ESCUELA DE INGENIERÍA EN SISTEMAS

Tema:

"Auditoría Informática para Optimizar el Manejo de la Información y Equipamiento Informático"

Disertación de grado previo a la obtención del Título de Ingeniero de Sistemas y Computación

Línea de Investigación:

Sistemas de la información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

César Santiago Bayas Escudero

Directora:

Ing. Mg. Teresa Milena Freire Aillón

Ambato – Ecuador
Julio 2015

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

Auditoría Informática para Optimizar el Manejo de La Información Y Equipamiento Informático

Línea de Investigación:

Sistemas de la información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

CÉSAR SANTIAGO BAYAS ESCUDERO

Teresa Milena Freire Aillón, Ing. Mg. **f.** _____

CALIFICADORA

Enrique Xavier Garcés Freire, Ing. Mg. **f.** _____

CALIFICADOR

Zandra Elizabeth Altamirano León, Ing. Mg. **f.** _____

CALIFICADORA

Teresa Milena Freire Aillón, Ing. Mg. **f.** _____

DIRECTORA ESCUELA DE INGENIERIA EN SISTEMAS

Hugo Rogelio Altamirano Villarroel, Dr. **f.** _____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Julio 2015

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, César Santiago Bayas Escudero portador de la cédula de ciudadanía No. 180328170-6 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Ingeniero en Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

César Santiago Bayas Escudero

CI. 180328170-6

AGRADECIMIENTO

Expreso mi gratitud a la **PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO,** a mis profesores y familia por el apoyo constante y por las enseñanzas y sobre todo por guiarme por el camino para el logro de los objetivos durante todos los años de estudio.

Gracias, mil gracias sus esfuerzos van a ser recompensados en la ética y moral que tendrá mi vida profesional.

César Santiago Bayas Escudero

DEDICATORIA

Este trabajo lo dedico con todo el amor y el cariño principalmente a mis seres queridos por brindarme toda la estabilidad la cual me brindo la ayuda necesaria para llegar a este punto, lo cual no hubiera sido posible sin ellos; mi familia siempre será la inspiración necesaria para poder alcanzar las metas propuestas todos sus esfuerzos serán reflejados en los triunfos conseguidos

RESUMEN

El presente documento de investigación está enfocado al desarrollo de una auditoría informática para optimizar el manejo de la información y equipamiento informático en la Agencia Nacional de Tránsito de Tungurahua, la misma que está desarrollada con la metodología CRMR *(Computer Resources Management Review).* La Auditoría surge por los diferentes problemas que tiene la Institución ya que el constante crecimiento de la información hace que el equipamiento informático no cubra todas las necesidades del usuario, el software innecesario, la contaminación del sistema por virus informáticos hace que los todos los equipos se tornen lentos y a su vez afecten a procedimientos importantes dentro de la Institución. La auditoría informática se enfoca en minimizar los riegos en el manejo de la información, aplicando un proceso metodológico que permitirá evaluar al equipamiento informático y el manejo de la información dentro de la ANT, dando como resultado una idea más clara de todos los riesgos o amenazas que podrían llevar al mal uso de la información para poder tomar acciones correctivas que permitan protegerla. Después de haber realizado la presente auditoría se obtuvo como resultados que existe software ilegal e innecesario, falta de una estructura organizacional en el área tecnológica, al igual que no existe un plan de contingencias y que los funcionarios necesitan capacitación en varios aspectos para que su mejor desenvolvimiento dentro de las funciones en la Institución.

ABSTRACT

This research project is focused on the development of an information technology audit to optimize the use of information and computer equipment at the National Transit Agency of Tungurahua. It has been developed with CRMR (Computer Resources Management Review) methodology. This audit emerged from the different problems that the institution has since the constant innovation of information causes that computer equipment no longer covers all the user's needs, unnecessary software, system contamination by computer viruses makes the equipment become slow and in turn they affect important procedures within the institution. The information technology audit is focused on minimizing the risks in the handling of information by applying a methodological process that will help to evaluate the computer equipment and the handling of information within the NTA, resulting in a clearer picture of all risks or threats which could lead to the misuse of information in order to take corrective actions to protect it. After having performed this audit, it was found that there is illegal and unnecessary software and lack of an organizational structure in the technological area. In addition, there is not contingency plan and the officials need training in several aspects in order to improve their development within functions of the institution.

ÍNDICE DE CONTENIDOS

PRELIMINARES

INDICE DE GRÁFICOS

TABLAS

ILUSTRACIONES

GRÁFICOS

INTRODUCCIÓN

El presente tema propuesto tiene como objetivo el desarrollo de una Auditoría Informática a los diferentes servicios que brinda la Agencia Nacional de Tránsito de Tungurahua (ANT), con este trabajo se pudieron detectar las deficiencias que se producen en el manejo de la información en los diferentes departamentos y plantear las posibles soluciones para mejorar el servicio dentro de la Institución.

Los recursos informáticos son adquiridos para el poder cumplir los objetivos y políticas que tiene toda Institución, por este motivo es primordial que las entidades ya sean públicas o privadas cuenten con la ayuda de la tecnología para reflejar la adaptación que se va realizando según el avance tecnológico en el mundo.

En el primer capítulo se encuentra los fundamentos teóricos los cuales sustentan el trabajo práctico, en el segundo capítulo se da a conocer la metodología de investigación y la metodología de desarrollo utilizadas para realizar el presente trabajo, el tercer capítulo se exponen los resultados obtenidos y las diferentes propuestas, en el penúltimo capítulo se realiza el análisis y la validación de los resultados obtenidos y el quinto capítulo contiene las conclusiones y recomendaciones.

CAPÍTULO I

REVISIÓN DE LA LITERATURA Y FUNDAMENTOS TEÓRICOS

1.1 Antecedentes

A la auditoría muchas veces se la relaciona a una rendición de cuentas en el cual el objetivo es verificar los diferentes errores que se presentan en las instituciones, sin embargo se puede decir más que eso, como por ejemplo que la auditoría es una revisión periódica, la cual se realiza con el objetivo de poder realizar una evaluación total de una institución o de parte de ella ya sea en el aspecto de su eficacia o eficiencia.

La información y el uso de la misma ha sido siempre un factor importante en la sociedad, y más aun con la llegada de la tecnología, la cual ha influenciado en los cambios que día a día va sufriendo la comunicación y consecuentemente la sociedad la cual maneja de cierta forma la información y los sistemas para administrarla. La Auditoría que se realizó en la Agencia Nacional de Tránsito de Tungurahua surge por los diferentes problemas que tiene la Institución ya que el constante crecimiento de la información hace que el equipamiento informático no cubra todas las necesidades del personal de la Institución, ya que con software innecesario que puede haber sido instalado y la contaminación del sistema por virus informáticos hace que todos los equipos se tornen lentos y a su vez afecten a procedimientos importantes dentro de la misma.

(Piattini, 2003) en su libro de “Auditoría informática: un Enfoque Práctico” expresa que la Auditoría Informática va orientada a que todos los procesos sean realizados de manera rápida y oportuna tales como la verificación de políticas de la empresa, los procedimientos y usos adecuados con el equipamiento informático y a su vez el uso de la información almacenada.

La auditoría informática pretende minimizar los riegos en el manejo de la información, esto se logra aplicando un proceso metodológico el cual permitirá evaluar al equipamiento informático y el manejo de la información dentro de la Agencia Nacional de Tránsito de Tungurahua, dando como resultado una idea más clara de todos los riesgos o amenazas que podrían llevar al mal uso de la información para poder tomar acciones correctivas que permitan protegerla.

1.2 Problema

La Agencia Nacional de Tránsito de Tungurahua (ANT), se dedica a “Planificar, regular y controlar la gestión del Transporte Terrestre, Tránsito y Seguridad Vial en el territorio nacional, para garantizar la libre y segura movilidad terrestre, prestando servicios de calidad que satisfagan la demanda ciudadana”. (Sitio Web ANT, 2014).

La institución gestiona información importante que está expuesta a múltiples amenazas que dependen directamente del mal manejo y estado de la

tecnología, por este motivo se concluye que información tiene un alto índice de riesgos y amenazas las cuales pueden provocar desastres informáticos que deriven en pérdidas para la Agencia Nacional de Tránsito.

1.2.1 Descripción del Problema

El problema surge por la deficiente gestión de la tecnología, y del procesamiento de la información al no saber si los procesos de TI los están llevando adecuadamente. Es por eso que la institución debería tener un plan de acción frente a las falencias, producto de una evaluación del estado de la situación informática, lo que se logra implementando procesos de auditoría informática.

Al igual que la Auditoría que se ha llevado a cabo en EMAPA en la cual según (Espinoza, 2007) en dicha empresa había falta de conocimiento falta de organización en los departamentos auditados y falta de seguridad encontrándose software ilegal, lo cual conlleva a la lentitud de los equipos y por consecuente lentitud en el servicio, situación que también se reflejan en los ejemplos de (Hernandez, 1997) y que serán tomados como referencia al momento de realizar la Auditoría en la ANT de Tungurahua ya que se aprecian similares inconvenientes en su servicio.

1.2.2 Preguntas Básicas

- **¿Por qué se origina?**

No se implementan procesos de control o auditorías informáticas proactivas que permitan sobre la marcha de la gestión de tecnologías ir identificando y corrigiendo los problemas que se presentan.

- **¿Dónde se detecta?**

La inconformidad de las personas frente a la lentitud en el servicio de la Institución en la cual no existe control interno tanto para los procesos de TI como para los funcionarios y con esto poder agilitar la atención a los usuarios.

1.3 Justificación

En la presente auditoría se van a realizar actualizaciones sobre los tipos de seguridad informática, para aplicarlas en la Institución, como por ejemplo, aplicar las técnicas de auditoría en informática, para así contar con sistemas de información seguros y confiables, los cuales eviten los diferentes riesgos que provocan las deficiencias que se encuentran en la institución auditada.

- Optimizar el manejo de la información conjuntamente con el manejo del equipamiento informático de la Agencia.

- Determinar los cambios o mejoras del Equipamiento Informático que deben realizar en la Agencia Nacional de Tránsito.
- Establecer planes de acción para mejorar los puntos críticos detectados.

1.4 Objetivos

1.4.1 Objetivo General

Realizar una auditoría informática para optimizar el manejo de la información y equipamiento informático en la Agencia Nacional de Tránsito de Tungurahua.

1.4.2 Objetivos Específicos

1. Realizar una evaluación al control interno informático para tener el diagnóstico de la situación informática de la ANT.
2. Analizar metodologías de Auditoría Informática para determinar la que mejor se adapte a las necesidades de la Institución.
3. Realizar la auditoría informática al departamento tecnológico de la ANT en base a la metodología seleccionada.
4. Socializar el resultado del informe final de la Auditoría realizada con el departamento de sistemas de la institución.

1.5 Meta

Gestionar de manera técnica la infraestructura tecnológica existente en la Agencia Nacional de Tránsito de Tungurahua.

1.6 Fundamentos Teóricos

1.6.1 Auditoría Informática

1.6.1.1 Concepto

Según su etimología la palabra auditoría proviene del verbo inglés "*to audit*" que significa "intervenir o revisar" la cual se entiende que cualquier tipo de auditoría permite revisar, examinar y evaluar resultados; el objetivo principal está dirigido hacia la eficacia de un proceso o a la eficiencia en la cual se está trabajando según varias normas o metodologías las cuales corrigen todos los errores para así evitar la eliminación de los mismos.

(Hernandez, 1997), asegura que una Auditoría Informática es un proceso que cualquier Institución necesita realizar para así poder asegurar de manera óptima cualquier tipo de información. Con esto se puede brindar a los directivos de las empresas cualquier tipo de recomendación necesaria para el avance continuo en las funciones de la entidad auditada.

Tomando en cuenta el concepto de una Auditoría Informática se puede mencionar que al realizar este tipo de procesos se logra:

- Disminuir los costos.
- Disminuir los riesgos de la Tecnología Informática
- Optimizar el ambiente de trabajo y relaciones internas
- Controlar la inversión en Tecnología Informática
- Mejorar el desempeño interno de la empresa
- Verificar cumplimientos de Normativas
- Analizar y gestionar los recursos tecnológicos

1.6.1.2 Tipos de Auditoría Informática

(Echenique, 2001), en su libro “Auditoría Informática” define algunos tipos de Auditoría Informática, tales como:

- **Auditoría Ofimática**

  Este tipo de Auditoría está enfocada hacia todos los programas informáticos los cuales le sirven al usuario como herramienta ya sea para procesar textos, editar gráficos, etc.

  Partiendo de la opinión de varios autores acerca de una Auditoría Ofimática se puede recalcar que se involucra con los sistemas

relacionados con el funcionamiento de la oficina los cuales generan, procesan, almacenan y presentan información de la misma, debe tomarse en cuenta que con el avance tecnológico se ha tratado de desplazar a las aplicaciones ofimáticas a plataformas microinformáticas.

Según (Echenique, 2001), afirma que la auditoría ofimática tiene dos características principales a ser analizadas: el tipo de distribución de cada uno de los programas utilizados por las diferentes áreas de la institución, y el traslado de responsabilidades de los varios controles de los sistemas de información a personas que tengan conocimiento de la importancia y utilización de los mismos.

- **Auditoría Física**

Este tipo de Auditoría implica el activo informático de la empresa o la entidad que va a ser auditada el mismo que debe estar o ser registrado en un inventario, además de comprobar la existencia de los medios físicos se comprueba la seguridad y funcionalidad de los mismos.

La seguridad física de acuerdo con (Echenique, 2001) afirma que no es más que asegurar el bienestar de todos los activos, sean humanos o materiales, para esto se debe tener en cuenta las áreas más vulnerables y los tipos de seguridad para los medios de información, caso contrario

se debe realizar planes de contingencia para así disminuir los riesgos del sistema e ir determinando las prioridades de los procesos.

Aquí también se debe tomar en cuenta que en ocasiones será factible el contratar algún tipo de seguro el cual cubra la perdida de los bienes por daños o por robos.

- **Auditoría de Redes**

Lo que básicamente se logra con este tipo de Auditoría es poner a prueba la red informática de la Institución, significa que se evalúa el desempeño y seguridad de la red haciendo un análisis de vulnerabilidad para proponer varias estrategias y planes de contingencia ante los posibles incidentes con el desempeño del sistema a fin de que sea una red más eficiente y asegure el traslado de la información. (Echenique, 2001).

Después de haber realizado un análisis de vulnerabilidades el cual es el punto más importante para cualquier tipo de Auditoría, y de haber realizado una estrategia de saneamiento en el cual se verifica los servidores internos, estaciones de trabajo y se reconfigura la red, se debe entregar un plan de contingencias general se pueden tomar en cuenta varios puntos para su mejora y a su vez seguir reportando nuevos fallos en la seguridad, con esto el riesgo disminuye notablemente.

- **Auditoría de la Seguridad**

Este tipo de auditoría según (Echenique, 2001), es una de las más importantes ya que la seguridad es el área principal que debe ser auditada, la importancia de la información de una empresa es primordial para que se mantenga un nivel de seguridad exclusiva y más aún si se tiene sistemas que se basen en el uso de la tecnología y de las comunicaciones, ya que de no existir algún tipo de seguridad la entidad tendría varias fallas, accesos no autorizados, etc.

Después de que se obtienen los resultados, se realiza un informe en el cual se detalla las diversas vulnerabilidades que se hayan presentado al revisar las estaciones de trabajo, servidores y las redes de comunicaciones, esto debe ser entregado a los responsables los mismos que tendrán que tomar medidas preventivas para poder prevenir o corregir la seguridad de los sistemas que son parte de la Institución.

- **Auditoría de Bases de Datos**

Después de que se identifique a la información como un recurso fundamental de cualquier empresa y la difusión de los Sistemas Administradores de Bases de Datos *(DBMS - Database Management*

Systems) se realiza las auditorías y controles internos de los mismos con mucha más profundidad.

Este tipo de auditorías y técnicas de control se basan en diferentes puntos que tienen relación la base de datos o a su ciclo de vida como por ejemplo: si se realizó un estudio previo para verificar la viabilidad y el plan de trabajo para alcanzar los objetivos, verificar el diseño ya sea lógico o físico donde se verifique las restricciones, seguridad y especificaciones del almacenamiento, saber si existen procesos de mantenimiento que soliciten autorización adecuada para que la información este segura, y que obviamente los resultados satisfagan las necesidades del usuario.

1.6.1.3 Procesos de Auditoría Informática

Dentro de los procesos de una Auditoría Informática detallados en (Acha Iturmendi, 1994) se encuentran los siguientes puntos:

- **Planificación**

  En cualquier tipo de Auditoría que se realiza en cualquier tipo de organización, el proceso de la planificación este es el primer paso en el cual se pueden definir todos las evaluaciones que se van a ejecutar a los

sistemas, procedimientos, equipos de cómputo y los procesos de datos; para esto se involucra a todos los departamentos de la empresa que van a ser auditados para así poder identificar los recursos necesarios y el planteamiento de objetivos.

Al plantear estas evaluaciones se logra conocer a la Institución y a sus procesos, para con esto poder establecer metas, pasos a seguir en la auditoría, fechas y presupuesto, otorgar responsabilidades al personal que realiza la auditoría que a su vez entregaran el debido informe de las actividades realizadas junto con la realidad de la organización evaluada, dentro de este informe se debe detallar los siguientes puntos:

- Recursos necesarios
- Alcance de la auditoría
- Información de las actividades que van a ser auditadas
- Canales de comunicación necesarios
- Procedimientos para inspección física
- Responsables para revisión final
- Plazos de tiempo
- Aprobación del plan de trabajo

Después de haberse detallado y aprobado todos los aspectos necesarios y según el acuerdo que se mantenga con los directivos de la Institución,

se procede a la revisión preliminar y con esto se da inicio a la siguiente etapa.

- **Ejecución**

En el proceso de ejecución se hace uso de técnicas, metodologías o herramientas que ayude a recolectar toda la información necesaria y detallada, como por ejemplo entrevistas, cuestionarios, encuestas, revisión y análisis de estándares y de información documentada, etc. Cualquier proceso que pueda ser comprendido y guíe a las respectivas conclusiones y recomendaciones

Es importante que la información que sea recolectada este completa y bien detallada para que pueda ser comprendida por la persona que va a realizar la auditoría, para que pueda demostrar con evidencias el conocimiento de los procesos de la empresa, dichas evidencias pueden ser documentales, físicas, analíticas y testimoniales.

- **Finalización**

Como proceso de finalización se emite un informe final que consta de las conclusiones, recomendaciones, resultados de la auditoría realizada la misma que debe ser entregada a la administración de la empresa para su

respectiva evaluación. El informe final generalmente tiene una estructura para su presentación a los directivos de cualquier empresa auditada:

- Debe indicar el tiempo en el que se realizó cada actividad de la auditoría
- Especificar las personas que hayan realizado todos los procesos
- Indicar los objetivos que se alcanza al realiza la evaluación de la auditoría
- Detallar la situación en la que se cual se encontraba la Institución
- Dar a conocer las causas que provocan la situación antes detallada
- Mencionar los efectos que tuvo la empresa al estar en la situación anterior
- Incluir las recomendaciones que debe seguir la administración para evitar los efectos antes mencionados

1.6.1.4. Metodologías y Estándares de Auditoría Informática

La utilización de una metodología es indispensable para una Auditoría Informática ya que con ellas se puede realizar cualquier proyecto de manera ordenada y eficaz.

Todas las metodologías que son utilizadas para seguridad de sistemas son encaminadas para establecer o mejorar puntos que garanticen que las

amenazas sean nulas o al menos se reduzca de una manera razonable al costo – beneficio.

Los tipos de metodologías para una Auditoría Informática son:

- **Metodologías de los auditores internos:** Estas son formuladas por recomendaciones de los planes de trabajo y de todo el proceso que se debe seguir junto con el objetivo a seguir los mismos que son descritos en el informe antes de empezar la auditoría. El auditor interno es el que se encarga de verificar las metodologías necesarias según las áreas que se vayan a auditar.

- **Controles Generales:** Estos son el producto estándar de una Auditoría Informática, el objetivo de estos es dar una opinión sobre la fiabilidad de los sistemas de información y las vulnerabilidades encontradas, este resultado también va incluido en el informe final de la Auditoría.

A continuación se detalla aspectos importantes de tres metodologías de auditoria informática tales como CRMR, MAGERIT e ITIL, para determinar cuál de estas metodologías es la más apropiada para la presente auditoria.

1.6.1.4.1. ITIL

ITIL significa *(Information Technology Infrastructure Library)* o traducido es Librería de Infraestructura de Tecnologías de Información, esta metodología fue

desarrollada en 1980 para las organizaciones que iban dependiendo mucho más de la informática como herramienta para poder cumplir sus objetivos, esta dependencia que ha aumentado hasta hoy en día ha ido generando una necesidad de servicios informáticos que van junto con los objetivos del negocio y que con esto se logre la satisfacción del cliente.

El objetivo que tiene esta metodología es el establecer estándares para el control, administración y operación de los recursos, a más de que plantea una revisión y reestructura de todos los procesos existentes de ser necesario, lo cual lleva a realizar una mejora continua.

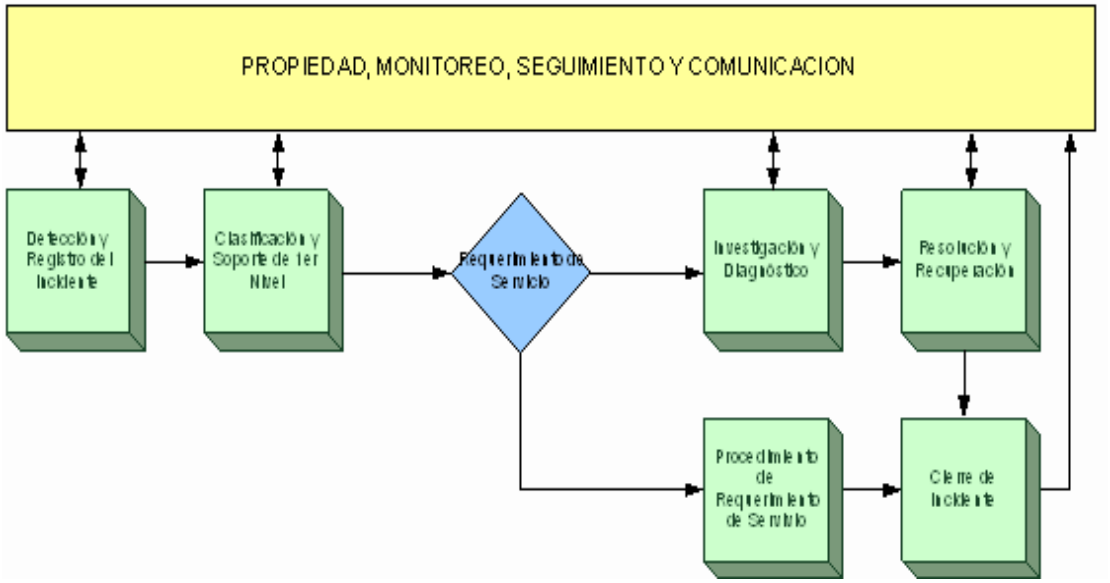
Otro objetivo es que para las actividades que se realice se debe generar una documentación la misma que sirve como información de los cambios realizados al personal del área auditada y con lo cual se tiene una constancia del trabajo. La metodología ITIL según (Naranjo, 2000), plantea cinco procesos para el servicio de soporte, administración y operación en cualquier empresa:

- **Manejo de Incidentes**

  El objetivo principal en un manejo de incidentes es el reestablecer el servicio lo más pronto posible, evitando así molestias del usuario, se debe tener en cuenta que en un manejo de incidentes el usuario no debería percatarse de las falencias que presente el sistema, para esto primero está la detección y

clasificación del incidente, la solicitud de servicio y finalmente la evaluación para verificar que se haya resuelto el problema tal como se explica en el siguiente diagrama.

Ilustración 1.1 Manejo de Incidentes



Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

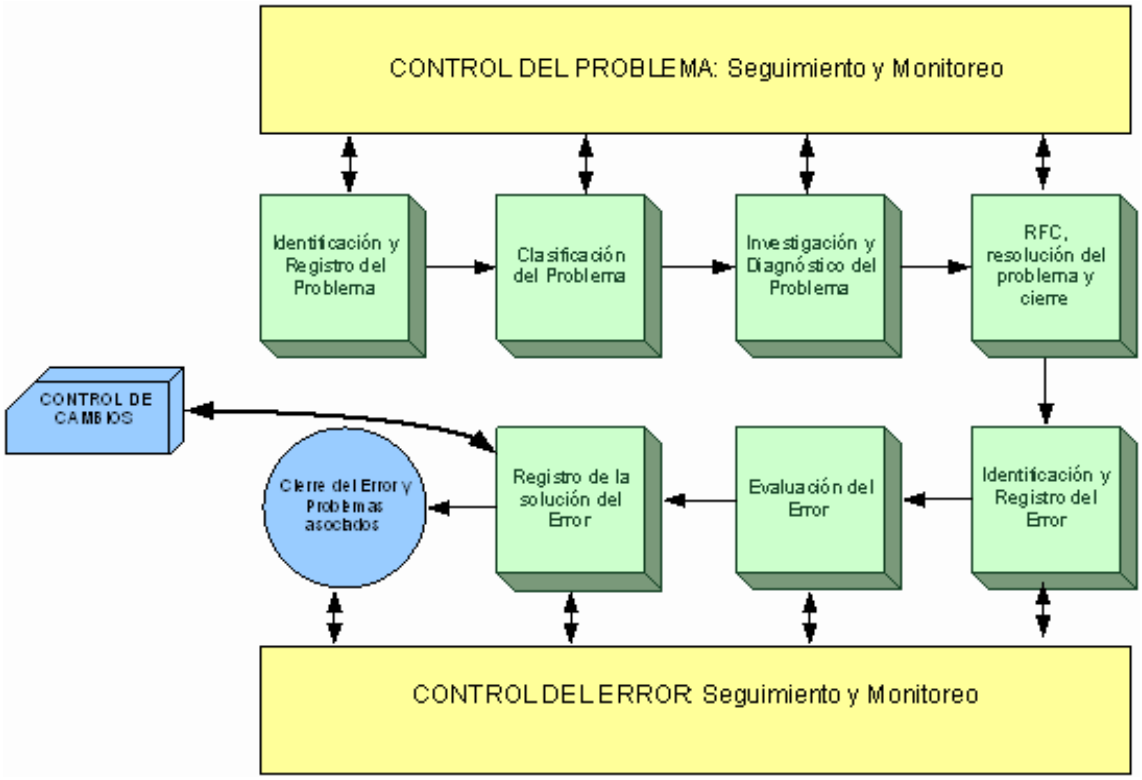
- **Manejo de Problemas**

Con el manejo de problemas se trata de conseguir la prevención y la reducción de los incidentes, teniendo el control total del problema junto con un seguimiento y un monitoreo del mismo. Este proceso se realiza en dos fases la primera es el control del problema, en la cual en base a los antecedentes se realiza los mismos pasos de un control de incidentes, posteriormente a estos pasos se implementa la solución y se realiza la

evaluación con el objetivo de haber solucionado totalmente el problema, y poder emitir la documentación.

La segunda fase de este proceso es el control del error la cual se realiza con una identificación del error en general para poder realizar un registro ya que con estos datos se lo puede clasificar y evaluar el daño que ocasiona o que puede llegar a ocasionar a futuro.

Ilustración 1.2 manejo de problemas

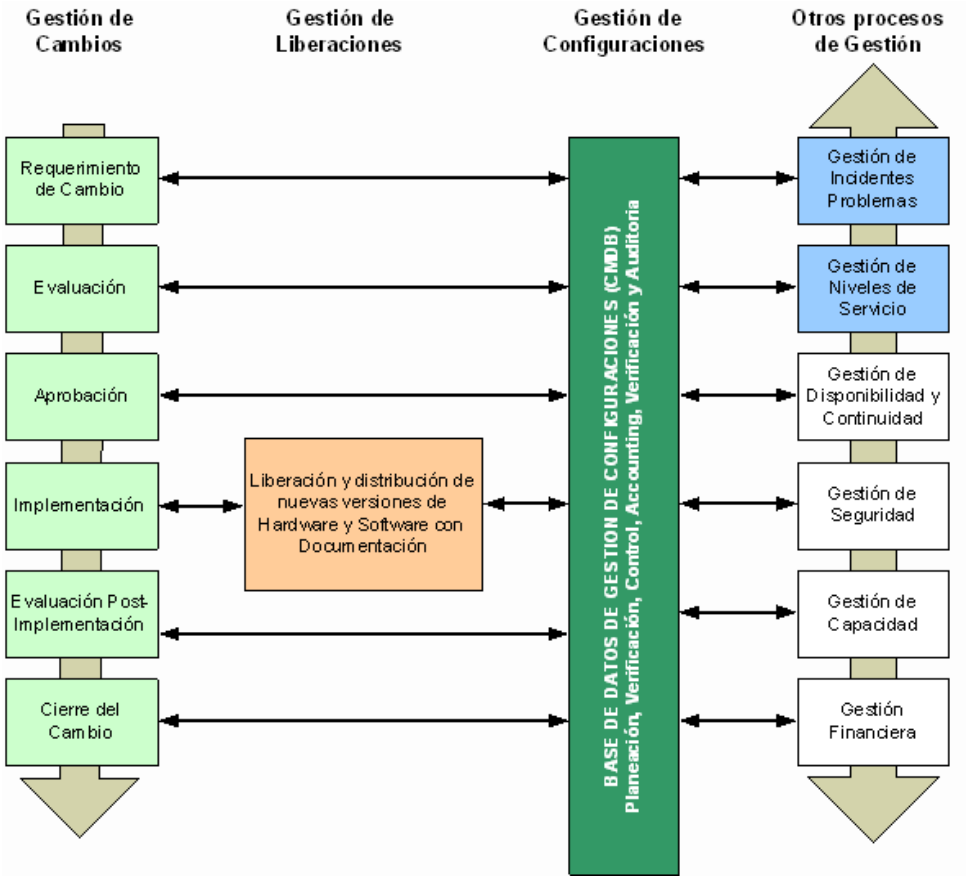


Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

- **Manejo de Configuraciones**

Este proceso tiene como finalidad el otorgar información verídica y actualizada de las configuraciones y sistemas instalados en los equipos de cada usuario, este es una de los procesos más complejos ya que influyen algunas variables y al ser la gran mayoría variables dinámicas afectan directamente al sistema en general ya que si cambia una o varias variables cambia todo tal como se observa en el siguiente cuadro.

Ilustración 1.3 Manejo de configuraciones



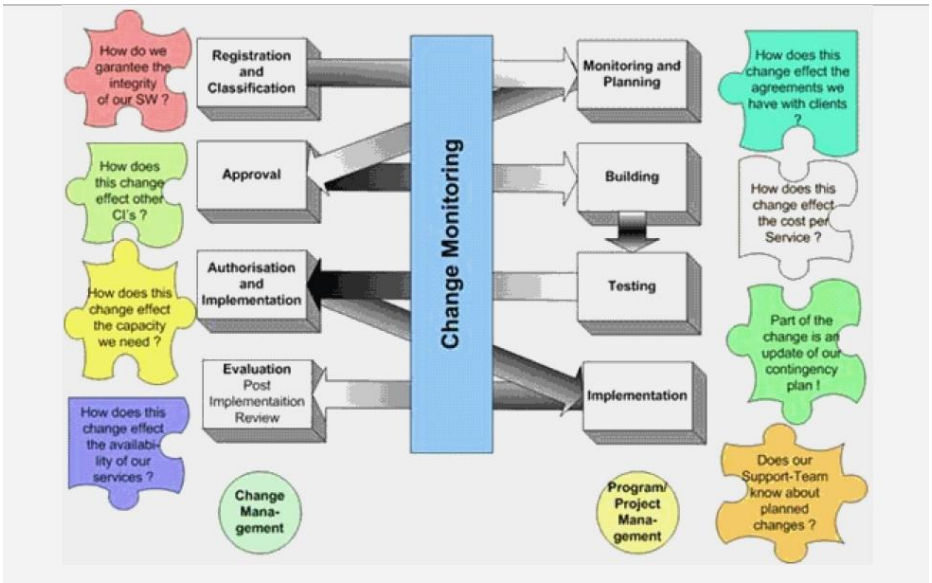
Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

En el manejo de configuraciones se puede observar las relaciones que tiene con la administración de problemas, significa que tiene un proceso tanto de planeación como de identificación, seguimiento de estatus, verificación y control. El manejo de cambios indica que se debe realizar una distribución de nuevas versiones y depende mucho que se disponga de un software o hardware este proceso no se puede completar ninguno de los pasos descritos hasta el punto de control de cambios.

- **Manejo de Cambios**

El objetivo de este proceso es el de disminuir los diferentes riesgos ya sean técnicos o económicos, el diagrama a continuación indica que entre cada una de las etapas se realiza una etapa de monitoreo.

Ilustración 1.4 Manejo de Cambios



Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

Se inicia registrando y clasificando los cambios que sean necesarios y continua con la etapa de monitoreo y planeación, para poder verificar si el rendimiento es satisfactorio y poder aprobar el cambio de lo contrario se realiza una reingeniería hasta que el proceso sea satisfactorio; en el momento que los cambios estén aprobados se construyen modelos en los que se van a realizar las pruebas las cuales indican las capacidades del sistema, y en el momento en el que este paso este aprobado se procede con la autorización e implementación, finalmente se verifican que no se haya desviado de los objetivos y se realizan ajustes según sus necesidades, a este paso se lo conoce como una revisión post-implementación.

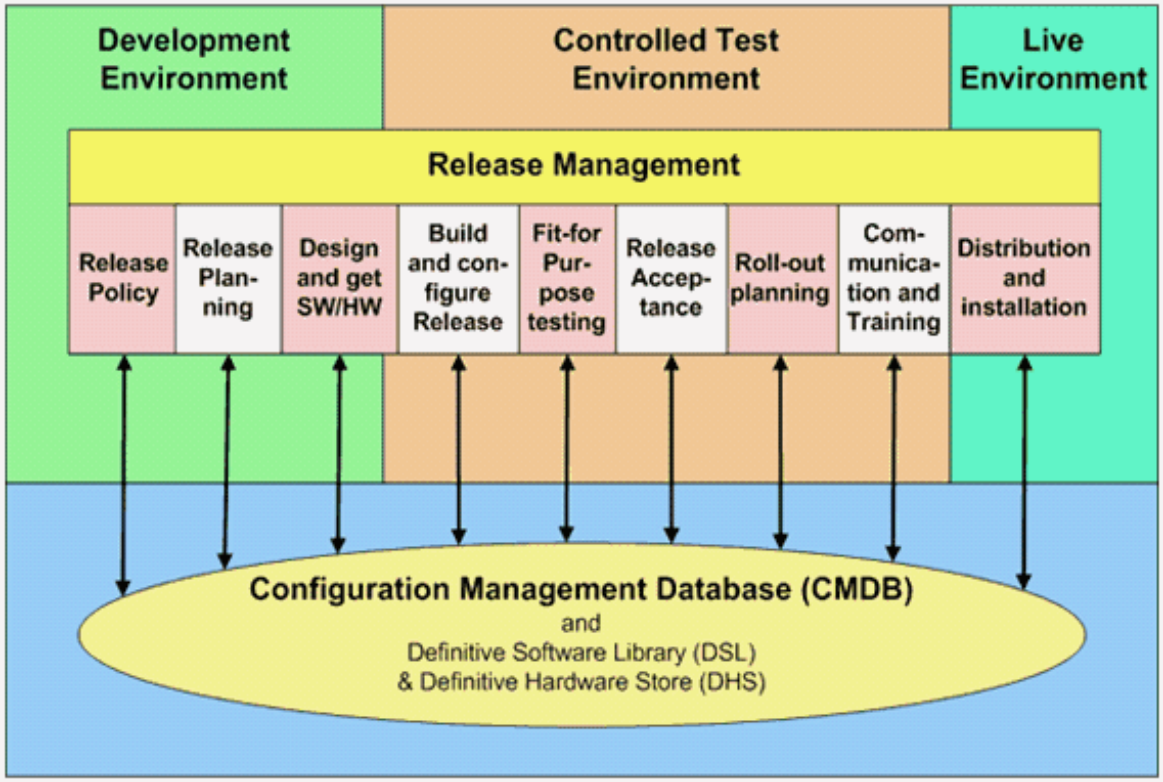
- **Manejo de Entregas**

En este proceso lo que se tiene como objetivo es el planificar y verificar la forma de instalación del software y hardware, como se puede verificar en el siguiente diagrama en el cual se nota la transición por los cuales el proyecto va a avanzando.

En el desarrollo se realiza el diseño lógico de la infraestructura, desarrollo de las políticas, planificación y la adquisición del hardware y software, en la sección de pruebas controladas se realiza la construcción y desarrollo de las configuraciones, se hacen las pruebas las cuales establecen los acuerdos de aceptación, posteriormente se realiza la planeación y finalmente las

pruebas, con estas fases concluidas sigue el ambiente real en el cual se da la distribución e instalación.

Ilustración 1.5 Manejo de Entregas



Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

1.6.1.4.2. MAGERIT

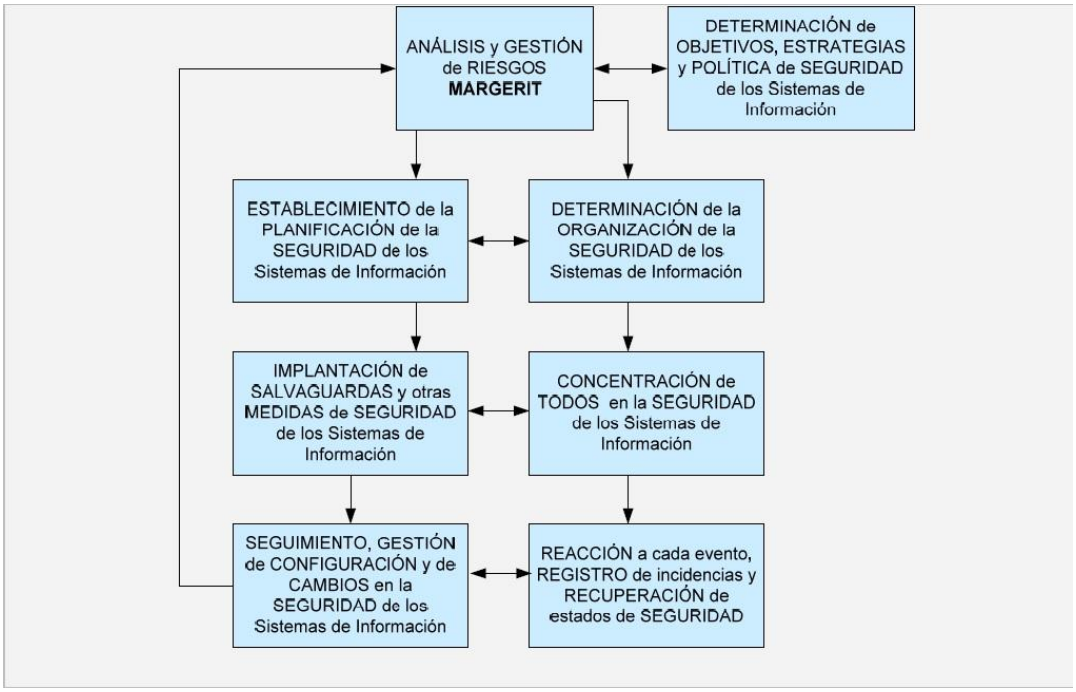
Magerit cuyo significado es Metodología de Análisis y Gestión de Riesgos de las Tecnologías de Información, con esta metodología se puede recomendar medidas apropiadas para controlar riesgos.

Según (Naranjo, 2000) en su libro “Metodología para una Evaluación Informática”, los dos objetivos principales que tiene la metodología MAGERIT son el análisis de riesgos de los sistemas de información y la gestión de los mismos; el primer objetivo implica realizar una evaluación para determinar el impacto que causa un riesgo de seguridad dentro de la Institución, para poder identificar los riesgos existentes, se debe identificar las amenazas y determinar la vulnerabilidad del sistema de seguridad.

Con los resultados anteriores se puede continuar hacia el segundo objetivo, en el cual se puede recomendar las medidas apropiadas que la empresa deberá tomar para poder identificar, prevenir y controlar los diferentes riesgos identificados y con esto disminuir los posibles problemas que estos riesgos ocasionen.

El analizar y gestionar los diferentes riesgos son la parte principal de cualquier organización al momento de hablar de seguridad, por lo tanto se encuentran en las fases y las diferentes actividades como objetivos y políticas y de tipo logístico como planificación, mantenimiento, implantación de salvaguardas. (Naranjo, 2000).

Ilustración 1.6 Análisis y Gestión de Riesgos MARGERIT



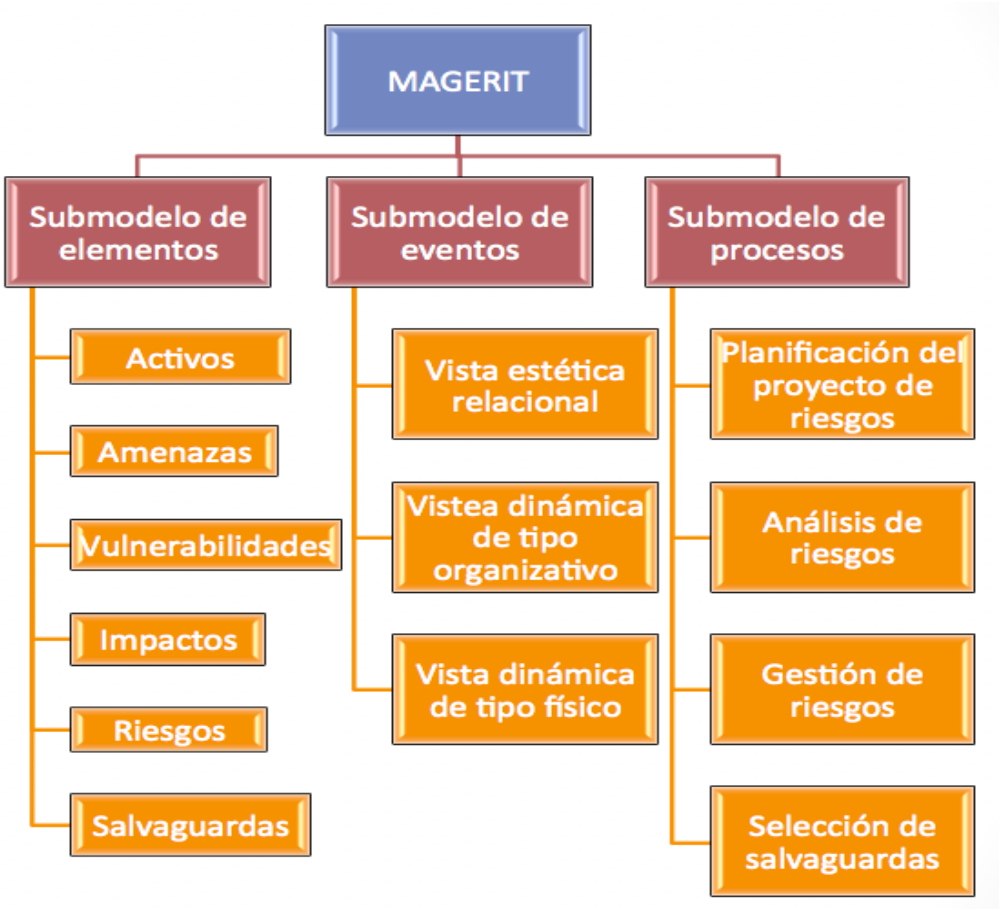
Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

MAGERIT está enfocado a las necesidades de las personas que tengan la idea de adaptar a cada organización y a los temas de la seguridad en las tecnologías de la información, existe tres situaciones específicas las cuales marcan diferencia como son:

- Situación: El ciclo de estudio abarca el marco estratégico, análisis y gestión de riesgos, determinación de estrategias específicas.
- Problemas específicos: seguridad lógica, de redes y comunicaciones, planes contingencia y de evacuación.

- Envergadura: complejidad del dominio estudiado, tipos de estudio ya sea corto o simplificado.

Ilustración 1.7 Submodelos MARGERIT



Fuente: Metodología para una Evaluación de una Unidad Informática (Naranjo, 2000)

Los tipos de técnicas utilizadas en MAGERIT son:

- Técnicas Comunes
- Técnicas Complementarias
- Técnicas Características de MAGERIT: algorítmicas, matriciales, de lógica difusa.

MAGERIT utiliza siete guías para sus procedimientos las cuales son:

- **Guía de Aproximación**

Los conceptos de seguridad básica que se utilizan en los sistemas de información para facilitar la comprensión de los mismos a personas que no están especializadas en el tema a más de que se redacta una introducción a los puntos básicos de Magerit.

- **Guía de Técnica**

Brinda las claves que se debe tener en cuenta para entender y seleccionar la técnica más adecuada para analizar y gestionar los riesgos de los sistemas de seguridad.

- **Guía para Desarrolladores de Aplicaciones**

Como su nombre lo indica está dirigida a los desarrolladores de la aplicación es ya que está relacionada con la planificación y con el desarrollo de los sistemas de información.

- **Guía de Procedimientos**

Está basado en las partes principales de la metodología que junto con la guía de técnicas forman un contenido completo con el cual se puede

entender de mejor manera la terminología y así realizar de mejor manera el análisis y la gestión de riesgos de los sistemas de información.

- **Guía para Responsables de Dominio**

Esta guía indica la participación de los Directivos que son los responsables del análisis y la gestión del riesgo de los sistemas.

- **Guía de la interfaz para el intercambio de datos**

Esta guía ayuda a la comunicación con otras aplicaciones y con esto se logra la incorporación hacia la metodología Magerit.

- **Guía de Referencia de Normas Legales y Técnicas**

Son las normas que se deben emplear para la seguridad en los sistemas de información. A más de estas guías Magerit en su primera versión hace uso de dos herramientas de apoyo las cuales son:

- **Introductoria:** Brinda una primera visión del análisis y gestión de riesgos, la cual se puede identificar los riesgos de mayor y menor nivel para poder aplicar alguna medida de seguridad según sea necesario. También hace uso de técnicas matriciales, lo que quiere decir que el

usuario no necesita tener suficiente experiencia para poder implementar la seguridad a los sistemas de información.

- **Avanzada:** Esta herramienta permite realizar de manera detallada el análisis y la gestión de riesgos, para así poder enfrentarse a los problemas de mayor escala que la herramienta anterior. Las técnicas que utiliza son la algorítmica y de lógica difusa, para lo cual se necesita un mayor nivel de conocimiento de la seguridad que se da a los sistemas de información para así lograr un análisis detallado de los activos de la entidad auditada; las dependencias y la relación entre estos.

1.6.1.4.3. CRMR

La Metodología CRMR *(Computer Resources Management Review)* lo que significa que realiza una evaluación de eficiencia de los recursos informáticos. Esta metodología tiene la gran ventaja de que los ciclos de desarrollo ayudan a tener una visibilidad temprana de los problemas y va aportando técnicas de implementación de las recomendaciones y conclusiones (Naranjo, 2000).

El método CRMR se lo aplica cuando:

- Se verifica el mal funcionamiento a las peticiones de los usuarios
- Existen costos altos de procesos en el centro de procesos de datos

- Existe sobrecarga frecuente de capacidad de proceso
- Se genera información errónea por fallo en los datos o procesos
- La información no es presentada en el momento oportuno

Las áreas a las cuales esta metodología puede ser aplicada según las condiciones de aplicación antes descritas son:

- Control de operaciones
- Gestión de Datos
- Control de Recursos Materiales y Humanos
- Interfaz y Relación con el Usuario
- Planificación
- Organización y Administración

El objetivo principal que tiene CRMR es el de evaluar el nivel de ineficiencia de los procedimientos que tiene el sistema y los métodos de gestión que se observan en el mismo, con estos pasos se llegan a las recomendaciones las cuales pueden relacionarse con los siguientes puntos según (Naranjo, 2000).

- Aumentar la productividad
- Disminuir los costos
- Mejorar los procedimientos
- Identificar y fijar responsables
- Mejorar el proceso de las actividades

Antes de implementar esta metodología se deben definir los alcances de la misma, para esto se puede dividir en tres clases:

- **Reducido:** Consiste en identificar las áreas en las cuales se va a proceder a actuar inmediatamente para la obtención de resultados y beneficios inmediatos.

- **Medio:** En esta clase, CRMR establece las conclusiones y las recomendaciones necesarias, de igual forma en la que se presenta en cualquier otra Auditoría.

- **Amplio:** Aquí la metodología CRMR incluye los diferentes planes de Acción, dando paso a las técnicas que se analizan en las recomendaciones y que conjuntamente dan paso a las conclusiones.

La información que se necesita para poder realizar la evaluación del CRMR es importante ya que sin los requisitos necesarios esta metodología no puede seguir adelante. Primero se deberá detallar un programa de trabajo, luego la persona que realiza la Auditoría reúne la información necesaria de la Institución para luego pasar a un trabajo clasificado por tareas.

Esta metodología dispone de una lista de datos necesarios los cuales serán verificados por la persona responsable ya que son importantes para que CRMR pueda realizar las tareas adecuadamente.

- Registros de mantenimiento de hardware y software
- Informes detallados de problemas de los sistemas
- Pasos para actualizaciones
- Procedimientos de emergencia
- Monitoreo
- Informes de rendimiento del sistema
- Gestión de espacio en unidad de almacenamiento
- Documentación de aplicaciones
- Registros de paginación de los sistemas
- Volumen total y libre de almacenamiento
- Manuales de procedimientos

Todo trabajo se debe dividir en tareas y estos deben llevar los siguientes pasos:

- Identificación de la tarea
- Descripción de la tarea
- Descripción de posibilidades para una tarea incorrecta
- Definición de ventajas, recomendaciones y beneficios para el cambio o modificación de una tarea
- Evaluación de la practica
- Ajustes determinados para el área auditada
- Posibilidad de agrupación de tareas
- Registro de resultados

1.6.1.4.4 Análisis Comparativo de Metodologías y Estándares de Auditorías Informáticas

De las metodologías existentes para realizar una auditoría informática de las cuales se toma la información de tres metodologías y se tiene como resultado el siguiente cuadro como un resumen breve de los objetivos y actividades que desempeña.

Tabla 1.1 Análisis Comparativo de metodologías

HERRAMIENTA / CARACTERISTICA	ITIL	MAGERIT	CRMR
OBJETIVO	Ayuda a organizar los diferentes departamentos. Alcanzar objetivos corporativos	Investigar los riesgos de los Sistemas de Información. Recomendar medidas apropiadas para controlar dichos riesgos.	Evaluar la gestión de los recursos informáticos Evaluar la eficiencia de la utilización de dichos recursos
BENEFICIO	A través de las directrices y las prácticas que se indican, si se ejecutan se tendría un ahorro económico considerable.	Aporta más conocimiento acerca del estado de la integridad de los sistemas de información	Evalúa el grado de ineficiencia de todos los procesos y métodos de gestión en el proceso de datos para dar una solución a los mismos.
FASES / PROCESOS	Manejo de Incidentes Manejo de Problemas Manejo de Configuraciones Manejo de Cambios Manejo de Entregas	Influye en las fases y actividades de tipo estratégico y condiciona las fases y actividades de tipo logístico	Identificar el alcance Realizar el estudio inicial Determinar recursos necesarios Elaborar plan de trabajo Realizar actividades de auditoría Elaborar informe final.

Elaborado por: Santiago Bayas

En el cuadro anterior se indican los objetivos principales los beneficios y los procesos de cada una de las metodologías analizadas.

Tomando en cuenta los objetivos se puede señalar que ITIL y MAGERIT se basan en la seguridad de los sistemas de información a diferencia de que CRMR a más de la seguridad de los Sistemas se enfoca también en el trabajo de Gestión de Recursos Informáticos que responde a las necesidades actuales de la organización.

En el punto de los beneficios de cada uno de estas se puede observar que CRMR evalúa la eficiencia de los procesos para dar solución a los mismos mientras que ITIL ahorra dinero para la empresa y MAGERIT brinda seguridad a la información.

En las fases o procesos que la metodología CRMR posee se puede notar que es un tipo de trabajo no muy complejo en cada una de las actividades que se desarrollan esto significa que se podrá realizarlas en poco tiempo e incluso no hace falta de un especialista en el tema de auditoría para poder aplicarla como con otras metodologías, por este motivo se ha optado por aplicar la auditoría informática en la Agencia Nacional de Tránsito de Tungurahua utilizado la metodología CRMR la cual según las características antes mencionadas realiza evaluaciones a todos los procesos, captando de mejor manera la ineficiencia de cada punto auditado para poder determinar los cambios necesarios.

1.6.2 Gestión de la Información

Dentro del concepto de gestión de información se puede decir que son aquellos procesos con los cuales se controla las etapas de la información, desde sus inicios, es decir desde su obtención o creación hasta lo que se puede entender como su final el cual podría ser archivarla o a su vez eliminarla según el objetivo con la cual se la obtuvo , en resumen, la gestión de Información se refiere al cómo conseguirla, para quién conseguirla y a qué costo conseguirla siempre y cuando ésta sea veraz y adecuada para la persona correcta para que se pueda tomar la mejor decisión posible.

1.6.2.1 Manejo de la información

En esta sección es en la cual se conoce todas las formas de manejo de la información como por ejemplo el almacenamiento adecuado de información y los respaldos de la investigación realizada ya que si existe un mal manejo de la misma puede ocasionar varios desperdicios de información y de recursos.

1.6.2.2 Seguridad de la Información

Consiste en la preservación de la información tanto su confidencialidad, integridad y disponibilidad, ya que hoy en día la información se considera como un activo fundamental de cualquier organización que vaya en busca del progreso y el mantenimiento en el mercado.

Esta área está enfocada a la estructura informática de la empresa y todo lo que se relacione con la misma, especialmente la información almacenada de diferentes formas según los diversos estándares, métodos, herramientas o protocolos con los cuales se logre minimizar el riesgo a que la información sea mal utilizada, en su libro “Auditoría Informática en la Empresa” (Acha Iturmendi, 1994) enuncia que se divide en dos tipos de seguridad:

- **Seguridad Física**

La seguridad física es la prevención de acceso de personas no autorizadas, además con este tipo de seguridad se pueden verificar varios puntos ya que aun si la empresa se considera segura en base a un ataque externo como hackers o virus siguen existiendo eventos los cuales también deben ser considerados como desastres naturales, imprudencias de los usuarios o ataques internos, este es el motivo por el cual a la seguridad física se la considera uno de los puntos de menor importancia al diseñar un sistema informático (Acha Iturmendi, 1994).

- **Seguridad Lógica**

Con este tipo de seguridad el cual es un complemento de la seguridad física se aplican mecanismos y barreras para resguardar la información dentro del sistema informático, existen varios tipos de técnicas las cuales deben ser

tomadas en cuenta por las instituciones como por ejemplo el restringir el acceso a sistemas, archivos y programas, asegurar que la información llegue solo a su destinatario y que la misma no sea alterada, verificar que los archivos y programas sean utilizados según el proceso que se realice (Acha Iturmendi, 1994)

1.6.2.3 Infraestructura de tecnologías de Información

Como infraestructura de TI se conoce a los diferentes recursos tecnológicos los cuales tienen diversos componentes tales como las diferentes plataformas ya sea de hardware, software, aplicaciones, administración en integración de los sistemas los mismos deben coordinarse entre sí para poder dar a la empresa una infraestructura estable.

CAPÍTULO II

METODOLOGÍA

2.1 Metodología de Investigación

En el presente proyecto se utilizaron los siguientes métodos de investigación:

2.1.1 Método Experimental

Con este método se realizan las pruebas respectivas en el proceso de la auditoría para comprobar si los diferentes procesos que se llevan a cabo se realizan adecuadamente y en cuál de ellos existe algún tipo de retraso.

Para el presente proyecto se realizó investigación bibliográfica, la misma que requirió una amplia búsqueda de información, su análisis y selección de los datos más importantes y necesarios para el desarrollo de la auditoría.

2.1.2 Técnicas

Las técnicas servirán para la recolección de información de los sistemas, políticas de seguridad y los diferentes riesgos informáticos dentro de la Institución.

2.1.2.1 Encuestas

La encuesta consta de 10 preguntas las mismas que buscan conocer cómo se maneja el sistema y que tanta seguridad tienen los usuarios del sistema dentro de la institución.

2.1.2.2 Población

La encuesta se realizó a los 31 funcionarios que trabajan en los departamentos de la Agencia Nacional de Tránsito de Tungurahua.

2.1.3 Análisis de Factibilidad

2.1.3.1 Resultados de las Encuestas

A continuación se describe las 10 preguntas realizadas a los funcionarios de la Agencia Nacional de Transito de Tungurahua junto con el respectivo resultado y análisis e interpretación.

- **Pregunta No. 1**

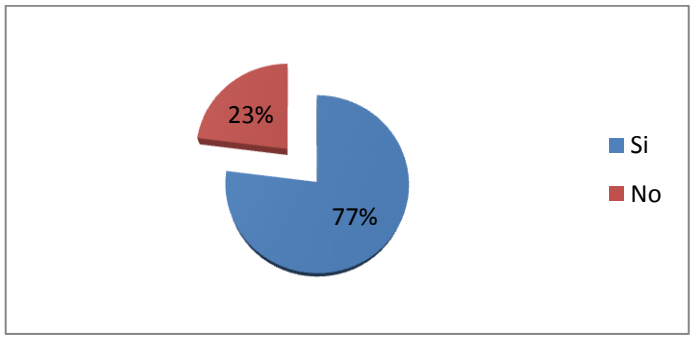
¿La estructura actual de su puesto de trabajo está acorde para que se puedan realizar las funciones eficientemente?

Tabla 2.1 Puesto de Trabajo

Respuesta	Frecuencia	Porcentaje
Si	7	23%
No	24	77%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.1 Puesto de Trabajo



Fuente: Encuesta.
Elaborado por: Santiago Bayas

Análisis e Interpretación.

De las 31 personas encuestadas el 77% dicen no tener un espacio o un lugar de trabajo óptimo para poder realizar las funciones encomendadas mientras que el 23% menciona que si dispone de un lugar de trabajo adecuado. Con esto se puede tomar en cuenta que la institución se vería beneficiada con la auditoría más aun cuando la mayoría está en desacuerdo con la estructura actual del puesto de trabajo asignado.

- **Pregunta No. 2**

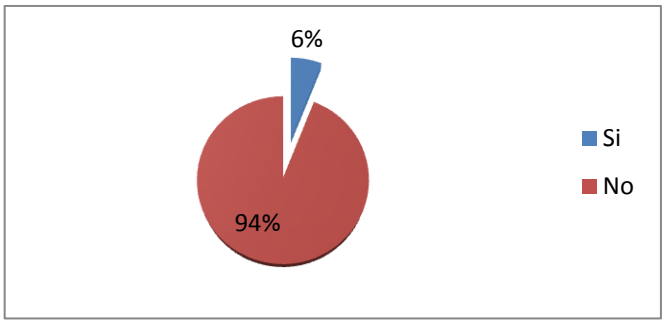
¿Posee Ud. una contraseña para acceder a los sistemas y empezar a realizar sus funciones?

Tabla 2.2 contraseña para accesos

Respuesta	Frecuencia	Porcentaje
Si	2	6%
No	29	94%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.2 Contraseña para accesos



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

Entre las 31 personas encuestadas el 94% dicen no tener contraseñas para poder acceder a los sistema a realizar sus funciones mientras que tan solo el 6% dice si poseer una contraseña, esto indica que la gran mayoría de usuarios corren el riesgo de que la información que poseen sea sustraída y mal utilizada y con la auditoría se podría verificar que tipos de accesos necesitan los usuarios según las diferentes funciones.

- **Pregunta No. 3**

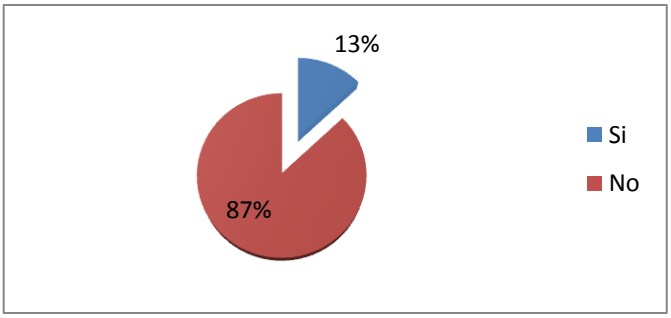
¿Conoce Ud. todo el software o programas que se encuentran instalados en su computador?

Tabla 2.3 Software instalado

Respuesta	Frecuencia	Porcentaje
Si	4	13%
No	27	87%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.3 Software Instalado



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

De las 31 personas encuestadas, el 87% dicen no estar conscientes de todo el software que se encuentra instalado en el computador que utilizan para realizar sus labores 13% dice que si tienen el conocimiento de los programas que han sido instalados. Con esto se determina que el personal de la institución estaría más capacitado en sus funciones al saber acerca del software instalado en los diferentes computadores para así agilitar sus funciones más aun cuando la mayoría está en desacuerdo con la forma de su puesto de trabajo.

- **Pregunta No. 4**

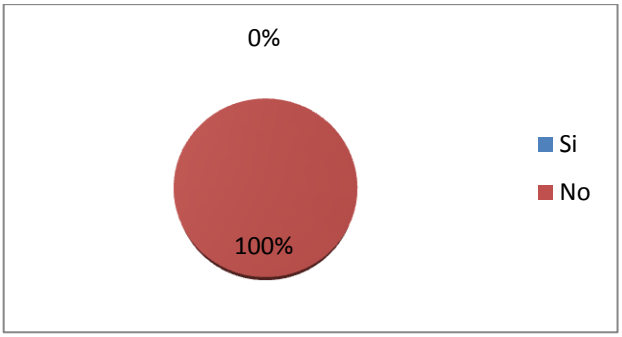
¿Se ha realizado algún proceso de Auditoría Informática en la Organización?

Tabla 2.4: proceso de auditoría

Respuesta	Frecuencia	Porcentaje
Si	0	0%
No	31	100%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.4 Proceso de Auditoría



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

Las 31 personas encuestadas o el 100% del personal de la institución afirman que no se ha realizado ningún proceso de auditoría informática con esto se toma en cuenta que la institución mejoraría todos sus servicios al realizar la misma ya que ayudaría a verificar todos los riesgos y falencias de los sistema de información.

- **Pregunta No. 5**

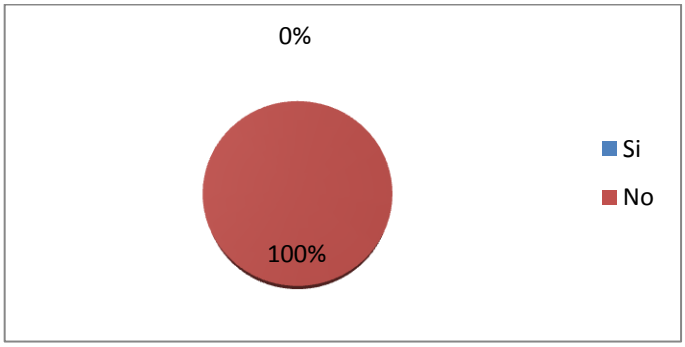
¿La institución tiene planes de contingencia para cualquier eventualidad?

Tabla 2.5 Planes de contingencia

Respuesta	Frecuencia	Porcentaje
Si	0	0%
No	31	100%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.5 Planes de Contingencia



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

Dentro de las 31 personas encuestadas el 100% dicen no tener ningún plan de contingencia o saber de uno implementado en la Agencia, por lo tanto ante cualquier eventualidad la Institución no pudiera solucionar los inconvenientes que se presenten en algún momento.

- **Pregunta No. 6**

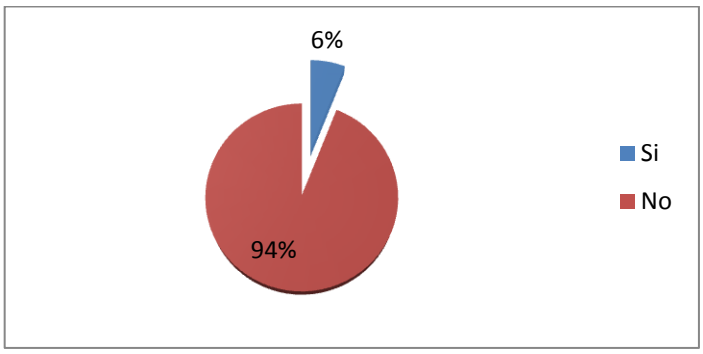
¿El personal de la Institución ha sido capacitado en algún momento en el ámbito tecnológico?

Tabla 2.6 capacitación tecnológica

Respuesta	Frecuencia	Porcentaje
Si	2	6%
No	29	94%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.6 Capacitación Tecnológica



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

De las 31 personas encuestadas el 94% dicen no haber tenido una capacitación en el ámbito tecnológico, mientras que el 6% afirma que ha sido capacitado en el área. Con esto podemos darnos cuenta que la capacitación a los funcionarios de la Institución es primordial para mejorar las funciones que realiza cada uno.

- **Pregunta No. 7**

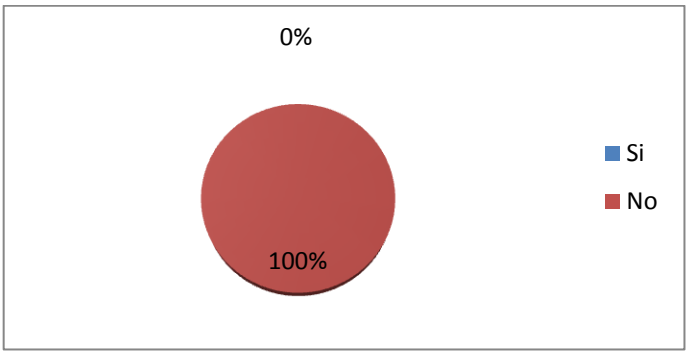
¿Se realizan actualizaciones periódicamente de los programas que son utilizados para cumplir sus funciones?

Tabla 2.7 Actualizaciones de software

Respuesta	Frecuencia	Porcentaje
Si	0	0%
No	31	100%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.7 Actualizaciones de Software



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

Dentro de las 31 personas encuestadas el 100% dicen que no se realiza actualizaciones de programas periódicamente del software instalado en los equipos informáticos, lo cual es primordial para el desempeño de los mismos.

- **Pregunta No. 8**

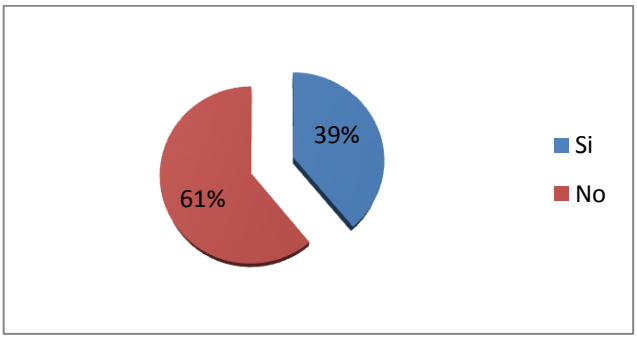
¿Existe algún tipo de seguridad para el acceso al sistema a los usuarios no autorizados?

Tabla 2.8 Seguridad de acceso

Respuesta	Frecuencia	Porcentaje
Si	12	39%
No	19	61%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.8 Seguridad de Accesos



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

Dentro de las 31 personas encuestadas el 61% mencionan que no disponen de algún tipo de seguridad para el acceso de usuarios no autorizados mientras que el 39% dice que poseen algunos tipos de seguridad para así evitar que terceras personas puedan manipular la información.

- **Pregunta No. 9**

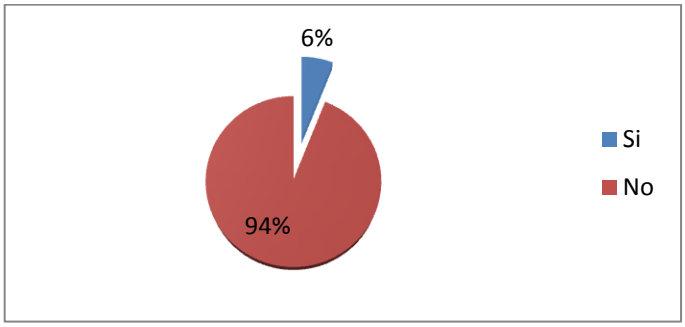
¿Los equipos informáticos responden eficazmente para las actividades diarias?

Tabla 2.9 Equipos informáticos

Respuesta	Frecuencia	Porcentaje
Si	2	6%
No	29	94%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.9 Equipos Informáticos



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

De las 31 personas encuestadas el 94% mencionan que los equipos informáticos no tienen una respuesta rápida en la funciones designadas y en la utilización del sistema mientras que el 6% dice que si tienen un funcionamiento adecuado de sus equipos. Por lo tanto se debería realizar una verificación de equipos para saber si son obsoletos o si solo depende de algún tipo de actualización.

- **Pregunta No. 10**

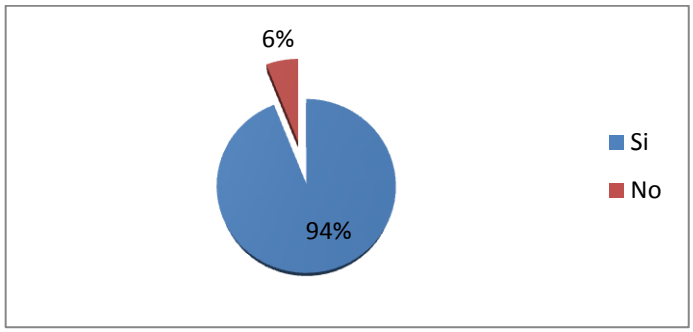
¿Cree Ud. necesario revisiones periódicas de puntos de trabajo para asegurar un buen servicio y evitar algún tipo de fraude con la información?

Tabla 2.10 revisiones periódicas

Respuesta	Frecuencia	Porcentaje
Si	31	100%
No	0	0%
Total	31	100%

Fuente: Encuesta
Elaborado por: Santiago Bayas

Gráfico: 2.10 Revisiones Periódicas



Fuente: Encuesta
Elaborado por: Santiago Bayas

Análisis e Interpretación

Dentro de las 31 personas encuestadas el 100% dicen que les parece muy conveniente realizar revisiones periódicas para evitar cualquier tipo de fraude y mejorar el servicio. Con esto se puede tomar en cuenta que la totalidad de integrantes de la institución está de acuerdo en el mejoramiento del sistema de atención y la toma de medidas para evitar cualquier tipo de fraude o robo informático.

2.1.3.2 Resumen de la Información

Después de haber realizado las encuestas a los funcionarios de la Agencia Nacional de Tránsito de Tungurahua se puede verificar que la institución está descuidando el área Informática la cual es parte primordial para las tareas que realizan cada uno de los funcionarios de la Institución, además el departamento de sistemas tiene que realizar mantenimientos y revisiones de todos equipamiento informático para corregir y evitar falencias que pueden presentarse en cualquier momento.

2.2 Metodología para el desarrollo de la aplicación.

En el presente proyecto se utilizó la metodología CRMR *(Computer Resources Management Review)* lo que significa que realiza una evaluación de la eficiencia de los recursos informáticos. Esta metodología tiene la gran ventaja de que realiza evaluaciones a todos los procesos, captando de mejor manera la ineficiencia de cada punto auditado para poder determinar los cambios necesarios.

Según (Kuna, 2006), en su trabajo titulado: “Asistente para la realización de Autoría de Sistemas en Organismos Públicos o Privados”, en la cual indica las fases de la metodología de desarrollo de Auditoría Informática las cuales son:

2.2.1 Fase 1: Alcance y objetivos de la Auditoría Informática

En esta fase se analizan los límites y el lugar en el cual se va a realizar la auditoría, aquí existe un acuerdo muy detallado entre directivos y auditores. La factibilidad de este proceso depende de una buena definición de esta etapa. (Kuna, 2006).

2.2.2 Fase 2: Planificación del Estudio de Auditoría Informática

En esta fase se especifican las fechas y las diferentes actividades a realizar, después este se envía a las autoridades para la respectiva aprobación. (Kuna, 2006).

2.2.3 Fase 3. Estudio inicial del Entorno Auditable

En esta fase es importante examinar las diferentes actividades generales en particular de las relacionadas con las tecnologías de la información de la Institución.

Se definen las relaciones funcionales de las diferentes áreas de la entidad, el flujo de la información y las personas responsables de cada uno de los puestos, la estructura organizativa, características tanto de software como hardware. (Kuna, 2006).

2.2.4 Fase 4. Recursos

En esta etapa después del estudio inicial del entorno, se determinan los recursos necesarios ya sean estos materiales o humanos para poder realizar la auditoría. (Kuna, 2006).

2.2.5 Fase 5. Actividades de Auditoría Informática

Se llevan a cabo las diferentes actividades planteadas en las fase 4, se aplican las técnicas y se hace uso de las herramientas para garantizar que todos los objetivos sean cumplidos. (Kuna, 2006).

2.2.6 Fase 6. Informe final

“La elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad.” (Kuna, 2006, p. 25). Esta es la última fase dentro de la auditoría se realiza el informe final que va dirigido a los directivos de la entidad auditada.

El modelo estándar indica que debe estar especificada la situación actual de la institución como sus falencias y amenazas hasta las recomendaciones y objetivos.

CAPÍTULO III

RESULTADOS

En este capítulo se detallan todas las fases antes descritas de la metodología CRMR la cual fue seleccionada para poder realizar la "**AUDITORÍA INFORMÁTICA PARA OPTIMIZAR EL MANEJO DE LA INFORMACIÓN Y EQUIPAMIENTO INFORMATICO"** en la Agencia Nacional de Tránsito de Tungurahua - Agencia Ambato. Cabe recalcar que existirán puntos que se han mencionado con anterioridad y que se podrán citar nuevamente según los puntos de la metodología que se vayan explicando

3.1 Fase I: Alcance y objetivos de la Auditoría Informática

3.1.1 Tema del Trabajo

Auditoría Informática Para Optimizar El Manejo De La Información Y Equipamiento Informatico.

3.1.2 Alcance de la Auditoría Informática

El proceso de Auditoría Informática se llevará a cabo en todas las áreas de la Agencia Ambato de la Agencia Nacional de Tránsito, ya que se dispone de la aprobación y total apoyo de las diferentes áreas de dicha Institución.

3.1.2.1 Áreas Auditables

Las Áreas auditables de la Agencia Nacional de Tránsito de Tungurahua son:

- Dirección Provincial
- Secretaria General
- Jefatura de Agencia
- Departamento de Licencias
- Recaudación
- Departamento Medico
- Departamento Psico Sensometrico
- Departamento Tecnológico

3.1.2.2 Áreas no Auditables

Las áreas no auditables se han definido a aquellas en las que se mantiene información confidencial y muy importante a la cual solo tienen acceso personal autorizado tales como:

- Departamento jurídico
- Departamento de Archivo

3.1.2.3 Excepciones del Alcance de la Auditoría

Dentro del presente proyecto es una excepción para el alcance de la auditoría informática a todos los proveedores y empresas que brindan los diferentes servicios externos a la Agencia Nacional de Tránsito de Tungurahua.

3.1.3 Objetivos de la Auditoría Informática

3.1.3.1 Objetivo General

- Realizar una Auditoría Informática para Optimizar el Manejo de la Información y Equipamiento Informático utilizado metodologías y técnicas actualizadas para la verificación de las falencias de la institución y determinar las respectivas soluciones.

3.1.3.2 Objetivos Específicos

1. Recolectar información de los departamentos en el tema informático.
2. Realizar un diagnóstico de la infraestructura de TI mediante el uso de metodologías para auditoría informática.
3. Evaluar las políticas dentro del área informática a nivel organizacional, técnicos y de recursos humanos.

4. Identificar los riesgos de la infraestructura organizacional y equipo informático.
5. Plantear soluciones posibles a los problemas encontrados mientras se realiza la auditoría.
6. Socializar el resultado del informe final de la Auditoría realizada con el departamento de sistemas de la institución.

.2 Fase II: Planificación del Trabajo de Auditoría Informática

3.2.1 Conformación del Equipo Auditor

3.2.1.1 Auditor

El Sr. Santiago Bayas autor del presente documento tiene la formación que se necesita para realizar la Auditoría informática en áreas como seguridad informática, redes, desarrollo de sistema, análisis de sistemas, entre otras.

3.2.1.2 Supervisor

Como supervisor para realizar la Auditoría informática la empresa ha designado a la Ing. Verónica Pérez que es la Jefe de Agencia y que será la encargada de revisar todos los avances del proyecto ya que posee todo el conocimiento acerca de la institución y sus diferentes procesos.

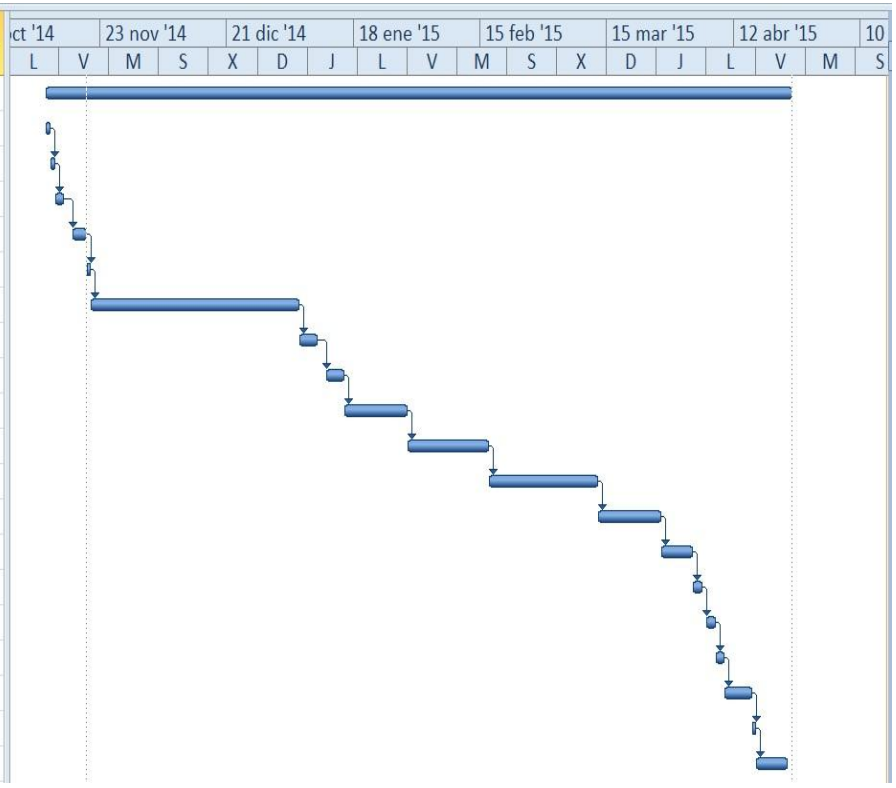
3.2.1.3 Interlocutor

La persona designada para interlocutor será el Sr. Juan Villacis quien trabaja en el puesto de Soporte Tecnológico, por este motivo conoce a todo el personal en los departamentos a auditar dentro de la Institución**.**

3.2.2 Cronograma de Actividades

Ilustración 1: 3.8 Cronograma de Actividades

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Auditoria Informatica**	120 días	mar 11/11/14	vie 24/04/15
2		Conformacion del Equipo Auditoria	1 día	mar 11/11/14	mar 11/11/14
3		Definicion del Alcance y Objetivos	1 día	mié 12/11/14	mié 12/11/14
4		Tramites en la Institucion	2 días	jue 13/11/14	vie 14/11/14
5		Formalizacion de la Auditoria en la Institucion	3 días	lun 17/11/14	mié 19/11/14
6		Elaboracion del Cronograma de Actividades	1 día	jue 20/11/14	jue 20/11/14
7		**Evaluacion del Control Interno Informatico**	32 días	vie 21/11/14	lun 05/01/15
8		Recopilacion de Informacion de la Institucion	4 días	mar 06/01/15	vie 09/01/15
9		Analisis de la Informacion Operacional	4 días	lun 12/01/15	jue 15/01/15
10		Recopilacion de Informacion Detallada	10 días	vie 16/01/15	jue 29/01/15
11		Analisis de Informacion Detallada	12 días	vie 30/01/15	lun 16/02/15
12		Recopilacion de Informacion Detallada	18 días	mar 17/02/15	jue 12/03/15
13		Analisis de Informacion Detallada	10 días	vie 13/03/15	jue 26/03/15
14		Definicion de Areas Criticas	5 días	vie 27/03/15	jue 02/04/15
15		Elaboracion de Carta a Gerencia	2 días	vie 03/04/15	sáb 04/04/15
16		Elaboracion del Informe Final	2 días	lun 06/04/15	mar 07/04/15
17		Revision del Borrador del Proyecto	2 días	mié 08/04/15	jue 09/04/15
18		Correccion del Documento	4 días	vie 10/04/15	mié 15/04/15
19		Revision Final	1 día	jue 16/04/15	jue 16/04/15
20		Presentacion	5 días	vie 17/04/15	jue 23/04/15



Elaborado por: Santiago Bayas

3.3 Fase III Estudio inicial del Entorno Auditable

3.3.1 Antecedentes y Evolución de la ANT

> “El 29 de marzo del 2011 la Asamblea Nacional Constituyente expuso en el Registro Oficial Suplemento 415, la Ley Orgánica Reformatoria a la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial, esta nueva ley realizó cambios sustanciales en la Organización del Sector de Transporte, con el objetivo de armonizar la ley con las disposiciones constitucionales que otorgan a los Gobiernos Regionales Autónomos Descentralizados” (Sitio Web ANT, 2014).

Desde ese entonces la Agencia Nacional de Tránsito (ANT) y la Comisión de Tránsito del Ecuador (CTE) tienen objetivos claros y bien definidos los mismos que garantizan el control del transporte terrestre, tránsito y de la seguridad vial en el Ecuador y la regulación del mismo.

Los diferentes objetivos para aumentar la calidad del servicio de transporte terrestre y el tránsito en la red vial, la eficiencia operacional, el nivel de seguridad vial, el uso eficaz del presupuesto y el desarrollo del talento humano, ha dado paso a que las Instituciones sigan buscando formas o técnicas que aseguren el cumplimiento de dichos objetivos y así garantizar la regulación

mediante la planeación y control del transporte terrestre, tránsito y seguridad vial.

El área informática es una de las más importantes dentro de cualquier empresa ya que sin este departamento toda la información que posea la Institución se vería afectada en el momento de que se ocasione algún problema inesperado, por este motivo se debe tomar medidas necesarias para evitar cualquier eventualidad.

3.3.2 Fundamentación Legal

La Agencia Nacional de Tránsito de Tungurahua (ANT), tiene como finalidad el controlar en todas las formas la gestión del Transporte Terrestre, Tránsito y Seguridad Vial, para poder garantizar la movilidad terrestre, prestando servicios de calidad que satisfagan a la ciudadanía teniendo en cuenta la preservación del medio ambiente y contribuyendo al desarrollo del País. (Sitio Web ANT, 2014).

Art. 1.- Principio de Publicidad de la Información Publica

Las organizaciones de trabajadores y funcionarios públicos del estado y demás están sometidos al principio de publicidad, es decir, toda información que posean es pública, con las respectivas excepciones.

Art. 2.- Objeto de la ley orgánica de transparencia y acceso a la información publica

Esta ley garantiza el derecho del público al acceso a la información en conformidad con las garantías detalladas en la Constitución Política de la República del Ecuador.

Art. 7.- Difusión de la Información Publica

La transparencia de la gestión administrativa al cual conocen todas las instituciones públicas del Estado en los términos del artículo 118 de la Constitución Política están especificados en el artículo 1 de la ley, difundidos a través de un portal de información, así como los medios necesarios que están a disposición de las personas e implementados en la institución.

A la Agencia Nacional de Tránsito le corresponde cumplir con los siguientes objetivos y funciones:

- Determinar reglas que faciliten la gestión y control óptimo del transporte terrestre, tránsito y seguridad vial.
- Diseñar sistemas modernos en la asistencia técnica de las escuelas de conducción.
- Reducir el número de accidentes de tránsito en las vías y carreteras a nivel nacional aumentando a su vez la seguridad vial.

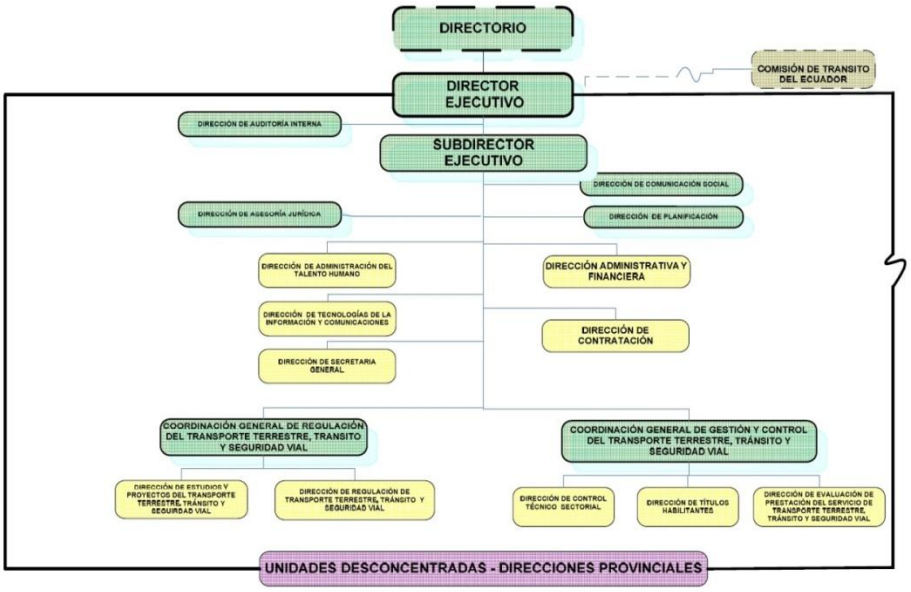
- Contribuir en lo que se refiere a tránsito, transporte y seguridad vial con las municipalidades en el proceso de descentralización y desarrollo local.
- Implementar técnicas para la supervisión y evaluación permanente de conductores de los diferentes transportes terrestres.
- Implementar sistemas de planificación y control administrativo a través de regulaciones sectoriales y proyectos que ayuden al cumplimiento de la misión de la ANT.
- Incentivar el desarrollo del transporte terrestre, tránsito y seguridad vial al igual que el mejoramiento continuo de la planificación con entidades nacionales e internacionales.

3.3.3 Entorno Organizacional

3.3.3.1 Organigrama Estructural de la Institución

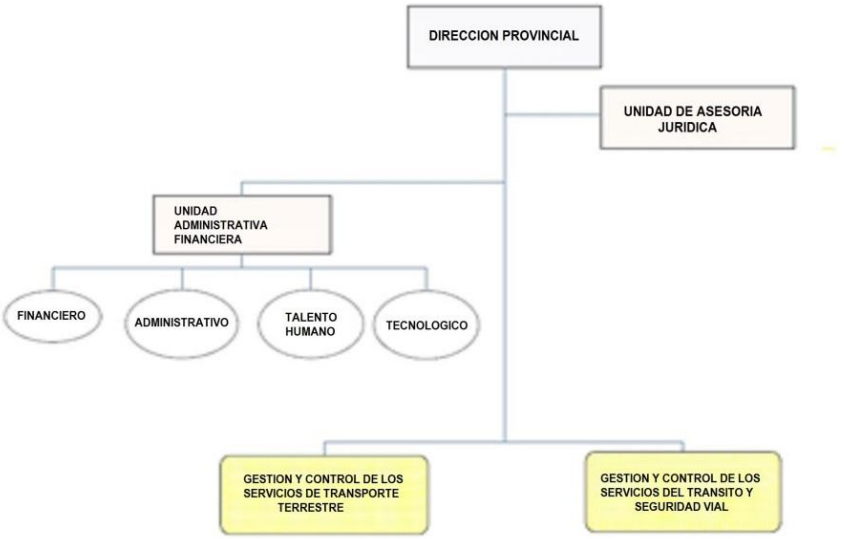
En el siguiente gráfico se encuentra detallado la estructura general de la Agencia Nacional de Transito a nivel nacional, cabe recalcar que cada provincia dispone de un tipo de estructura similar la cual depende de cada provincia y de las diferentes áreas, la forma en la cual está estructurada.

Ilustración 3.9 Estructura Organizacional Nacional



Fuente: www.ant.gob.ec (2004)

Ilustración 2: 3.10 Estructura Organizacional Provincial

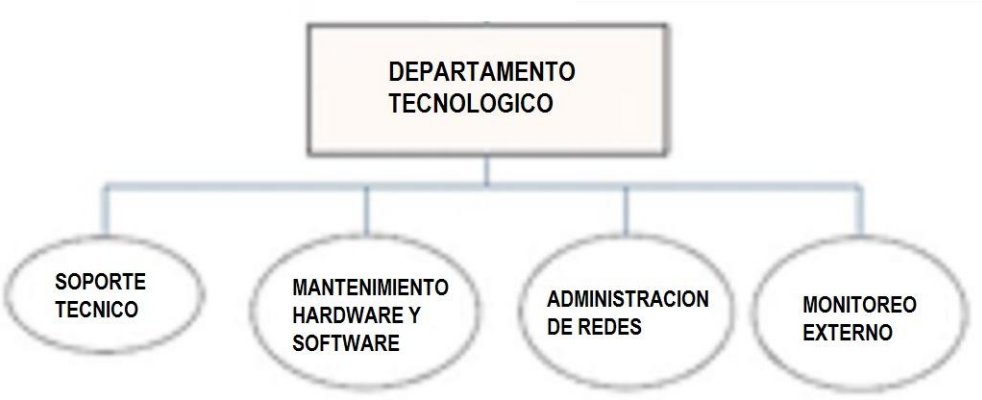


Fuente: www.ant.gob.ec (2004)

Según el organigrama estructural provincial se puede observar que dentro de la unidad administrativa se encuentra el área tecnológica la cual se encarga de todo el equipamiento informático y los diferentes sistemas de información su mantenimiento y actualización, que utiliza cada agencia para el desarrollo de sus funciones, cabe indicar que en la Agencia Ambato el área tecnológica no cuenta con un organigrama estructural el cual pueda delimitar funciones e interacciones de cada sección tecnológica.

Por el motivo de que el departamento tecnológico no dispone de una estructura organizacional se puede sugerir un organigrama aunque se debe tomar en cuenta los diferentes procesos que se realizan en el área tecnológica y dividirlas en áreas específicas.

Ilustración 3.11 Organigrama estructural departamento tecnológico



Elaborado por: Santiago Bayas

3.3.3.2 Descripción de Funciones

En este punto se realiza un análisis del Departamento Tecnológico y de todas sus secciones.

- **Departamento Tecnológico**

El objetivo que tiene el Departamento Tecnológico de la Agencia Ambato de la ANT es el de mantener y dar soporte al hardware y software que posee la Institución así como sigue los procedimientos de custodia de sistemas de información.

Funciones:

- Proponer un plan de tecnologías de la información y comunicaciones.
- Administrar y verificar la utilización de los recursos tecnológicos que tiene la ANT.
- Participar como contraparte técnica en la adquisición de bienes y servicios tecnológicos.
- Presentación de informes del cumplimiento de objetivos y resultados de la unidad.
- Asegurar la utilización de los sistemas y paquetes informáticos de la institución a los usuarios internos y externos.

- Utilizar nuevas tecnologías de información para la innovación de los procesos organizacionales de la Agencia Nacional de Tránsito.

Según la recomendación del organigrama estructural del área de tecnologías de la Información se llevan a cabo algunas actividades por áreas las cuales son:

- **Área de Mantenimiento de Hardware y Software**

Esta área es la encargada de asistir, mantener, instalar y actualizar todo el equipamiento informático de la ANT con el fin de garantizar el mejor desempeño posible definiendo funciones y programando las diferentes actividades que sean necesarias para poder llegar al objetivo del área.

- **Área Soporte Técnico**

El área de soporte técnico es la responsable de atender requerimiento y prestar atención correctiva a las áreas que necesiten resolver algún tipo de inconveniente como por ejemplo se pueden mencionar el ayudar a resolver problemas que se puedan presentar con el equipamiento informático, sistemas de información, bases de datos, entre otros.

- **Administración de Redes**

Esta área es encargada de la administración de la red, en esta área se configura la red, se asigna contraseñas, permisos y ayuda a los usuarios, además de que se supervisa y se controla el hardware y software de una red incluyendo el esquema de seguridad y administración de procesos y aplicaciones en red.

- **Monitoreo Externo**

En esta área se desarrollan un monitoreo periódico de las instituciones públicas las cuales migran la información indispensable de cada usuario la cual se va actualizando según las necesidades de cada institución, por este motivo el monitoreo debe ser verificado a cada momento por el personal designado el cual debe tener suficiente conocimiento del tema.

3.3.3.3 Talento Humano

En el departamento tecnológico de la Agencia Nacional de Tránsito de Tungurahua están a cargos dos personas las cuales se encargan de todo el trabajo requerido por las demás áreas en el aspecto informático.

- **Puesto:** Jefe del Departamento Tecnológico.

Nombre: Ing. Leonardo Tenelema.

Objetivo:

- Supervisión, dirección y planificación del control y mantenimiento del equipamiento informático y de los sistemas de información de la Agencia Nacional de Tránsito.

Funciones

- Planificar, dirigir, coordinar, y controlar los sistemas de información que se maneja en la Institución.
- Gestionar el mantenimiento del equipamiento informático.
- Coordinar las revisiones periódicas de los equipos de comunicaciones.
- Verificar el buen funcionamiento de la red interna de la institución.
- Realizar las actualizaciones respectivas de los equipos y de los sistemas de información para poder asegurar el buen funcionamiento de los mismos.

Escolaridad

Título Profesional de Ingeniería en Sistemas de la Universidad Técnica de Ambato

Experiencia

Cuatro años en Jefatura de Departamento Tecnológico.

Conocimientos

Mantenimiento de hardware y software, administración de redes y usuarios, configuración de servidores.

Habilidades

Aptitud en manejo de grupos, ejecución en labores de control de sistemas, registros.

- **Puesto:** Asistente del Departamento Tecnológico.

Nombre: Sr. Juan Villacis.

Objetivo:

- Mantenimiento, soporte del equipamiento informático y de los sistemas de información de la Agencia Nacional de Tránsito.

Funciones

- Organizar los reportes emitidos por los sistemas de información de le institución.
- Reportar las necesidades de insumos y materiales propios del área.

- Realizar respaldos de información siguiendo procedimientos establecidos.
- Elaborar informes periódicos de las actividades realizadas.
- Detectar fallas técnicas de los equipos y sistemas de información.

Escolaridad

Egresado de la Escuela de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ambato.

Experiencia

Dos años

Conocimientos

Paquetes informáticos, mantenimiento hardware y software, configuración de redes.

Habilidades

Apto para ejecución de sistemas varios.

Discreción, iniciativa y orden en seguir funciones designadas.

3.3.3.4 Análisis del entorno Organizacional

3.3.3.4.1 Relaciones Jerárquicas y Funcionales

La Agencia Nacional de Tránsito tiene los siguientes niveles jerárquicos los cuales son indispensables para el cumplimiento de sus fines y objetivos.

- **Primer Nivel:** En este primer nivel pertenecen las siguientes áreas.
    - Directorio
    - Jefe de Agencia
    - Auditoría Interna
    - Departamento Jurídico
    - Secretaria General

- **Segundo Nivel:** en este nivel están los siguientes departamentos.
    - Dirección Financiera
    - Dirección Administrativa
    - Dirección Técnica

- **Tercer Nivel:** en el Tercer nivel se encuentra las siguientes áreas.
    - Tesorería
    - Departamento Medico
    - Archivo
    - Departamento Tecnológico
    - Actualización de Datos

3.3.3.5 Flujo de la información

Las diferentes secciones deberían acatar las órdenes de la persona inmediata superior, significa que en el momento de tomar alguna decisión esta se debería realizar por medio de solicitudes ya que existen relaciones entre las diferentes direcciones.

Para el área tecnológica de igual forma se acatan órdenes de la persona superior además esta área responde al área administrativa según el organigrama provincial ya que está dentro de este departamento; el inconveniente es que no cuenta con un organigrama estructural que permita verificar las funciones y actividades a realizar, aunque el personal de esta área esté debidamente capacitado para el puesto en el que se encuentran cabe recalcar que el personal no es suficiente para las actividades que deben ser realizadas en la Institución.

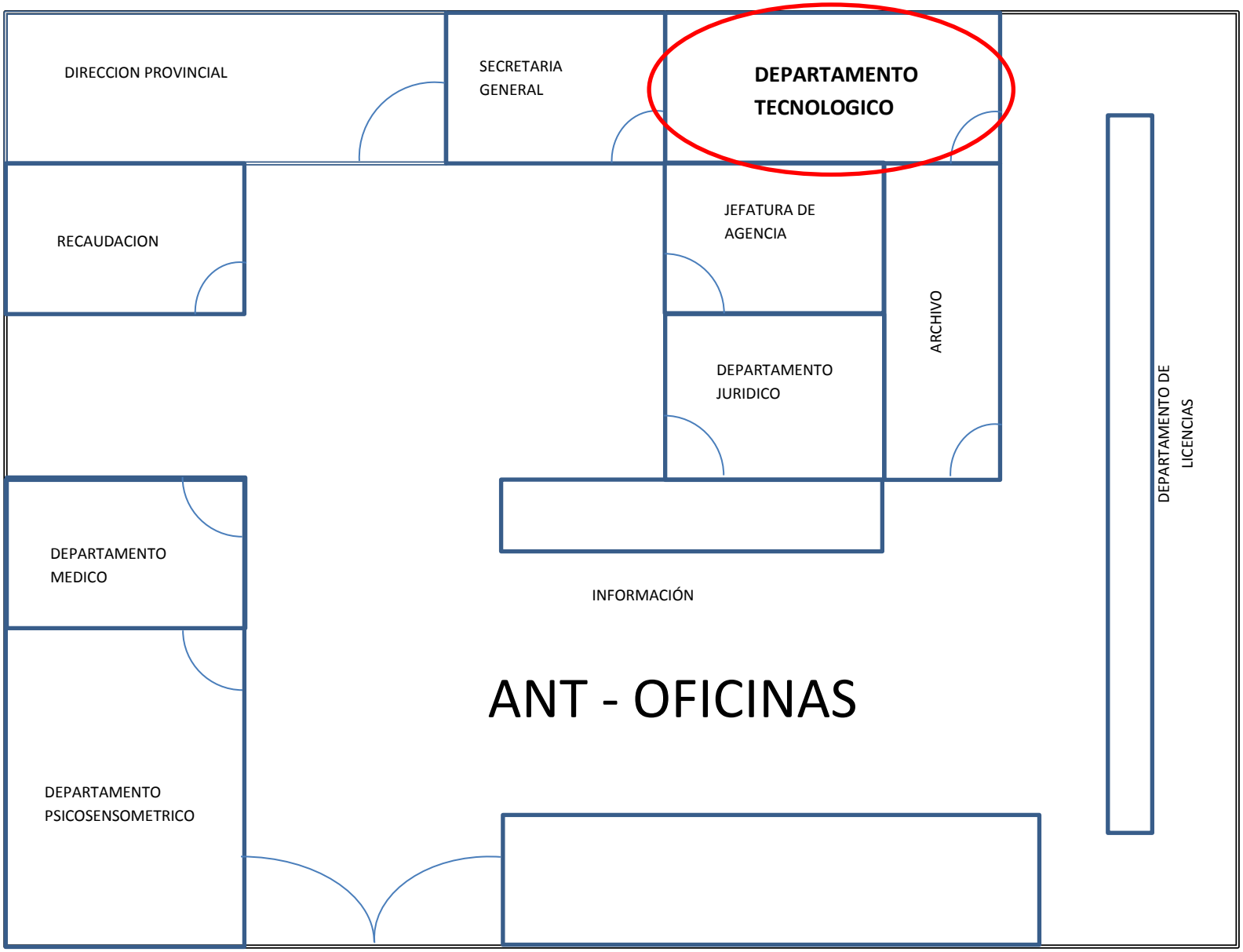
3.3.4 Entorno Operacional

3.3.4.1 Situación Geográfica del Área Tecnológica

La Agencia Nacional de Tránsito de Tungurahua se encuentra ubicada junto al Parque Troya y al cetro de exposiciones PROA en la calle Galo Vela Álvarez, y consta de un solo ingreso tanto para los funcionarios de la Agencia como para todos los usuarios que se benefician de los servicios que brinda la Institución.

La estructura de la Agencia está distribuida en un solo piso en el cual están divididas todos los departamentos para brindar los diferentes servicios como por ejemplo, el Área Administrativa, Licencias, Departamento Medico, Recaudación, Departamento Jurídico, Recursos Humanos, etc.

Ilustración3.12 Diagrama de Disposición Física



Elaborado por: Santiago Bayas

El área tecnológica está ubicada atrás de las áreas de secretaria general, jefatura de agencia y de archivo, frente al área de licencias en la cual se encuentra su puerta de acceso, con esto se corre riesgo para que terceras personas puedan ingresar al departamento tecnológico sin ser vistas ya que no existe seguridad para el ingreso a esta área, existe también algunos aspectos deficientes en los diferentes departamentos los cuales se verifican en las siguientes tablas.

Tabla 3.11 conexiones eléctricas y datos

CONEXIONES ELÉCTRICAS Y DATOS						
	PCS	UPS	ACCESS POINTS	SWITCH	CONEXIÓN A TIERRA	CANALETAS
DIRECCIÓN PROVINCIAL	1	1	--	1	X	X
SECRETARÍA GENERAL	1	--	1	--	X	X
JEFATURA DE AGENCIA	1	1	--	1	--	X
RECAUDACIÓN	1	--	1	--	--	X
LICENCIAS	4	1	--	1	X	X
DEPARTAMENTO PSICOSENSOMÉTRICO	2	--	--	--	--	X
DEPARTAMENTO MÉDICO	1	--	1	--	--	X
DEPARTAMENTO TECNOLÓGICO	2	1	1	1	X	X

Elaborado Por: Santiago Bayas

Tabla 3.12 seguridad física

SEGURIDAD FISICA						
	EXTINTORES	ALARMAS	VIGILACIA	ILUMINACION	VENTILACION	HUMEDAD
DIRECCIÓN PROVINCIAL	1	--	--	X	1	X
SECRETARÍA GENERAL	--	X	--	--	--	X
JEFATURA DE AGENCIA	--	--	--	X	1	--
RECAUDACIÓN	--	--	X	--	--	X
LICENCIAS	1	--	X	X	--	--
DEPARTAMENTO PSICOSENSOMÉTRICO	--	--	--	--	--	X
DEPARTAMENTO MÉDICO	--	X	--	--	--	X
DEPARTAMENTO TECNOLÓGICO	--	--	--	--	--	--

Elaborado Por: Santiago Bayas

Las tablas anteriores detallan lo que se encontró según cada departamento de la institución.

La seguridad física de la institución según los resultados obtenidos en la auditoria es escaza ya que no se ha realizado antes un estudio para las diferentes necesidades de la institución como por ejemplo: no disponen de suficientes extintores ni alarmas, como se indicó el equipo de seguridad no es suficiente para el gran número de personas que ingresa a la institución.

De igual forma el tema de la ventilación es escaza no existe sistemas de aire acondicionado solo ventiladores por esta razón la humedad que se concentra en los departamentos puede afectar al equipamiento informático de toda la institución y a los sistemas de información que son utilizados para el desarrollo de las funciones.

En el departamento tecnológico las conexiones eléctricas son defectuosas y algunas no tienen la debida seguridad, aparte de que se encuentran equipos informáticos o partes de los mismos encima de los escritorios al igual que cables de red que generan la desorganización de todo el departamento como se demuestra en las siguientes fotografías.

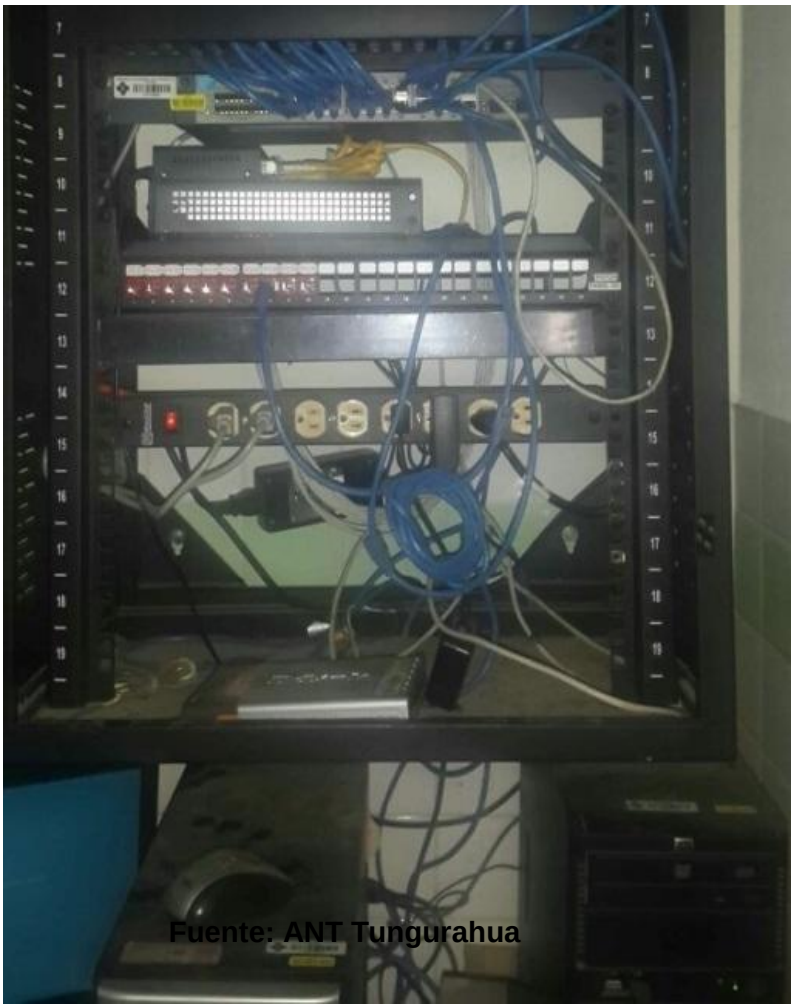
Ilustración 3.13 Departamento Tecnológico

Fuente: ANT Tungurahua

Ilustración 3.14 Desorganización de Equipos

Fuente: ANT Tungurahua

Ilustración 3.15 Cables de Seguridad



Fuente: ANT Tungurahua

3.3.4.2 Problemas

Tabla 3.13: Problemas

PROBLEMA	DESCRIPCION	RESPONSABLE
Instalaciones eléctricas en malas condiciones	El 50% de las tomas de corriente no tienen protección y los cables están vistos.	Jefe de departamento tecnológico
El cableado de red está sin identificación	Los cables de red no se encuentran identificados a más de que están por encima de los equipos	Asistente de departamento tecnológico
No hay control en el acceso de personas	El departamento informático no cuenta con algún tipo de seguridad para el ingreso de personal, cualquier persona puede ingresar aun sin ser vista por el equipo de seguridad	Jefe de departamento tecnológico
Desorganización de equipos en el departamento informático	Los equipos que están siendo revisado se encuentran desarmados o encima de los escritorios junto con cajas de equipos anteriores o de suministros de oficina	Asistente de departamento tecnológico
No hay suficientes extintores	Solo existe dos extintores en la agencia uno en la dirección provincial y otro en el área de licencias los otros departamentos no cuentan con un extintor cerca	Jefe de departamento tecnológico
No existe suficiente ventilación	No hay ventilación en la mayoría de áreas es por este motivo que algunas áreas se concentra demasiada humedad la que puede causar daños en las instalaciones eléctricas	Jefe de departamento tecnológico

Elaborado por: Santiago Bayas

3.3.4.3 Recomendaciones

Tabla 3.14: Recomendaciones

RECOMENDACION	DESCRIPCION	RESPONSABLE
Mejorar las Instalaciones eléctricas	Deberá gestionarse para que personal adecuado pueda realizar el cambios y revisión de las instalaciones eléctricas	Jefe de departamento tecnológico
Identificación del cableado de la red	Todo el cableado de la agencia debe ser revisado para poder etiquetarlo y así ganar organización del área	Asistente de departamento tecnológico
Seguridad para el ingreso del personal	Gestionar adecuadamente para poder colocar algún tipo de seguridad de ingreso al departamento tecnológico	Jefe de departamento tecnológico
Reorganización de equipos en el departamento informático	Reorganizar el área técnica para lo cual se debe sacar materiales u objetos inservibles y así poder disponer de más espacio para realizar el trabajo adecuadamente	Asistente de departamento tecnológico
Adquisición de extintores	Coordinar con los directivos la adquisición de extintores y alarmas contra incendios para los departamentos de la agencia y poder colocarlos en puntos adecuados	Jefe de departamento tecnológico
Implementación de ventilación	La implementación de mas ventilación seria adecuada ya que existe demasiada humedad en algunas áreas de la agencia arriesgando la integridad de instalaciones eléctricas y demás, cabe recalcar de que se también el número de personas que ingresa a la institución provoca en el ambiente incomodidad en funcionarios y usuarios	Jefe de departamento tecnológico

Elaborado por: Santiago Bayas

3.3.5 Inventario

Se realizó un inventario tanto de hardware como de software en la Agencia Ambato de la ANT con la herramienta PC – AUDIT la cual recoge datos del sistema, software instalado y de los procesos en ejecución.

3.3.5.1 Hardware y Software

3.3.5.1.1 Vigente

La Agencia Nacional de Tránsito de Tungurahua en la actualidad no cuenta con un inventario en el cual se pueda constatar la existencia, cambios o perdidas de equipos informáticos, accesorios, entre otros ya que el inventario se lo manejaba desde la matriz de la ciudad de Quito, pero en los últimos años se eliminó ese inventario ya que se realizaron cambios y actualizaciones de equipos los cuales no se inventariaron, tan solo se codificaron de manera general para en un futuro poder realizar el inventario total.

3.3.5.1.2 Real

Se realizó un inventario de los equipos de las áreas auditables tomando en cuenta los códigos que se habían asignado a cada equipo informático.

- **Dirección Provincial**

Responsable: Lic. Lourdes Mayorga

Tabla 3.15 Equipo dirección provincial

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A18,02,1,022,4	Xtratech	W7006S-97F1569012291
Teclado	A18,02,1,97,3	Hp	BAUDUQ0VB0V4DU
Mouse	S/C	Hp	600553-002
Regulador	A18,02,1,023,7	Speedmind	654342146345531
Impresora	A18,02,1,015,4	Lexmark E460 DW	72HGYWQ
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A18,02,1,01,1	Intel	---
Procesador	A18,02,1,01,1	Intel	---
Memoria RAM	A18,02,1,01,1	Markvision	---
Disco Duro	A18,02,1,01,1	Lg	CRD250HDETDC23455
DVD-RW	A18,02,1,01,1	Lg	HJKDVDRWFH-209833
SOFTWARE			
NOMBRE		**VERSION**	**LICENCIA**
Adobe Flas Player 10 ActiveX		10.0.42.34	---
Adobe Flash Player 16 NPAPI		16.0.0.305	---
Adobe Reader XI (11.0.10)		11.0.10	---
Ares 2.2.5		2.2.5	---
Avira Antivirus		15.0.9.504	---
Avira		1.1.34.19732	---
CCleaner		3.17	---
ColorClick 1.3		1.3	---
CyberLink PowerDVD 10		10.0.1830	---

Microsoft Office 2007 Service Pack 3		YFKBB-PQJJV-G996G-VWGXY-2V3X8
Microsoft Visual Web Developer	12.0.6612.1000	---
Microsoft Windows 7 Home Premium	6.1.7601	00359-OEM-8992687-00006
Mozilla Firefox 37.0.1 (x86 es-ES)	37.0.1	---
MySQL Tools for 5.0	5.0.16	---
Nero 7 Ultra Edition	7.02.0936	1A20-020E-0000-1486-1210-5583
SQL Server System CLR Types	10.0.1600.22	---
Tr@nslation Plus		---
USB Disk Security		---
Visual C++ 2008 x86 Runtime	9.0.30729.01	---
Visual Studio .NET English	9.0.30729	---
VLC media Player 1.1.7	1.1.7	---
Windows Mobile 5.0 SDK R2	5.00.170.06	---

Elaborado por: Santiago Bayas

- **Secretaria General**

Responsable: Lic. Jacqueline Urbina

Tabla 3.16: equipo secretaría general

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A01,33,5498,1	Dell	CN-04-FF47-64180-3AS-0F48
Teclado	A01,01,261,15	Hp	TECUS B-281
Mouse	A01,33,5499,4	Dell	C-0411D3V71581399-0458
Regulador	A01,03,252,1	Speedmind	654342146345531
Impresora	A01,03,252,3	Lexmark E460 DW	76IUTCZSQ
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**

Mainboard	A01,02,114,01	Intel	---
Procesador	A01,02,114,01	Intel	---
Tarjeta de Video	A01,02,114,01	Nvidia G-Force	---
Memoria RAM	A01,02,114,01	Markvision	---
Disco Duro	A01,02,114,01	Samsung	HDD320AYJKDFBNV0245
DVD-RW	A01,02,114,01	Samsung	QWDVDRWFH-0827452
SOFTWARE			
NOMBRE		**VERSION**	**LICENCIA**
Actualización de NVIDIA		1.11.3	---
Adobe Flash Player 16 NPAPI		16.0.0.296	---
Adobe Reader Español		9.5.5	---
Ares		2.2.5	---
Avira Free Antivirus		14.0.7.468	---
Facebook Video Calling		3.1.521	---
Java 7 Update 45		7.0.450	---
LimeWire		5.6.2	---
Microsoft Office Enterprise 2007		12.0.4518.1014	KGFVY-7733B-8WCK9-KTG64-BC7D8
Microsoft Visual Studio 2010			---
Microsoft Visual Studio			---
Microsoft Windows 7 Home Premium		6.1.7601	00426-OEM-8992662-00497
Mozilla Firefox (x86 es-ES)		32.0.1	---
SQL Server System CLR Types			---
Tr@nslation Plus			---
USB Disk Security			---
Visual Studio .NET Prerequisites			---
VLC media player		1.1.7	---
Windows Mobile 5.0 SDK		5.00.1700.5.14343.06	---

Elaborado por: Santiago Bayas

- **Jefatura de Agencia**

Responsable: Ing. Verónica Pérez

Tabla 3.17: Equipo Jefatura de Agencia

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A14,02,1,022,4	Hacer	ESJS42082334891
Teclado	A14,12,11,02,2	Genius	KJLSA2309
Mouse	A14,02,10,22,6	Genius	SGF83234SDKL
Regulador	A14,02,10,24,23	Speedmind	654342146345531
Impresora	A14,02,10,25,8	Lexmark E460 DW	923JLXZWCX
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A14,9,14,23	Intel	---
Procesador	A14,9,14,23	Intel	---
Memoria RAM	A14,9,14,23	Kingston	---
Disco Duro	A14,9,14,23	Lg	CRD250HDETDC23455
DVD-RW	A14,9,14,23	Lg	HJKDVDRWFH-209833
SOFTWARE			
NOMBRE		**VERSION**	**LICENCIA**
Adobe Flash Player 16 NPAPI		16.0.0.296	---
Adobe Reader Español		9.5.5	---
Avira Antivirus		12.27.0.890	---
Avira		14.0.6.448	---
CCleaner		1.1.27.25527	---
ColorClick 1.3			---
Compresor WinRAR			---
Microsoft .NET Framework 4.5.1		4.0.30319	---
Microsoft Document Explorer 2008		12.0.4518.1014	---

Microsoft Office 2007 Service Pack 3 (SP3)	12.0.4518.1014	KGFVY-7733B-8WCK9-KTG64-BC7D8
Microsoft Windows 7 Home Premium	6.1.7601	00254-OEM-36773362-01548
Mozilla Firefox 37.0.1 (x86 es-ES)		---
Mozilla Maintenance Service	12.0.4518.1014	---
MySQL Tools for 5.0	12.0.4518.1014	---
SQL Server System CLR Types		---
USB Disk Security		---
Visual C++ 2008 x86	32.0.1	---
Mozilla Maintenance Service		---
MySQL Tools for 5.0		---
Nero 7 Ultra Edition		---
Tr@nslation Plus		---
USB Disk Security		---
Visual C++ 2008 x86 Runtime	9.0.30729.01	---
Visual Studio .NET Prerequisites - English		---
VLC media player	1.1.7	---
Windows Mobile 5.0 SDK R2	5.00.1700.5.14343.06	---

Elaborado por: Santiago Bayas

- **Recaudación**

Responsable: Ing. Verónica Pérez

Tabla 3.18: Equipo Recaudación

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A08,05,4,02	Lg	LKMSDVLGCGD90
Teclado	A08,15,6,04	Genius	KJLVADWADS

Mouse	A08,15,4,01	Genius	SGF425209SAH
Regulador	A08,17,4,23	Speedmind	5698414909289Y6
Impresora	A08,13,4,09	Lexmark E460 DW	41652SDSDLXZA
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A08,12,11,22	Intel	---
Procesador	A08,12,11,22	Intel	---
Memoria RAM	A08,12,11,22	Kingston	---
Disco Duro	A08,12,11,22	Seagate	SGD180A-SD23
DVD-RW	A08,12,11,22	Lg	HJKDVDRWFH-209833

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Adobe Flash Player 16 NPAPI	16.0.0.296	---
Adobe Reader Español	9.5.5	---
Ares	2.2.5	---
Avira Antivirus	12.27.0.970	---
Avira	14.0.7.468	---
CCleaner	1.1.27.25527	---
Compresor WinRAR		---
CyberLink PowerDVD 10	3.1.521	---
D3DX10	7.0.450	---
Citrix online plug-in	12.0.0.6410	---
Microsoft Office 2007 Service Pack 3 (SP3)	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
Microsoft Windows 7 Home Premium	6.1.7601	00426-OEM-8992662-00400
HydraVision	4.2.210.0	---
SITCON	1.0 07.01.2013-08.00	---
USB Disk Security		---
Visual C++ 2008 x86 Runtime	32.0.1	---

NiceLabel Suite	3.6.2	---
UltraVnc	3.0.9379	---
WampServer	2.2	---

Elaborado por: Santiago Bayas

- **Licencias**

Responsable: Ing. Gabriela Barona

Tabla 3.19: Equipo Uno de Licencias

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A03,02,7,10	Samsung	SDCV420QD-LDSG
Teclado	A03,02,7,10	Speedmind	1906732
Mouse	A03,02,7,10	Speedmind	78387NMS
Regulador	A03,02,7,10	Speedmind	0191265394011K6
Impresora	A03,02,7,10	Lexmark E460 DW	914383FSLELXPC
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A03,09,4,11	Intel	---
Procesador	A03,09,4,11	Intel	---
Memoria RAM	A03,09,4,11	Markvision	---
Disco Duro	A03,09,4,11	Samsung	SGD180A-SD23
Lector de Memorias	A03,09,4,11	Genérico	---
DVD-RW	A03,09,4,11	Lg	HJKDVDRWFH-209833
SOFTWARE			
NOMBRE	**VERSION**	**LICENCIA**	
Adobe Flash Player 16 NPAPI	16.0.0.296	---	
SITCON	1.0 07.01.2013-	---	

	08.00	
UltraVnc	3.0.9379	---
Adobe Reader Español	9.5.5	---
Ares	2.2.5.1	---
Avira Antivirus	12.27.0.970	---
CCleaner	1.1.27.25527	---
Microsoft Office 2007 Service Pack 3 (SP3)	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
Compresor WinRAR	---	---
CyberLink PowerDVD 10	3.1.521	---
Citrix online plug-in	12.0.0.6410	---
Microsoft Windows 7 Home Premium	6.1.7601	01602-OEM-62204556-00321
HydraVision	4.2.210.0	---
Mozilla Maintenance Service	12.0.4518.1014	---
MySQL Tools for 5.0	12.0.4518.1014	---
USB Disk Security	---	---
PDFCreator	1.2.2	---
Realtek High Definition Audio Driver	6.0.1.6383	---
VLC media player	1.1.7	---
WampServer	2.2	---

Elaborado por: Santiago Bayas

Responsable: Ing. Paulina Tejada

Tabla 3.20: Equipo dos de Licencias

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A04,22,7,01	Samsung	SDCJ638BQ-JESG
Teclado	A04,20,4,02	Speedmind	7323419

Mouse	A04,20,5,03	Speedmind	10462KSGN
Regulador	A04,12,7,09	Speedmind	903Q98R272WE99
Impresora	A04,19,8,09	Lexmark E460 DW	835631AHBELXFG
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A04,20,3,07	Intel	---
Procesador	A04,20,3,07	Intel	---
Memoria RAM	A04,20,3,07	Kingston	---
Lector de Memorias	A04,20,3,07	Genérico	---
Disco Duro	A04,20,3,07	Samsung	SGD180A-KD47
DVD-RW	A04,20,3,07	Lg	SDFDVDRWOE-871329

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Adobe Flash Player 16 NPAPI	16.0.0.278	---
Mozilla Maintenance Service	12.0.4518.1014	---
MySQL Tools for 5.0	12.0.4518.1014	---
SITCON	1.0 07.01.2013-08.00	---
USB Disk Security	---	---
Microsoft Office 2007 Service Pack 3	12.0.4518.1014	JFRWL-2266R-8FSL4-KTG64-KS5G8
Microsoft Office Excel	12.0.4518.1014	---
Microsoft Windows 7 Home Premium	6.1.7601	03971-OEM-4663004-01267
D3DX10	7.0.450	---
Google Chrome	5.6.2	---
Microsoft .NET Framework	4.5.1	---
PDFCreator	1.2.0	---
VLC media player	1.1.7	---
WampServer	2.2	---
HydraVision	4.2.210.0	---

Adobe Reader Español	9.5.5	---
Ares	2.2.5	---
Avira	14.0.7.520	---
Citrix online plug-in	12.0.0.6410	---
Visual C++ 2008 x86 Runtime	32.0.1	---
NiceLabel Suite	3.6.2	---

Elaborado por: Santiago Bayas

Responsable: Srta. Lady Yépez

Tabla 3.21 Equipo tres de Licencias

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A05,03,9,23	Samsung	SDJWFSDS-KD36
Teclado	A05,03,9,23	Speedmind	EKNEMWEASL
Mouse	A05,03,9,23	Speedmind	SDF8723523LOS
Regulador	A05,03,9,23	Speedmind	98U234590210Y08
Impresora	A05,03,9,23	Lexmark E460 DW	912367JDQLXEW
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A05,03,8,18	Intel	---
Procesador	A05,03,8,18	Intel	---
Memoria RAM	A05,03,8,18	Markvision	---
Lector de Memorias	A05,03,8,18	Genérico	---
Disco Duro	A05,03,8,18	Samsung	SGD180A-WS93
DVD-RW	A05,03,8,18	Lg	ASEDVDRWQD-24579

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Adobe Reader Español	9.5.5	---

UltraVnc	3.0.9379	---
Realtek High Definition Audio Driver	6.0.1.6383	---
VLC media player	1.1.7	---
WampServer	2.2	---
Avira Antivirus	12.27.0.980	---
Avira	14.0.7.468	---
Google Chrome	5.6.2	---
Microsoft .NET Framework	4.0.30319	---
Citrix online plug-in	12.0.0.6410	---
Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
Microsoft Office Excel MUI	12.0.4518.1014	---
Microsoft Windows 7 Home	6.1.7601	00426-OEM-8992662-00400
HydraVision	4.2.210.0	---
Mozilla Maintenance Service	12.0.4518.1014	---
MySQL Tools for 5.0	12.0.4518.1014	---
SITCON	1.0 07.01.2013-08	---
USB Disk Security		---
Visual C++ 2008 x86 Runtime	32.0.1	---
NiceLabel Suite	3.6.2	---

Elaborado por: Santiago Bayas

Responsable: Ing. Franklin Cuyachamin

Tabla 3.22: Equipo Cuatro de Licencias

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A06,13,6,12	Samsung	SDFLKEFXC-SD32
Teclado	A06,13,6,12	Speedmind	MQWDFVXZK

Mouse	A06,13,6,12	Speedmind	SGF89433DSF
Regulador	A06,13,6,12	Speedmind	98234654554D43
Impresora	A06,13,6,12	Lexmark E460 DW	35232DFMSLXWEF
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A06,23,3,14	Intel	---
Procesador	A06,23,3,14	Intel	---
Lector de Memorias	A06,23,3,14	Genérico	---
Memoria RAM	A06,23,3,14	Kingston	---
Disco Duro	A06,23,3,14	Seagate	SGD180A-SD23
DVD-RW	A06,23,3,14	Lg	HJKDVDRWFH-209833
SOFTWARE			
NOMBRE		**VERSION**	**LICENCIA**
Adobe Reader Español		9.5.5	---
USB Disk Security			---
Avira		14.0.7.468	---
CCleaner		1.1.27.25527	---
Compresor WinRAR			---
UltraVnc		3.0.9379	---
Google Chrome		5.6.2	---
Microsoft .NET Fram		4.0.30319	---
Citrix online plug-in		12.0.0.6410	---
Microsoft Office 2007		12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
Microsoft Windows 7		6.1.7601	76460-OEM-0061914-63674
HydraVision		4.2.210.0	---
Mozilla Maintenance Service		12.0.4518.1014	---
MySQL Tools for 5.0		12.0.4518.1014	---
SITCON		1.0 07.01.20	---
VLC media player		1.1.7	---

WampServer	2.2	---

Elaborado por: Santiago Bayas

- **Departamento Médico**

Responsable: Dra. Sandra Villacis

Tabla 3.23: Equipo Departamento Médico

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A12,04,16,2	Samsung	JNDSJKWEJKSD
Teclado	A12,04,16,2	Genérico	983683982
Mouse	A12,04,16,2	Genérico	67T233653
Regulador	A12,04,16,2	Speedmind	7623094523KS98
Impresora	A12,04,16,2	Lexmark E460 DW	983WE8X90LXWJD
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A12,24,8,2	Intel	---
Procesador	A12,24,8,2	Intel	---
Memoria RAM	A12,24,8,2	Markvision	---
Disco Duro	A12,24,8,2	Lg	LKAJ-JAD90834
DVD-RW	A12,24,8,2	Lg	KHASGVEFQ-123335
SOFTWARE			
NOMBRE		**VERSION**	**LICENCIA**
Adobe Reader Español		9.5.5	---
Google Chrome		5.6.2	---
Microsoft .NET		4.0.30319	---
Microsoft .NET Framework		4.0.30319	---
Citrix online plug-in		12.0.0.6410	---

Microsoft Office 2007 Service	12.0.4518.1014	LSGBF--8D84L-HSDR3-KSDH3
Microsoft Office Excel MUI	12.0.4518.1014	---
USB Disk Security		---
Visual C++ 2008 x86 Runtime	32.0.1	---
Avira Antivirus	12.27.0.970	---
Avira	14.0.7.468	---
CCleaner	1.1.27.25527	---
Compresor WinRAR		---
NiceLabel Suite	3.6.2	---
UltraVnc	3.0.9379	---
Microsoft Windows 7 Home	6.1.7601	91062-OEM-0814905-82550
HydraVision	4.2.210.0	---
Mozilla Maintenance Service	12.0.4518.1014	---
MySQL Tools for 5.0	12.0.4518.1014	---
SITCON	1.0 07.01.2013-08.00	---
VLC media player	1.1.7	---
WampServer	2.2	---

Elaborado por: Santiago Bayas

- **Departamento Psico – Sensométrico**

Responsable: Abg. David Martínez

Tabla 3.24: Equipo Departamento Psico-Sensométrico

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A13,16,6,0	AOC	SDFLKEFXC-SD32
Teclado	A13,9,16,0	Genérico	893278340
Mouse	A13,24,9,3	Genérico	98KJQWE234
Regulador	A13,16,6,7	Speedmind	092308WEWF35

Impresora	A13,03,6,9	Lexmark E460 DW	89QKSD93LXSDK

COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A13,26,16,1	Intel	---
CPU PENTIUM IV	A13,26,16,1	Intel	---
Memoria RAM 2GB	A13,26,16,1	Kingston	---
Disco Duro	A13,26,16,1	Seagate	LKAJKSKJ-82893
DVD-RW	A13,26,16,1	Lg	KWEIU393F-IKJSD352

SOFTWARE		
NOMBRE	**VERSION**	**LICENCIA**
Adobe Reader Español	9.5.5	---
USB Disk Security		---
Avira	14.0.7.468	---
CCleaner	1.1.27.25527	---
Compresor WinRAR		---
NiceLabel Suite	3.6.2	---
UltraVnc	3.0.9379	---
Citrix online plug-in	12.0.0.6410	---
Microsoft Office 2007 Sp3	12.0.4518.1014	KNS39-939C7-9DN37-KSJW3-JSWB6
Microsoft Office Excel MUI	12.0.4518.1014	---
Microsoft Windows 7	12.0.4518.1014	79272-OEM-0082528-03284
HydraVision	4.2.210.0	---
Mozilla Maintenance Service	12.0.4518.1014	---
SITCON	1.0 07.01.2013-08.00	---
VLC media player	1.1.7	---
WampServer	2.2	---

HARDWARE ADICIONAL			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**

Monitor	A1,02,1,022,4	Xtratech	W7006S-97F1569012291
Monitor	A1,02,1,022,5	Xtratech	D6260H-873S389324784
Monitor	A1,02,1,022,6	Xtratech	D398SD-98D8723893402
Monitor	A1,02,1,022,7	Xtratech	K3223D-23L9832YT3453
Monitor	A1,02,1,022,8	Xtratech	D3625X-872K298733424
CPU Psico-Sensometrico	S/C	AGX	CPUAGX175
CPU Psico-Sensometrico	S/C	AGX	CNSAGX-1
CPU Psico-Sensometrico	S/C	AGX	CPUAGX-184
CPU Psico-Sensometrico	S/C	AGX	CNSDKE-74
CPU Psico-Sensometrico	S/C	AGX	CJASSD-23
Impresora	A1,021,02,19	Lexmark E460 DW	9823OASDK
Impresora	A1,021,02,20	Lexmark E460 DW	3234735NSX

Elaborado por: Santiago Bayas

- **Departamento Tecnológico**

Responsable: Ing. Leonardo Tenelema

Tabla 3.25 Equipo Departamento Tecnológico

HARDWARE			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Monitor	A06,13,6,12	Samsung	SDFLKEFXC-SD32
Teclado	A06,13,6,12	Speedmind	MQWDFVXZK
Mouse	A06,13,6,12	Speedmind	SGF89433DSF
Regulador	A06,13,6,12	Speedmind	98234654554D43

Impresora	A06,13,6,12	Lexmark E460 DW	35232DFMSLXWEF
COMPONENTES LOGICOS			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Mainboard	A06,23,3,14	Intel	---
Procesador	A06,23,3,14	Intel	---
Lector de Memorias	A06,23,3,14	Genérico	---
Memoria RAM	A06,23,3,14	Kingston	---
Disco Duro	A06,23,3,14	Seagate	SGJKSJNA500SNS39
DVD-RW	A06,23,3,14	Lg	JASJHDANKSA-983JNAS
SOFTWARE			
NOMBRE		**VERSION**	**LICENCIA**
Adobe Reader Español		9.5.5	---
USB Disk Security		---	---
Visual C++ 2008 x86 Runtime		32.0.1	---
Realtek High Definition Audio Driver		6.0.1.6383	---
Avira Antivirus		12.27.0.970	---
Avira		14.0.7.468	---
CCleaner		1.1.27.25527	---
Compresor WinRAR		---	---
NiceLabel Suite		3.6.2	---
UltraVnc		3.0.9379	---
Google Chrome		5.6.2	---
Citrix online plug-in		12.0.0.6410	---
Microsoft Office 2007		12.0.4518.1014	MHAS3-83HFC-7V73X-MEJS3-MDSJ2
Microsoft Office Excel MUI		12.0.4518.1014	---
Microsoft Windows 7 Home Premium		12.0.4518.1014	98284-OEM-0092830-9334F

HydraVision	4.2.210.0	---
Mozilla Maintenance Service	12.0.4518.1014	---
MySQL Tools for 5.0	12.0.4518.1014	---
SITCON	1.0 07.01.2013-08.00	---

HARDWARE ADICIONAL			
COMPONENTE	**CODIGO**	**MARCA**	**SERIE**
Impresora Térmica	S/C	ZEBRA P640I	P640G0810134
Impresora Térmica	S/C	STAR TCP-100	23007030615
Impresora Térmica	S/C	STAR TCP-100	75003020492
Impresora	A11,02,1,05,4	LEXMARK - E460 DW	72HGYWQ
Laptop	A11,02,05,15	DELL VOSTRO	89236239822JKSDHS-A2623
HD Externo 500GB	S/C	Toshiba	LKSJHWE234244

Elaborado por: Santiago Bayas

3.3.5.1.3 Equipos Dañados

Tabla 3.26: Equipos Dañados

COMPONENTE	CODIGO	MARCA	SERIE	ESTADO
TECLADO	S/C	BEVOD	K8D60080400261	MALO
TECLADO	S/C	GENIUS	WE1B92011130	MALO
CPU	S/C	XTRATECH	---	MALO
MONITOR LCD	S/C	HACER	ETL72081326480	MALO
TECLADO	S/C	HP	LNSDIUDW453	MALO
ROUTER	S/C	D-LINK	F316164001205	MALO
TECLADO	S/C	GENIUS	SKFJH3298389	MALO
IMPRESORA TERMICA	S/C	STAR	IUE28739490231	MALO
DVD R/RW	S/C	SANSUNG	SH-W162D1CSBN	MALO
MOUSE	S/C	HP	P0508072469	MALO
MOUSE	S/C	OMEGA	---	MALO
MOUSE	S/C	GENIUS	X69286407747	MALO

MOUSE	S/C	GENIUS	156425607	MALO
MOUSE	S/C	XTRATECH	M482090800928	MALO
MONITOR LCD	S/C	HP	CNC121RKY	MALO
IMPRESORA	S/C	LEXMARK	72HGYWQ	MALO
LAPTOP	S/C	DELL	IU12378958242RJHFV	MALO
TECLADO	S/C	XTRATECH	73482931	MALO
MOUSE	S/C	GENIUS	KSJD2139457	MALO
MONITOR	S/C	HP	---	MALO
CPU	S/C	HP	---	MALO
TECLADO	S/C	---	ZM720KWUEU326	MALO
MOUSE	S/C	GENIUS	ERGFFG426	MALO
MONITOR	S/C	HP	LQKJEKJSDJF2050	MALO
CPU	S/C	HP	---	MALO
TECLADO	S/C	---	SDLJVJHWE246	MALO
MOUSE	S/C	---	LKJHIR34572	MALO
MONITOR	S/C	LG	MNBVXHT23OI	MALO
CPU	S/C	SP	---	MALO
TECLADO	S/C	---	DJFKOP3836	MALO
MOUSE	S/C	---	NBSDGHQW2223	MALO

Elaborado por: Santiago Bayas

Este es el inventario que se obtuvo con la herramienta PC-Audit, no se puede verificar cambios o faltantes de equipos ya que no se dispone de un inventario anterior, los equipos son actuales y tienen las mismas características en componentes lógicos ya que fueron adquiridos en conjunto, cabe recalcar que existen 3 funcionarios en el área de licencias y que no disponen de equipos

informáticos los cuales comparten sus actividades con sus compañeros de área.

3.3.5.2 Software

3.3.5.2.1 Software Legal

El software en ningún momento fue inventariado por la agencia y tampoco por su oficina matriz en el siguiente cuadro se detalla el software legal el mismo que fue adquirido por la Institución desde sus inicios para poder brindar los diferentes servicios.

Tabla 3.27: Software Legal

DIRECCCION PROVINCIAL			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
LIC. LOURDES MAYORGA	Microsoft Windows 7	6.1.7601	00359-OEM-8992687-00006
	Nero 7 Ultra Edition	7.02.0936	1A20-020E-0000-1486-1210-5583
	Microsoft Office	---	YFKBB-PQJJV-G996G-VWGXY-2V3X8
	Adobe Reader	5.0.0.0	7.0.8.2006051600
SECRETARIA GENERAL			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
LIC. JACQUELINE URBINA	Microsoft Windows 7	---	00426-OEM-8992662-00497
	Nero 7 Ultra Edition	---	1A20-020E-0000-1349-1210-6697
	Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-8WCK9-KTG64-BC7D8
	Windows Mobile	5.00.1700.5.14343.06	

JEFATURA DE AGENCIA			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
ING. VERONICA PEREZ	Microsoft Windows 7	12.0.4518.1014	00254-OEM-36773362-01548
	Visual C++ 2008	9.0.30729.01	
	SITCON	---	1.0 07.01.2013-08.00
	Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
	Nero 7 Ultra Edition	---	1A20-020E-0000-1349-1210-6697
RECAUDACION			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
ING. VERONICA PEREZ	Microsoft Windows 7	12.0.4518.1014	00426-OEM-8992662-00400
	Nero 7 Ultra Edition	---	1A20-020E-0000-1349-1210-6697
	SITCON	---	1.0 07.01.2013-08.00
	Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-8WCK9-KTG64-BC7D8
LICENCIAS			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
ING. GABRIELA BARONA	Microsoft Windows 7	6.1.7601	01602-OEM-62204556-00321
	Microsoft Windows 7	6.1.7601	03971-OEM-4663004-01267
	Microsoft Windows 7	6.1.7601	00426-OEM-8992662-00400
	Microsoft Windows 7	6.1.7601	76460-OEM-0061914-63674
ING. PAULINA TEJADA	Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
SRTA. LADY YEPEZ	Microsoft Office 2007	12.0.4518.1014	JFRWL-2266R-8FSL4-KTG64-KS5G8
ING. FRANKLIN CUYACHAMIN	Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
	Microsoft Office 2007	12.0.4518.1014	LSNHW-9933S-9XMS6-GET35-KSD7S

	Nero 7 Ultra Edition	---	1A20-020E-0000-1349-1210-6697
	Nero 7 Ultra Edition	---	---
	Nero 7 Ultra Edition	---	---
	Nero 7 Ultra Edition	---	---
	SITCON	---	1.0 07.01.2013-08.00
DEPARTAMENTO MEDICO			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
DRA. SANDRA VILLACIS	Microsoft Windows 7	6.1.7601	91062-OEM-0814905-82550
	Citrix online plug-in	12.0.0.6410	---
	Microsoft Office 2007	12.0.4518.1014	LSGBF--8D84L-HSDR3-KSDH3
	UltraVnc	3.0.9379	---
PSICO - SENSOMETRICO			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
ABG. DAVID MARTINEZ	Microsoft Windows 7	12.0.4518.1014	00254-OEM-36773362-01548
	Visual C++ 2008	9.0.30729.01	---
	Microsoft Office 2007	12.0.4518.1014	KGFVY-7733B-6XGH7-KTG64-AF3J0
	Nero 7 Ultra Edition	---	1A20-020E-0000-1349-1210-6697
DEPARTAMENTO TECNOLOGICO			
RESPONSABLE	**NOMBRE**	**VERSION**	**LICENCIA**
ING. LEONARDO TENELEMA	Microsoft Windows 7	12.0.4518.1014	98284-OEM-0092830-9334F
	Visual C++ 2008	9.0.30729.01	---
	SITCON	---	1.0 07.01.2013-08.00
	Microsoft Office 2007	12.0.4518.1014	MHAS3-83HFC-7V73X-MEJS3-MDSJ2
	Citrix online plug-in	12.0.0.6410	

Elaborado por: Santiago Bayas

3.3.5.2.2 Software Ilegal

A continuación se detalla el software ilegal encontrado en el equipamiento informático de la Institución, cabe recalcar que el termino ilegal se utiliza para definir los programas que son innecesarios para el trabajo de cada uno de los funcionarios y que estos fueron instalados por el personal sin la debida autorización, y que al ser descargados desde internet puede ocasionar diferentes problemas en la funcionalidad del sistema.

Tabla 3.28: Software Innecesario

DIRECCCION PROVINCIAL		
RESPONSABLE	**NOMBRE**	**VERSION**
LIC. LOURDES MAYORGA	Visual C++ 2008 x86 Runtime	32.0.1
	Realtek High Definition Audio	6.0.1.6383
	CyberLink PowerDVD 10	3.1.521
	D3DX10	7.0.450
	Avira Antivirus	12.27.0.970
	Adobe Flash Player 10 ActiveX	10.0.42.34
	Adobe Flash Player 16 NPAPI	16.0.0.305
	Ares 2.2.5	2.2.5
SECRETARIA GENERAL		
RESPONSABLE	**NOMBRE**	**VERSION**
LIC. JACQUELINE URBINA	Ares	2.2.5
	Avira	1.1.27.25527
	CCleaner (remove only)	---
	Facebook Video Calling	3.1.521
	LimeWire	5.6.2

	Windows Mobile	5.00.1700.5.14343.06
JEFATURA DE AGENCIA		
RESPONSABLE	**NOMBRE**	**VERSION**
ING. VERONICA PEREZ	Windows Mobile SDK R2 for Smartphone	5.00.1700.5.14343.06
	CyberLink PowerDVD 10	3.1.521
	D3DX10	7.0.450
RECAUDACION		
RESPONSABLE	**NOMBRE**	**VERSION**
ING. VERONICA PEREZ	Adobe Flash Player 16 NPAPI	16.0.0.296
	Adobe Reader Español	9.5.5
	Ares	2.2.5
	Avira	14.0.7.468
	CCleaner	1.1.27.25527
LICENCIAS		
RESPONSABLE	**NOMBRE**	**VERSION**
ING. GABRIELA BARONA ING. PAULINA TEJADA SRTA. LADY YEPEZ ING. FRANKLIN CUYACHAMIN	Adobe Flash Player	16.0.0.296
	Mozilla	12.0.4518.1014
	Ares	2.2.5.1
	Avira Antivirus	12.27.0.970
	Avira	14.0.7.452
	CCleaner	1.1.27.25527
	CyberLink PowerDVD 10	3.1.521
	D3DX10	7.0.450
	Google Chrome	5.6.2
	VLC media player	1.1.7
	NiceLabel Suite	3.6.2
DEPARTAMENTO MEDICO		
RESPONSABLE	**NOMBRE**	**VERSION**

DRA. SANDRA VILLACIS	Adobe Reader Español	9.5.5
	Microsoft .NET Framework	4.0.30319
	Avira	14.0.7.468
	CCleaner	1.1.27.25527
	Compresor WinRAR	---
PSICO - SENSOMETRICO		
RESPONSABLE	**NOMBRE**	**VERSION**
ABG. DAVID MARTINEZ	Adobe Reader Español	9.5.5
	USB Disk Security	---
	CyberLink PowerDVD 10	3.1.521
	D3DX10	7.0.450
	Facebook Video Calling	3.1.521
	Avira Antivirus	12.27.0.970
	CCleaner	1.1.27.25527
DEPARTAMENTO TECNOLOGICO		
RESPONSABLE	**NOMBRE**	**VERSION**
ING. LEONARDO TENELEMA	CCleaner	1.1.27.25527
	Compresor WinRAR	---
	NiceLabel Suite	3.6.2
	UltraVnc	3.0.9379
	Facebook Video Calling	3.1.521
	LimeWire	5.6.2
	Ares	2.2.5
	CyberLink PowerDVD 10	3.1.521

Elaborado por: Santiago Bayas

En base al inventario de software realizado y al análisis de necesidades según los puestos de trabajo se sugiere los siguientes puntos los cuales incluyen software por adquirir y por eliminar.

3.3.5.2.3 Adquirir

El Software que debe ser adquirido de manera primordial para la Institución, es un programa Antivirus y el paquete completo de Office los cuales al disponer de una licencia original se puede obtener actualizaciones de todas sus librerías para así evitar el contagio del sistema por virus o el mal funcionamiento del mismo respectivamente; en la actualidad se encuentra instalado el Programa de Antivirus Avira al igual que Office 2007 los cuales no disponen de licencia original ya que han sido instalados con su crack respectivo para así evitar inconvenientes y conflictos en el desempeño de cada equipo informático.

3.3.5.2.4 Eliminar

La mayoría del software que se encuentra instalado en los equipos informáticos son los que el personal utiliza para el desempeño de sus funciones, los programas que deberían ser eliminados son los que fueron instalados sin autorización para fines de interés personal como por ejemplo:

- asistentes para descargas de música y videos
- reproductores de música, juegos

- traductores
- editores de gráficos y fotografías
- aplicaciones para interfaz de usuarios
- aplicaciones telefónicas

El tipo de software antes detallado no es necesario para las funciones designadas al personal sino que ayudan a la proliferación de virus e incluso disminuyen la velocidad de procesamiento de datos de cada computador.

3.3.5.2.5 Gráfica Comparativa entre Software Legal e Ilegal

Las gráficas que se muestran a continuación representan el porcentaje tanto del software legal e ilegal que poseen los equipos informáticos de cada una de las áreas antes auditadas.

Gráfico: 3.11 Comparativo individual entre software legal e ilegal

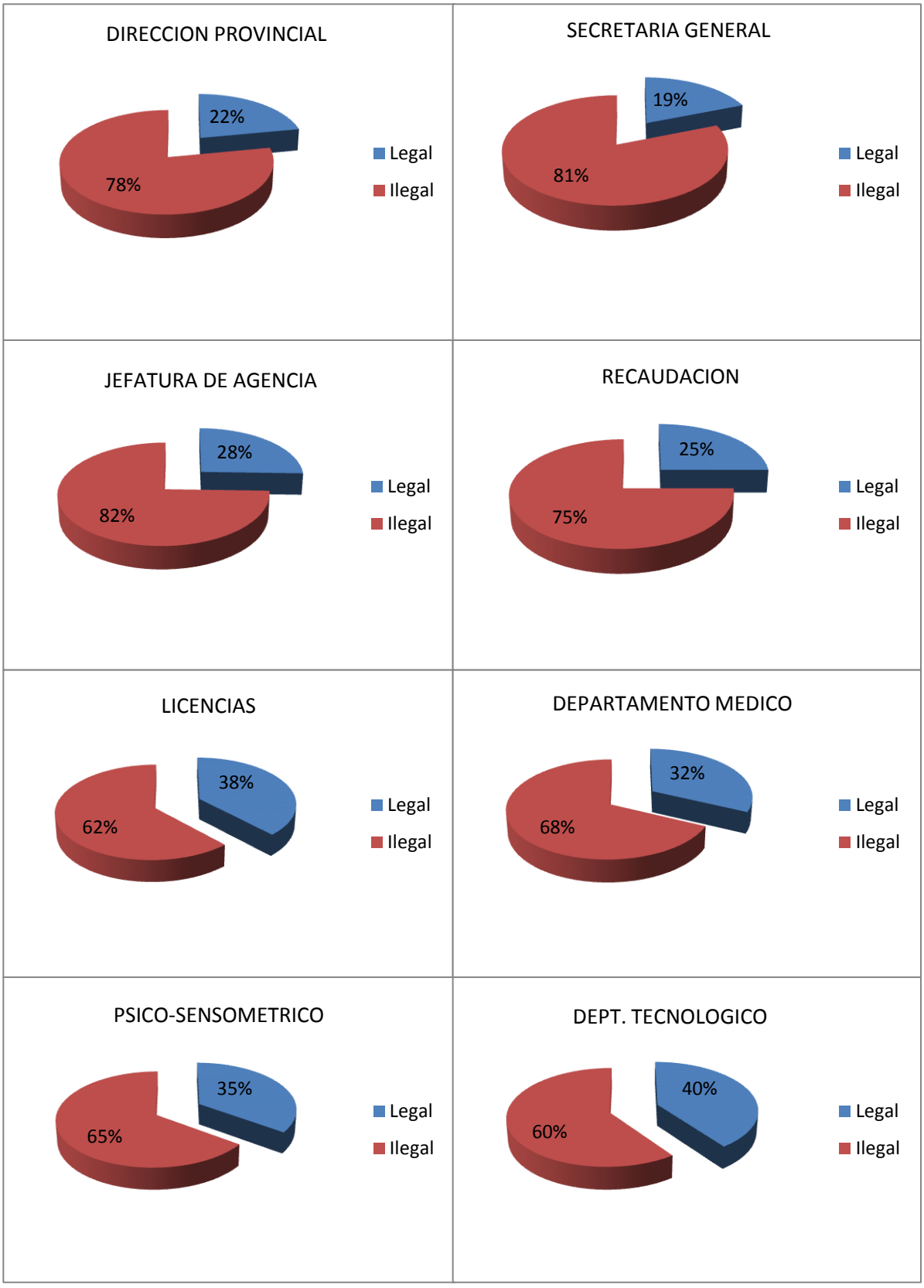
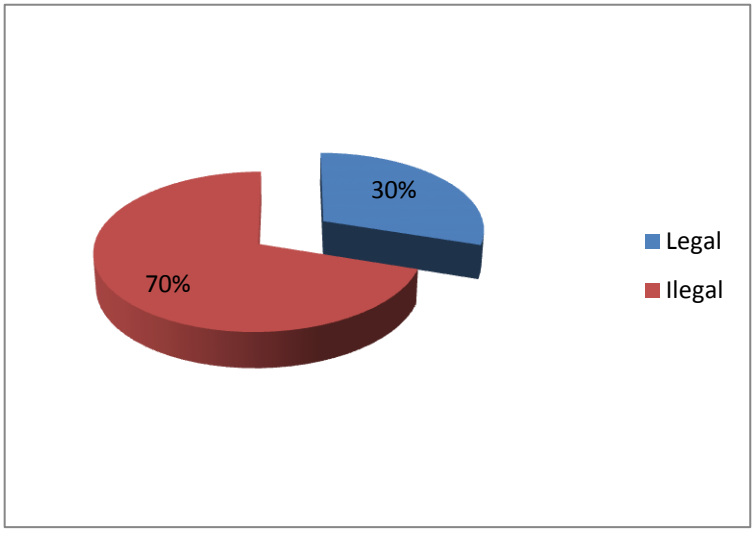


Gráfico: 3.12 Comparativo general entre software legal e



Elaborado por: Santiago Bayas

- **Análisis**

El Gráfico: anterior se puede observar que el 30% del software instalado en los equipos informáticos tienen licencia o pertenecen al software legal, mientras que el restante 70% pertenece al software ilegal el mismo que va incrementando según las descargas e instalaciones sin autorización por parte de los funcionarios.

- **Conclusión**

El software es una herramienta informática indispensable para determinadas funciones en cualquier empresa sin importar los servicios que ofrece, facilitando las funciones del personal por este motivo es indispensable administrarlos de

manera óptima y no correr el riesgo de instalar programas no autorizados los cuales pueden causar consecuencias legales para la institución.

3.3.5.3 Comunicaciones

3.3.5.3.1 Inventario de Hardware

Tabla 3.29: Inventario de Hardware

COMPONENTE	CODIGO	MARCA	SERIE
Router	S/C	D-LINK	F316164001205
Router	S/C	TP-LINK	1366730445
Router - Access Point	S/C	TP-LINK	1366735258
Router	S/C	D-LINK	F617331919390
Switch	S/C	D-LINK	F617331919390
Switch	S/C	3COM	20003242F1E30082228
Switch	S/C	D-LINK	F723648032740
Switch	S/C	TP-LINK	1354209347
Servidor	A11,01,1,177,1	HP - PROLITE ML110G6	MX211100VN

Elaborado por: Santiago Bayas

- Además cada uno de los computadores dispone de tarjeta de red aunque vale la pena mencionar que tres computadores de las áreas de secretaría general, recaudación y departamento médico no se encuentran conectados a la red.
- UPS
- Canaletas

3.3.5.3.2 Inventario de Software

Los sistemas operativos utilizados en los departamentos de la Institución son:

- Windows 2003 en los servidores
- Windows XP para clientes

No se puede detallar más a fondo ya que el área de servidores tiene restricciones.

3.3.5.3.3 Seguridades

En el tema de seguridades se dispone de Firewall actualizando el antivirus a todos los equipos de la institución, y el manejo de los usuarios y contraseñas para los sistemas de información se los realiza por medio del servidor de dominio.

3.3.5.4 Gestión y Administración

El monitoreo de la red según el procesamiento de datos se lo efectúa diariamente, por otro lado el mantenimiento de la red se lo realiza periódicamente, al igual que la gestión de usuarios se utiliza permisos y contraseñas, para efectuar todos estos procesos los encargados son el personal del departamento informático de la institución.

3.3.5.4.1 Programas y Aplicaciones informáticas

El software que está implementado en la Institución se maneja desde la matriz ubicada en la ciudad de Quito, a continuación se detalla:

- **SITCON**

Sistema regulador perteneciente a la ANT y que únicamente es dirigido por la misma institución, sistema en el cual se puede consultar y emitir licencias, matrículas y todos los datos importantes y relacionados con el vehículo además de que este permite editar y actualizar datos que se hayan emitido en la matrícula del vehículo.

- **AXIS**

A diferencia del sistema SITCON, el Sistema Regulador AXIS es manejado por las instituciones: Agencia Nacional de Tránsito (ANT), Comisión de Tránsito del Guayas (CTG) y Comisión de Tránsito del Ecuador (CTE), este sistema brinda similar ayuda a las diferentes instituciones para que se pueda actualizar, verificar y editar la información vehicular.

- **ZIMBRA**

Zimbra brinda el servicio de email y chat con el cual este se obtiene acceso a un correo institucional interno, mediante este sistema los funcionarios están

conectados a nivel nacional para poder subsanar cualquier solicitud a funcionarios de otras ciudades según su necesidad.

- **QUIPUX**

Es el sistema de gestión de documentos que es manejado por la mayoría de instituciones públicas ya que es de propiedad del Gobierno Ecuatoriano, el cual permite el envío y la recepción de documentos a través de la web siendo utilizado dentro y fuera de la institución.

- **ASISTENCIA D2 WEB**

Este sistema es el que se utiliza para la verificación de los horarios de entrada y salida de cada uno de los funcionarios a nivel nacional, esto es mediante un reloj biométrico ubicado en la puerta principal de cada una de las Instituciones.

3.4 Fase IV: Recursos

3.4.1 Recursos Humanos

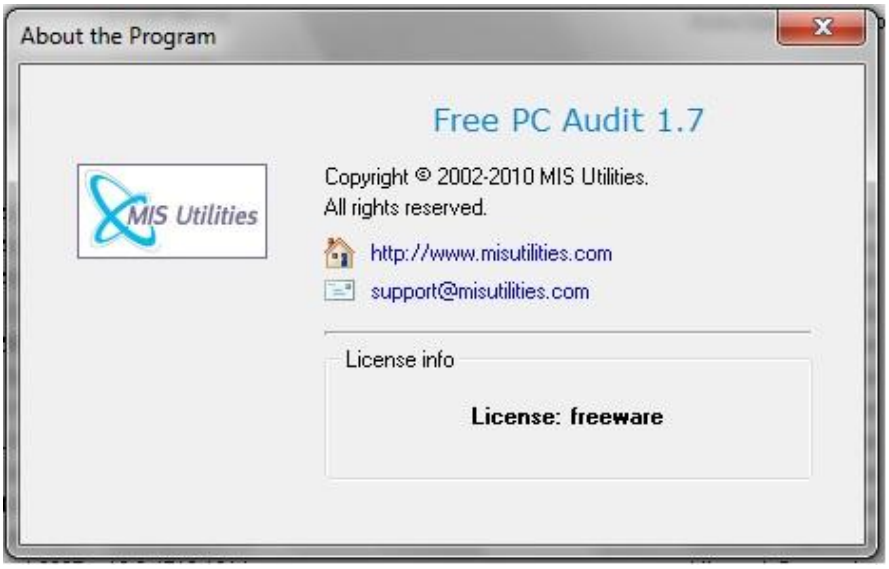
El recurso humano que realizó la Auditoria son las personas descritas como Auditor, Supervisor e Interlocutor, que con el apoyo incondicional del personal de las áreas auditables de la Institución se logró obtener los resultados expuestos en el presente documento.

3.4.2 Recursos Materiales

Los recursos materiales que se han empleado para realizar la auditoria son:

- El equipamiento informático de la Institución ya que los procesos de control deben realizarse necesariamente en los equipos de las áreas auditables de la Agencia Nacional de Transito de Tungurahua.

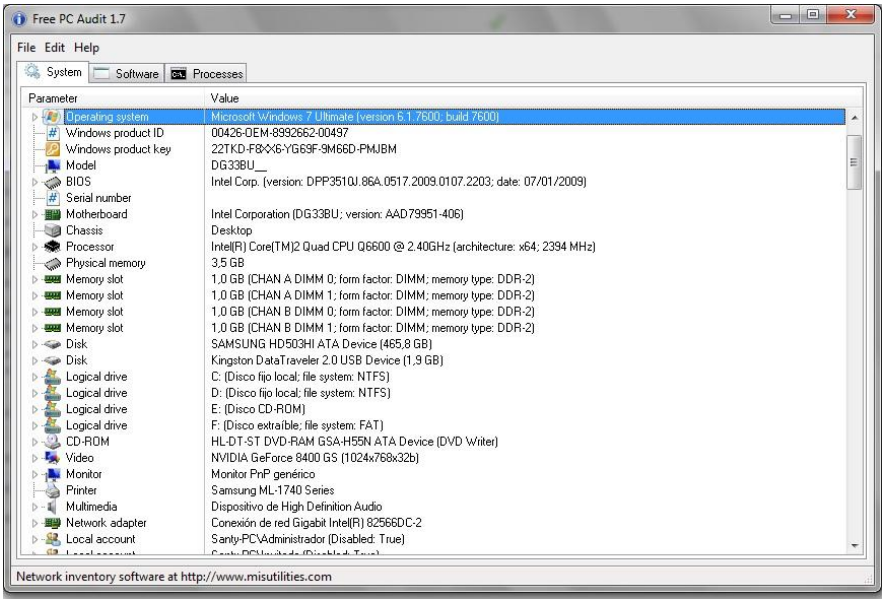
Ilustración 3.16 Free PC Audit



Fuente: Software Free PC audit

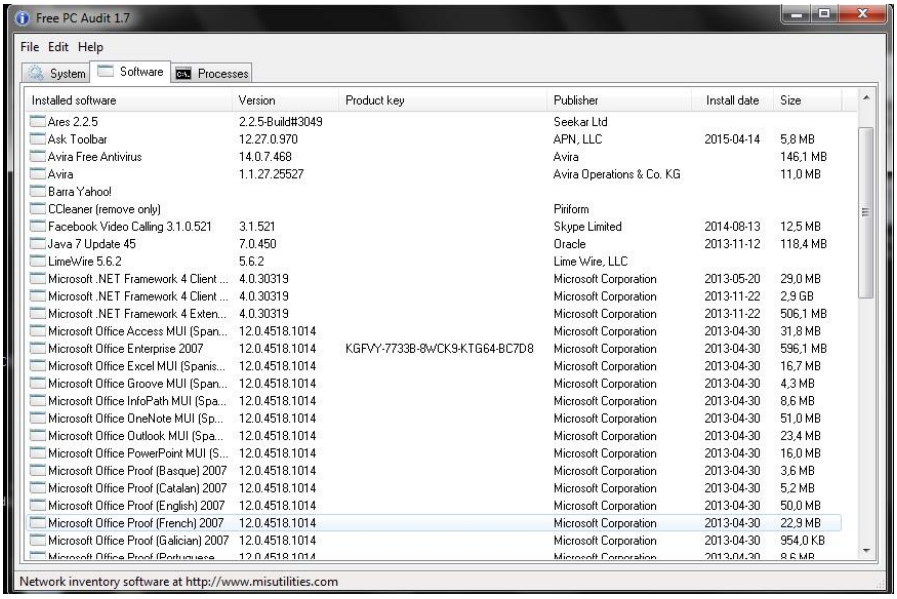
- Herramienta PC-Audit es de manejo rápido y fácil y puede ser utilizada aun desde un dispositivo USB para obtener resultados como se presentan en las siguientes imágenes.

Ilustración 3.17 Ejemplo inventario del sistema



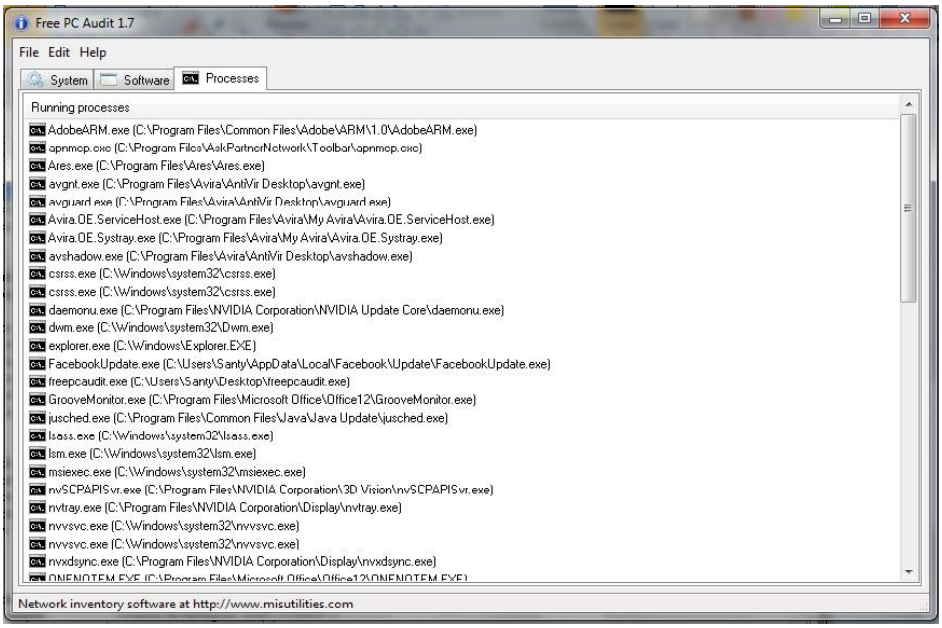
Fuente: Software Free PC audit

Ilustración 3.18 Ejemplo inventario de software



Fuente: Software Free PC audit

Ilustración 3.19 Ejemplo inventario Procesos



Fuente: Software Free PC audit

3.5 Fase V: Actividades de Auditoría Informática

3.5.1 Técnicas y Herramientas de Auditoría Informática

Para poder recolectar la información necesaria para el proceso de auditoría informática se realizaron encuestas para evaluar las distintas áreas de la Institución, además de las seguridades lógicas y seguridades físicas y comprobar a través del criterio de los usuarios los hechos observados anteriormente.

3.5.2 Seguridades y Controles de la Organización

3.5.2.1 Objetivo

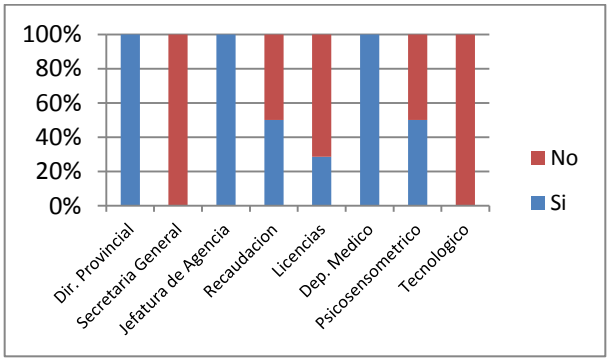
Evaluar los controles y seguridades de la estructura organizacional analizando la disponibilidad de documentos, manuales y la estructura de cada departamento de la Agencia Nacional de Tránsito.

La siguiente encuesta brinda información sobre las funciones, objetivos y políticas administrativas de la Institución para lo cual se encuestaron al personal de las áreas auditables.

3.5.2.2 Preguntas

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

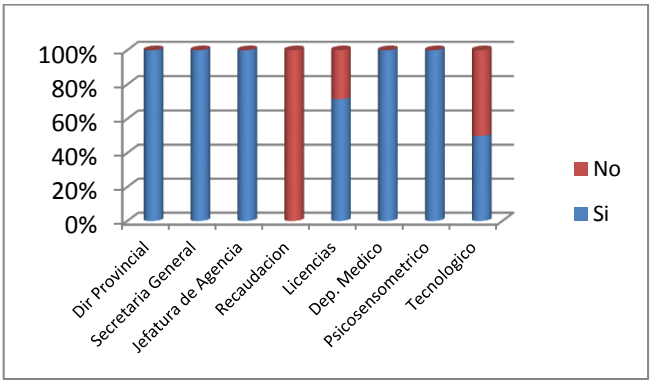
Gráfico 3.13 Estructura actual



Fuente: Encuesta
Elaborado por: Santiago Bayas

2. **¿La estructura actual está dada para que se realicen con eficiencia el trabajo asignado?**

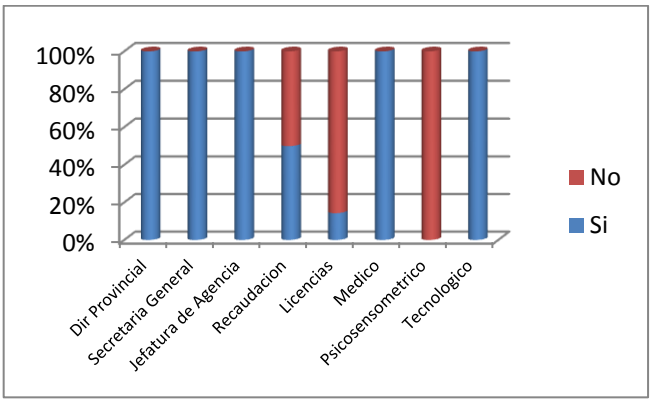
Gráfico 3.14 Trabajo Asignado



Fuente: Encuesta
Elaborado por: Santiago Bayas

3. **¿Los niveles jerárquicos actuales son necesarios y suficientes para la actividad normal de cada departamento?**

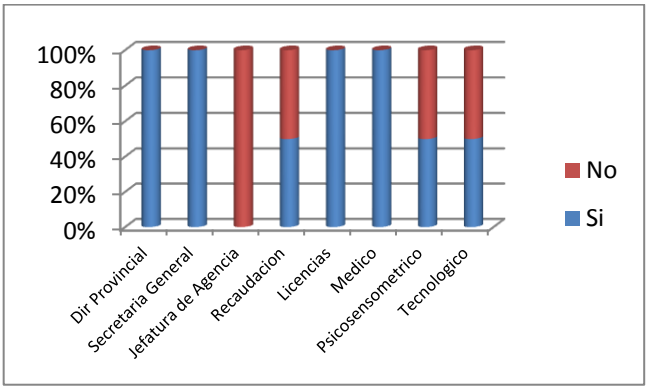
Gráfico 3.15 Niveles Jerárquicos



Fuente: Encuesta
Elaborado por: Santiago Bayas

4. De acuerdo a la estructura jerárquica de la institución se dispone de una adecuada comunicación entre las áreas

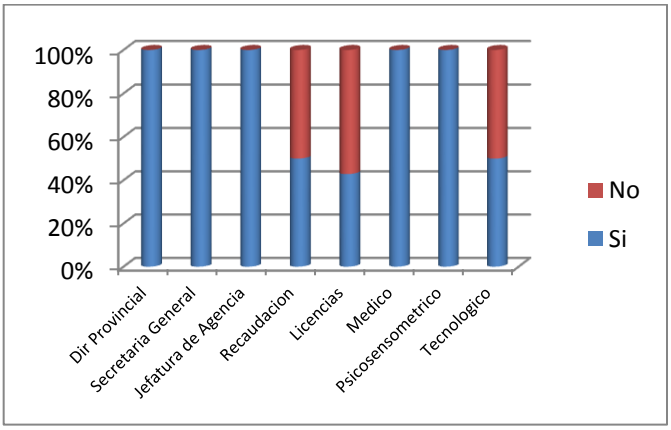
Gráfico 3.16 Estructura Jerárquica



Fuente: Encuesta
Elaborado por: Santiago Bayas

5. ¿Todos los departamentos tienen definidas sus funciones y responsabilidades?

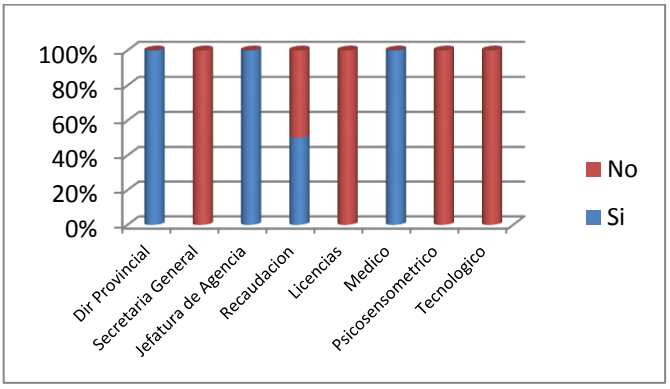
Gráfico 3.17 Funciones y Responsabilidades Definidas



Fuente: Encuesta
Elaborado por: Santiago Bayas

6. ¿Los puestos de trabajo van acorde con las necesidades del área para realizar sus funciones?

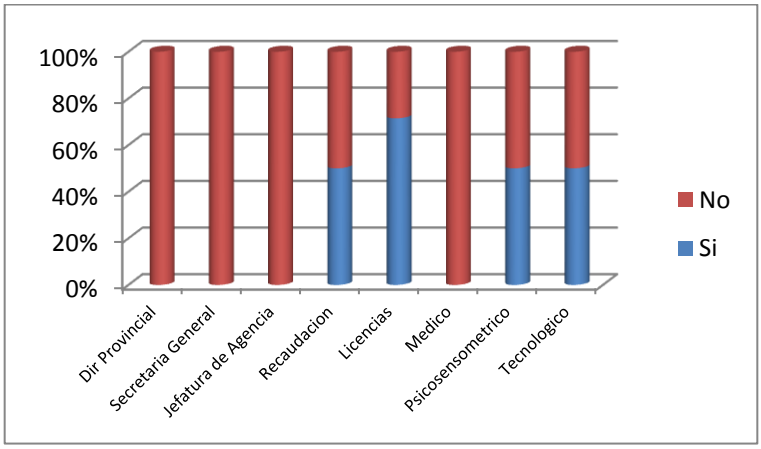
Gráfico 3.18 Puestos acordes



Fuente: Encuesta
Elaborado por: Santiago Bayas

7. ¿Se divide el trabajo de área en funciones?

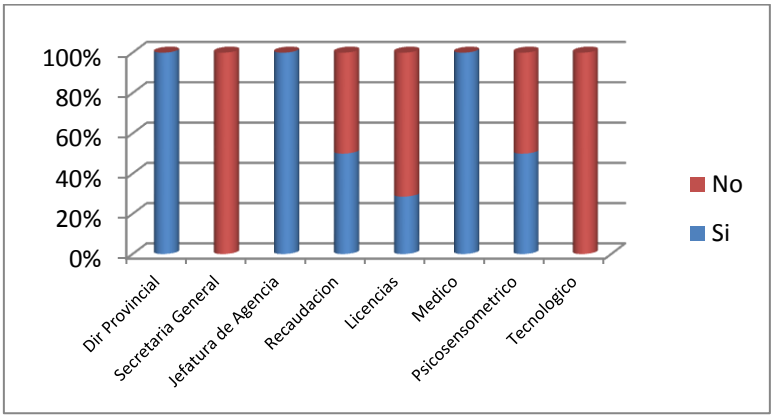
Gráfico 3.19 Trabajo dividido



Fuente: Encuesta
Elaborado por: Santiago Bayas

8 ¿Se encuentran establecidas en algún documento las funciones del área?

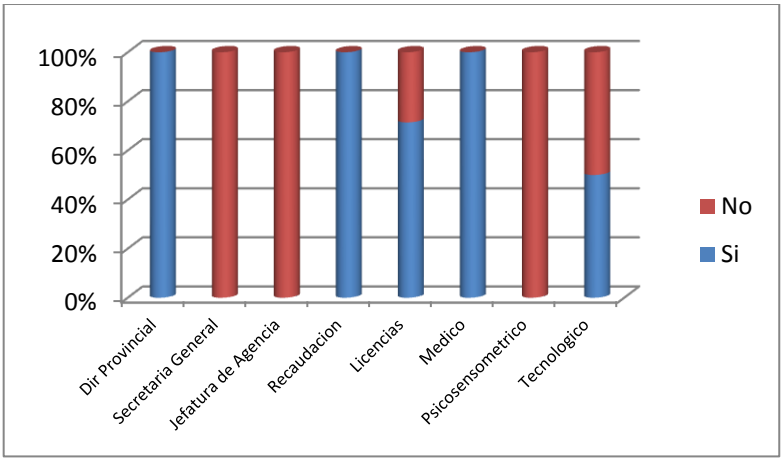
Gráfico 3.20 Funciones Establecidas en Documentos



Fuente: Encuesta
Elaborado por: Santiago Bayas

9. ¿El personal del área participa en la elaboración de las funciones?

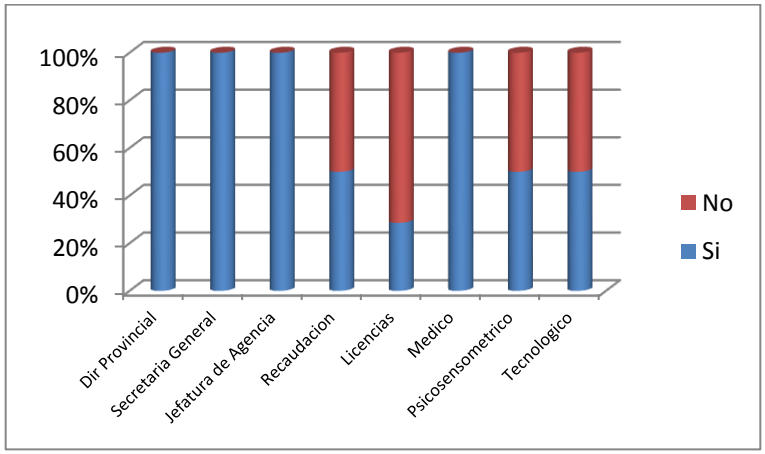
Gráfico 3.21 Personal participante en elaboración de funciones



Fuente: Encuesta.
Elaborado por: Santiago Bayas

10 ¿Las funciones del área van acorde al reglamento interno de la Institución?

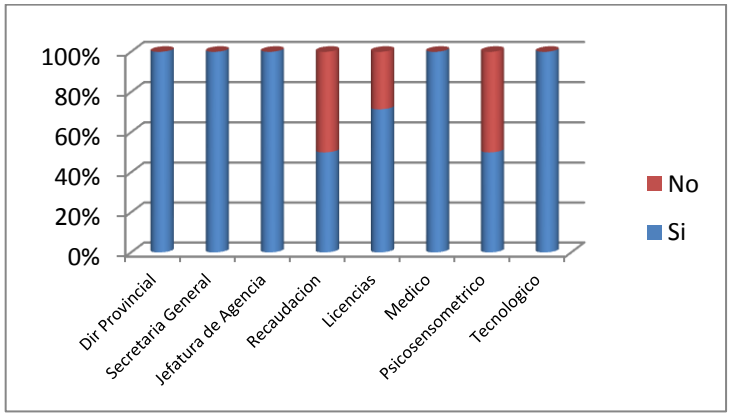
Gráfico: 3.22 Funciones Acordes al Reglamento



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

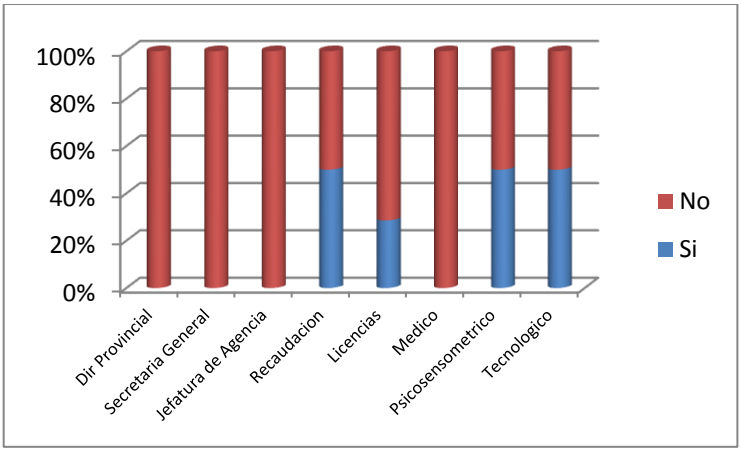
Gráfico: 3.23. Reemplazo en Funciones



Fuente: Encuesta
Elaborado por: Santiago Bayas

12. ¿Para cumplir con las funciones del área se requiere apoyo de otras?

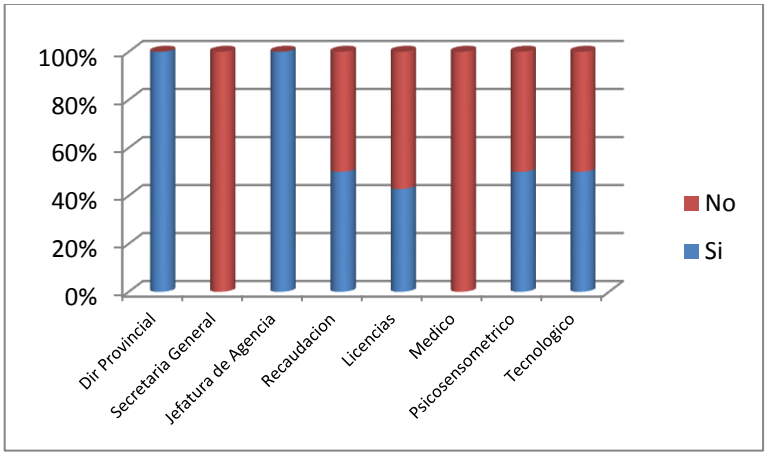
Gráfico: 3.24. Apoyo entre Funciones



Fuente: Encuesta
Elaborado por: Santiago Bayas

13. ¿Tiene conocimiento si existe doble asignación de funciones en otras áreas?

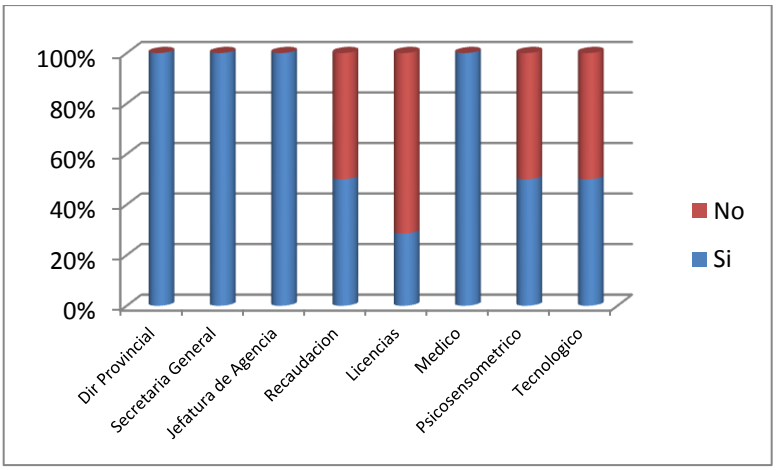
Gráfico: 3.25. Conocimiento de Doble asignación



Fuente: Encuesta
Elaborado por: Santiago Bayas

14. ¿Los objetivos están de acuerdo a las funciones del área?

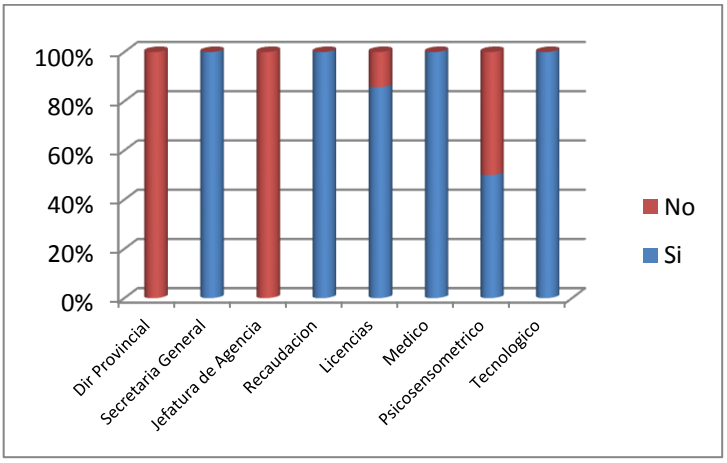
Gráfico: 3.26. Objetivos de Área



Fuente: Encuesta
Elaborado por: Santiago Bayas

15. ¿Se deja de realizar alguna actividad por falta de personal en la Institución?

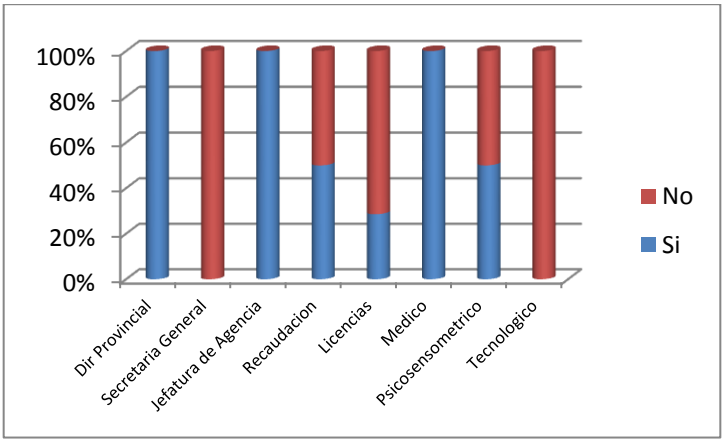
Gráfico: 3.27. Falta de personal



Fuente: Encuesta
Elaborado por: Santiago Bayas

16. Se da cumplimiento por parte del personal con las políticas procedimientos y normas establecidas en el área

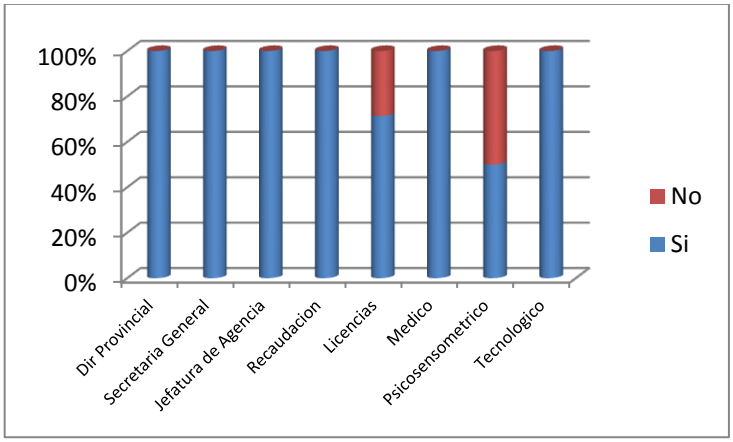
Gráfico: 3.28. Cumplimiento de políticas



Fuente: Encuesta
Elaborado por: Santiago Bayas

17. ¿Sabe si existen políticas para la seguridad cuando termina la relación laboral con un empleado?

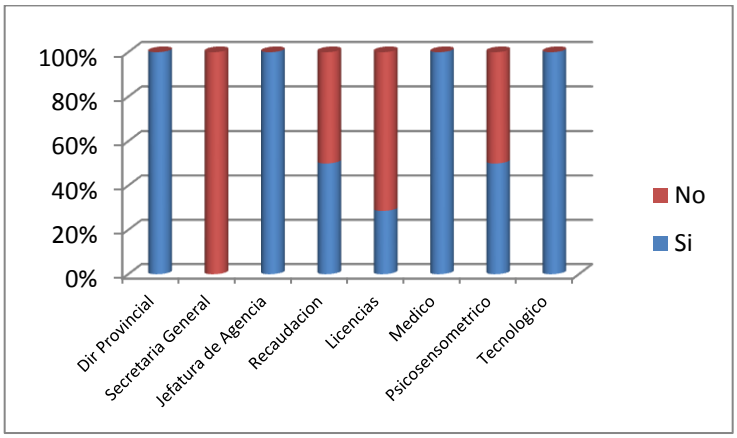
Gráfico: 3.29. Políticas de Seguridad



Fuente: Encuesta
Elaborado por: Santiago Bayas

18. ¿Se adapta el personal al mejoramiento administrativo del área?

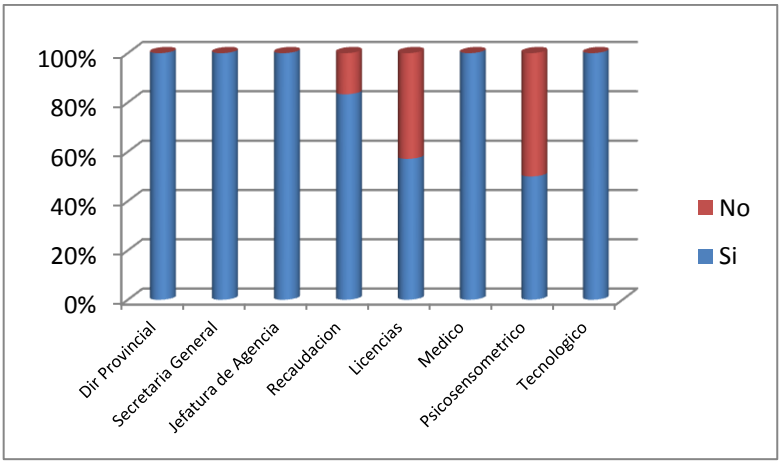
Gráfico: 3.30. Adaptación de personal a cambios



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

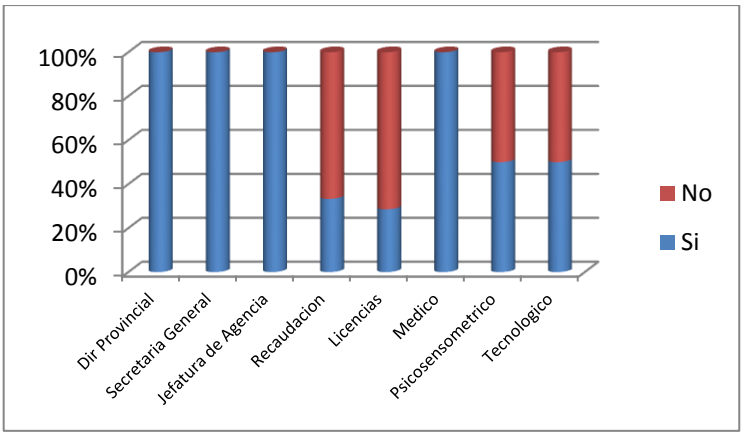
Gráfico: 3.31. Conocimiento del Reglamento



Fuente: Encuesta
Elaborado por: Santiago Bayas

20. ¿Sabe si el área posee un plan de selección de personal?

Gráfico: 3.32. Selección de Personal



Fuente: Encuesta
Elaborado por: Santiago Bayas

CONCLUSIONES

- Cada departamento tiene establecidas las responsabilidades que están basadas en el Estatuto Orgánico por procesos de la ANT, sin embargo algunas responsabilidades no son acatadas y son enviadas a otras áreas, acumulando y retrasándolo.

- Se deja de realizar actividades por falta de personal sobre todo en el área tecnológica debido a que solo existen dos personas en el área que además deben prestar asesoría a otras dependencia de la Institución las cuales están ubicadas en otras zonas.

- La adaptabilidad con respecto a mejoras implementadas sobre todo a nivel informático no son aceptadas inmediatamente por su dificultad de entendimiento y manejo.

RECOMENDACIONES

- Las funciones y las responsabilidades son normas que guían al buen desempeño laboral en toda institución por lo que se recomienda que sean acatados a cabalidad con el fin de mejorar el servicio y cumplir los objetivos de la Institución.
- Plantear a la dirección de contratación de personal que las funciones sean repartidas de mejor manera para que el trabajo no se acumule en un solo funcionario.
- Las mejoras son necesarias y esenciales en toda institución ya que con esto se facilita el trabajo para los funcionarios por este motivo se debe realizar capacitaciones a todos los funcionarios que junto a la iniciativa de cada persona se pueda obtener un mejor nivel de conocimientos.

3.5.3 Controles y Seguridades Físicas

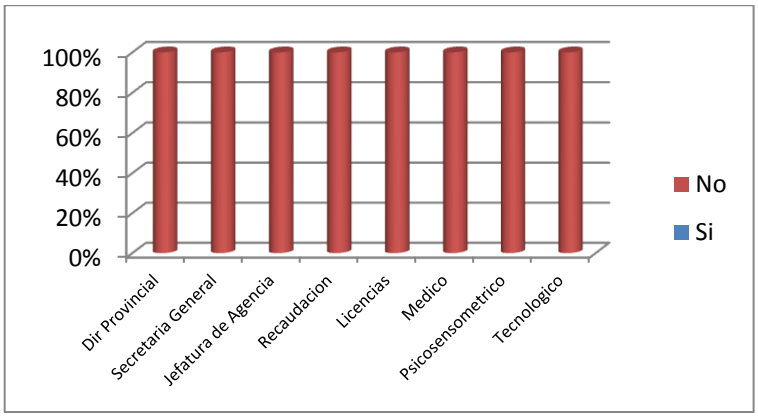
3.5.3.1 Objetivo

Evaluar el control interno de las seguridades físicas de los departamentos auditados incluyendo el procedimiento ante desastres.

3.5.3.2 Preguntas

1. ¿El área donde usted trabaja tiene seguridades contra desastres naturales?

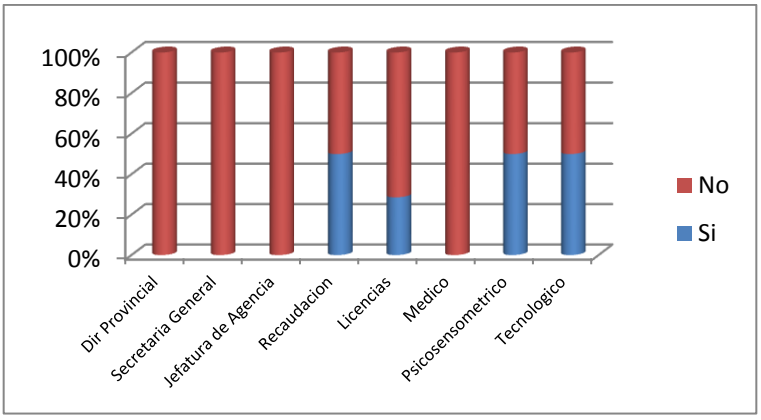
Gráfico: 3.33. Seguridad contra Desastres Naturales



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

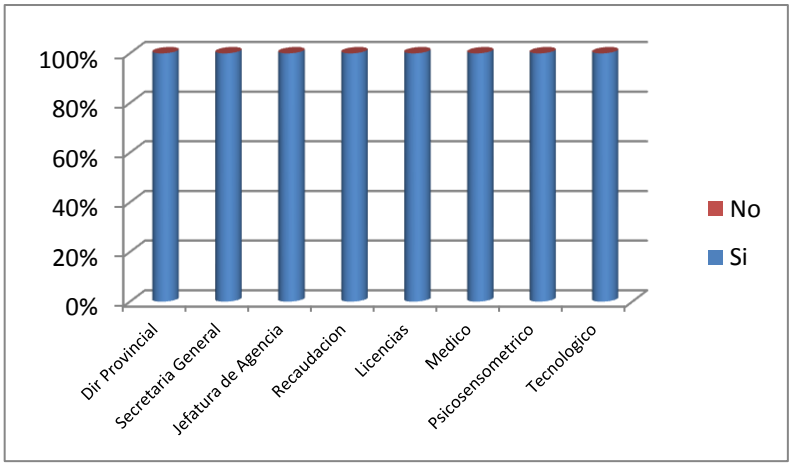
Gráfico: 3.34. Plan de Evacuación



Fuente: Encuesta
Elaborado por: Santiago Bayas

3. ¿Cuentan con horarios de entrada y salida?

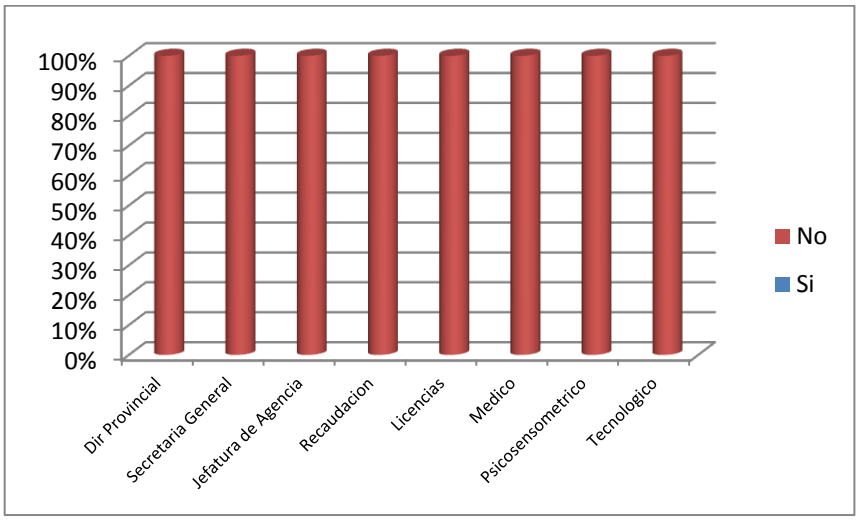
Gráfico: 3.35. Horarios Entrada y Salida



Fuente: Encuesta
Elaborado por: Santiago Bayas

4. ¿Se registra el acceso de personas ajenas al área?

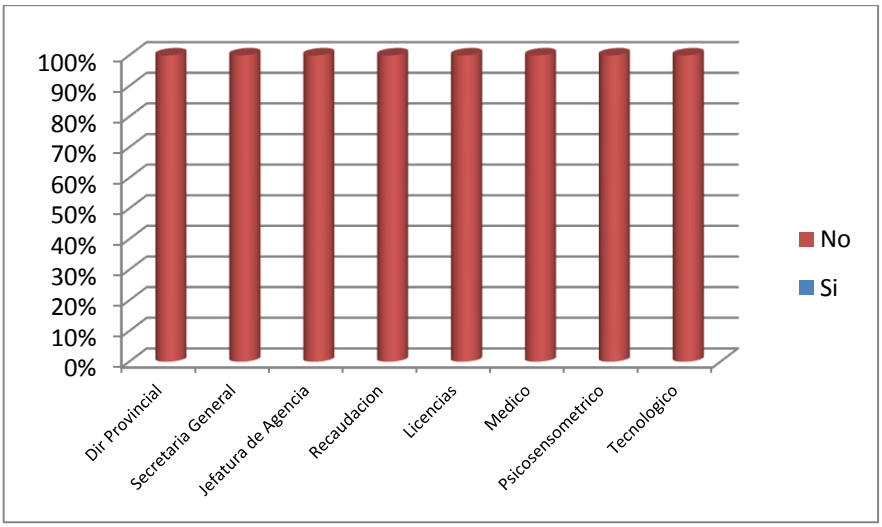
Gráfico: 3.36. Registro de Acceso



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

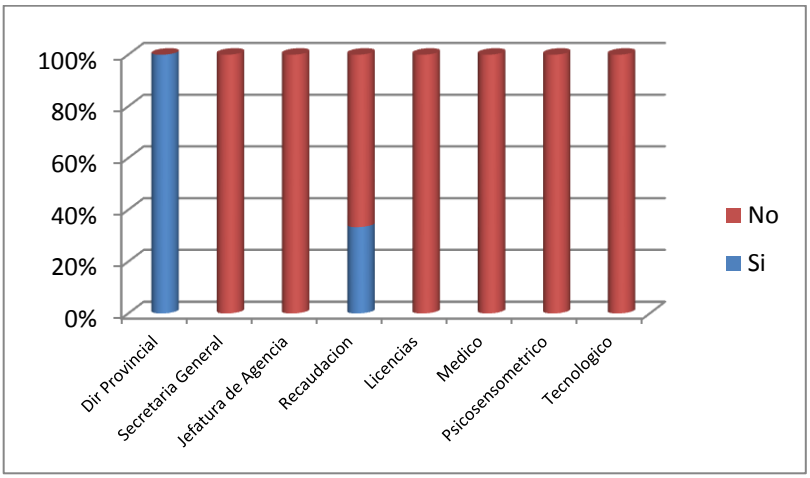
Gráfico: 3.37. Alarmas Automáticas



Fuente: Encuesta
Elaborado por: Santiago Bayas

6. ¿Existen en el departamento extintores de fuego

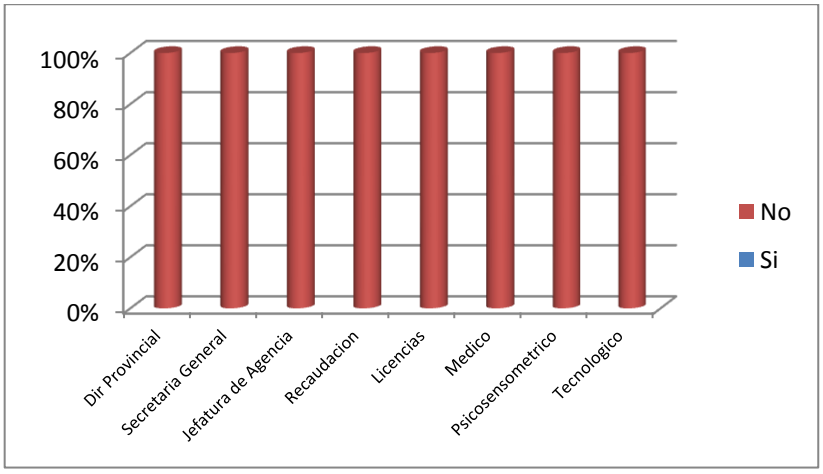
Gráfico: 3.38. Extintores en el Área



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

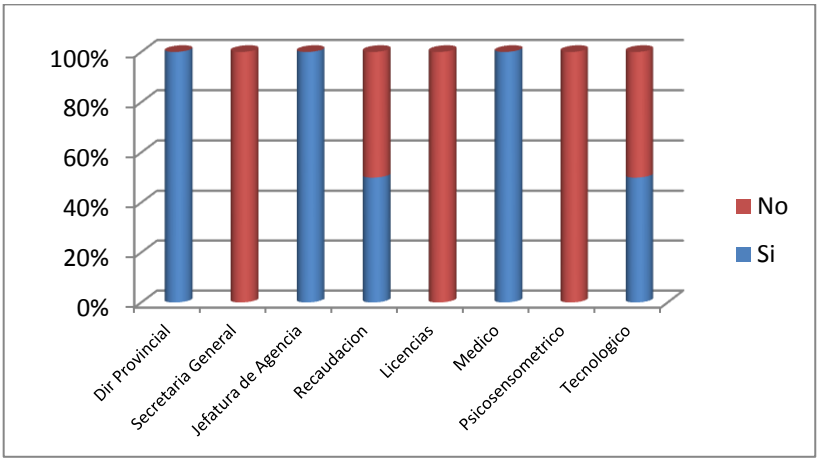
Gráfico: 3.39. Personal Capacitado en el manejo de extintores



Fuente: Encuesta
Elaborado por: Santiago Bayas

8. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos?

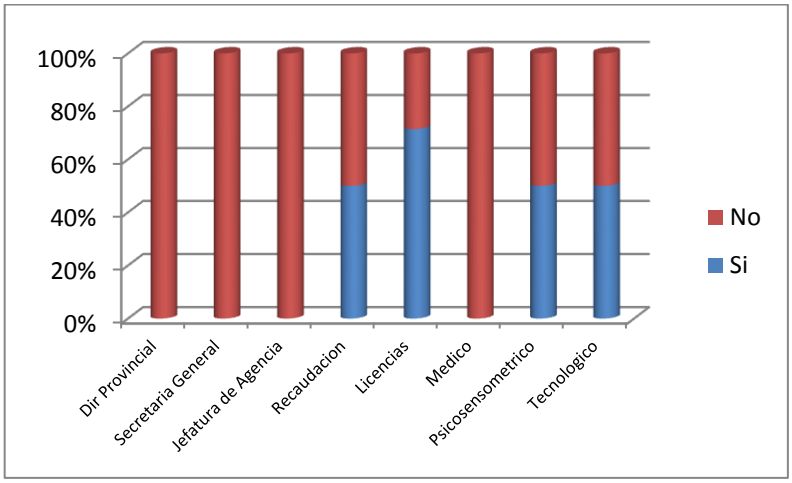
Gráfico: 3.40. Interruptores debidamente protegidos



Fuente: Encuesta
Elaborado por: Santiago Bayas

9. ¿Saben cómo actuar en el momento de una emergencia ocasionada por fuego?

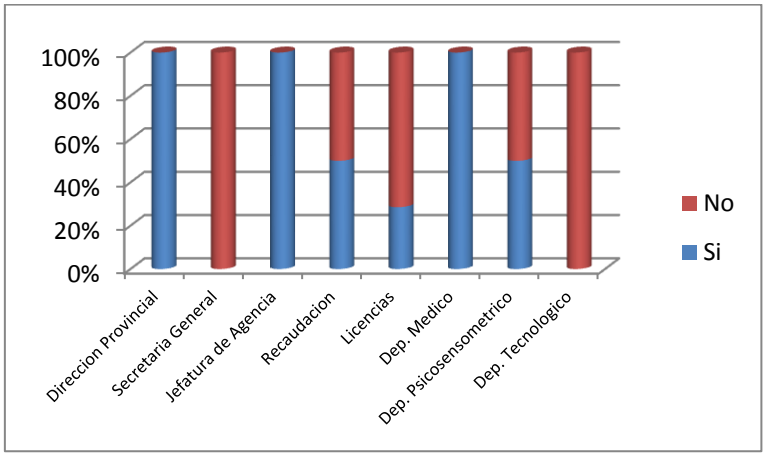
Gráfico: 3.41. Conocimiento de cómo actuar en emergencia



Fuente: Encuesta.
Elaborado por: Santiago Bayas

10. ¿Se ha indicado al personal la forma en la que se debe desalojar a todo el personal en caso de emergencia?

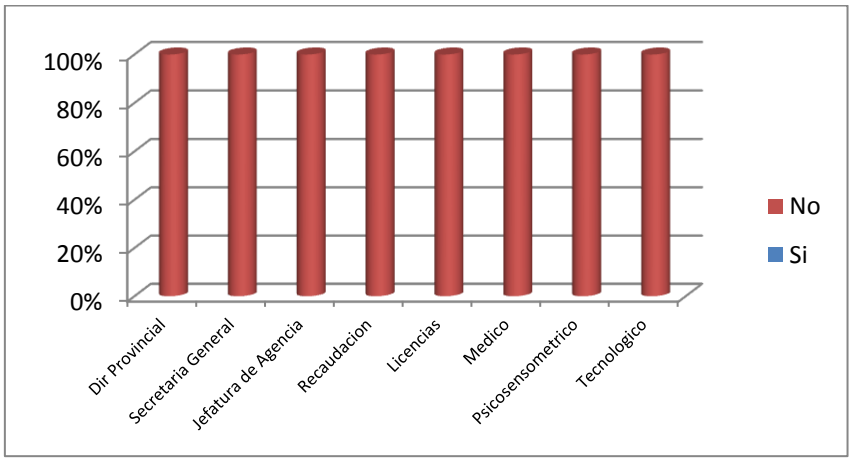
Gráfico: 3.42. Conocimiento de la Forma de Desalojar al Personal



Fuente: Encuesta
Elaborado por: Santiago Bayas

11. ¿Se han tomado medidas para minimizar la posibilidad de fuego?

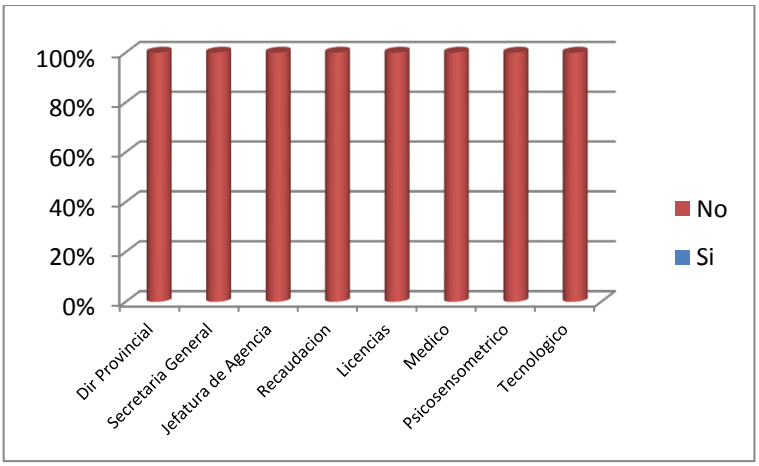
Gráfico: 3.43 Medidas para minimizar el riesgo de fuego



Fuente: Encuesta
Elaborado por: Santiago Bayas

12. ¿Se realiza mantenimiento periódico a los computadores?

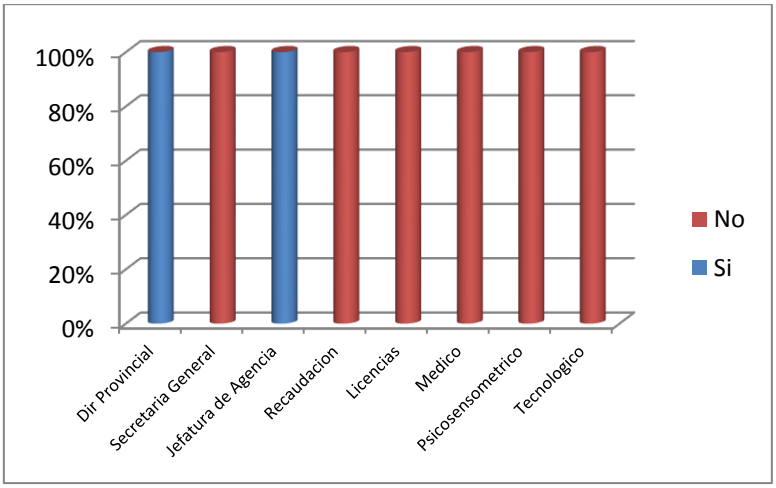
Gráfico: 3.44. Mantenimiento Periódico



Fuente: Encuesta
Elaborado por: Santiago Bayas

13. ¿Tiene conocimiento de la existencia de un plan de contingencia informático?

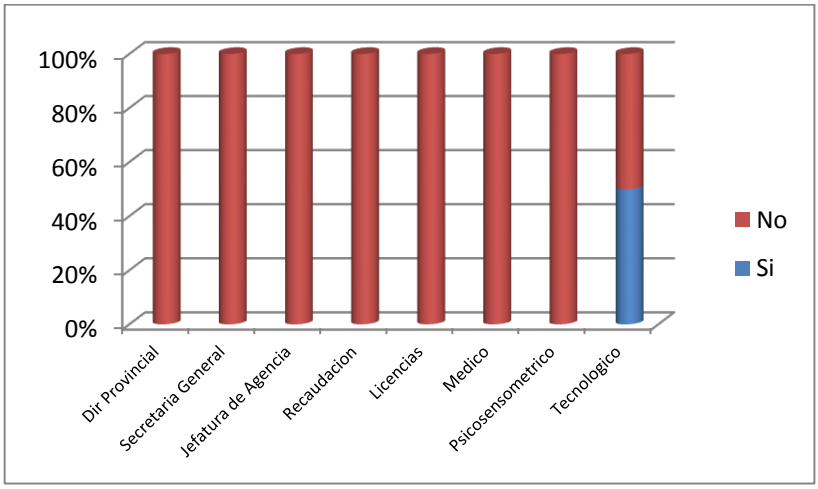
Gráfico: 3.45. Conocimiento de un Plan de Contingencia



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

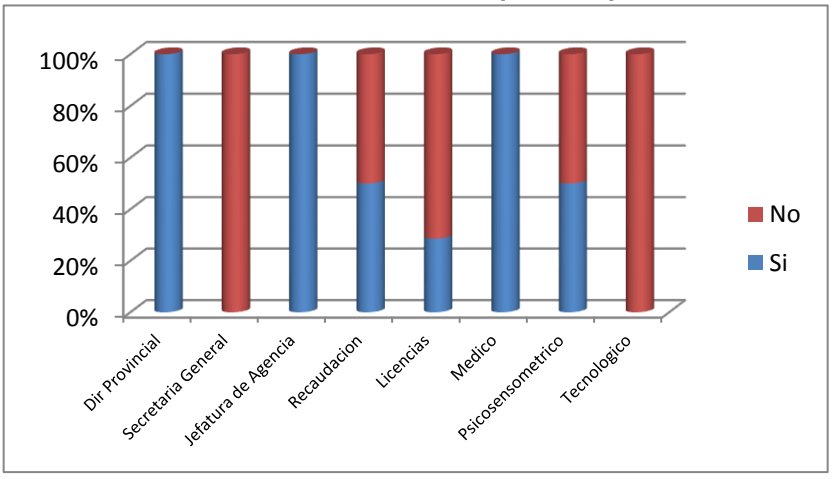
Gráfico: 3.46. Cableado Etiquetado



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

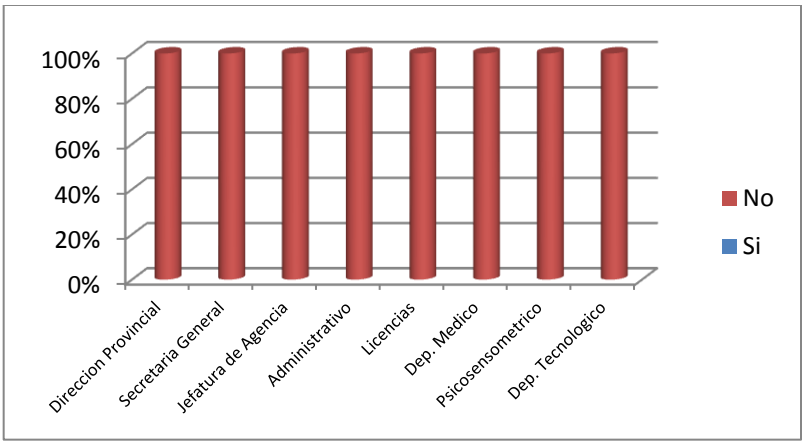
Gráfico: 3.47. Personal de Limpieza Capacitado



Fuente: Encuesta
Elaborado por: Santiago Bayas

16. ¿Existen salidas de emergencia en caso de algún desastre?

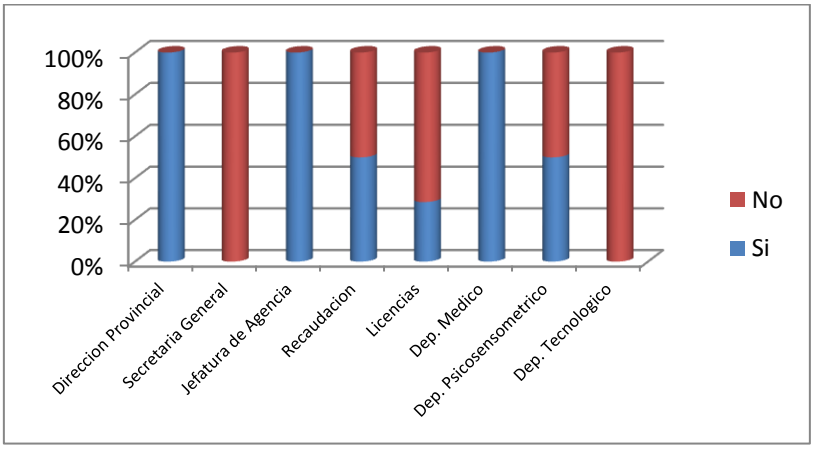
Gráfico: 3.48. Salidas de Emergencias



Fuente: Encuesta
Elaborado por: Santiago Bayas

17. ¿Se vigila la moral y el comportamiento del personal con el fin de mantener una buena imagen?

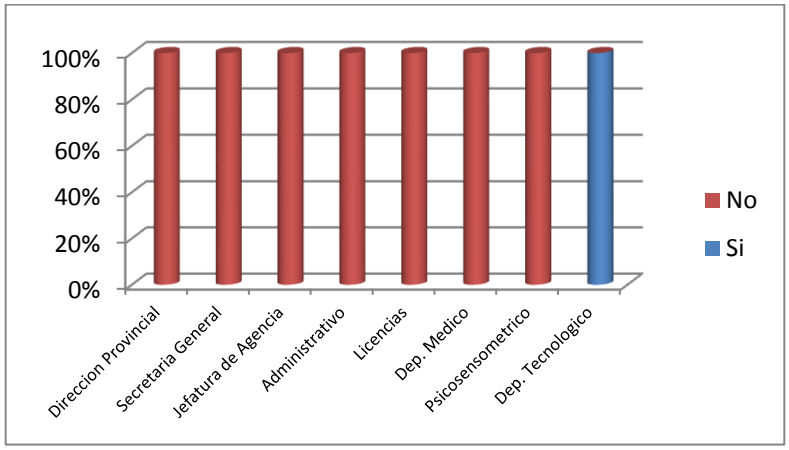
Gráfico: 3.49. Vigilancia del comportamiento del personal



Fuente: Encuesta
Elaborado por: Santiago Bayas

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

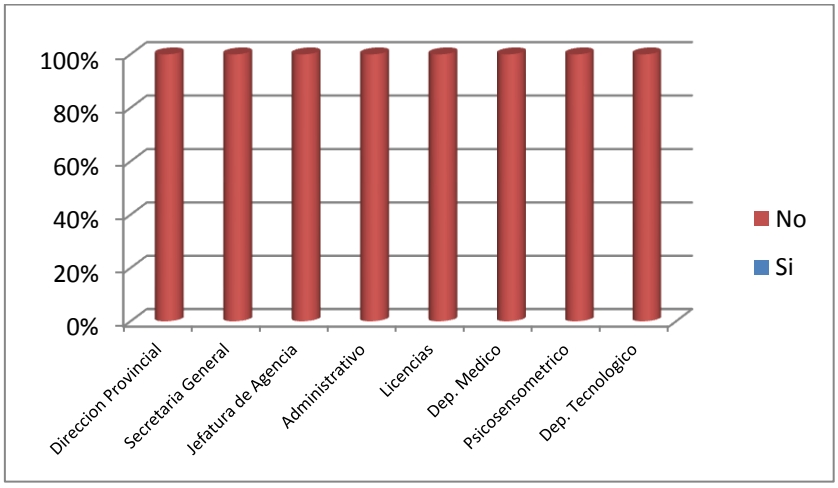
Gráfico: 3.50. Persona a cargo de la Seguridad Informática



Fuente: Encuesta
Elaborado por: Santiago Bayas

19. ¿Existen alarmas para detectar condiciones anormales en el ambiente?

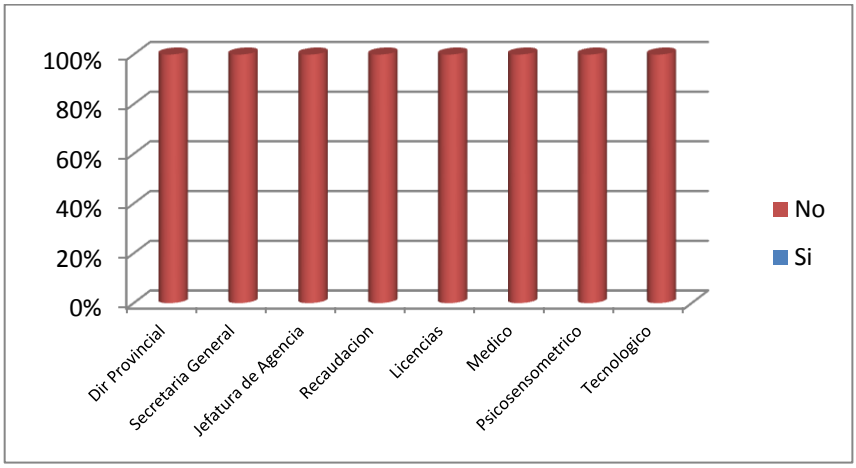
Gráfico: 3.51. Alarmas para controlar condiciones anormales



Fuente: Encuesta
Elaborado por: Santiago Bayas

20. ¿Dentro de su área existe un plan de mantenimiento de equipos de cómputo?

Gráfico: 3.52. Plan de mantenimiento de equipos



Fuente: Encuesta
Elaborado por: Santiago Bayas

CONCLUSIONES

- No existe en la institución un plan de evacuación ante desastres, manejo de extintores, ya que no se ha presentado algún problema para la toma de medidas preventivas.
- No existen suficientes extintores en las áreas, los pocos existentes se encuentran ubicados en áreas despejadas.
- El mantenimiento de computadoras no se realiza periódicamente ya que el personal no se abastece para poder realizar dicha labor.
- La seguridad en la institución no lleva un control de acceso de personas ajenas a cada departamento.
- No existe un plan de contingencias para cualquier eventualidad.

RECOMENDACIONES

- Tomar en cuenta planes de evacuación, seguridad ante desastres, capacitación a funcionarios en manejo de extintores, con el objetivo de salvaguardar la vida de los funcionarios y la información de la institución.
- Aplicar medidas de seguridad en el ingreso de personas ajenas a la institución para evitar posibles pérdidas para la Institución.
- Para asegurar el buen funcionamiento del equipamiento informático se debe elaborar un plan de mantenimientos periódicos y contar con el suficiente personal capacitado para ejecutar dicha actividad.
- Elaborar planes de contingencia.

3.5.4 Controles y Seguridades Lógicas

3.5.4.1 Objetivo

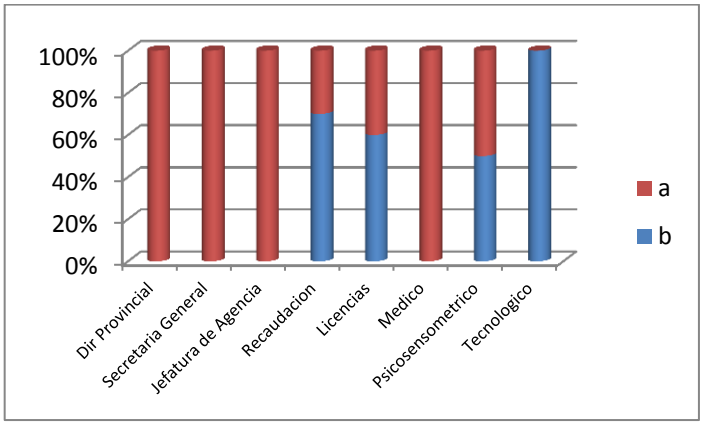
Conocer más a fondo acerca de la seguridad lógica que los usuarios utilizan para proteger los sistemas y equipos a su cargo en cada área de la Agencia Nacional de Tránsito de Tungurahua.

3.5.4.2 Preguntas

1. Si tiene algún problema informático usted

a. Solicita ayuda al departamento técnico
b. Trata de solucionarlo

Gráfico: 3.53. Problema Informático

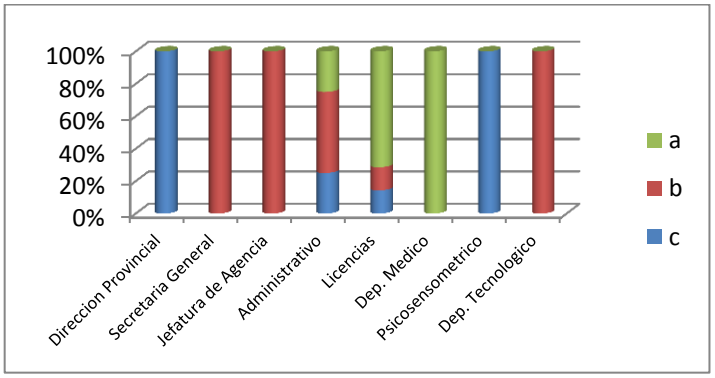


Fuente: Encuesta
Elaborado por: Santiago Bayas

2. Cuándo usted retira de su puesto de trabajo

a. Apaga el computador
b. Ingresa una contraseña para reiniciar actividades
c. Ninguna de las anteriores

Gráfico: 3.54. Cuando abandona el puesto de trabajo

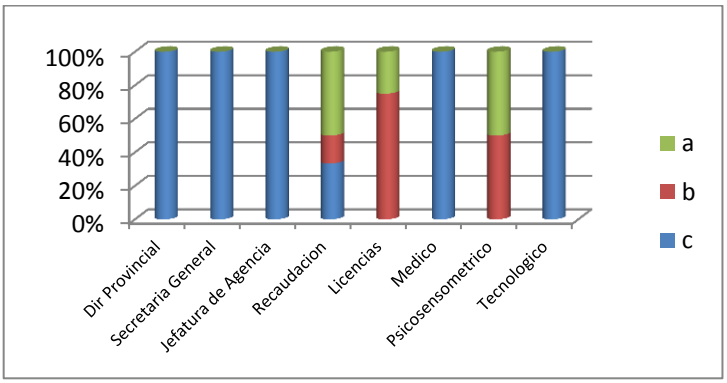


Fuente: Encuesta
Elaborado por: Santiago Bayas

3. ¿Con que frecuencia cambia la contraseña?

a. Cada semana
b. Cada mes
c. Nunca

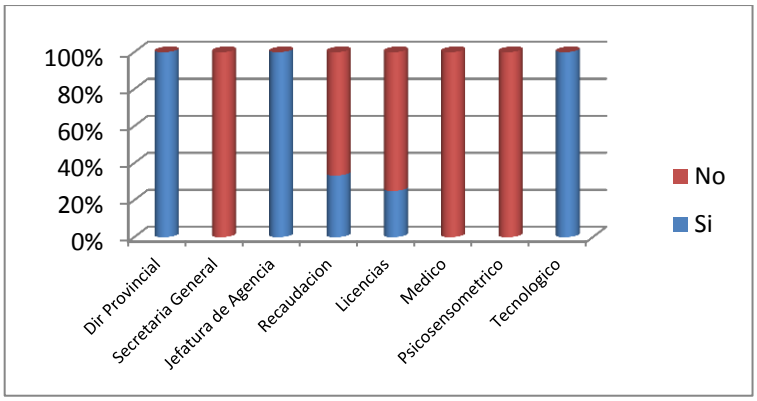
Gráfico: 3.55. Frecuencia de cambio de contraseña



Fuente: Encuesta
Elaborado por: Santiago Bayas

4. ¿Su computador está conectado a un UPS?

Gráfico: 3.56. Computador conectado a un UPS

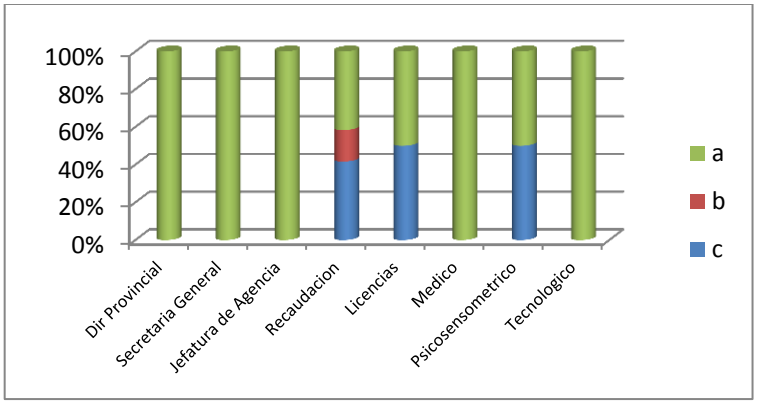


Fuente: Encuesta
Elaborado por: Santiago Bayas

5. ¿Qué proceso sigue para apagar su computador?

a. Botón inicio, opción apagar
b. Mantiene presionado el botón del CPU
c. Otro

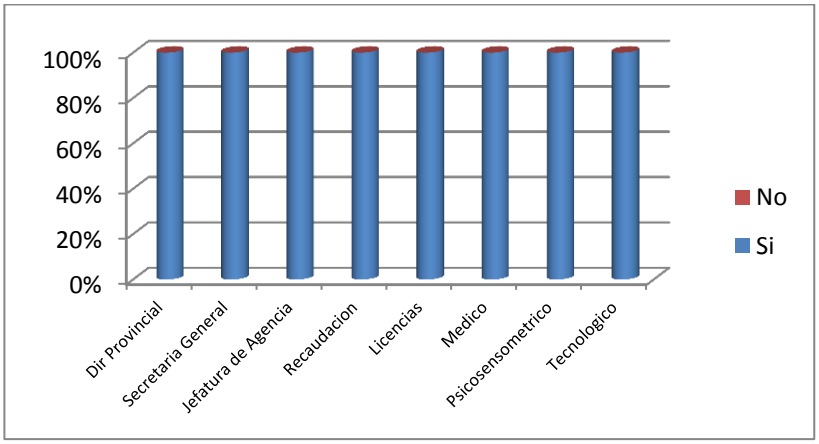
Gráfico: 3.57. Proceso para apagar el computador



Fuente: Encuesta
Elaborado por: Santiago Bayas

6. ¿Posee una contraseña para el uso de los sistemas de la Institución?

Gráfico: 3.58. Contraseña personal

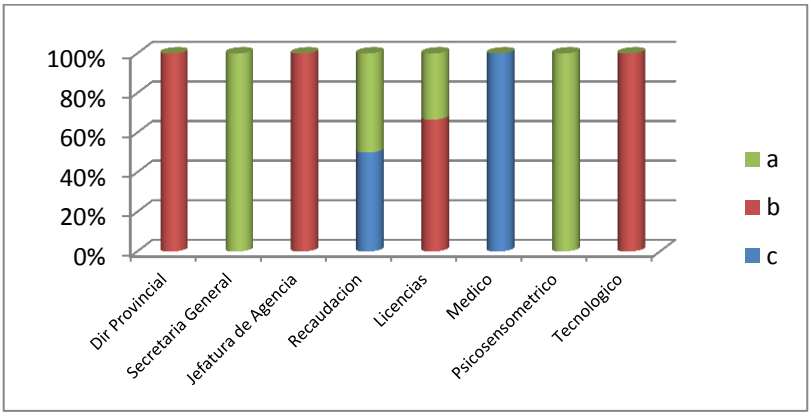


Fuente: Encuesta
Elaborado por: Santiago Bayas

7. ¿Para el uso del internet usted necesita?

a. Pedir acceso al Departamento de Sistemas
b. Tiene acceso autorizado
c. No ingresa

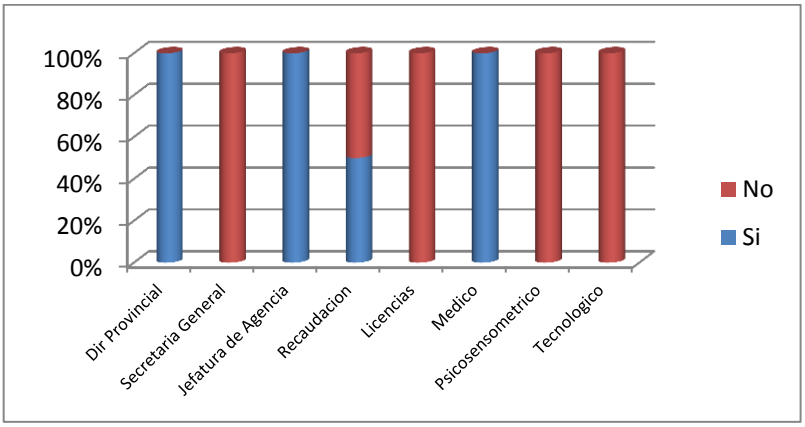
Gráfico: 3.59. Permisos para uso de internet



Fuente: Encuesta
Elaborado por: Santiago Bayas

8. ¿Cree usted que necesita capacitación para el uso de los sistemas en la Institución?

Gráfico: 3.60. Capacitación de los Sistemas de Información

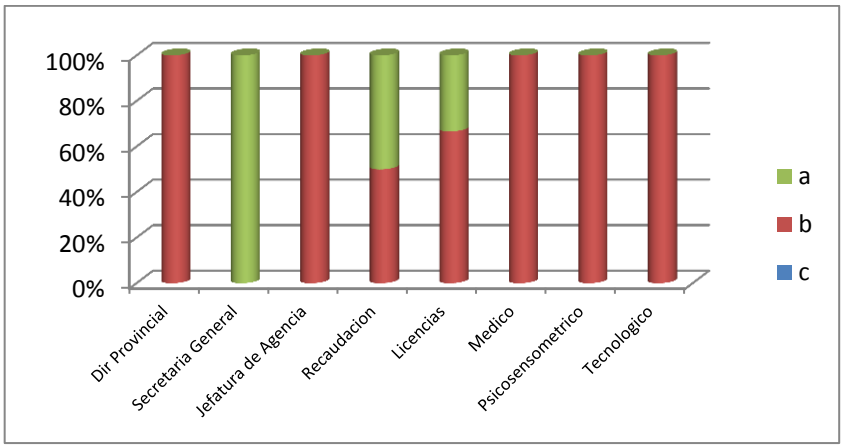


Fuente: Encuesta
Elaborado por: Santiago Bayas

9. Para instalar nuevos programas en su computador usted

a. Solicita permiso al Departamento Tecnológico
b. Solo lo instala
c. No lo instala

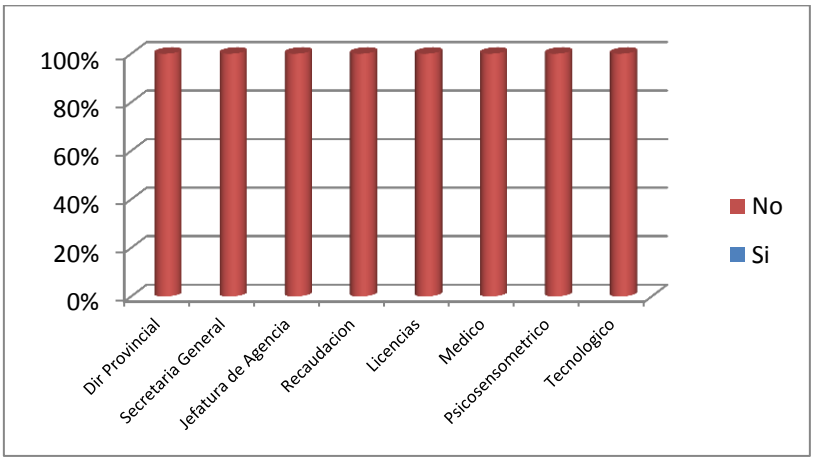
Gráfico: 3.61. Permisos para instalación de programas



Fuente: Encuesta
Elaborado por: Santiago Bayas

10. ¿Se hacen revisiones sin previo aviso para verificar todo lo almacenado en el computador?

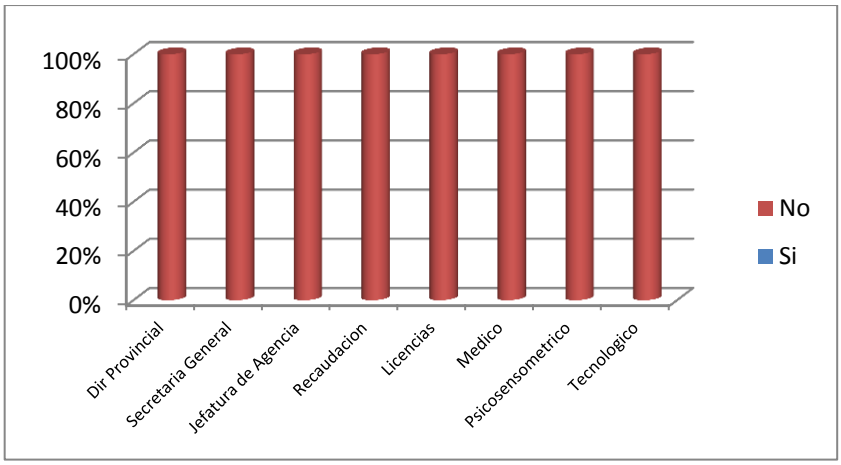
Gráfico: 3.62. Revisiones Sorpresa



Fuente: Encuesta
Elaborado por: Santiago Bayas

11. ¿Tiene algún tipo de protección para copiar información desde su computador?

Gráfico: 3.63. Seguridad para copiar información



Fuente: Encuesta
Elaborado por: Santiago Bayas

CONCLUSIONES

- Cuando el funcionario deja su puesto de trabajo para realizar otra actividad ya sea dentro o fuera de la Institución deja prendido el computador y en su mayoría no poseen claves para el acceso al sistema operativo.
- La mayoría de funcionarios no cambian su contraseña por el temor a olvidar la misma y no poder ingresar nuevamente al sistema.
- El acceso al internet es libre pero existen restricciones a varias páginas de entretenimiento pero los funcionarios pueden descargar programas y juegos.

- La mayoría de funcionarios desconocen acerca de los programas instalados en el computador.

RECOMENDACIONES

- Bloquear el computador al abandonar el puesto de trabajo para evitar que personas no autorizadas puedan sustraer información.
- Cambiar periódicamente las claves de acceso a los sistemas de información.
- No instalar software sin la debida autorización ya que esto puede ocasionar descarga y proliferación de virus en los archivos.
- Proteger el acceso a páginas de entretenimiento y redes sociales para evitar la distracción del personal.

3.5.5 Estudio Y Examen Detallado de Áreas Críticas

A continuación se detalla todas las áreas críticas que fueron identificadas después de realizar la auditoria informática en la Agencia Nacional de Transito de Tungurahua, las mismas que son detectadas para poder tomar en cuenta los posibles cambios que se deban realizar para el mejor desempeño de la institución.

- Seguridades físicas en la Institución.
- El área tecnológica no cuenta con su propia estructura organizacional.
- Manejo del Inventario de hardware y software.
- Software ilegal.
- Plan de contingencias informático.

3.5.5.1 Informe Detallado de Áreas Críticas

A continuación se detallan las áreas críticas en los formularios de hallazgos determinando todos los puntos necesarios según la deficiencia para que las recomendaciones sean tomadas en cuenta como posibles cambios

Tabla 3.30 Seguridades Físicas en la Institución

NOMBRE DE LA DEFICIENCIA: SEGURIDAD FISICA EN LA INSTITUCIÓN	
CONDICIÓN	Las áreas auditadas de la ANT de Tungurahua, no cuentan con la suficiente seguridad física para la protección del equipamiento informático, documentación y materiales de oficina, ya que no poseen tipos de seguridad para el ingreso de terceras personas, o planes de evacuación y contingencia.
CRITERIO	Todas las áreas deben poseer planes de contingencia frente a posibles desastres naturales o provocados, al igual que todas las seguridades físicas que sean necesarias para evitar cualquier inconveniente dentro de la Institución.
CAUSAS	• Falta de planificación de las diferentes áreas en el aspecto informático • Falta de control de accesos a personas ajenas a la Institución • Falta de capacitación al personal en el manejo de extintores • Falta de presupuesto
EFECTOS	• Perdidas de documentación importante para el área. • Ingreso sin autorización de personas ajenas a la institución • Desconocimiento de acciones ante posibles eventualidades
CONCLUSIONES	Por la falta de planificación de parte de la institución y de sus diferentes áreas no se ha realizado un análisis de las seguridades necesarias en el aspecto informático para poder plantear medidas preventivas para asegurar la integridad del equipamiento informático.
RECOMEN- DACION	• CORTO PLAZO o El personal encargado de la unidad informática deberá analizar los diferentes y posibles tipos de seguridad físicas que se necesite en la Institución según el área para poder implementarlas. • MEDIANO PLAZO o Se debe plantear una forma de control de acceso junto con el personal de seguridad para las personas ajenas a la Institución. o Elaboración de planes de contingencia ante posibles desastres naturales o provocados. • LARGO PLAZO o Gestionar la capacitación del personal en el aspecto de seguridad física de los equipos informáticos.

Elaborado por: Santiago Bayas

Tabla 3.31 El Área Tecnológica no tiene Estructura organizacional

NOMBRE DE LA DEFICIENCIA: EL AREA TECNOLÓGICA NO TIENE ESTRUCTURA ORGANIZACIONAL	
CONDICIÓN	El Departamento Tecnológico no dispones de una estructura organizacional la cual defina funciones a cada uno de los funcionarios de la misma.
CRITERIO	Así como todos los departamentos el área tecnológica debe disponer de una estructura organizacional por medio de la cual los funcionarios de esta área puedan tener definidas sus funciones para el buen desempeño y desenvolvimiento en la institución.
CAUSAS	• Falta de organización • Falta de planificación del departamento tecnológico
EFECTOS	• Desconocimiento de actividades puntuales • Desorganización en funciones • Incumplimiento de actividades • Descoordinación del personal
CONCLUSIONES	La falta de una estructura organizacional hace que el departamento tecnológico desconozca de las actividades específicas que debe realizar y de las áreas de las cuales está encargado.
RECOMENDACIONES	• CORTO PLAZO o El personal encargado de la unidad informática deberá planificar las actividades a realizar. • MEDIANO PLAZO o El jefe de la UI deberá determinar funciones para cada funcionario que conforma el departamento tecnológico. • LARGO PLAZO o Gestionar con los directivos de la empresa la asignación de funciones a todo el personal según el organigrama estructural. o Verificar que todas las áreas tengan su propia estructura organizacional.

Elaborado por: Santiago Bayas

Tabla 3.32. Manejo del inventario de Hardware y Software

NOMBRE DE LA DEFICIENCIA: MANEJO DEL INVENTARIO DE HARDWARE Y SOFTWARE	
CONDICION	La institución no cuenta con un inventario de hardware y software, tanto de equipos que están siendo utilizados como en los equipos dañados.
CRITERIO	El inventario de hardware y software de la institución es primordial para tener una mejor organización en cada uno de los departamentos, asignando códigos que facilite la revisión de los mismos.
CAUSAS	• Falta de planificación del departamento tecnológico • Falta de tiempo • Falta de personal • Evitar interrupciones a los funcionarios
EFECTOS	• Perdidas de dispositivos • Desconocimiento de los activos fijos de la institución • Desconocimiento de cambios imprevistos entre áreas • Desconocimiento de instalaciones de software sin autorización • Desorganización del equipamiento informático
CONCLUSIONES	La falta de personal y de planificación del departamento informático conlleva a la desorganización y desconocimiento de todo el equipamiento informático y de los sistemas de información que posee la institución.
RECOMENDACION	• CORTO PLAZO o El personal encargado del departamento informático deberá verificar que todos los equipos dañados y los que están en uso tengan su código. • MEDIANO PLAZO o El equipamiento informático deberá ser verificado para que vaya acorde a cada área según las necesidades de las mismas. • LARGO PLAZO o Realizar inventarios periódicamente para tener el conocimiento de todos los activos fijos de la Institución y así evitar la desorganización y pérdida de los mismos.

Elaborado por: Santiago Bayas

Tabla 3 Tabla 3.33 Software Ilegal

NOMBRE DE LA DEFICIENCIA: SOFTWARE ILEGAL	
CONDICIÓN	Según el estudio y el inventario que se realizó se encontró el 70% de software ilegal dentro de los cuales están aplicaciones innecesarias y de uso personal y tan solo un 30% de software legal en la Institución.
CRITERIO	Los programas necesarios para el correcto desempeño de cada uno de los funcionarios de la institución son instalados por el departamento tecnológico, fuera de estos existen programas instalados sin autorización que son utilizados según la necesidad personal del usuario.
CAUSAS	• Recursos insuficientes • Falta de conocimiento • Falta de control del Departamento Tecnológico
EFECTOS	• Mal funcionamiento de los programas • Imposibilidad de actualización del software • Problemas Legales para la Institución
CONCLUSIONES	La falta de control y de seguridad del Departamento Tecnológico ocasiona que los programas instalados no dispongan de licencias además de que los funcionarios pueden descargar e instalar programas según sus necesidades e intereses.

RECOMENDACION	• CORTO PLAZO
	  ○ Revisión minuciosa del equipamiento informático con el objetivo de eliminar el software innecesario y verificar el software ilegal.
	• MEDIANO PLAZO
	  ○ Realizar el estudio pertinente de las necesidades según los puestos de trabajo para la utilización de software libre.
	• LARGO PLAZO
	  ○ La institución debe adquirir software con su respectiva licencia según las necesidades de cada puesto.

Elaborado por: Santiago Bayas

Tabla 3.34 Plan de Contingencias Informática

NOMBRE DE LA DEFICIENCIA: PLAN DE CONTINGENCIAS INFORMATICO	
CONDICIÓN	Los funcionarios no están capacitados en varios aspectos tales como seguridad y tecnología, por este motivo la mayoría no conoce el procedimiento a seguir en el momento que se presente cualquier imprevisto y en el caso de que se necesite del Departamento Tecnológico el funcionario tendría que esperar para que se pueda solucionar el inconveniente.
CRITERIO	Todos los funcionarios deberían conocer el procedimiento a seguir en el momento de que se presenten inconvenientes informáticos y así no se genere una dependencia del personal informático ya que los funcionarios aun sin conocer la forma de resolver el inconveniente tratan de solucionarlo.
CAUSAS	• Falta de personal • Falta de Control del Departamento Tecnológico • Falta de Capacitación • Mal manejo del computador
EFECTOS	• Perdida de Información • Tiempo perdido • Falta de mantenimiento del equipamiento tecnológico • Retraso en las labores cotidianas del personal
CONCLUSIONES	La falta de capacitación a los funcionarios y el no disponer de un plan de contingencias ocasionan varios inconvenientes ya sea por el uso inadecuado o la falta de conocimiento frente a un imprevisto.

RECOMEN-
DACION
	• CORTO PLAZO
	  ○ Elaborar planes de mantenimiento preventivos y correctivos del equipamiento informático de la Institución.
	• MEDIANO PLAZO
	  ○ Planear capacitaciones a los funcionarios con respecto a temas tecnológicos y de seguridad de los mismos.
	• LARGO PLAZO
	  ○ Gestionar con los directivos la posibilidad de nuevas contrataciones de personal para el área informática.

Elaborado por: Santiago Bayas

3.6 Fase VI: Informe Final

Ambato, 20 de abril de 2015

La Auditoría informática realizada en la Agencia Nacional de Tránsito de Tungurahua inicio el día 11 de Noviembre del 2014, la persona encargada de realizar la auditoría es el Sr. Santiago Bayas estudiante de la Escuela de Ingeniería en Sistemas de la Pontifica Universidad Católica del Ecuador Sede Ambato, con la colaboración de la Ing. Verónica Pérez quien fue la persona designada de la supervisión de todos los procesos que junto al interlocutor el Sr. Juan Villacis brindaron el apoyo necesario para tener el acercamiento respectivo a cada funcionario.

Para esta Auditoría informática se utilizaron herramientas y metodologías actualizadas en el aspecto informático las cuales permitieron determinar las diferentes falencias y las posibles soluciones, dentro de los alcances los cuales estuvieron orientados a evaluar los diferentes departamentos que conforman la Agencia Nacional de Tránsito de Tungurahua, teniendo las restricciones correspondientes a los departamentos que almacenan información de gran importancia y a la cual no se tiene acceso.

Las actividades que se realizaron en la Auditoría son:

- Obtención de información necesaria de las áreas a auditar

- Realizar el inventario de hardware y software mediante el uso de herramientas y técnicas de auditoría informática
- Analizar el software legal y software ilegal instalado en el equipamiento informático de cada departamento para poder detectar posibles errores en el sistema
- Plantear diferentes soluciones a los problemas que se encuentren en el transcurso de la auditoría

AREAS Y PROCESOS AUDITADOS

Durante el proceso investigativo se tomó en cuenta diferentes aspectos tales como:

- **Seguridad Lógica**

La seguridad de los equipos por contraseñas debe ser actualizada cada tres meses por parte de las personas responsables de los mismos con esto se evita el fácil acceso y manipulación de la información almacenada. La eliminación de programas innecesarios debe ser primordial para evitar falencias en el sistema y la verificación por parte del departamento tecnológico del software ilegal.

- **Seguridad Física**

En la seguridad física se ha verificado que existe una falta de control en el ingreso y salida de las diferentes áreas de los funcionarios y de los usuarios,

esto se debe realizar para poder disminuir o eliminar el riesgo de pérdida de objetos valiosos o de documentación importante, otro de los aspectos en la seguridad física es la capacitación al personal en el tema de planes de evacuación, y tipos de medida de seguridad en caso de algún siniestro. Además de la capacitación en el tema de seguridad se debe tomar en cuenta el aspecto informático ya que en todos los departamentos los funcionarios deben saber cómo actuar en el momento de que exista algún tipo de contratiempo informático para evitar el mal funcionamiento del sistema o la perdida de información.

- **Mantenimiento de Hardware y Software**

Se encontró que el equipamiento informático de las áreas auditadas de la Agencia Nacional de Tránsito de Tungurahua no recibe el mantenimiento adecuado periódicamente además de que en el momento de que existe algún inconveniente el personal encargado se encuentra demasiado ocupado para poder resolverlo, el mantenimiento total y preventivo se debe realizar periódicamente para evitar estos inconvenientes a futuro.

- **Áreas Críticas**

Según el análisis de las diferentes áreas críticas encontradas en el proceso de auditoria existen varios puntos los cuales deberían ser tomados en cuenta tales como la falta de una estructura organizacional para el área tecnológica, el

software innecesario e ilegal instalado en los computadores de cada funcionario, la falta de capacitación al personal en el tema de seguridad informática y la falta de planes de contingencia ante los posibles acontecimientos.

Todos los puntos antes descritos son los que en base a la auditoría realizada en con ayuda de herramientas y metodologías han sido tomados en cuenta para que sean tomados en cuenta para los cambios necesarios para que la Agencia Nacional de Transito de Tungurahua pueda mejorar el servicio y el desarrollo del trabajo de sus funcionarios.

CAPÍTULO IV

ANALISIS Y VALIDACION DE RESULTADOS

4.1 Análisis De Resultados

Los resultados anteriormente expuestos han sido obtenidos en base a la Auditoria Informática realizada a la Agencia Nacional de Transito de Tungurahua la misma que se materializa a través del informe final antes detallado y la carta a la Dirección Provincial.

4.1.2 Carta a la Gerencia

En la carta se detalla todas las diferentes áreas que se revisaron y los resultados que se obtuvieron al finalizar la auditoria la carta se la puede encontrar en los Anexos

4.2 Validación de Resultados

Se presenta la evidencia que se socializo el informe final con el personal de la Agencia Nacional de Transito de Tungurahua a través de una carta emitida por la Directora Provincial de la Institución. *(Anexos 5 y 6).*

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- No existe mantenimientos periódicos y tampoco plan de contingencias que puedan evitar fallos en el sistema e inseguridad para el respaldo de la información.

- Se pudo analizar tres tipos de metodologías de las cuales la metodología que mejor se adaptó a las necesidades de la institución fue la metodología CRMR.

- Se realizó la auditoria informática según las fases de la metodología CRMR con la cual se pudo determinar las diferentes falencias dentro de la Institución.

- El informe final fue entregado a la Directiva de la Institución socializando junto con el departamento tecnológico el resultado de la Auditoria para así poder realizar los cambios necesarios para el mejor desempeño de la Agencia.

5.2 Recomendaciones

- Proteger las contraseñas y cambiarlas cada tres meses para evitar que terceras personas puedan acceder a la información.
- Contratar personal con experiencia para cubrir las funciones fundamentales del Departamento Tecnológico.
- Implementar un plan de contingencias para que la Institución se encuentre preparada para cualquier eventualidad ya sea por causas naturales o por errores humanos.
- Realizar mantenimientos preventivos y correctivos periódicos del equipamiento informático para lograr un eficiente desempeño en las funciones de cada usuario.
- Adquirir un software antivirus con licencias originales para evitar problemas provocados por la proliferación de virus.

Bibliografía

Agencia Nacional de Transito. (2012). Obtenido en https://www.ant.gob.ec

Echenique, J. (2001). *Auditoria Informática.* Mexico: Mc Graw Hill.

Espinoza, A. (2007). *Auditoría Informática para los Departamentos Financiero, Tesorería, Proveeduría, Agencia Norte y Agencia Sur de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato.*

Freire, T. M. (2012). *Guia Didáctica de Auditoria Informática.* Universidad Técnica de Ambato, Facultad de Ingeniería en Sistemas.

Hernandez, E. H. (1997). *Auditoria Informática, Un Enfoque Metodologico y Practico.* Mexico: Continental.

Iturmendi, J. A. (1994). *Auditoria Informática en la Empresa.* Madrid : Paraninfo.

Kuna, H. (2006). *Asistente para la realización de Autoría de Sistemas en Organismos Públicos o Privados.* Madrid.

Ley de Propiedad Intelectual. (2009). Obtenido en http://www.propiedadintelectual.gob.ec

Leyes Orgánicas de Transporte Terrestre, Transito y Seguridad Vial. (2012). Obtenido en http://www.ant.gob.ec/index.php/ant/base-legal/ley-organica-reformatoria-a-la-ley-organica-de-transporte-terrestre-tránsito-y-seguridad-vial

Naranjo, J. (2000). *Metodología Para La Evaluación de una Unidad Informática* (Escuela Politecnica Nacional ed.). Quito.

Piattini, M. (2003). *Auditoria Informática. Un Enfoque Practico .* España: RAMA.

Pinilla, J. (1997). *Auditoria Informática, Aplicaciones en Produccion.* Bogota: Ecoe.

Pinilla, J. (1997). *Auditoria Informática: Un Enfoque Operacional.* Bogota: Ecoe.

Quintuña, k. (2012). *Auditoria Informática a la Superintendencia de Telecomunicaciones.*

Quintuña, k. (2012). *Auditoria informática a la Supertintendencia de Telecomunicaciones.*

Rivas, G. A. (1988). *Auditoria Informática.* Madrid: Diaz de Santos, S.A.

Seguridad Lógica para una Auditoria Informática (2010). Obtenido en https://www.slideshare.net/ingenieroutpl2/seguridad-lgica

Seguridad Física dentro de la Auditoria Informática. (2007). Obtenido en www.segu-info.com.ar/fisica/seguridadfisica.htm

Tipos de Auditoria de Sistemas (2009). Obtenido en https://www.auditoríasistemas.com

Anexos

- ## Anexo 1

ENCUESTA

La siguiente encuesta está dirigida a todos los funcionarios de la Agencia Nacional de Tránsito de Tungurahua para el conocimiento del manejo de los sistemas de información y entorno de trabajo.

1.- ¿La estructura actual de su puesto de trabajo es óptima para que se realicen las funciones encomendadas eficientemente?

SI	NO

2.- ¿Posee Ud. una contraseña para acceder al sistema y empezar a realizar sus funciones?

SI	NO

3.- ¿Conoce Ud. todo el software o programas que se encuentran instalados en su computador?

SI	NO

4.- ¿Se ha realizado algún proceso de Auditoría Informática en la Organización?

SI	NO

5.- ¿La institución tiene planes de contingencia para cualquier eventualidad?

SI	NO

6.- ¿El personal de la Institución ha sido capacitado en algún momento en el ámbito tecnológico?

SI	NO

7.- ¿Se realizan actualizaciones periódicamente de los programas que son utilizados para cumplir sus funciones?

SI	NO

8.- ¿Existe algún tipo de seguridad para el acceso al sistema a los usuarios no autorizados?

SI	NO

9.- ¿Los equipos informáticos responden eficazmente para las actividades diarias?

SI	NO

10.- ¿Cree Ud. necesario revisiones periódicas de puntos de trabajo para asegurar un buen servicio y evitar algún tipo de fraude con la información?

SI	NO

Área a la que pertenece: .....

Gracias por su colaboración

- **Anexo 2**

ENCUESTA DE SEGURIDAD Y CONTROL DE LA ORGANIZACIÓN

La siguiente encuesta está dirigida a todos los funcionarios de la Agencia Nacional de Transito de Tungurahua para el conocimiento de la seguridad y control de la organización.

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

SI	NO

2. **¿La estructura actual está dada para que se realicen con eficiencia el trabajo asignado?**

SI	NO

3. **¿Los niveles jerárquicos actuales son necesarios y suficientes para la actividad normal de cada departamento?**

SI	NO

4. **De acuerdo a la estructura jerárquica de la institución se dispone de una adecuada comunicación entre las áreas**

SI	NO

5. ¿Todos los departamentos tienen definidas sus funciones y responsabilidades?

SI	NO

6. ¿Los puestos de trabajo van acorde con las necesidades del área para realizar sus funciones?

SI	NO

7. ¿Se divide el trabajo de área en funciones?

SI	NO

8 ¿Se encuentran establecidas en algún documento las funciones del área?

SI	NO

9. ¿El personal del área participa en la elaboración de las funciones?

SI	NO

10. ¿Las funciones del área van acorde al reglamento interno de la Institución?

SI	NO

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

SI	NO

12. ¿Para cumplir con las funciones del área se requiere apoyo de otras?

SI	NO

13. ¿Tiene conocimiento si existe doble asignación de funciones en otras áreas?

SI	NO

14. ¿Los objetivos están de acuerdo a las funciones del área?

SI	NO

15. ¿Se deja de realizar alguna actividad por falta de personal en la Institución?

SI	NO

16. Se da cumplimiento por parte del personal con las políticas procedimientos y normas establecidas en el área

SI	NO

17. ¿Sabe si existen políticas para la seguridad cuando termina la relación laboral con un empleado?

SI	NO

18. ¿Se adapta el personal al mejoramiento administrativo del área?

SI	NO

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

SI	NO

20. ¿Sabe si el área posee un plan de selección de personal?

SI	NO

Área a la que pertenece: _____

Gracias su colaboración

- **Anexo 3**

ENCUESTA DE CONTROL Y SEGURIDAD FISICA

La siguiente encuesta está dirigida a todos los funcionarios de la Agencia Nacional de Transito de Tungurahua para el conocimiento del control y la seguridad física.

1. **¿El área donde usted trabaja tiene seguridades contra desastres naturales?**

SI	NO

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

SI	NO

3. **¿Cuentan con horarios de entrada y salida?**

SI	NO

4. **¿Se registra el acceso de personas ajenas al área?**

SI	NO

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

SI	NO

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

SI	NO

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

SI	NO

8. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos?

SI	NO

9. ¿Saben cómo actuar en el momento de una emergencia ocasionada por fuego?

SI	NO

10. ¿Se ha indicado al personal la forma en la que se debe desalojar a todo el personal en caso de emergencia?

SI	NO

11. ¿Se han tomado medidas para minimizar la posibilidad de fuego?

SI	NO

12. ¿Se realiza mantenimiento periódico a los computadores?

SI	NO

13. ¿Tiene conocimiento de la existencia de un plan de contingencia informático?

SI	NO

14. ¿los cables de red switch, hubs, etc, se encuentran debidamente etiquetados?

SI	NO

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

SI	NO

16. ¿Existen salidas de emergencia en caso de algún desastre?

SI	NO

17. ¿Se vigila la moral y el comportamiento del personal con el fin de mantener una buena imagen?

SI	NO

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

SI	NO

19. ¿Existen alarmas para detectar condiciones anormales en el ambiente?

SI	NO

20. ¿Dentro de su área existe un plan de mantenimiento de equipos de cómputo?

SI	NO

Área a la que pertenece: _____

Gracias su colaboración

- **Anexo 4**

ENCUESTA DE CONTROL Y SEGURIDAD LÓGICA

La siguiente encuesta está dirigida a todos los funcionarios de la Agencia Nacional de Transito de Tungurahua para el conocimiento del control y la seguridad lógica.

1. Si tiene algún problema informático usted

a. Solicita ayuda al departamento técnico
b. Trata de solucionarlo

2. Cuándo usted retira de su puesto de trabajo

a. Apaga el computador
b. Ingresa una contraseña para reiniciar actividades
c. Ninguna de las anteriores

3. ¿Con que frecuencia cambia la contraseña?

a. Cada semana
b. Cada mes
c. Nunca

4. ¿Su computador está conectado a un UPS?

SI	NO

5. ¿Qué proceso sigue para apagar su computador?

a. Botón inicio, opción apagar
b. Mantiene presionado el botón del CPU
c. Otro

6. ¿Posee una contraseña para el uso de los sistemas de la Institución?

SI	NO

7. ¿Para el uso del internet usted necesita?

a. Pedir acceso al Departamento de Sistemas
b. Tiene acceso autorizado
c. No ingresa

8. ¿Cree usted que necesita capacitación para el uso de los sistemas en la Institución?

SI	NO

9. Para instalar nuevos programas en su computador usted

a. Solicita permiso al Departamento Tecnológico
b. Solo lo instala
c. No lo instala

11. ¿Se hacen revisiones sin previo aviso para verificar todo lo almacenado en el computador?

SI	NO

12. ¿Tiene algún tipo de protección para copiar información desde su computador

SI	NO

Área a la que pertenece: _____

Gracias su colaboración

- **Anexo 5**

Ambato, 15 de abril de 2015

Licenciada,

Lourdes Mayorga

DIRECTORA PROVINCIAL ANT DE TUNGURAHUA

De mis consideraciones:

Reciba un cordial saludo de parte del Sr. César Santiago Bayas Escudero, estudiante de la Escuela de Ingeniería de Sistemas de la Pontifica Universidad Católica del Ecuador Sede Ambato, quien por medio de la presente le realiza la entrega de los resultados de la Auditoría Informática realizada a los Departamentos de la Agencia Nacional de Tránsito de Tungurahua que usted acertadamente dirige, la Auditoría se la realizo desde el día 11 de Noviembre del 2014, que con la colaboración de la Ing. Verónica Pérez quien fue designada de la supervisión de todos los procesos y el Sr. Juan Villacis brindaron el apoyo necesario para tener el acercamiento respectivo a cada funcionario.

El objetivo general fue realizar una Auditoría Informática para optimizar el manejo de la información y del equipamiento informático de la Agencia Nacional de Tránsito de Tungurahua, lo cual se realizó con los datos recolectados referentes al control y seguridad física y lógica para determinar las posibles falencias y a su vez plantear las diferentes soluciones para que el documento pueda ser tomado en cuenta como documento fundamental para el mejor desempeño de las actividades y la disminución de riesgos y vulnerabilidades que pueden ocasionar problemas.

Los puntos los cuales se las debe tomar en cuenta y de los cuales se obtuvieron los resultados son:

- **Seguridad Lógica**

La seguridad de los equipos por contraseñas debe ser actualizada cada tres meses por parte de las personas responsables de los mismos con esto se evita el fácil acceso y manipulación de la información almacenada.

La eliminación de programas innecesarios debe ser primordial para evitar falencias en el sistema y la verificación por parte del departamento tecnológico del software innecesario.

- **Seguridad Física**

En la seguridad física se ha verificado que existe una falta de control en el ingreso y salida de las diferentes áreas de los funcionarios y de los usuarios, esto se debe realizar para poder disminuir o eliminar el riesgo de pérdida de objetos valiosos o de documentación importante, otro de los aspectos en la seguridad física es la capacitación al personal en el tema de planes de evacuación, y tipos de medida de seguridad en caso de algún siniestro.

Se debe tomar en cuenta el aspecto informático ya que en todos los departamentos los funcionarios deben saber cómo actuar en el momento de que exista algún tipo de contratiempo informático para evitar el mal funcionamiento del sistema o la perdida de información.

- **Mantenimiento de Hardware y Software**

Se encontró que el equipamiento informático de las áreas auditadas de la Agencia Nacional de Tránsito de Tungurahua no recibe el mantenimiento adecuado periódicamente además de que en el momento de que existe algún inconveniente el personal encargado se encuentra demasiado ocupado para poder resolverlo, el mantenimiento total y preventivo se debe realizar periódicamente para evitar estos inconvenientes a futuro.

- **Áreas Criticas**

Según el análisis de las diferentes áreas críticas encontradas en el proceso de auditoria existen varios puntos los cuales deberían ser tomados en cuenta tales como la falta de una estructura organizacional para el área tecnológica, el software innecesario e ilegal instalado en los computadores de cada funcionario, la falta de capacitación al personal en el tema de seguridad informática y la falta de planes de contingencia ante los posibles acontecimientos.

El presente proyecto finalizo cumpliéndolos objetivos con gran satisfacción y logrando un beneficio para la Institución, para el mejor desempeño de la misma

Atentamente,

César Santiago Bayas Escudero

180328170-6

- **Anexo 6**

Agencia Nacional de Tránsito

Memorando Nro. ANT-DTHA-2014-0642

Ambato, 10 de Noviembre del 2014

ASUNTO: Resolución

De mi consideración:

Por medio de la presente me permito indicar que de acuerdo a la petición presentada por parte del Sr. Cesar Santiago Bayas Escudero para la realización de un proyecto de disertación el cual corresponde al desarrollo de una auditoria informática para optimizar el manejo de la información y equipamiento informático de la Agencia Nacional de Transito de Tungurahua, se aprueba el desarrollo del proyecto antes indicado.

Para este proceso intervendrán tres partes las cuales están autorizadas a recolectar la información necesaria y supervisar todos los procesos que sean ejecutados dentro de los departamentos de la Institución

Personal a cargo de supervisar el trabajo autorizado

Sra. Ing. Verónica Pérez

Jefa de Agencia – Ambato

Sr. Juan Villacís

Asistente del Departamento Tecnológico

Se realizaran los procesos en las diferentes oficinas de la Institución, con la finalidad de socializar este servicio, se solicita a las personas designadas brindar el poyo correspondiente y la apertura necesaria

Atentamente,

AGENCIA NACIONAL DE TRÁNSITO Agencia Nacional de Tránsito DIRECCIÓN PROVINCIAL TUNGURAHUA

Documento firmado electrónicamente

Lic. Lourdes Mayorga

DIRECTORA PROVINCIAL ANT - TUNGURAHUA

Agencia Nacional de Tránsito

Ambato, 12 de Abril del 2015

CERTIFICADO

Certifico que el Sr. Cesar Santiago Bayas Escudero con número de cédula 180328170-6 realizó una Auditoria Informática en la Agencia Nacional de Transito de Tungurahua trabajo el cual tengo a bien validar y dar constancia de que los resultados presentados fueron socializados con todo el personal de la Institución.

Es todo en cuanto puedo certificar en honor a la verdad, el interesado puede hacer uso del presente certificado como mejor le convenga

Atentamente,

AGENCIA NACIONAL DE TRÁNSITO
Agencia Nacional de Tránsito
DIRECCIÓN PROVINCIAL TUNGURAHUA

Lic. Lourdes Mayorga
DIRECTORA PROVINCIAL ANT - TUNGURAHUA