pueda ocurrir en la institución, mas no esperar a que ocurra y allí plantear un medidas de seguridad.

- **Seguridad Lógicas**

La no actualización de contraseñas en cada ordenador por parte del personal en caso de que el usuario tenga información importante y que la misma no sea vulnerada y manipulada.

Se debe tomar en cuenta que la mayoría de software que tiene la institución es ilegal e inclusive innecesario la cual debería ser eliminado mediante la revisión periódica del técnico en informática.

- **Capacitación de los usuarios**

Es necesario que el personal se encuentre capacitado para enfrentar los contratiempos informáticos, además capacitarlos si la institución adquiere nuevos sistemas o software actualizados, es decir realizar un plan de capacitación de personal en los diferentes departamentos si el caso lo amerita.

- **Mantenimiento de Hardware y Software**

A los computadores de las diferentes departamentos no se les da mantenimiento periódico, y cuando algún computador tiene problemas no existe personal disponible para solucionar los contratiempos de los usuarios, si se realizara un mantenimiento preventivo el personal no requeriría frecuentemente de los servicios.

Con todos los puntos citados anteriormente se posee un informe que contiene detalladamente todo el proceso de auditoría.

6.7. BIBLIOGRAFIA

- PAZMAY, Galo (2004) "*Guia practica para la elaboración de tesis y trabajos de investigación*", Editorial Freire, Riobamba.

- PIATTINI, M. y otros (2001) "*Auditoria Informática.*" Un Enfoque Práctico. 2ª Edición" Ed. RA-MA Editorial.

- AGUILAR, Adriana (2007) *"Auditoria Informática para los Departamentos Comercial, Acometidas y Procesamiento de Datos de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato",* Proyecto de Pasantía de Grado, previo a la obtención del Título de Ingeniera en Sistemas Computacionales e Informáticos, Universidad Técnica de Ambato, Facultad de ingeniería en sistemas Electrónica e Industrial, Ciudad Ambato, Ecuador.

- CANSECO, Fernanda (2007) *"Auditoria Informática En Los Departamentos De Personal, Médico, Trabajo Social, Coactivas, Planificación De La Empresa Municipal De Agua Potable Y Alcantarillado",* Proyecto de Pasantía de Grado, previo a la obtención del Título de Ingeniera en Sistemas Computacionales e Informáticos, Universidad Técnica de Ambato, Facultad de ingeniería en sistemas Electrónica e Industrial, Ciudad Ambato, Ecuador.

- **INFORMACION DE DOCUMENTOS ELECTRONICOS**

- RIOS, Julio. Seguridad Informática. Disponible en (http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml) (3 marzo 2012).
- Asamblea Nacional del Ecuador (2008). Constitución del Ecuador. Disponible en (http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf). (28 Febrero 2012)

- *HUERTA, Antonio(2000) "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License. Disponible en http://www.kriptopolis.org* (11 Noviembre 2011).

- Seguridad Física Disponible en http://www.segu-info.com.ar/fisica/seguridadfisica.htm

- Seguridad Lógica Disponible en: http://www.slideshare.net/ingenieroutpl2/seguridad-lgica (julio 2012)

- Sistemas Utilizados por MIES-INFA Disponible en www.infa.gob.ec/micasa

- Estatutos MIES-INFA Disponible en: www.infa.gov.ec (2008, Folio Nº 01405)

- MARTINEZ, Jose. (2009) "*Seguridad Informática*" Disponible en http://www.gulag.org.mx/eventos/2009-02-03-uane-seguridad_informatica/seguridad_informatica.pdf (26 de junio 2012)

- Planificación de la Auditoria Disponible en : http://es.scribd.com/doc/53381984/10/Planificacion-de-la-auditoria-Informatica

GLOSARIO DE TERMINOS

Activo:

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenazas

Son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indica como amenazas a las fallas, a los ingresos no autorizados, a los virus, al uso inadecuado de software, etc.

Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Auditoría

Es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

Auditoría Informática

Es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

Hardware

Maquinaria. Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

Impacto:

Consecuencia de la materialización de una amenaza.

Integridad

Es el servicio ofrecido por el departamento de informática. Debe ser adecuado, completo y auténtico en el momento de ser procesada, presentada, guardada o transmitida la información.

Plan de contingencia

Es proteger a la organización en el evento de que todas o parte de sus operaciones y/o servicios informáticos se vuelven inutilizados como resultado de un desastre informático.

Riesgo

Es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Es decir un riesgo conlleva dos tipos de consecuencias ganancias o pérdidas.

Seguridad Informática

Determina qué necesita ser protegido y por qué, de qué necesita protegerse, y cómo protegerlo mientras exista.

Servidor

Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes). También puede referirse a un software específico, como lo es el servidor WWW. Una computadora puede tener distintos software de servidor, proporcionando muchos servidores a clientes en la red. Por ejemplo, las computadoras que contienen sitios web se llaman servidores ya que “sirven” recursos de web para aplicaciones liente como los navegadores o browsers.

Sistema Operativo

Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

Software

Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

Software libre

Programas desarrollados y distribuidos dándole al usuario la libertad de ejecutar, copiar, distribuir, cambiar y mejorar dicho programa (Linux es un ejemplo) mediante su código fuente El software libre no es siempre software gratuito (equivocación bastante habitual que tiene su origen de la palabra en inglés "free" que significa tanto "libre" como "gratuito").

Software Ilegal

Programas que no poseen las licencias respectivas que acreditan su uso y en caso que el usuario lo utilice estará faltando a la ética.

Virus

Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras como son:

1. _ Solamente advertir al usuario de su presencia, sin causar daño aparente.

2. _ Tratar de pasar desapercibidos para causar el mayor daño posible.

3. _ Adueñarse de las funciones principales (infectar los archivos de sistema).

Vulnerabilidad

Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Área Crítica

Se considera como el estudio detallado de las áreas en las cuales se han encontrado algún tipo de problema o inconveniente.

Componentes Lógicos

Se considera todo dispositivo físico (tangible) del computador que se encuentre dentro de la unidad central de proceso (CPU) como pueden ser tarjetas de video, de red, de sonido, etc.

Estación de Trabajo

Forma parte de la red de la empresa, este puede acceder a los servidores y dispositivos de la red.

Estructura Organizacional

Es el conjunto de funciones y relaciones que determinan formalmente lo que cada unidad deber cumplir y el modo de comunicación entre cada unidad.

Firewall (Cortafuegos**)**

Puede ser un dispositivo o software utilizado en la red de computadoras, que impide a que otras redes accedan a la red privada.

Flujo de información

Es la manera en que se comunican las diferentes áreas de una empresa, según la estructura organizativa, sea una comunicación horizontal o vertical.

ISO 27001/27002

La norma internacional para la seguridad de la información ayuda a gestionar la seguridad de la información desde dentro de la organización.

ISO/TIA/EIA -568-A

Se basa en el cableado estructurado para edificios.

Seguridad Física

Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Seguridad Lógica

Consiste en la aplicación de barreras y procedimientos, por medio de software que resguarden el acceso a los datos.