ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

TESIS DE GRADO

Previo a la obtención del título de:

INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA.

"AUDITORÍA INFORMÁTICA A LA EMPRESA PÚBLICA-EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA, PERÍODO 2012".

AUTOR:

WASHINGTON ROLANDO PERALTA VILLACRÉS

RIOBAMBA – Ecuador

2014.

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de investigación sobre el tema "AUDITORÍA INFORMÁTICA A LA EMPRESA PÚBLICA- EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA, PERÍODO 2012" previo a la obtención del título de Ingeniero en Contabilidad y Auditoría C.P.A., ha sido desarrollado por el Sr. PERALTA VILLACRÉS WASHINGTON ROLANDO, ha cumplido con las normas de investigación científica y una vez analizado su contenido, se Autoriza su presentación.

Mgs. Richard Armando Caiza Castillo

DIRECTOR DE TESIS

Ing. Wilson Antonio Velasteguí Ojeda

MIEMBRO DEL TRIBUNAL

CERTIFICADO DE RESPONSABILIDAD

Yo, **PERALTA VILLACRÉS WASHINGTON ROLANDO,** estudiante de la Escuela de Ingeniería en Contabilidad y Auditoría de la Facultad de Administración de Empresas, declaro que la tesis que presento es auténtica y original. Soy responsable de las ideas expuestas y los derechos de autoría corresponden a la Escuela Superior Politécnica de Chimborazo.

PERALTA VILLACRÉS WASHINGTON ROLANDO

DEDICATORIA

Es muy grato para mí, dedicar de todo corazón el presente trabajo de investigación a mis queridos padres y hermanos, quienes siempre han estado en los momentos más difíciles apoyando y dando ánimos cuando más lo necesite.

ROLANDO PERALTA V.

AGRADECIMIENTO

Mi sincero agradecimiento, a Dios por darme la oportunidad de concluir mis estudios, a todos y cada uno de nuestros familiares que con su apoyo diario me han dirigido hacia la conclusión de nuestra investigación, a todos nuestros maestros que cada día con sus enseñanzas y experiencias me han encaminado hacia un futuro lleno de oportunidades; y finalmente, de manera especial al Mgs. Richard Caiza y al Ingeniero Wilson Velasteguí quienes me ofrecieron todas las facilidades para iniciar y finalizar con éxito el presente trabajo.

RESUMEN

La presente investigación es una "Auditoria Informática a la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012". Encaminada en el desarrollo y análisis de Seguridad Lógica, Seguridad Física, Utilización y aprovechamiento de Tecnologías de Información y Comunicación y Gestión Informática.

Antes de realizar la auditoria se realizó un análisis previo a la empresa, en donde se obtuvo un conocimiento de la misma. Con este análisis previo se elaboró una planificación adecuada, permitiendo integrar los programas correspondientes a las diferentes áreas de análisis; en donde se aplicó técnicas y procedimientos de auditoría prevista en el marco teórico, considerando las Normas de Control Interno grupo 410, emitidas por la Contraloría General del Estado.

Como resultado de la Auditoria Informática tenemos la falta de políticas sobre actualización periódica de claves de acceso a los sistemas y eliminación de archivos, ausencia de medidas adecuadas de seguridad física en la Unidad de Informática, falta de capacitación informática, inadecuada segregación de funciones.

Se recomienda a la EP-EMAPAR tomar en cuenta los aspectos estipulados en el informe de Auditoría. Y aplicar cada año una auditoria Informática, para medir el grado de cumplimiento de las Normas de Control Interno emitidas por la CGE.

SUMMARY

This research work is a “Computer Processes Audit done to the Public Municipal Water Supply and Sewerage Company of Riobamba (EP-EMAPAR- acronym for the Spanish Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba) during 2012.” It is aimed to promote the development and analysis of logical security, physical security, procedure and good use of information and communication technologies, and computer systems management.

Before doing the audit, a previous analysis was carried out in the enterprise in order to get acquainted with it. With this previous analysis, an adequate planning was done by integrating the corresponding programs in the different analyzed areas. Here, different techniques and produces described in the theoretical framework were applied considering the Internal Control Regulations group 410 given by General State Comptroller.

As a result of this Computer Process Audit, it can be seen there is lack of policies about changing password periodically and file deleting; there is also, lack of adequate physical security in the Computer Systems Unit; there is lack of computer use training, and inadequate duties segregation.

It is recommended that EP-EMAPAR consider the different aspects prescribed in the audit report and do a yearly computer processes audit to see the degree of compliance they have of the Internal Control Regulations given by the General State Comptroller.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

No. DESCRIPCIÓN PÁG.

ÍNDICE DE TABLAS

No. DESCRIPCIÓN PÁG.

ÍNDICE DE TABLAS

No. DESCRIPCIÓN PÁG.

ÍNDICE DE ANEXOS

No. DESCRIPCIÓN PÁG.

CAPÍTULO I

1. EL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

A partir de los años 50, la informática se convierte en una herramienta muy importante en las labores de auditoría financiera, que permite llevar a cabo, de forma rápida y precisa, operaciones que manualmente consumirían demasiados recursos. Empieza la denominada "auditoría con el ordenador", en la que se utiliza el ordenador como herramienta del auditor financiero.

Sin embargo, al hacerse las organizaciones cada vez más dependientes de los sistemas de información, surge la necesidad de verificar que éstos funcionen correctamente, empezándose a finales de los años 60 a descubrirse varios casos de fraude cometidos con la ayuda del ordenador , que hacen inviable seguir conformándose con la auditoría "alrededor del ordenador". De ahí la necesidad de una nueva especialidad dentro de la auditoría, la "auditoría del ordenador", cuyo objetivo es precisamente verificar el funcionamiento correcto, eficaz y eficiente de las tecnologías y sistemas informáticos.

En la actualidad nadie duda que la información se haya convertido en uno de los activos principales de las empresas, representando las tecnologías y sistemas relacionados con la información, su principal ventaja estratégica. Las organizaciones invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información y en la adquisición y desarrollo de tecnologías que les ofrezcan la mayor productividad y calidad posible. Es por eso que los temas relativos a la auditoría de TSI cobran cada vez más relevancia a nivel mundial. (Mario Piattini Velthuis, Emilio del Peso Navarro, & Mar del Peso Ruiz, 2008) P. xxxv

Dentro del análisis previo se determina que en la Empresa Pública Empresa Municipal de Agua Potable y Alcantarillado de Riobamba no se ha realizado una Auditoría Informática que mida el nivel de cumplimiento de las Normas de

Control Interno emitidas por la Contraloría General del Estado, grupo 410 referente a Tecnologías de Información. Por lo que se ha generado un nivel de perplejidad en el cumplimiento de dichas normas.

1.1.1. Formulación del Problema de Investigación.

A continuación se formula la interrogante a la que se pretende dar respuesta:

¿Cómo una Auditoría Informática a la Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012, permitirá el cumplimiento de las Normas de Control Interno de Tecnologías de Información?

1.1.2. Delimitación del Problema

El problema antes descrito tiene como objeto la Auditoría informática en las Instituciones Públicas, y como campo el uso de tecnologías de información y comunicación de la Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012.

1.2. OBJETIVOS

1.2.1. Objetivo General

Realizar la Auditoría Informática a la Empresa Pública-Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012, para medir el grado de cumplimiento de las Normas de Control Interno sobre Tecnologías de la Información.

1.2.2. Objetivos Específicos

- ✓ Diagnosticar los aspectos generales sobre el grado de cumplimiento de las Normas de Control Interno de Tecnologías de la Información emitidos por la Contraloría General del Estado.

- ✓ Ejecutar la Auditoría Informática mediante la elaboración de un plan de trabajo para la obtención de evidencias suficientes y pertinentes.
- ✓ Emitir un informe final proponiendo mejoras y soluciones que se adapten en la utilización más eficiente y segura de la información para una adecuada toma de decisiones.

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Actualmente, la información es el centro de las estrategias productivas, por tal razón las instituciones tienen la necesidad de automatizar sus procesos e implantar sistemas de información que beneficien el desempeño laboral del personal, pero así mismo se requiere que éstos sean continuamente monitoreados, mejorados y adaptados a las nuevas exigencias del entorno, como son las normas de control interno emitidas por la Contraloría General del Estado. Por ello es de gran interés realizar una Auditoría Informática que permita proporcionar un reporte donde se detalle los puntos críticos de la institución en el ámbito de tecnologías de la información que permita tomar medidas correctivas, asegurando confiabilidad, confidencialidad y disponibilidad de la información encaminado a guiar el buen desarrollo y correcto funcionamiento del área auditada en la institución.

El desarrollo del trabajo de investigación es de gran interés, importancia y beneficio para la Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, funcionarios de la misma y demás usuarios de tecnologías de información y comunicación, por ende puedan tomar decisiones sobre el cumplimiento de las Normas de Control Interno sobre Tecnologías de Información grupo 410, esto generaría un beneficioso impacto público mediante el cumplimiento de ciertas características como el desempeño, eficacia, seguridad, privacidad, recomendaciones y soluciones a los problemas.

CAPÍTULO II

2. AUDITORÍA INFORMÁTICA

2.1. Generalidades de la Auditoría Informática

2.1.1. Antecedentes

La auditoría informática apoyada en el resto de auditorías; para la siguiente investigación se basa en los siguientes Autores, según (Muñoz Razo , 2002. P., págs. 9-10):

Tabla 1: Antecedentes de la Auditoria Informática.

Autor	Año	Referencia
Echenique	1988	Publicó su libro auditoría de sistemas, en el cual establece sus principales bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico práctico sobre el tema.
Lee	1992	Presentó un libro en el cual enuncia los principales aspectos a evaluar en una auditoría de sistemas, mediante una especie de guía que le indica al auditor los aspectos que debe evaluar en este campo.
Rosalba Escobedo Valenzuela	1993	Presenta una tesis de auditoría a los centros de cómputo, como apoyo a la gerencia destacando sus aspectos más importantes.
G. Haffes, F. Holguín y A. Galán,	1994	En su libro sobre auditoría sobre los estados financieros, presenta una parte relacionada con la auditoría de sistemas que profundice los aspectos básicos de control de sistemas y se complementa con una serie de preguntas que permiten evaluar aspectos relacionados con este campo.
Ma. Guadalupe Buendía Aguilar y Edith Antonieta Campos	1995	Presentan un tratado de auditoría informática (apoyándose en lo señalado con el maestro Echenique), en el cual presentan metodologías y cuestionarios útiles para realizar esta especialidad.
Yann Darrien	1995	Presenta un enfoque particular sobre la auditoría de sistemas.
Alvin A. Arens y James K. Loebbecke	1996	En su libro de auditoría un enfoque integral, de Prentice Hall Hispanoamericana, S.A., nos presentan una parte de esta obra como auditoría de sistemas complejos.
Hernández Hernández	1996	Propone la auditoría en informática, en la cual da ciertos aspectos relacionados con esta disciplina.

Autor	Año	Referencia
Francisco Ávila	1997	Obtiene mención honorifica en su examen profesional, en la Universidad de Valle de México, Campus San Rafael, con una tesis en la cual propone un caso práctico de la auditoría de sistemas realizado en una empresa paraestatal.
Yann Darrien	1998	Presenta Técnicas de auditoría, donde hace una propuesta de diversas herramientas de esta disciplina.
Mario Piattini y Emilio del Peso	1998	Presentan Auditoría informática, un enfoque práctico, donde mencionan diversos enfoques y aplicaciones de esta disciplina.

Fuente: (Muñoz Razo , 2002. P., págs. 10-11)
Elaborado por: El Autor

2.1.2. Alcance

Según Vandama N.; Lescay M.; Castillo G. y García F. Auditoría Informática, El alcance de la auditoría define con precisión el entorno y los límites en que va a desarrollarse la auditoría informática y se complementa con los objetivos de ésta. El alcance se concretará expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. (Vandama N., Lescay M., & García F. , 2002).

2.1.3. Definición

Auditoría Informática: Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y de más componentes.

Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumos necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la

emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas informáticos a la empresa

Esta es la definición de **Ron Weber** en Auditing Conceptual Foundations and Practice sobre auditoría informática:

Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

Mientras que **Mair William** define lo siguiente:

La auditoría informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones. (Muñoz Razo , 2002. P., págs. 23-24).

2.1.4. Objetivos de la Auditoría Informática

La evaluación a los sistemas computacionales, a la administración al centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos, (Muñoz Razo , 2002. P., págs. 39-40):

- ✓ Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

- ✓ Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.

- ✓ Evaluar el aprovechamiento del sistema operativo, programas, software de producción disponible.

- ✓ Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.

- ✓ Evaluar la disponibilidad de seguridades necesarias a fin de proteger y salvaguardar los equipos de tecnología disponibles para el desarrollo de actividades.

- ✓ Realizar una evaluación en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área informática.

2.1.5. Tipos de Controles Internos

Históricamente, los tipos de los controles informáticos se han clasificados en las siguientes categorías, (Mario Piattini Velthuis, Emilio del Peso Navarro, & Mar del Peso Ruiz, 2008, pág. 31):

- ✓ **Controles preventivos:** para tratar de evitar el hecho, como un software de seguridad que impida los accesos no Autorizados al sistema.
- ✓ **Controles detectivos:** cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de accesos no

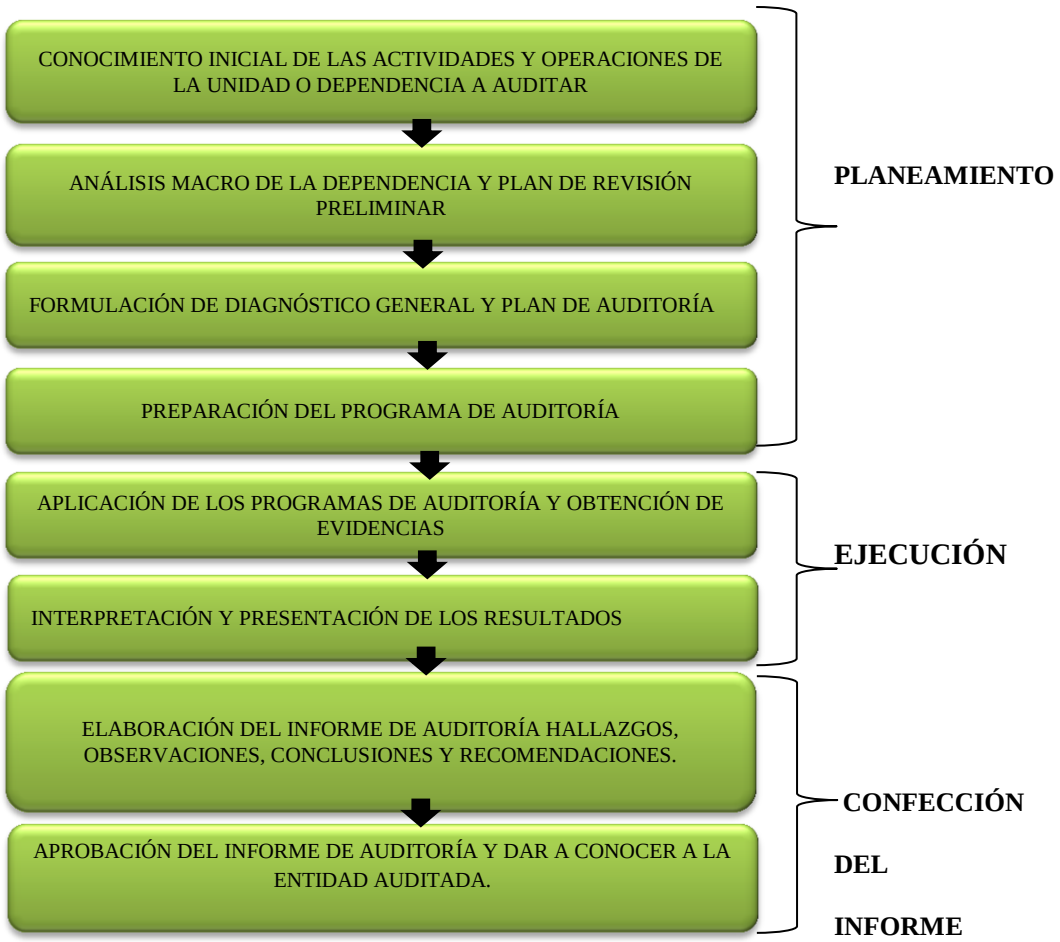
autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

- ✓ **Controles correctivos**: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo la recuperación de un archivo dañado a partir de las copias de seguridad.

2.2. Proceso de una Auditoría Informática

Todo proceso posee una metodología para ser realizado, es así que el método de trabajo del auditor pasa por las siguientes etapas:

Ilustración 1: Proceso de la Auditoría Informática.



Fuente: Investigación
Elaborado por: El Autor

2.2.1. Planificación de la Auditoría Informática.

La etapa de planificación es una de las más importantes dentro del proceso de auditoría debido a que se define las actividades que se van a desarrollar en el transcurso de la misma, así como las técnicas, procedimientos y programas necesarios para llevar acabo la fase de ejecución y de esta forma poder obtener información que respalde el dictamen de auditoría.

2.2.2. Ejecución de la Auditoría Informática.

Concretamente, tenemos lo siguiente:

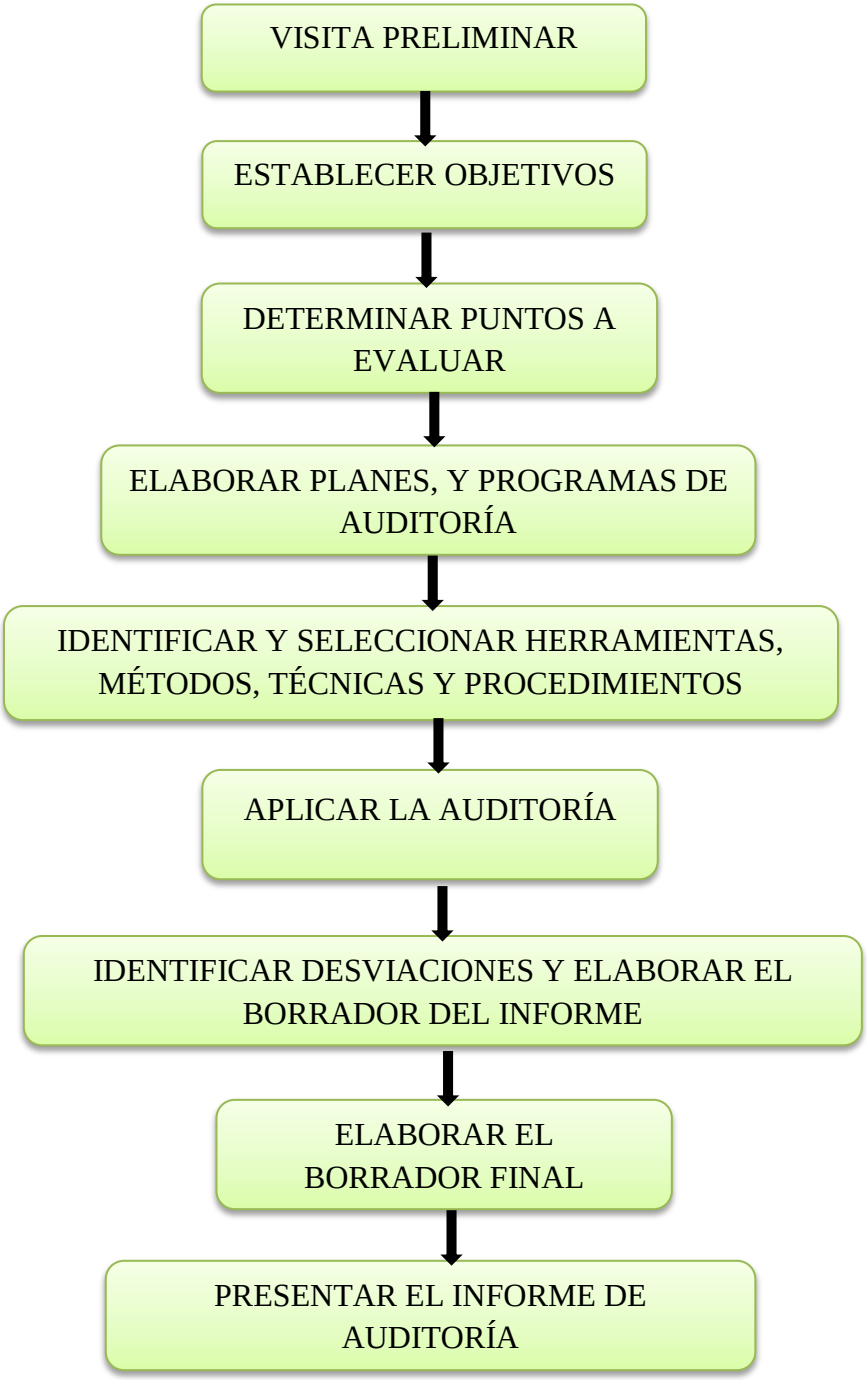
- ✓ Realizar las acciones programadas para la auditoría.
- ✓ Aplicar los instrumentos y herramientas para la auditoría.
- ✓ Identificar y elaborar los hallazgos de auditoría.
- ✓ Elaborar el dictamen de auditoría y presentarlo a discusión.

2.2.3. Dictamen de la Auditoría Informática

- ✓ Preparación y redacción del informe final
- ✓ Redacción de la carta de introducción o carta de presentación del informe final y seguimiento de las medidas correctivas. (Muñoz Razo , 2002. P., págs. 186-236) (Figura 2):

2.3. Esquema de la Auditoria Informática

Ilustración 2: Esquema de la Auditoría Informática



Fuente: Investigación
Elaborado por: El Autor

2.4. Instrumentos de recopilación de información dentro de auditoría informática.

El auditor debe aprovechar las técnicas, procedimientos y herramientas tradicionales de auditoría aplicables en la auditoría informática; el propósito es que las diseñe y las utilice para hacer una evaluación correcta del funcionamiento de dicha área, de la operación del propio sistema o de su gestión informática, beneficiándose con ello debido a la ya aprobada eficiencia y eficacia en otros tipos de auditoría; entre las cuales tenemos:

- ✓ Entrevistas
- ✓ Cuestionarios
- ✓ Encuestas
- ✓ Observación
- ✓ Inventarios
- ✓ Muestreo

2.5. Técnicas de evaluación aplicables a la auditoría informática

- ✓ Inspección
- ✓ Revisión Documental
- ✓ Matriz FODA

2.6. Normas de Control Interno para la Auditoría Informática

En este tema, tomamos como base las **Normas de Control Interno de la Contraloría General de Estado**, ya que estas son de obligatoriedad para las instituciones del sector público y sirven como marco de referencia para las instituciones y organizaciones a nivel privado para adoptar puntos referentes de evaluación y control de sus procesos.

Dentro del grupo 400, subgrupo 410, encontramos las normas para la evaluación del control interno en el área de la Informática.

Así, las normas emitidas por la Contraloría General del Estado referente a Sistemas de Información y Comunicación son:

- ✓ 410.- Tecnología de la información

Normas de Tecnología de la información. Sub grupo 410 (,Contraloría General del Estado, 2009, págs. 73-83):

410 TECNOLOGÍA DE LA INFORMACIÓN

410-01 Organización informática.- Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones.- Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente Autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410–03 Plan informático estratégico de tecnología.- La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario.

La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico.

El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima Autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos.- La máxima Autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre

otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.
Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.

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

410-05 Modelo de información organizacional.- La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.

El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los

objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente.
Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos.- La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.
2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.
3. La formulación de los proyectos considerará el *Costo Total de Propiedad CTP*; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.
4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y Autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.
5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.
6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.

7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.
8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.
9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.
10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo.- La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán Autorizadas por la máxima Autoridad previa justificación técnica documentada.
2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.
3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.
4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de

aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de Autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.
6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.
7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de Autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de Autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima Autoridad o su delegado.
8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

9. Los derechos de Autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.
10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.
11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica.- La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán Autorizadas por la máxima Autoridad previa justificación técnica documentada.
2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.
3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones

técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

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

410-09 Mantenimiento y control de la infraestructura tecnológica.- La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.
2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y Autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
3. Control y registro de las versiones del software que ingresa a producción.
4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información.- La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;
2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;
4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con

temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;

7. Consideración y disposición de sitios de procesamiento alternativos.
8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias.- Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado. Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.
2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.
3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.
4. Plan de recuperación de desastres que comprenderá:
    - ✓ Actividades previas al desastre (bitácora de operaciones)
    - ✓ Actividades durante el desastre (plan de emergencias, entrenamiento)
    - ✓ Actividades después del desastre.

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

6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.
7. El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información.- La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
3. Estandarización de la identificación, autenticación y Autorización de los usuarios, así como la administración de sus cuentas.
4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.
5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.

6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.
7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.
8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.
9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.
10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.
11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios.- Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet. Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

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

410-15 Capacitación informática Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

410-16 Comité informático Para la creación de un comité informático institucional, se considerarán los siguientes aspectos:

- ✓ El tamaño y complejidad de la entidad y su interrelación con entidades adscritas.
- ✓ La definición clara de los objetivos que persigue la creación de un comité de informática, como un órgano de decisión, consultivo y de gestión que tiene como

propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad.

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

410-17 Firmas electrónicas.- Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.

El uso de la firma electrónica en la administración pública se sujetará a las garantías, reconocimiento, efectos y validez señalados en estas disposiciones legales y su normativa secundaria de aplicación.

Las servidoras y servidores Autorizados por las instituciones del sector público podrán utilizar la firma electrónica contenida en un mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público que ocupan.

Los aplicativos que incluyan firma electrónica dispondrán de mecanismos y reportes que faciliten una auditoría de los mensajes de datos firmados electrónicamente.

a) Verificación de autenticidad de la firma electrónica

Es responsabilidad de las servidoras y servidores de las entidades o dependencias del sector público verificar mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida sea emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.

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

Con el propósito de que exista uniformidad y compatibilidad en el uso de la firma electrónica, las entidades del sector público sujetos a este ordenamiento coordinarán y definirán los formatos y tipos de archivo digitales que serán aplicables para facilitar su utilización.

Las instituciones públicas adoptarán y aplicar los estándares tecnológicos para firmas electrónicas que las entidades oficiales promulguen, conforme a sus competencias y ámbitos de acción.

c) Conservación de archivos electrónicos

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

d) Actualización de datos de los certificados de firmas electrónicas

Las servidoras y servidores de las entidades, organismos y dependencias del sector público titulares de un certificado notificarán a la entidad de certificación de Información sobre cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado.

Cuando un servidor público deje de prestar sus servicios temporal o definitivamente y cuente con un certificado de firma electrónica en virtud de sus funciones, solicitará a la entidad de certificación de información, la revocación del mismo, además, el superior jerárquico ordenará su cancelación inmediata.

El dispositivo portable seguro será considerado un bien de la entidad o dependencia pública y por tanto, a la cesación del servidor, será devuelto con la correspondiente acta de entrega recepción.

e) Seguridad de los certificados y dispositivos portables seguros

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

f) Renovación del certificado de firma electrónica

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

g) Capacitación en el uso de las firmas electrónicas

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

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. HIPÓTESIS

Al realizar la Auditoría informática, a la Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012, permitirá cumplir las Normas de Control Interno del grupo 410 emitidos por la Contraloría General del Estado.

3.2. VARIABLES

3.2.1. Variable Independiente

Auditoría Informática

3.2.2. Variable Dependiente

Cumplimiento de las Normas de Control Interno de Tecnologías de Información.

3.3. TIPO DE INVESTIGACIÓN

3.3.1. Investigación Cuantitativa.

Se utiliza para comprobar la hipótesis puesto que se enfoca principalmente a recolectar y analizar datos en este caso toda la información necesaria que se obtenga de la EP-EMAPAR (número de funcionarios, número de departamentos, y otros usuarios del sistema informático).

3.3.2. Investigación Cualitativa.

Se centrará en crear pruebas que demuestren con fundamento lo que estamos investigando (que estrategias utilizan en la EP-EMAPAR) pero esta a su vez se limitará a utilizar números y datos estadísticos lo cual es contrario a la variable cuantitativa que esta si lo hace.

3.3.3. Investigación Mixta.

El tipo de investigación a utilizarse en este proyecto es mixta, puesto que, ayudará a definir y clarificar mejor cada uno de los problemas que se vayan encontrando en la Empresa, durante la realización de la Auditoría Informática.
En la investigación mixta existen dos tipos de variables tanto la cuantitativa como la cualitativa como se expresa en los puntos anteriores.

3.4. POBLACIÓN Y MUESTRA

Para la obtención de la información del análisis FODA, se aplicó las encuestas a: jefe y colaboradores del departamento de Informática y para los funcionarios que usan el sistema informático de la EP-EMAPAR se aplicó la técnica de muestreo para determinar el número de encuestas a aplicar.

Según los datos proporcionados por el jefe de Informática:

POBLACIÓN	NÚMERO DE USUARIOS	MUESTRA
GERENCIA	6	5
ADMINISTRATIVO	4	3
FINANCIERO	12	10
ATENCIÓN AL CLIENTE	3	3
CATASTRO	4	3
COMERCIALIZACIÓN	14	12
INGENIERÍA	11	10
TÉCNICOS	10	9
TOTAL	**64**	**55**

FÓRMULA DE MUESTREO PARA APLICAR ENCUESTAS

Fórmula: $$n = \frac{Z^2.p.q.N}{\mathrm{N}.E^2 + Z^2.p.q}$$

***n*=**tamaño de la muestra

Z= nivel de Confianza

p= variabilidad positiva

q= variabilidad negativa

N= tamaño de la población

E= margen de error

$$n = \frac{1{,}96^2 * 0{,}5 * 0{,}5 * 64}{64 * 0{,}05^2 + 1{,}96^2 * 0{,}5 * 0{,}5}$$

$$n = \frac{61{,}4656}{1{,}1204}$$

$$\boldsymbol{n = 55}$$ **Encuestas**

3.5. MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.5.1. Métodos

Además de las investigaciones detalladas anteriormente se utilizan diversos métodos exploratorios, los mismos que facilitan la realización de los procesos necesarios investigativos a utilizarse en este proyecto. Estos métodos han sido seleccionados de acuerdo al tipo de investigación que se realiza y los cuales están explicados a continuación:

- Método Teórico
- Método Empírico
- Método Inductivo - deductivo.

3.5.2. Técnicas

- Observación directa,
- Entrevistas,
- Encuestas.

3.5.3. Instrumentos

- Guía de entrevistas
- Cuestionario.

3.6. DIAGNÓSTICO SITUACIONAL DE LA EMPRESA DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA

3.6.1. Diagnóstico Situacional

Previo al análisis FODA dentro de la Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, se hizo un reconocimiento dentro de la misma de toda la información que nos daría la base para realizar este análisis, el mismo que se obtuvo mediante la aplicación de encuestas a: personal ejecutivo de la empresa y demás usuarios de tecnologías de información y personal de la unidad de informática, el mismo que permite realizar una comparación entre las perspectivas que tienen cada uno de ellos para determinar el diagnóstico situacional basado en fortalezas, oportunidades, debilidades y amenazas.

3.6.2. Análisis FODA

El análisis FODA consiste en identificar las fortalezas, oportunidades, debilidades y amenazas para de esta forma aprovechar de la mejor manera las fortalezas y oportunidades que se presenten en el análisis y tratando de disminuir al máximo las debilidades y amenazas que se presentan para de esta forma mantener un adecuado sistema de control interno.

3.6.3. Planificación para el desarrollo de la Matriz FODA

Objetivo: Conocer cuáles son las perspectivas que mantienen cada uno de los sectores involucrados para el análisis interno a través de la aplicación de encuestas.

Tabla 2: Planificación para el desarrollo de la Matriz FODA

N°	DETALLE	PROCEDIMIENTOS	ACTIVIDADES ESPECIFICAS	TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN
1.	Determinar quiénes son los involucrados para obtener información en el análisis interno.	1.1. Determinar quiénes son las Autoridades de la EP-EMAPAR. 1.2. Determinar quiénes son los jefes de los departamentos de la empresa. 1.3. Conocer quiénes son y cuantas personas trabajan en el departamento de Sistemas de la empresa. 1.4. Determinar quiénes son los usuarios internos del sistema informático.	1.1.1 Realizar una visita preliminar al Gerente y Jefes Departamentales. 1.3.1 Mantener un conversatorio con el personal operativo de Sistemas. 1.4.1 Solicitar información a la dirección del departamento de Sistemas. 1.4.2 Solicitar información a cada una de los departamentos para determinar el número total de los usuarios internos del sistema.	Observación directa Indagación Entrevista.
2.	Diseñar un modelo de entrevista para el Gerente y Jefes Departamentales.	2.1 Establecer preguntas en el ámbito táctico-estratégico referente a tecnologías de información y comunicación.	2.1.1 Mantener un conversatorio normal a fin de conocer sobre las estrategias que mantienen las Autoridades de turno referente a tecnologías de información y comunicación.	Indagación Entrevista
3.	Diseñar un modelo de encuesta para Gerente, Jefes Departamentales y demás usuarios internos del sistema informático a través de la herramienta GOOGLE.DOCS.	3.1. Establecer una lista de preguntas. 3.1.1. Seleccionar las preguntas más adecuadas considerando el ámbito táctico estratégico de Tics.	3.1.1.1. Aplicar la encuesta explicando cual es el motivo de la misma y la finalidad que se espera de ella.	Encuesta
4.	Diseñar un modelo de la encuesta para el personal operativo de la unidad de informática	4.1. Establecer una lista de preguntas. 4.1.1. Seleccionar las preguntas más adecuadas considerando el ámbito operativo de tecnologías. 4.1.2. Establecer preguntas de tipo cerrada.	4.1.2.1. Aplicar la encuesta al personal responsable de esta área.	Encuesta

N°	DETALLE	PROCEDIMIENTOS	ACTIVIDADES ESPECIFICAS	TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN
5	Recibir toda la información de todas las encuestas aplicadas: a nivel de Autoridades, personal operativo del sistema informático y demás usuarios del mismo.	5.1. Determinar que las encuestas que se tenía previsto estén aplicadas.	5.1.1 Clasificar cada una de las encuestas de acuerdo al grupo y al modelo de encuestas aplicadas.	Confirmación.
6.	Tabulación de resultados	6.1. Diseñar formatos de tabulación de resultados para cada una de las encuestas aplicadas.	6.1.1. Tabular los resultados a nivel de Autoridades, personal operativo y demás usuarios del sistema informático.	Tabulación
7.	Interpretación de información.	7.1. De los resultados de la tabulación determinar las fortalezas y debilidades para el análisis interno.	7.1.1. Tomar en cuenta los resultados a nivel del personal operativo. 7.1.2. Hacer énfasis en los resultados obtenidos a nivel de usuarios de las Tics.	Análisis Confirmación.

Elaborado por: El Autor
Fuente: Investigación

3.6.4. Resultados de encuestas aplicadas a Gerente, Directores, Jefes y demás empleados.

OBJETIVO: Conocer aspectos relacionados sobre las estrategias realizadas por parte de las Autoridades de la Empresa en lo concerniente a la administración de los Sistemas de Información y Comunicación.

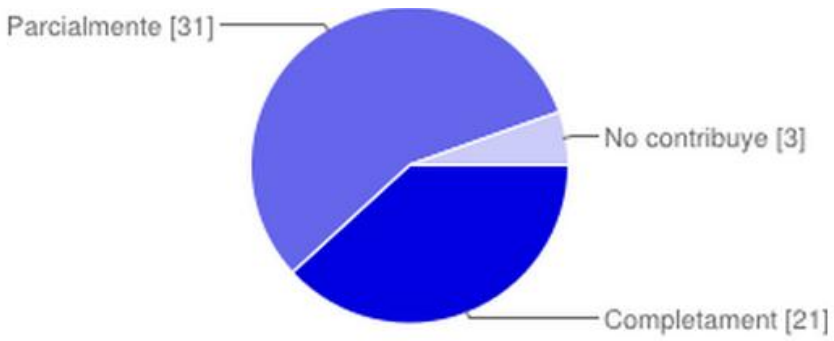
1. ¿De acuerdo a la situación actual de los departamentos cree usted que esto contribuye a la Misión y Visión de la EP-EMAPAR?

Tabla 3: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, jefes y demás empleados pregunta N° 01.

Completamente cierto	21	38%
Parcialmente cierto	31	56%
No contribuye	3	6%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 3: Representación de la tabulación. Pregunta N° 01.



Interpretación:

Mediante la aplicación de la encuesta a los usuarios del parque informático de la EP-EMAPAR se determina que de acuerdo a la situación actual de los departamentos el 38% completamente cierto que contribuye con la misión y visión de la empresa, un 56% parcialmente cierto, y un 6% no contribuye.

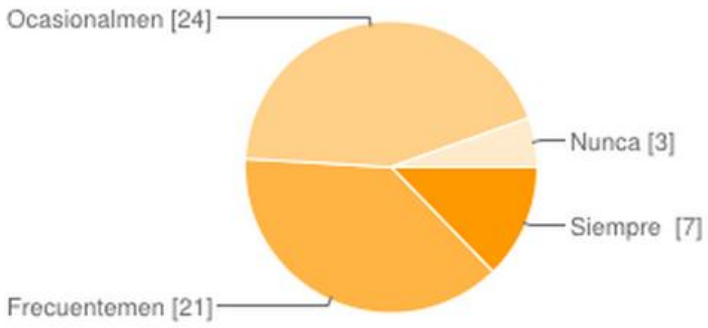
2. ¿Existen planes de inversión periódicos en lo que corresponde a la adquisición y equipamiento del parque tecnológico de la EP-EMAPAR?

Tabla 4: Tabulación del resultado de las encuestas aplicadas a Gerente, directores, jefes y demás empleados pregunta N° 02.

Siempre	7	13%
Frecuentemente	21	38%
Ocasionalmente	24	44%
Nunca	3	5%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 4: Representación de la tabulación. Pregunta N° 02.



Interpretación:

Mediante la aplicación de la encuesta a los usuarios del parque informático de la EP-EMAPAR se determina que existe planes de inversión periódicos con un 13% siempre, el 38% frecuentemente, el 44% ocasionalmente y nunca existe el 5%.

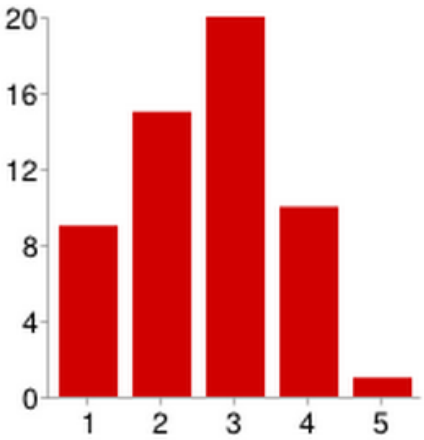
3. ¿Considera usted que se cuenta con un adecuado parque informático dentro de la empresa?

Tabla 5: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, jefes y demás empleados pregunta N° 03.

Siempre (1)	9	16%
Casi siempre (2)	15	27%
Esporádicamente (3)	20	36%
Casi nunca (4)	10	18%
Nunca (5)	1	2%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 5: Representación de la tabulación. Pregunta N° 03.



Interpretación:

Mediante la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 16% considera que se cuenta con un adecuado parque informático, el 27% casi siempre existe, el 36% indica que esporádicamente existe, el 18% casi nunca y el 2 % indica que nunca existe un adecuado parque informático.

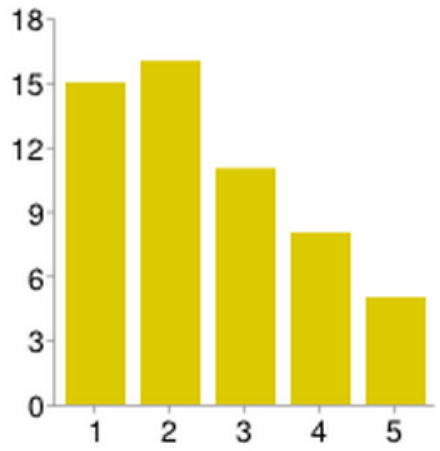
4. ¿Existen Software aplicativo o módulos de acuerdo a cada uno de los departamentos de la empresa?

Tabla 6: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y demás empleados pregunta N° 04.

Siempre (1)	15	27%
Casi siempre (2)	16	29%
Esporádicamente (3)	11	20%
Casi nunca (4)	8	15%
Nunca (5)	5	9%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 6: Representación de la tabulación. Pregunta N° 04.



Interpretación:

Mediante la aplicación de la encuesta a los usuarios del parque informático de la empresa se determina que el 27% considera que existe software aplicativo o módulos de acuerdo a cada uno de los departamentos, el 29% casi siempre existe, el 20% indica que esporádicamente existe, el 15% casi nunca y el 9 % indica que nunca existe el software aplicativo o módulos.

5. ¿Considera usted necesario que se realice una Auditoría Informática en la Empresa que permita cumplir las Normas de Control Interno emitidas por la Contraloría General del Estado del grupo 410 referente a tecnologías de información?

Tabla 7: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y demás empleados pregunta N° 05.

SI	55	100%
NO	0	0%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 7: Representación de la tabulación. Pregunta N° 05.

Interpretación:

Mediante la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 100% considera necesario la realización de una Auditoría Informática en la Empresa que permita cumplir las Normas de Control Interno emitidas por la Contraloría General del Estado del grupo 410 referente a tecnologías de información.

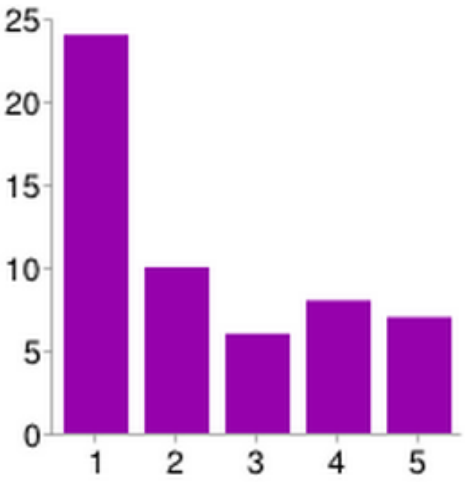
6. ¿Cree usted que mediante la ejecución de la Auditoría Informática a la empresa permita cumplir con las Normas de Control Interno del grupo 410 referente a Tecnologías de Información?

Tabla 8: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y demás empleados pregunta N° 06.

Siempre (1)	24	44%
Casi siempre (2)	10	18%
Esporádicamente (3)	6	11%
Casi nunca (4)	8	15%
Nunca (5)	7	13%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 8: Representación de la tabulación. Pregunta N° 06.



Interpretación:

Mediante la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 44% cree que mediante la Auditoría Informática a la empresa permitirá cumplir con las Normas de Control Interno del grupo 410 referente a Tecnologías de Información, el 18% casi siempre, el 11% indica que esporádicamente, el 15% casi nunca y el 13 % indica que no permitirá.

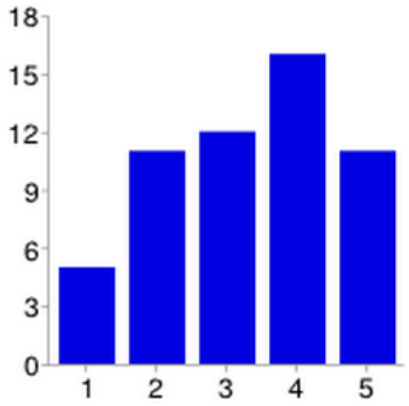
7. ¿Se realiza cambios periódicos de sus claves de acceso a los sistemas de información?

Tabla 9: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y demás empleados pregunta **N° 07.**

Siempre (1)	5	9%
Casi siempre (2)	11	20%
Esporádicamente (3)	12	22%
Casi nunca (4)	16	29%
Nunca (5)	11	20%
TOTAL	**55**	100%

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 9: Representación de la tabulación. Pregunta N° 07.



Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 9% considera que siempre se realiza cambios periódicos de las claves de acceso a los sistemas de información, el 20% casi siempre existe, el 22% indica que esporádicamente existe, el 29% casi nunca y el 20% indica que nunca existe un cambio periódico en las claves de acceso.

8. ¿Considera usted que es importante cambiar periódicamente las claves de acceso a la información por motivos de seguridad?

Tabla 10: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y demás empleados pregunta N° 08.

SI	53	96%
NO	2	4%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 10: Representación de la tabulación. Pregunta N° 08.

Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 96% considera que es importante cambiar esporádicamente las claves de acceso a la información por motivos de seguridad, mientras que el 4% considera lo contrario.

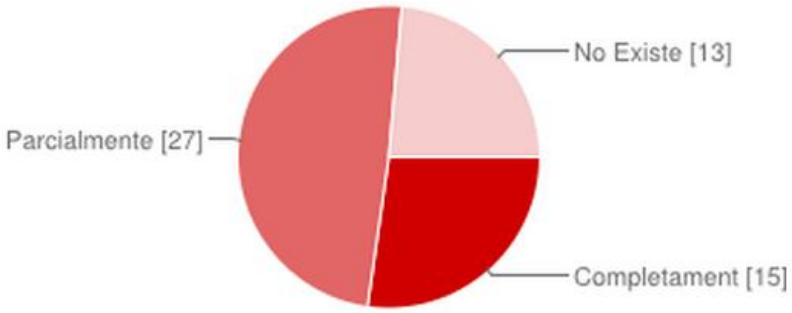
9. ¿Existen las medidas de seguridad que permita salvaguardar y evitar pérdidas de los equipos informáticos dentro de la empresa?

Tabla 11: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y otros. Pregunta N° 09.

Completamente	15	27%
Parcialmente	27	49%
No Existe	13	24%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 11: Representación de la tabulación. Pregunta N° 09.



Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 27% considera completamente que existen las medidas de seguridad que permita salvaguardar y evitar pérdidas de los equipos informáticos dentro de la empresa, el 49% considera parcialmente y el 24% considera que no existen dichas medidas de seguridad.

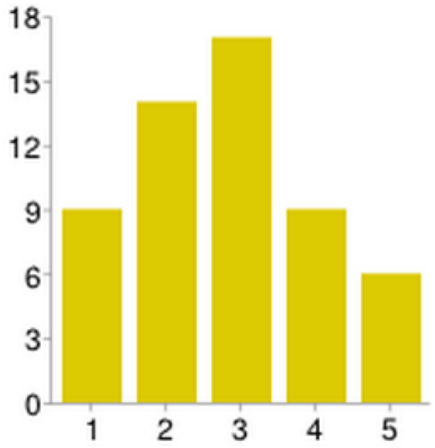
10. ¿El servicio de Internet dentro de la Empresa satisface las necesidades de los usuarios sean estos Gerente, Directores, Jefes departamentales y demás?

Tabla 12: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y otros. Pregunta N° 10.

Siempre (1)	9	16%
Casi siempre (2)	14	25%
Esporádicamente (3)	17	31%
Casi nunca (4)	9	16%
Nunca (5)	6	11%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 12: Representación de la tabulación. Pregunta N° 10.



Interpretación:

Mediante la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 16% consideran que el servicio de internet satisface las necesidades de los usuarios, el 25% casi siempre satisface, el 31% indica que esporádicamente satisface, el 16% casi nunca y el 11% indica que el servicio de internet nunca satisface las necesidades .

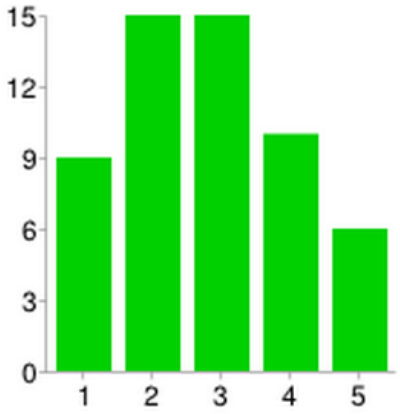
11. ¿Los mantenimientos preventivos que se efectúan en los equipos informáticos son realizados de forma permanente?

Tabla 13: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y otros. Pregunta N° 11.

Siempre (1)	9	16%
Casi siempre (2)	15	27%
Esporádicamente (3)	15	27%
Casi nunca (4)	10	18%
Nunca (5)	6	11%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 13: Representación de la tabulación. Pregunta N° 11.



Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 16% considera que siempre los mantenimientos a los equipos informáticos son realizados de forma permanente, el 27% casi siempre son permanentes, el 18% indica que esporádicamente es permanente, el 18% casi nunca y el 11% indica que nunca existe mantenimientos preventivos a los equipos informáticos.

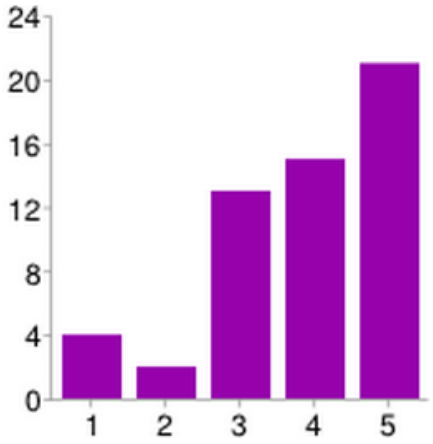
12. ¿Existen capacitaciones informáticas periódicas que sean organizadas por el personal de informática conjuntamente con la Unidad de Talento Humano de la Empresa?

Tabla 14: Tabulación del resultado de las encuestas aplicadas a Gerente, Directores, Jefes y otros. Pregunta N° 12.

Siempre (1)	4	7%
Casi siempre (2)	2	4%
Esporádicamente (3)	13	24%
Casi nunca (4)	15	27%
Nunca (5)	21	38%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 14: Representación de la tabulación. Pregunta N° 12.



Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 7% considera que siempre existen capacitaciones periódicas que sean organizadas por el personal de informática conjuntamente con la unidad de talento humano de la empresa, el 4% casi siempre existe, el 24% indica que esporádicamente existe, el 27% casi nunca y el 38 % indica que nunca existe dichas capacitaciones.

3.6.5. Resultados de las encuestas aplicadas al nivel operativo de la empresa.

OBJETIVO: Conocer aspectos relacionados con las actividades que desarrolla el personal del departamento de informática de la EP-EMAPAR.

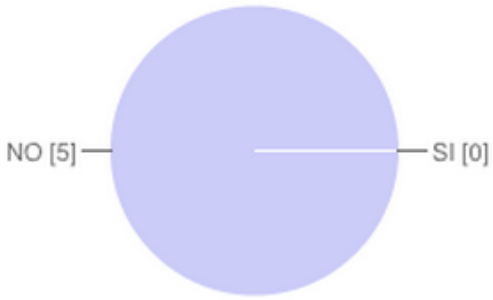
1. ¿En la dirección del departamento de informática existen misión, visión, y objetivos claramente definidos y socializados?

Tabla 15: Tabulación del resultado de las encuestas aplicadas al nivel operativo de tecnologías. Pregunta N° 01.

SI	0	0%
NO	5	100%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 15: Representación de la tabulación. Pregunta N° 01.



Interpretación:

Mediante la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 0% indica que en la dirección del departamento de informática existen misión, visión y objetivos claramente definidos y socializados, mientras que el 100% considera que no existen.

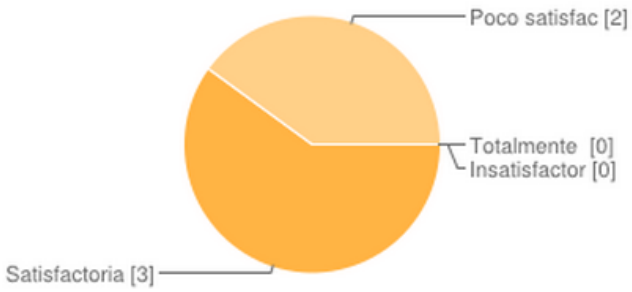
2. ¿El número de computadoras son adecuadas y suficientes de acuerdo al número de empleados?

Tabla 16: Tabulación del resultado de las encuestas aplicadas al nivel operativo de tecnologías. Pregunta N° 02.

Totalmente	0	0%
Satisfactoriamente	3	60%
Poco Satisfactorio	2	40%
Insatisfactorio	0	0%
TOTAL	**55**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 16: Representación de la tabulación. Pregunta N° 02.



Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 0% totalmente considera que el número de computadoras son adecuadas y suficientes de acuerdo al número de empleados, el 60% satisfactoriamente, el 40% poco satisfactorio y el 0% restante considera insatisfactorio.

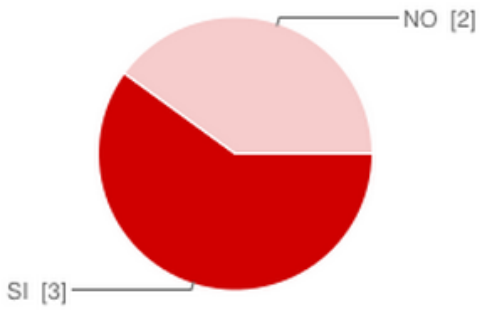
3. ¿Existe personal suficiente con conocimientos y experiencia para realizar las actividades dentro del área de informática?

Tabla 17: Tabulación del resultado de las encuestas aplicadas al nivel operativo de tecnologías. Pregunta N° 03.

SI	3	60%
NO	2	40%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 17: Representación de la tabulación. Pregunta N° 03.



Interpretación:

Según la aplicación de la encuestas a los usuarios del parque informático de la empresa se determina que el 60% indica que existe personal suficiente con conocimientos y experiencia, mientras que el 40% considera que no existen.

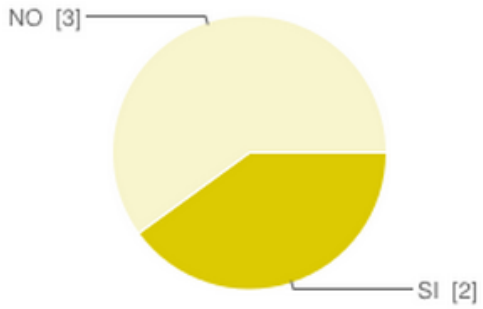
4. ¿Existe manuales de políticas y procedimientos sobre el personal que labora dentro del área?

Tabla 18: Tabulación del resultado de las encuestas aplicadas al nivel operativo de tecnologías. Pregunta N° 4.

SI	2	40%
NO	3	60%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 18: Representación de la tabulación. Pregunta N° 04.



Interpretación:

Mediante la aplicación de la encuestas a la empresa se determina que el 40% indica que existe manuales de políticas y procedimientos sobre el personal que labora dentro del área de informática, mientras que 60% considera que no existen.

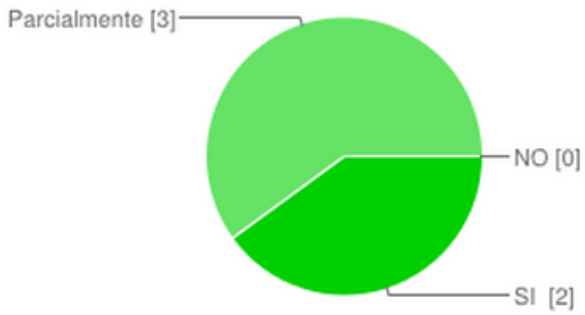
5. ¿Existen seguridades físicas adecuadas dentro del departamento de informática, tales como: extintores, salidas de emergencia, aire acondicionado, entre otras?

Tabla 19: Tabulación del resultado de las encuestas aplicadas al nivel operativo de tecnologías. Pregunta N° 5.

SI	2	40%
PARCIALMENTE	3	60%
NO	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 19: Representación de la tabulación. Pregunta N° 05.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 40% indica que existe seguridades físicas adecuadas dentro del departamento de informática, el 60% considera que parcialmente existen y el 0% restante considera que no existe.

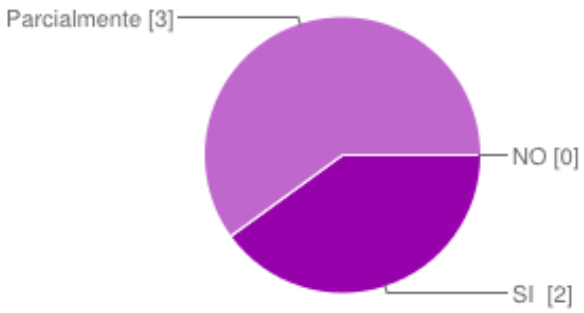
6. ¿Conoce el lugar que ocupa en el organigrama el área de sistemas informáticos?

Tabla 20: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 06.

SI	2	40%
PARCIALMENTE	3	60%
NO	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 20: Representación de la tabulación. Pregunta N° 06.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 40% indica que conoce el lugar que ocupa en el organigrama el área de sistemas informáticos, el 60% considera que parcialmente conocen y el 0% restante considera que no conocen.

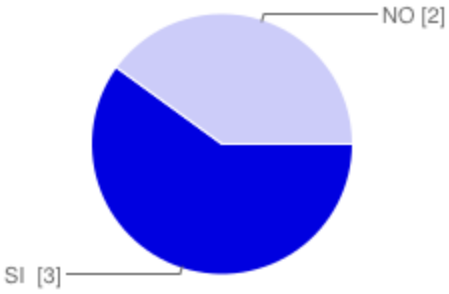
7. ¿Cree que dicha estructura orgánica es adecuada para satisfacer la prestación de soporte y ayuda hacia los demás departamentos?

Tabla 21: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 07.

SI	3	60%
NO	2	40%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 21: Representación de la tabulación. Pregunta N° 07.



Interpretación:

Mediante la aplicación de la encuestas a la empresa se determina que el 60% cree que dicha estructura orgánica es adecuada para satisfacer la prestación de soporte y ayuda hacia los demás departamentos, el 40% considera que no satisface la prestación de soporte.

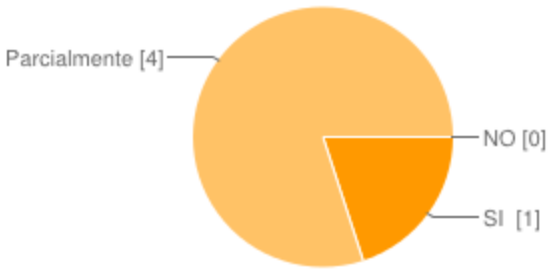
8. ¿El servicio de Internet satisface las necesidades de los usuarios del parque Informático en base a las actividades de la Empresa?

Tabla 22: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 08.

SI	1	20%
PARCIALMENTE	4	80%
NO	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 22: Representación de la tabulación. Pregunta N° 08.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 20% indica que el servicio de internet si satisface las necesidades de los usuarios del parque informático en base a las actividades de la empresa, el 80% considera que parcialmente satisface estas necesidades y el 0% restante considera que no satisface.

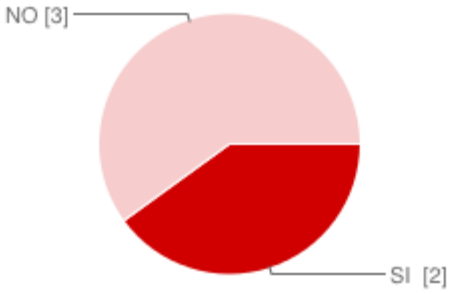
9. ¿Existen planes de contingencia ante desastres dentro del Departamento Informático?

Tabla 23: Tabulación del resultado de las encuestas aplicadas al nivel operativo de tecnología. Pregunta N° 09.

SI	2	40%
NO	3	60%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 23: Representación de la tabulación. Pregunta N° 09.



Interpretación:

Mediante la aplicación de la encuestas a la empresa se determina que el 40% indica que existen planes de contingencia ante desastres dentro del departamento informático, el 60% considera que no existe este plan de contingencias.

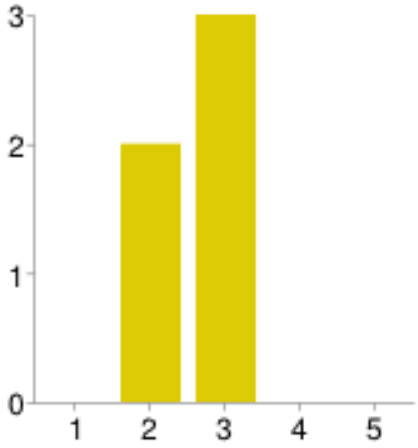
10. ¿Los recursos económicos asignados por las Autoridades de la Empresa satisfacen las necesidades del área de Tecnología?

Tabla 24: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 10.

Siempre (1)	0	0%
Casi siempre (2)	2	40%
Esporádicamente (3)	3	60%
Casi nunca (4)	0	0%
Nunca (5)	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 24: Representación de la tabulación. Pregunta N° 10.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 0% indica que los recursos financieros asignados no satisface las necesidades del área de tecnología, el 40% considera que casi siempre satisface, el 60% indica que esporádicamente satisface, el 0% menciona que casi nunca satisface y el 0% restante considera que no satisface estas necesidades.

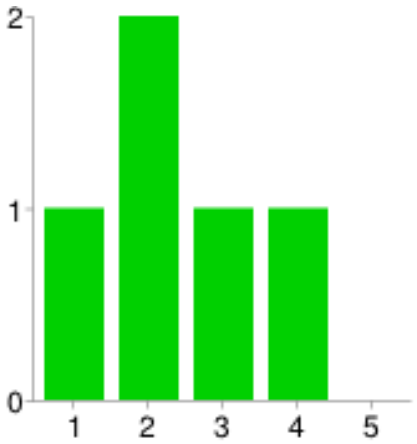
11. ¿Existe planes y programas de capacitación, adiestramiento y promoción para los empleados de la empresa por parte del área de Sistemas Informáticos?

Tabla 25: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 11.

Siempre (1)	1	20%
Casi siempre (2)	1	40%
Esporádicamente (3)	1	20%
Casi nunca (4)	1	20%
Nunca (5)	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 25: Representación de la tabulación. Pregunta N° 11.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 20% indica que existen planes y programas de adestramiento y promoción para los empleados de la empresa por parte del área de informática, el 40% considera que casi siempre existe, el 20% indica que esporádicamente existe, el 20% menciona que casi nunca existe y el 0% restante considera que no existe.

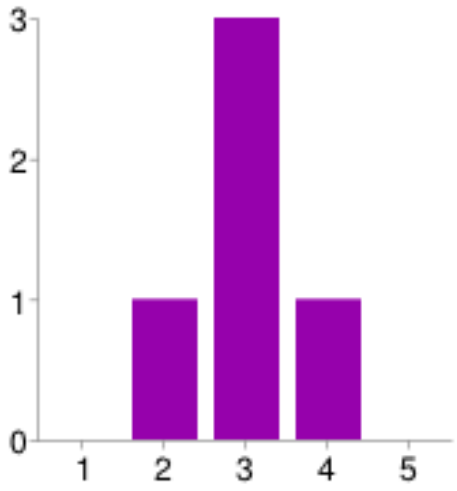
12. ¿Se realiza un cronograma de mantenimiento al parque informático de la empresa?

Tabla 26: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 12.

Siempre (1)	0	0%
Casi siempre (2)	1	20%
Esporádicamente (3)	3	60%
Casi nunca (4)	1	20%
Nunca (5)	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 26: Representación de la tabulación. Pregunta N° 12.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 0% indica que se realiza un cronograma de mantenimiento al parque informático de la empresa, el 20% considera que casi siempre se realiza, el 60% indica que esporádicamente se realiza, el 20% menciona que casi nunca se realiza y el 0% restante considera que nunca se realiza.

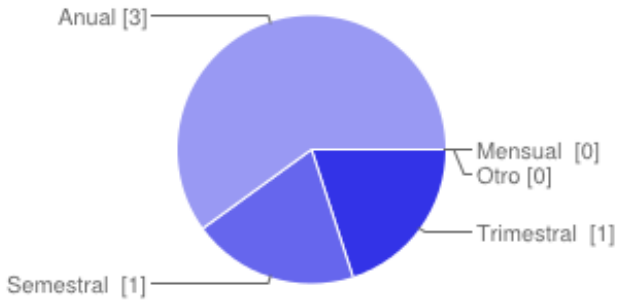
13. Si la respuesta anterior es positiva. ¿Cada qué período de tiempo se realiza el mantenimiento del parque informático?

Tabla 27: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 13.

Mensual	0	0%
Trimestral	1	20%
Semestral	1	20%
Anual	3	60%
Otro	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 27: Representación de la tabulación. Pregunta N° 13.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 0% indica que el periodo de tiempo en el mantenimiento de los equipos se realiza de manera mensual, el 20% considera que se realiza de manera trimestral, el 20% indica que se realiza de manera semestral, el 60% menciona que se realiza de manera anual.

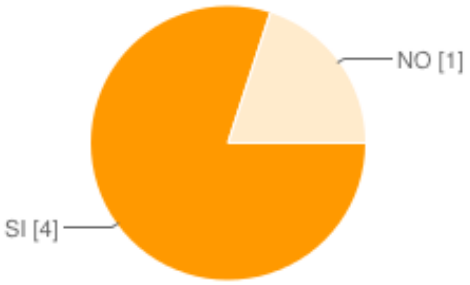
14. ¿Los recursos materiales que se le proporcionan al área, son suficientes para cumplir con las funciones encomendadas?

Tabla 28: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 14.

SI	4	80%
NO	1	20%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 28: Representación de la tabulación. Pregunta N° 14.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 80% indica que los recursos y materiales que se le proporcionan al área de informática, si son suficientes para cumplir con las funciones encomendadas mientras que el 20% restante considera que no son suficientes.

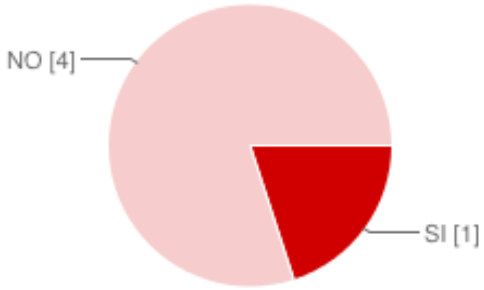
15. ¿Existe prohibiciones para fumar, tomar alimentos y refrescos en el Departamento de Informática?

Tabla 29: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 15.

SI	1	20%
NO	4	80%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 29: Representación de la tabulación. Pregunta N° 15.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 20% indica que existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de informática, mientras que el 80% restante considera que no existen esas prohibiciones.

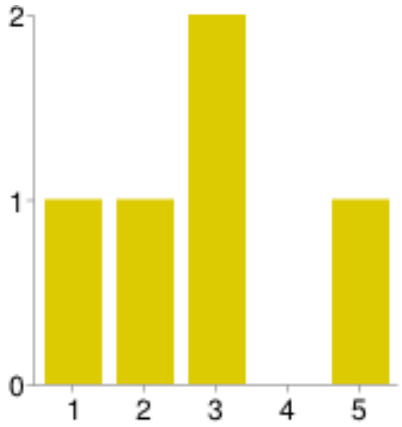
16. ¿Los usuarios tienen el debido cuidado en los recursos informáticos al momento de utilizarlos?

Tabla 30: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 16.

Siempre (1)	1	20%
Casi siempre (2)	1	20%
Esporádicamente (3)	2	40%
Casi nunca (4)	0	0%
Nunca (5)	1	20%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 30: Representación de la tabulación. Pregunta N° 16.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 20% indica que siempre los usuarios tienen el debido cuidado en los recursos informáticos al momento de utilizarlos, el 20% casi siempre tiene el debido cuidado, el 40% esporádicamente tiene el debido cuidado, el 0% casi nunca tiene cuidado y el 20% nunca tiene cuidado.

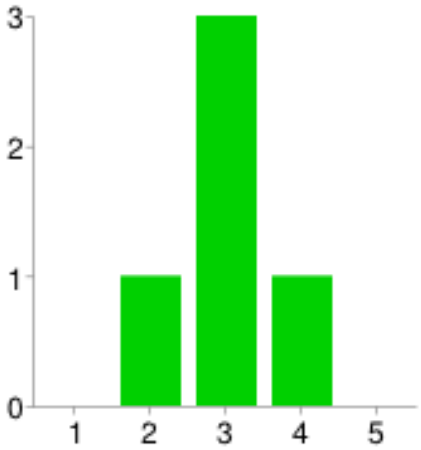
17. ¿Considera Ud. que existe las medidas de seguridad adecuadas para evitar la pérdida o sustracción de los recursos informáticos?

Tabla 31: Tabulación del resultado de las encuestas aplicadas al nivel operativo. Pregunta N° 17.

Siempre (1)	0	0%
Casi siempre (2)	1	20%
Esporádicamente (3)	3	60%
Casi nunca (4)	1	20%
Nunca (5)	0	0%
TOTAL	**5**	**100%**

FUENTE: Investigación
ELABORADO POR: El Autor

Ilustración 31: Representación de la tabulación. Pregunta N° 17.



Interpretación:

Según la aplicación de la encuestas a la empresa se determina que el 0% indica que existe las medidas de seguridad para evitar la pérdida o sustracción de los recursos informáticos, el 20% casi siempre existe las medidas de seguridad, el 60% esporádicamente, el 20% casi nunca y el 0% nunca o no existe estas medidas de seguridad.

3.6.6. Matriz FODA

Tabla 32: Matriz FODA

FORTALEZAS	OPORTUNIDADES
✓ La información interna está protegida contra posibles sabotajes. ✓ Claves de acceso asignado por personal con conocimientos en el área. ✓ El número de computadoras son adecuadas satisfactoriamente y suficientes de acuerdo al número de empleados. ✓ Existen planes y programas de capacitación adiestramiento y promoción para los empleados de la empresa por parte del área de informática. ✓ Los recursos materiales que se le proporcional al área, son suficientes para cumplir con las funciones encomendadas.	✓ Existe personal suficiente con conocimientos y experiencia para realizar las actividades dentro del área de informática. ✓ La estructura orgánica es adecuada para satisfacer la prestación de soporte y ayuda hacia los demás departamentos. ✓ Disponibilidad de software libre acorde a las necesidades.
DEBILIDADES	**AMENAZAS**
✓ Servicio de Internet poco satisfactorio. ✓ No existe un software adecuado para cada una de las áreas. ✓ Falta de medidas de seguridad para evitar pérdidas de los recursos informáticos ✓ En la dirección de informática no existe misión, visión y objetivos claramente definidos y socializados. ✓ No existen manuales de políticas y procedimientos sobre el personal que labora dentro del área.	✓ Cambio de políticas de Estado en materia de Normas de Control Interno. ✓ Criminalidad (robo, hurto, fraude, espionaje, virus) ✓ Desastres naturales.

✓ Existen seguridades físicas parciamente adecuadas dentro del departamento de informática, tales como: extintores, salidas de emergencia, aire acondicionado, entre otras. ✓ Falta de conocimiento del lugar que ocupa el área de sistemas informáticos dentro del organigrama de la empresa. ✓ El servicio de internet satisface parcialmente las necesidades de los usuarios del parque informático de la empresa. ✓ No existen planes de contingencia dentro del departamento de informática. ✓ Los recursos económicos asignados por las Autoridades de la empresa satisfacen esporádicamente las necesidades del área de informática. ✓ Se realiza mantenimientos de forma anual. ✓ No existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de informática ✓ Esporádicamente los usuarios tienen el debido cuidado en los recursos informáticos al momento de utilizarlos ✓ Existen parcialmente medidas de seguridad para evitar la pérdida o sustracción de los recursos informáticos.	

FUENTE: Investigación
ELABORADO POR: El Autor

3.6.7. Matriz de Medios Internos

Se entiende por medio interno a todas las relaciones y actividades que se harán al interior de la organización lo cual se realiza mediante un análisis exhaustivo en el desarrollo de sus funciones en términos de gestión administrativos, etc.

El análisis de los medios internos conocido también como diagnóstico, permite interpretar la situación de la institución, establecer la relación causa y efecto y concluir en una síntesis de puntos sólidos y problemas.

En suma el análisis del medio interno constituye una evaluación de la organización cuyo objetivo es identificar fortalezas (logros) y debilidades (problemas). Se empieza indagando como están actualmente los elementos más importantes de la organización, como son la visión, misión y los grandes objetivos y políticas institucionales.

Fortalezas: Para una institución tener fortalezas es sentirse fuerte, haber conseguido una buena posición, haber alcanzado un grado de solidez, poseer energía, firmeza y constancia en determinado campo, área o aspecto del quehacer institucional.

Debilidades: Son manifestaciones que denotan un problema, desventaja, dificultad o insatisfacción de necesidades.

DEPARTAMENTO DE INFORMÁTICA DE LA EMPRESA PÚBLICA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EP-EMAPAR

Tabla 33: Perfil Estratégico Interno

	CLASIFICACIÓN DEL IMPACTO				
	DEBILIDAD		Equilibrio	FORTALEZA	
ASPECTOS INTERNOS	Debilidad Grave	Debilidad Menor		Fortaleza Menor	Fortaleza Importante
La información interna está protegida contra posibles sabotajes.					
Claves de acceso asignado por personal de informática con conocimientos adecuados.					
El número de computadoras son adecuadas satisfactoriamente y suficientes de acuerdo al número de empleados.					
Existen planes y programas de capacitación adiestramiento y promoción para los empleados de la empresa por parte del área de informática.					
Los recursos materiales que se le proporcionan al área, son suficientes para cumplir con las funciones encomendadas.					
Servicio de Internet poco satisfactorio.					
No existe un software adecuado para cada una de las áreas.					
Falta de medidas de seguridad para evitar pérdidas de los recursos informáticos					
En la dirección de informática no existe misión, visión y objetivos claramente definidos y socializados.					
No existen manuales de políticas y procedimientos claramente definidos.					
Existen seguridades físicas parciamente adecuadas dentro del departamento de informática, tales como: extintores, salidas de emergencia, aire acondicionado, entre otras.					

Falta de conocimiento del lugar que ocupa el área de sistemas informáticos dentro del organigrama de la empresa.					
No existen planes de contingencia dentro del departamento de informática.					
Los recursos económicos asignados por las Autoridades de la empresa satisfacen esporádicamente las necesidades del área de informática.					
Se realiza mantenimientos de forma anual.					
No existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de informática					
Esporádicamente los usuarios tienen cuidado en los recursos informáticos al momento de utilizarlos					

FUENTE: Investigación
ELABORADO POR: El Autor

Para la evaluación del desenvolvimiento de la organización la ponderación será la siguiente: Cada factor tendrá una ponderación, la misma que fluctuará de 0 hasta 1 por lo que la suma será igual a 1.

La clasificación que se usará en los parámetros será:

1. = debilidad grave o muy importante
2. = debilidad menor
3. = equilibrio
4. = fortaleza menor
5. = fortaleza importante

El resultado ponderado se obtiene entre la ponderación y el parámetro asignado. Se suma el resultado ponderado de cada uno de los factores.

Para resultados internos la calificación puede ser 5 máximo que implica que el Departamento de Sistemas está estable y 1 mínimo que indica que tiene problemas. Cuando el resultado es inferior al promedio se tienen más debilidades que fortalezas, y si el resultado es mayor al promedio se poseen las fortalezas que debilidades.

DEPARTAMENTO DE INFORMÁTICA EP-EMAPAR

Tabla 34: Ponderación Perfil Estratégico Interno.

ASPECTOS INTERNOS CLAVES	PONDERACIÓN	CALIFICACIÓN	RESULTADO PONDERADO
La información interna está protegida contra posibles sabotajes.	**0,059**	**4**	**0,236**
Claves de acceso asignado por personal con conocimientos en el área.	**0,059**	**5**	**0,295**
El número de computadoras son adecuadas satisfactoriamente y suficientes de acuerdo al número de empleados.	**0,059**	**4**	**0,236**
Existen planes y programas de capacitación adiestramiento y promoción para los empleados de la empresa por parte del área de informática.	**0,059**	**4**	**0,236**
Los recursos materiales que se le proporcional al área, son suficientes para cumplir con las funciones encomendadas.	**0,059**	**4**	**0,236**
Servicio de Internet poco satisfactorio.	**0,059**	**2**	**0,118**
No existe un software adecuado para cada una de las áreas.	**0,059**	**1**	**0,059**
Falta de medidas de seguridad para evitar pérdidas de los recursos informáticos	**0,059**	**1**	**0,059**
En la dirección de informática no existe misión, visión y objetivos claramente definidos y socializados.	**0,059**	**1**	**0,059**
No existen manuales de políticas y procedimientos claramente definidos.	**0,059**	**1**	**0,059**
Existen seguridades físicas parciamente adecuadas dentro del departamento de	**0,059**	**2**	**0,118**

informática, tales como: extintores, salidas de emergencia, aire acondicionado, entre otras.			
Falta de conocimiento del lugar que ocupa el área de sistemas informáticos dentro del organigrama de la empresa.	**0,059**	**2**	**0,118**
No existen planes de contingencia dentro del departamento de informática.	**0,059**	**1**	**0,059**
Los recursos económicos asignados por las Autoridades de la empresa satisfacen esporádicamente las necesidades del área de informática.	**0,059**	**2**	**0,118**
Se realiza mantenimientos de forma anual.	**0,059**	**1**	**0,059**
No existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de informática	**0,059**	**3**	**0,177**
Esporádicamente los usuarios tienen el debido cuidado en los recursos informáticos al momento de utilizarlos.	**0,059**	**2**	**0,118**
TOTALES	**1**	**40**	**2,36**

FUENTE: Investigación
ELABORADO POR: El Autor

ANÁLISIS:

Como resultado del análisis se obtiene **2,36** lo cual nos indica que el Departamento de Informática tiene más debilidades que fortalezas:

- ✓ Dentro de los aspectos favorables se destaca la información interna está protegida contra posibles sabotajes;
- ✓ Claves de acceso asignado por personal con conocimientos en el área;
- ✓ El número de computadoras son adecuadas satisfactoriamente y suficientes de acuerdo al número de empleados;
- ✓ Existen planes y programas de capacitación adiestramiento y promoción para los empleados de la empresa por parte del área de informática;
- ✓ Los recursos materiales que se le proporciona al área, son suficientes para cumplir con las funciones encomendadas.

Dentro de las debilidades detectadas a través de las encuestas y por ende se debe reformar determinados aspectos como:

- ✓ Mejorar el sistema de internet en toda Empresa, especialmente en áreas donde es importante el uso de internet y por tanto el servicio es poco satisfactorio,
- ✓ No existe un software adecuado para cada una de las áreas,
- ✓ Falta de medidas de seguridad para evitar pérdidas de los recursos informáticos,
- ✓ en la dirección de informática no existe misión, visión y objetivos claramente definidos y socializados por ende no existen también manuales de políticas y procedimientos claramente definidos por lo que el personal del área no conoce exactamente de sus actividades.
- ✓ Inexistencia de seguridades físicas adecuadas dentro del departamento de informática, tales como: extintores, salidas de emergencia, aire acondicionado, entre otras.
- ✓ Conocimiento insuficiente del lugar que ocupa el área de sistemas informáticos dentro del organigrama de la empresa.
- ✓ Ausencia de planes de contingencia dentro del departamento de informática, los recursos económicos asignados por las autoridades de la empresa satisfacen esporádicamente las necesidades del área de informática.
- ✓ Se realiza mantenimientos de forma anual cuando lo recomendable debería ser de manera trimestral hasta semestral y así evitar riesgos ambientales,
- ✓ No existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de informática, los usuarios no tienen el debido cuidado en los recursos informáticos al momento de utilizarlos.

3.6.8. Matriz de Medios Externos

El medio externo es todo lo que ocurre en el entorno de la organización y que influye directa o indirectamente en el cumplimiento de su misión. El medio externo no es estático y los cambios son cada vez más rápidos, continuos que precisan ser conocidos e interpretados adecuada y permanentemente.

El ambiente externo está conformado por la combinación de varios fenómenos o elementos: fuerzas, actores, eventos y hechos, que afectan en forma directa o indirecta a la institución. Cuando cualquiera de estos elementos afecta directamente de forma positiva o negativa, el desempeño general de algunas actividades de la empresa, nos encontramos frente a un "factor crítico externo" que deberá ser considerado en la estructuración de los escenarios, objetivos, políticas y alternativas de cambio de consolidación.

Oportunidades: Son cualquier elemento o circunstancia del ambiente externo que a pesar de no estar bajo el control directo de la institución, puede constituirse alguna contribución para alguna de sus actividades importantes. Las oportunidades deben ser conocidas para ser aprovechadas estratégicamente.

Amenazas: Son cualquier elemento relevante del ambiente externo que puede constituirse en una desventaja-riesgo-peligro para el desempeño de alguna de las actividades más importantes de una institución o programa.

DEPARTAMENTO DE INFORMÁTICA DE LA EP-EMAPAR

PERFIL ESTRATÉGICO EXTERNO

Tabla 35: Perfil Estratégico Externo

ASPECTOS EXTERNOS	CLASIFICACIÓN DEL IMPACTO				
	Gran Amenaza	Amenaza	Equilibrio	Oportunidad	Gran Oportunidad
Existe personal suficiente con conocimientos y experiencia					
La estructura orgánica es adecuada.					
Nuevas alternativas de software acorde a las necesidades.					
Cambio de políticas de Estado en materia de Normas de Control Interno.					
Criminalidad (robo, hurto, fraude, espionaje, virus)					
Desastres naturales.					

FUENTE: Investigación
ELABORADO POR: El Autor

PERFIL ESTRATÉGICO EXTERNO

Tabla 36: Ponderación Perfil Estratégico Externo.

ASPECTOS INTERNOS CLAVES	PONDERACIÓN	CALIFICACIÓN	RESULTADO PONDERADO
Existe personal suficiente con conocimientos y experiencia	0,167	5	0,835
La estructura orgánica es adecuada.	0,167	4	0,668
Nuevas alternativas de software acorde a las necesidades.	0,167	4	0,668
Cambio de políticas de Estado en materia de Normas de Control Interno.	0,167	2	0,334
Criminalidad (robo, hurto, fraude, espionaje, virus)	0,167	1	0,167
Desastres naturales.	0,167	1	0,167
TOTALES	**1**	**17**	**2,84**

FUENTE: Investigación
ELABORADO POR: El Autor

ANÁLISIS:

Como resultado del análisis se obtiene **2,84** lo cual indica que el departamento de informática de la empresa en lo referente a Tecnologías de Información y Comunicación tienen más oportunidades que amenazas lo cual podría beneficiarse disponiendo de software de acuerdo a los diferentes departamentos, de manera que pueda contribuir a mejorar la calidad de las actividades de la empresa, debido a cambios en las políticas de Estado en materia de Normas de Control Interno por lo que hasta se pueda cambiar de manera relativa el parque informático. Dentro de lo que corresponde a la criminalidad se puede mejorar la seguridad tanto física como lógica (robo, hurto, sabotaje, fraude, espionaje, virus), en lo que se refiere a desastres naturales se puede tomar medidas necesarias para evitar la pérdida de recursos informáticos en cantidad.

CAPÍTULO IV

4. ANÁLISIS DE RESULTADOS

4.1. Procedimiento de Implementación

"Auditoria Informática a la Empresa Pública - Municipal de Agua Potable y Alcantarillado de Riobamba, periodo 2012".

4.1.1. Generalidades

4.1.1.1. Alcance

La Auditoria informática aplicada a la Empresa Pública - Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, con énfasis al Departamento de Informática, comprende el estudio y análisis sobre la Seguridad Física, Seguridad Lógica, Tecnologías de Información y Comunicación Tics y Gestión de la Informática.

4.1.1.2. Objetivo

El Objetivo General de realizar una Auditoria Informática a la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, es evaluar las seguridades tanto lógica como física, utilización y aprovechamiento adecuado de las Tics, y Gestión Informática

4.1.1.3. Base Legal

Para el desarrollo del presente proyecto de tesis tomamos como referencia las Normas de Control Interno del grupo 410, referente a Tecnologías de Información y Comunicación emitidas por la Contraloría General del Estado.

4.1.1.4. Hoja de Marcas

✓	=	**Verificación mediante inspección física**
@	=	**Analizado**
↹	=	**Comprado**
Θ	=	**Determinación del Hallazgo**
©	=	**Cotejado con Inventarios**
ϡ	=	**Incluir en Informe**
☆	=	**Cotejado con documentos**

4.1.1.5. Abreviaturas

AF	=	**Análisis FODA**
PA	=	**Programa de Auditoria**
ESL	=	**Encuesta de Seguridad Lógica**
ESF	=	**Encuesta de Seguridad Física**
ETIC	=	**Encuesta de Tecnologías de Información y Comunicación**
EGI	=	**Encuesta de Gestión Informática**
EPAS	=	**Encuesta personal Administrativo Secretarias**
FP	=	**Fase Preliminar**
FE	=	**Fase de Ejecución**
HA	=	**Hoja de Hallazgos**
FCR	=	**Fase de Comunicación de Resultados**
EP-EMAPAR	=	**Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba**
CGE	=	**Contraloría General del Estado**

FP

ETAPAS DE LA AUDITORIA INFORMÁTICA

PRIMERA ETAPA: PLANEACIÓN

PROGRAMA DE AUDITORIA

Entidad: Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba.
Área: Departamento de Informática de la EP- EMAPAR
Tipo de Auditoria: Auditoria Informática.
Fase: Planeación.
Objetivo: Conocer las actividades que desarrollan el personal operativo del Departamento de Informática para iniciar con el desarrollo de la Auditoria Informática.

N°	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA.
PROCEDIMIENTOS				
1	Realice una carta de compromiso indicando que se iniciará con el desarrollo de la auditoría, a fin de que se brinde las facilidades necesarias para el desarrollo de la misma.	FP1	WRPV	24/01/2014
2	Realice una entrevista al jefe del departamento de Informática, para obtener información general de esta área.	FP2	WRPV	27/01/2014
3	Solicite el organigrama de la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba.	FP3	WRPV	28/01/2014
4	Solicite el manual de funciones del personal del área.	FP4	WRPV	29/01/2014
5	Solicite el Manual de políticas y procedimientos del área.	FP5	WRPV	29/01/2014

Elaborado por:	Fecha:
WRPV	22/01/2014
Aprobado por:	Fecha:
RC	23/01/2014

Riobamba, 24 de enero del 2014

FP1

Ingeniero

Víctor Méndez

GERENTE DE LA EP-EMAPAR

Presente,

De nuestra consideración:

El trabajo se realizó por la razón que en la Empresa Pública-Empresa Municipal de Agua Potable y Alcantarillado de Riobamba no se ha realizado Auditoria Informática. Considerando esta situación desarrollamos nuestro proyecto de tesis en la Empresa con énfasis y mayor estudio al Departamento de Informática de manera que el beneficio sea para las dos partes involucradas.

El Señor Peralta Villacrés Washington Rolando, realizará la Auditoria Informática de acuerdo a las normas de control interno emitidas por la Contraloría General del Estado grupo 410 en lo referente a tecnologías de información y comunicación, con el fin de obtener una opinión acerca de aspectos relacionados con la seguridad lógica, seguridad física, aprovechamiento y utilización de las Tics y gestión de la informática, el mismo que se llevará a cabo a través de la aplicación de encuestas, entrevistas, inspecciones físicas, pruebas técnicas y de campo, revisión de documentos y análisis de los mismos con el fin de obtener evidencia que sustente nuestra opinión.

Al mismo tiempo de la manera más comedida solicitamos la completa colaboración y facilidades por parte del personal que labora en la Empresa en especial al personal operativo del Departamento de Informática, para acceder a la respectiva documentación, para evaluar los parámetros establecidos y el cumplimiento de los objetivos y la optimización y buen uso de los recursos, por el periodo determinado.

Hago propicia la oportunidad para reiterarle mi agradecimiento.

Atentamente,

Rolando Peralta

AUDITOR

ENTREVISTA: Jefe del Departamento de Informática de la EP-EMAPAR

FP2 1/2

FECHA: 27 de enero de 2014

1. **¿Cuál es la fecha de creación del Departamento de Informática de la Empresa?**

   El departamento de informática existía al inicio como unidad de la empresa, era la parte de apoyo para la gerencia desde el momento mismo de creación de la empresa, cuando se separó del municipio dejó de ser una dirección del municipio y paso a ser una empresa privada en el año 2007, a posterior hubo una reforma en el año 2010 el cual pasó a ser empresa pública de agua potable el cual se organizó el orgánico funcional y estructural, paso a ser parte de una unidad dependiente de la dirección de ingeniería en el 2010.

2. **¿Con que finalidad se creó el Departamento de Informática de la Empresa?**

   En primera instancia en el 2007 fué como una unidad de apoyo a las demás áreas para solucionar problemas especialmente sobre "HELP DESK" o "MESA DE AYUDA" ayuda al usuario final en problemas y conflictos con equipos, software del usuario final para el uso, con esto de la reforma del orgánico se transformó la unidad de informática también en SIG y Catastros maneja también la parte de la ubicación geográfica y también la parte del catastro. En cierta forma se le considera a la unidad de informática como el custodio de información y se ha presentado también la idea de ir desarrollando. Se adquirió un software en el año 2008 donde nos transfirieron el código fuente donde comenzamos hacer el desarrollo de algún tipo de sistema, modificaciones del mismo sistema o aumentos de módulos, y obviamente también a telemática se posee algunos radioenlaces igual que la red informática.

3. **¿Quiénes son los responsables y que funciones y actividades cumple el personal operativo de esta área?**

   El personal que integra el departamento de Informática de la EP-EMAPAR son:

FP2 2/2

Tabla 37: Cuadro del personal que integra el departamento de Informática

NOMBRE	CARGO
Ing. Andrés Yépez	Jefe de Informática
Ing. Henry Villa	Técnico informático
Ing. Fabricio Carbajal	Técnico informático
Ing. Walter Parra	Técnico informático
Ing. Hugo Trujillo	Técnico informático
Sr. Ángel Guadalupe	Conserje

Fuente: Investigación
Elaborado por: El Autor

Entre las funciones de los técnicos informáticos tenemos:

- Instalación de equipos nuevos con todos los parámetros establecidos.
- Proporcionar soporte técnico, asesoría y capacitación al usuario del sistema informático LOTUS, paquetes de ofimática, y otros.
- Analizar, diseñar, implementar redes informáticas que permita compartir la información en forma segura y eficiente.
- Analizar, desarrollar, implementar sistemas informáticos que proporcionen información confiable y oportuna para la toma de decisiones.
- Dar mantenimiento preventivo y correctivo a los equipos.

Entre las funciones que realizan el personal de limpieza están:

- Realizar la limpieza y aseo de las oficinas, talleres, patios etc.
- Abrir y cerrar oportunamente las seguridades de la oficina.
- Efectuar el aseo, cuidado, mantenimiento y traslado de muebles, enseres, máquinas, equipos y materiales de oficina.

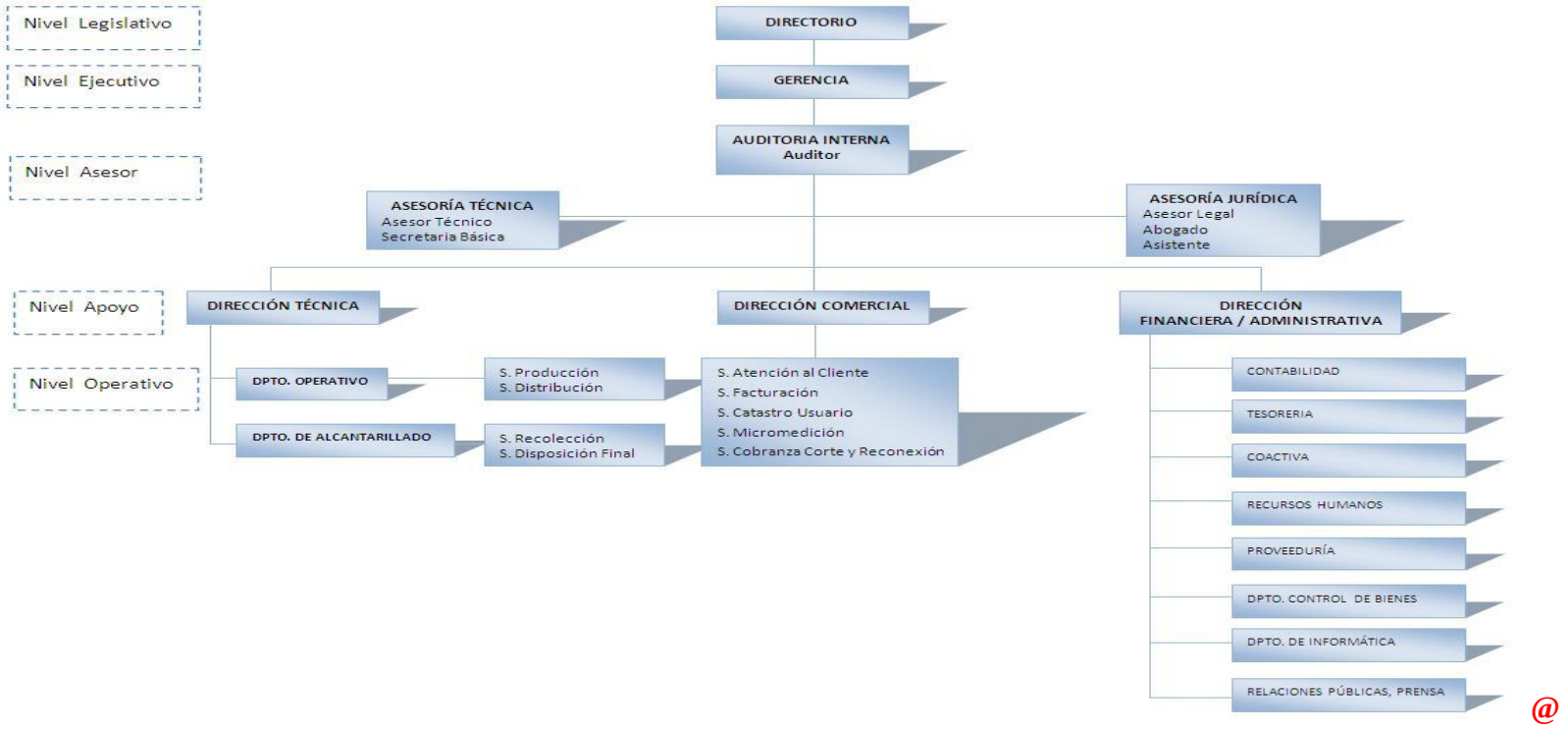
4. **¿Cuál es el horario de atención del departamento de Informática?**

   El horario de atención del departamento de informática a los usuarios finales es de 7:30 am hasta las 4:00 pm

FP3

Organigrama de la EP-EMAPAR

Ilustración 32: Organigrama de la EP-EMAPAR.



@

Fuente: EP-EMAPAR Departamento de Fortalecimiento**.**

Elaborado por:	Fecha:
WRPV	28/01/2014
Aprobado por:	Fecha:
RC	29/01/2014

MANUAL DE FUNCIONES DEL PERSONAL DE INFORMÁTICA. **FP4**

DEL JEFE DE INFORMÁTICA

a) Dirigir la implementación de proyectos informáticos en la EP-EMAPAR.
b) Coordinar la presentación de proyectos de innovación tecnológica para la Institución
c) Liderar la administración que permita mantener la operatividad y seguridad de los sistemas informáticos de la institución.
d) Formular y supervisar el cumplimiento de las normas de seguridad en los procesos informáticos correspondientes.
e) Brindar asistencia especializada en tecnología a todos los niveles y dependencias institucionales.
f) Generar políticas de administración de las cuentas y perfiles de usuarios de la red central institucional.
g) Autorizar la movilización interna o externa (con otras dependencias de la empresa) de los equipos de la EP-EMAPAR; e informar al Director Financiero, para el registro de la unidad encargada de Activos Fijos.
h) Autorizar la movilización fuera de predios de la empresa de los equipos de la institución solo cuando se trate de realizar reparaciones, que no se puedan realizar en el Departamento de Informática, SIG y Catastros, o en casos de suma exclusividad. *(VER ANEXO 3)*

DE LOS TÉCNICOS INFORMÁTICOS

No existen políticas específicas establecidas **Θ**

DEL ENCARGADO DE CATASTROS

No existen políticas establecidas **Θ**

Elaborado por:	Fecha:
WRPV	29/01/2014
Aprobado por:	Fecha:
RC	30/01/2014

FP5

MANUAL DE PROCEDIMIENTOS INFORMÁTICOS PARA EL USO DEL PARQUE TECNOLÓGICO E INTERNET.

Entre los aspectos relevantes del departamento de informática podemos mencionar la distribución de equipos y racionalización de productos, de las redes que abarca la incorporación de Backbone Central los servidores existentes en otras dependencias de la empresa, proporcionar a los usuarios de las redes locales los servicios de Internet, Correo Electrónico.

De la obligación del personal en todos los niveles a utilizar sus cuentas de correo electrónico institucional para realizar la comunicación interna, y/o el sistema documental oficial que se encuentra en la empresa.

Se prohíbe a los funcionarios, empleados, obreros; responsables de los recursos informáticos de la EP-EMAPAR:

Instalar o usar productos de aplicación sin licencia de uso certificada (documento original) para la EP-EMAPAR.

Permitir el uso de los equipos a personas extrañas a la EP-EMAPAR.

Utilizar los equipos en actividades no relacionadas con las inherentes a la EP-EMAPAR.

Reproducir, duplicar, copiar o utilizar sistemas de propiedad EP-EMAPAR o productos de aplicación instalados en los servidores y estaciones de trabajo de las dependencias de la empresa.

Movilizar fuera del departamento, unidad o de la institución los equipos y/o dispositivos de computación, productos de aplicación y sistemas de información e informáticos de propiedad de la EP-EMAPAR.

Realizar trámites de adquisición de equipos y/o suministros informáticos sin la Autorización del Departamento de Informática, SIG y Catastros.

Instalar y utilizar juegos en los equipos de computación de la EP-EMAPAR.

Ceder o dar a conocer a segundas personas, las claves registradas para el acceso a equipos y/o software informático perteneciente a la EP-EMAPAR, ya que las claves utilizadas son personales e intransferibles, para uso de personal no Autorizado.

Ver Anexo 3

FE

SEGUNDA ETAPA: EJECUCIÓN

PROGRAMA DE AUDITORIA

Entidad: Empresa Pública-Empresa Municipal de Agua Potable y Alcantarillado de Riobamba.

Área: Departamento de Informática.

Tipo de Auditoria: Auditoria Informática.

Fase: Ejecución.

Objetivo: Analizar aspectos relacionados con seguridad lógica, seguridad física, utilización y aprovechamiento de las Tics y gestión de la informática.

N°	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA	OBSERVACIÓN
PROCEDIMIENTOS					
1	Aplique la encuesta al personal operativo del Departamento de Informática relacionado a: ✓ Seguridad Lógica. ✓ Seguridad Física. ✓ Tecnologías de Información y comunicación. ✓ Gestión Informática	FE SL 1 FE SF 1 FE TIC 1 FE GI 1	WRPV	03/02/2014	
2	Aplique encuesta al Jefe de Informática.	FE 2	WRPV	03/02/2014	
3	Aplique encuestas al personal administrativo (Secretarias).	FE 3	WRPV	03/02/2014	
4	Realice la verificación de políticas de cambio de claves de acceso por parte del personal administrativo (secretarias)	FE 4	WRPV	03/02/2014	
5	Realice la verificación física sobre medidas de seguridad disponibles en el departamento de Informática.	FE 5	WRPV	03/02/2014	
6	Realice la verificación física de las condiciones de los servidores.	FE 6	WRPV	04/02/2014	

Nº	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA	OBSERVACIÓN
7	Realice la verificación de software disponible para cada uno de los departamentos de la Empresa.	FE 7	WRPV	05/02/2014	
8	Solicite la Planificación del mantenimiento de Equipos.	FE 8	WRPV	06/02/2014	El personal del área de sistemas recién está elaborando por lo que no disponen de ello
9	Solicite las Políticas de documentación y eliminación de archivo.	FE 9	WRPV	06/02/3014	NO EXISTE Ø
10	Solicite el cronograma de actividades, metas y objetivos del Departamento de Informática.	FE 10	WRPV	07/02/2014	El personal del área de sistemas recién está elaborando por lo que no disponen de ello
11	Solicite los Planes de contingencia.	FE 11	WRPV	07/02/2014	NO EXISTE Ø
12	Solicite el reporte de las características de los equipos de los diferentes departamentos.	FE 12	WRPV	07/02/2014	El reporte se recibió de forma individual.
13	Mediante inspección física seleccione al azar determinado número de máquinas y verifique el reporte de las características.	FE 13	WRPV	10/02/2014	
14	Solicite inventario de Hardware	FE 14	WRPV	11/02/2014	NO EXISTE Ø
15	Realice la determinación de Riesgo	FE 15	WRPV	14/02/2014	

Elaborado por:	Fecha:
WRPV	18-02-2014
Aprobado por:	Fecha:
R.C.	19-02-2014

4.1.2. Resultados de las encuestas a los Técnicos Informáticos del Departamento de Informática en relación a la Seguridad Lógica.

OBJETIVO: conocer si el Departamento de Informática cuenta con políticas de seguridad adecuada a fin de proteger y salvaguardar la información ante posibles daños y sabotajes ocasionados por terceros.

Ilustración 33: Resultados de las encuestas a los Técnicos Informáticos - Seguridad Lógica

6. ¿Se cuenta con los CDs de instalación del sistema operativo que sirva como apoyo en caso de perdida o daños del mismo?

SI	3	75%
NO	1	25%

7. ¿Se cuenta con copias de los archivos en un lugar distinto al lugar de trabajo?

SI	4	100%
NO	0	0%

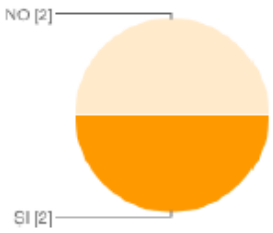
8. ¿Explique la forma de como están protegidas físicamente estas copias (bóvedas, cajas de seguridad) que garantice su integridad en caso de un siniestro?

SERVIDOR ESPEJO | SERVIDOR ESPEJO EN UN CUARTO SEGURO | CUARTO DE SERVIDORES

9. ¿Existen archivos que se consideren como confidenciales que estén debidamente asegurados?

SI	4	100%
NO	0	0%

10. ¿Se lleva un registro del acceso a estos archivos confidenciales?

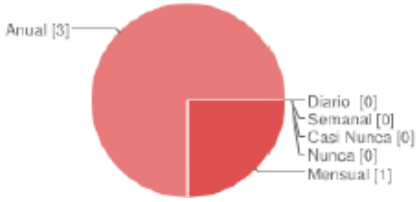


SI	2	50%
NO	2	50%

11. ¿Dónde se almacenan dichos archivos y en el caso de ya no considerarlos necesarios de qué manera se los desecha?

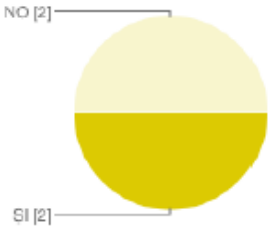
DISCO EXTRAIBLE | SE RESPALDA | SERVIDOR, USABILIDAD

12. ¿Indique la periodicidad con que se realiza el respaldo de información importante?



Diario	0	0%
Semanal	0	0%
Mensual	1	25%
Anual	3	75%
Casi Nunca	0	0%
Nunca	0	0%

13. ¿Se han realizado auditorias a los respaldos de información?



SI	2	50%
NO	2	50%

14. ¿Permite las claves de acceso limitar las funciones del sistema de acuerdo al perfil de cada usuario?

SI	4	100%
NO	0	0%

15. ¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado periodo de tiempo en lo referente a sistemas operativos y correo electrónico para cada usuario?

SI	3	75%
NO	1	25%

16. ¿Se realizan cambios de claves de acceso a los sistemas informáticos?

SI	3	75%
NO	1	25%

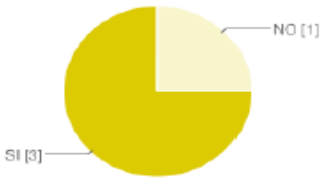
17. ¿Se han definido las características mínimas del Hardware para soportar eficientemente el funcionamiento del sistema operativo?

SI	4	100%
NO	0	0%

18. ¿Se tienen estándares y políticas definidas para realizar actualizaciones al sistema operativo?

SI	4	100%
NO	0	0%

19. ¿Se tienen definidas las características y/o aspectos específicos para la instalación del sistema operativo?



SI	3	75%
NO	1	25%

20. ¿Los servidores disponibles cumplen con las características adecuadas para el desarrollo de las actividades ?

SI	4	100%
NO	0	0%

21. ¿Estos servidores cuentan con una ventilación adecuada, así como medidas de seguridad cerradura especial, protección contra fuego etc.?

SI	3	75%
NO	1	25%

22. Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos en el sistema?

SI	4	100%
NO	0	0%

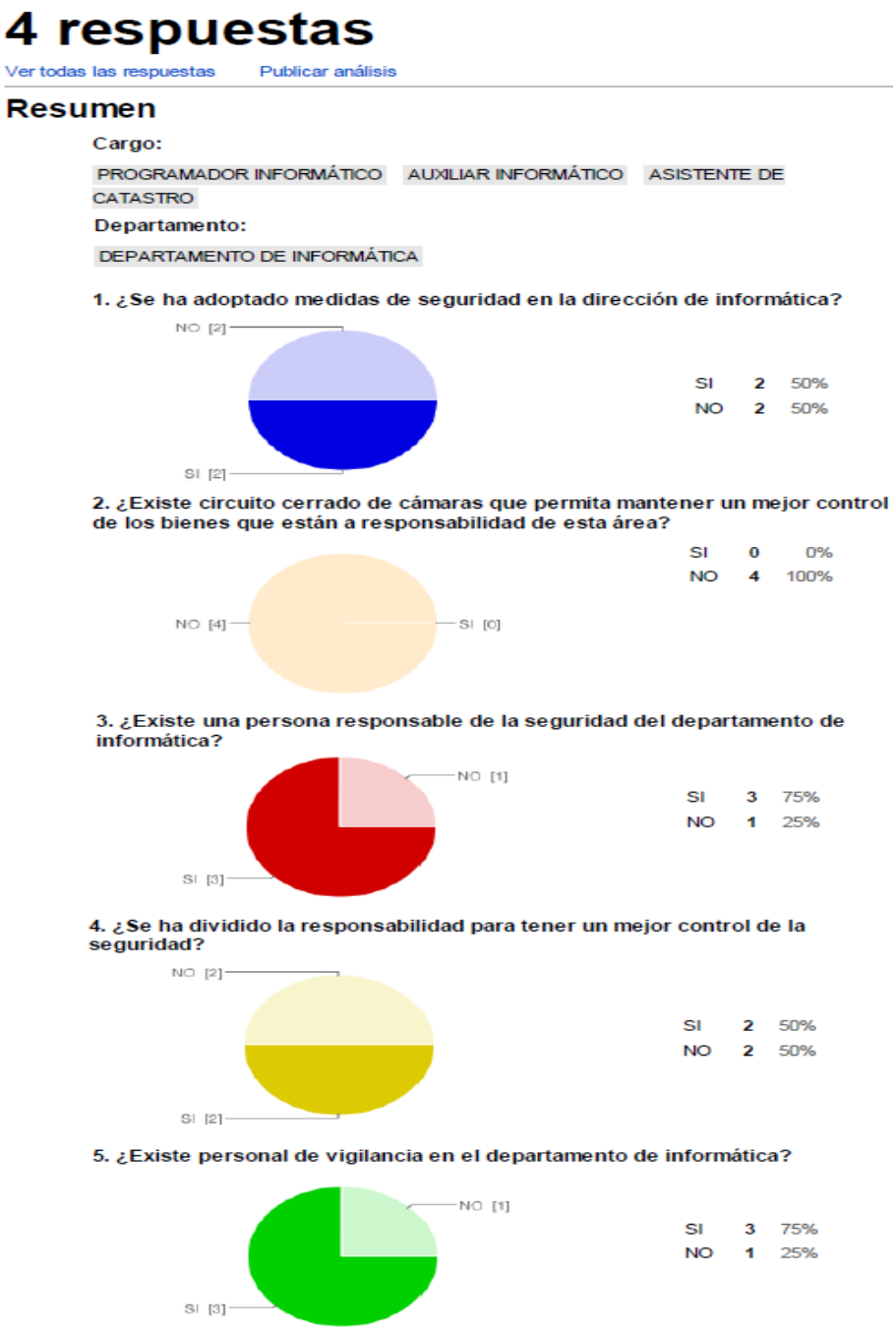
ANÁLISIS DE RESULTADOS

La empresa cuenta con **WINDOWS 7.** La falta de un registro de las modificaciones y/o actualizaciones de la configuración del sistema de la empresa. No se lleva un registro de acceso a los archivos confidenciales de la empresa en la que en tema de seguridad lógica decae. Se realizan respaldos anuales de la información importante por lo que debería hacerse de manera periódica (tres meses). No se han realizado auditorías a los respaldos de la información.

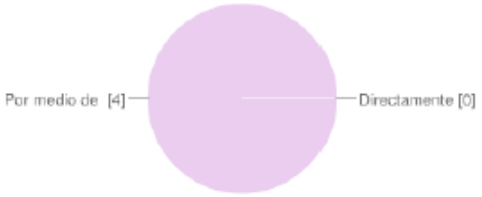
4.1.3. Resultados de las encuestas a los Técnicos Informáticos del Departamento de Informática en relación a la Seguridad Física.

OBJETIVO: Conocer si el Departamento de Informática cuenta con políticas de seguridad física a fin de proteger y salvaguardar los equipos que están bajo disponibilidad del área de informática de la empresa.

Ilustración 34: Resultados de las encuestas a los Técnicos Informáticos - Seguridad Física

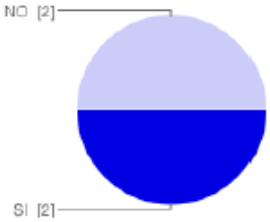


6. La vigilancia se contrata:



Directamente	0	0%
Por medio de empresas que brinden ese servicio	4	100%

7. ¿Se investiga a los vigilantes cuando son contratados directamente?

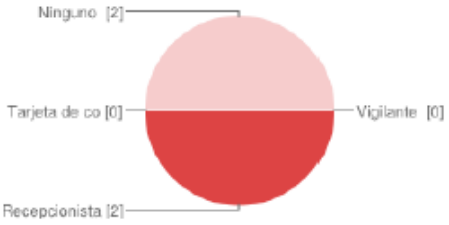


SI	2	50%
NO	2	50%

8. ¿Existe vigilancia en el lugar de los servidores y máquinas las 24 Horas?

SI	4	100%
NO	0	0%

9. A la entrada del cuarto de maquinas existe:

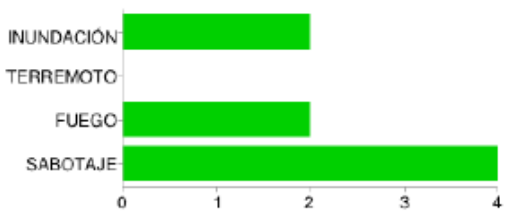


Vigilante	0	0%
Recepcionista	2	50%
Tarjeta de control de acceso	0	0%
Ninguno	2	50%

10. ¿Se ha instruido a personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?

SI	3	75%
NO	1	25%

11. El edificio donde se encuentra los equipos de computo está situado a salvo de:

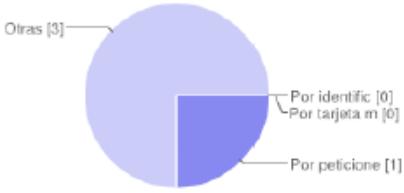


INUNDACIÓN	2	25%
TERREMOTO	0	0%
FUEGO	2	25%
SABOTAJE	4	50%

12. ¿Pueden ser rotos los vidrios con facilidad?

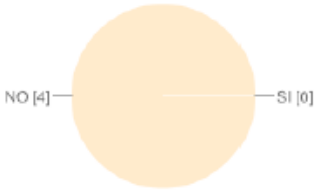
SI	3	75%
NO	1	25%

13. Existe control en el acceso al departamento de informática:



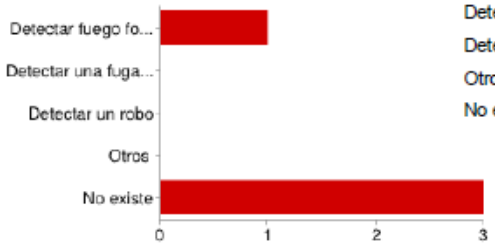
Por identificación personal	0	0%
Por tarjeta magnética	0	0%
Por peticiones verbales	1	25%
Otras	3	75%

14. ¿Se lleva un registro de acceso al cuarto de personas ajenas a la dirección de informática?



SI	0	0%
NO	4	100%

15. Existe alarma para:

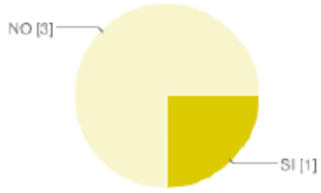


Detectar fuego forma manual	1	25%
Detectar una fuga de agua	0	0%
Detectar un robo	0	0%
Otros	0	0%
No existe	3	75%

16. ¿Donde están ubicadas las alarmas?

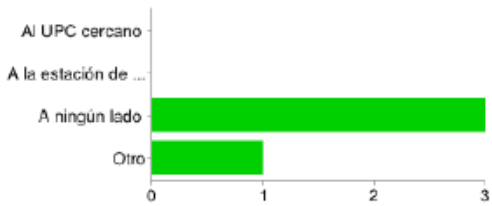
- CUARTO DE MÁQUINAS

17. ¿La alarma es perfectamente audible?



SI	1	25%
NO	3	75%

18. Esta alarma también esta conectada a:

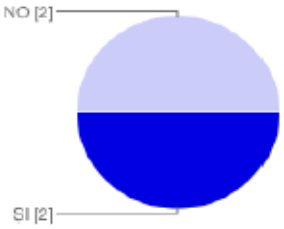


Al UPC cercano	0	0%
A la estación de bomberos	0	0%
A ningún lado	3	75%
Otro	1	25%

19. ¿Existen extintores de fuego?

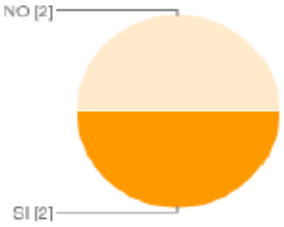
Manuales	4	100%
Automáticos	0	0%
No Existen	0	0%

20. ¿Se ha adiestrado al personal en el manejo de los extintores?



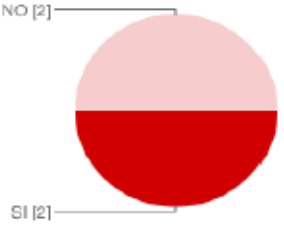
SI	2	50%
NO	2	50%

21. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?



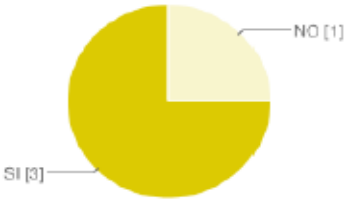
SI	2	50%
NO	2	50%

22. ¿Existe salida de emergencia?



SI	2	50%
NO	2	50%

23. ¿Se ha prohibido a los usuarios el consumo de alimentos y bebidas en el interior de los cuartos de máquinas?



SI	3	75%
NO	1	25%

24. ¿Se limpia con frecuencia las instalaciones a fin de que no se acumule el polvo en los equipos?

SI	4	100%
NO	0	0%

ANÁLISIS DE RESULTADOS

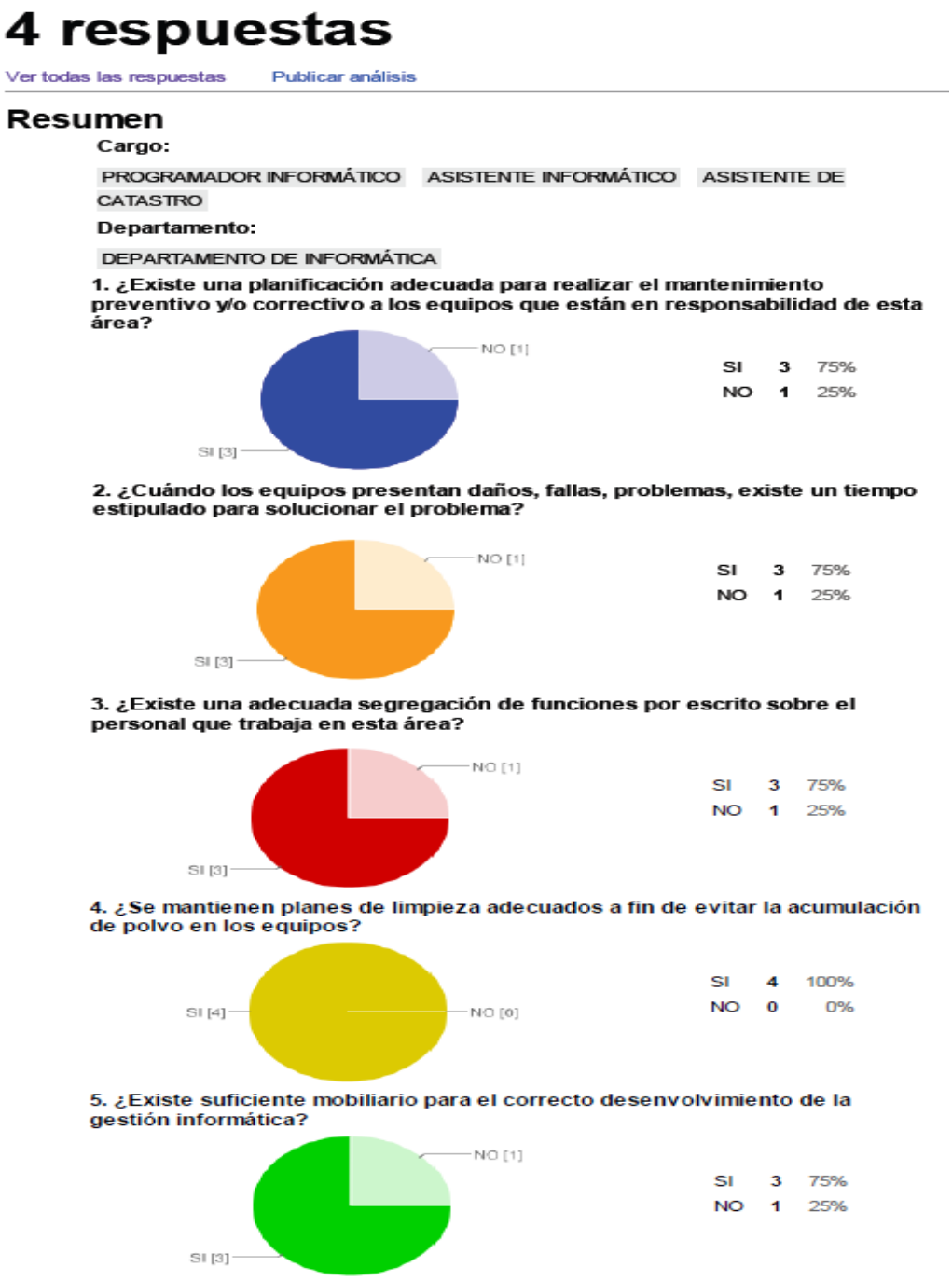
En el departamento de informática no se han adoptado medidas de seguridad física. Inexistencia de un circuito cerrado de cámaras que permita mantener un mejor control de los bienes que están a responsabilidad del área de informática. No se ha dividido en su totalidad la responsabilidad en el personal del departamento de informática de la empresa para tener un mejor control de la seguridad **Θ**. El departamento de informática no investiga a los vigilantes cuando son contratados directamente. El edificio donde funciona el departamento de informática parcialmente está a salvo de inundación terremoto y fuego. Los vidrios pueden ser rotos con facilidad. No existe una alarma específica para la zona donde se almacena la información importante; a la vez esta alarma no es totalmente audible y que sea conectado a un UPC más cercano. Se ha adiestrado de manera esporádica al personal sobre el uso de extintores. No esta rotulado las salidas de emergencia en la zona de informática de la empresa.

Elaborado por:	Fecha:
WRPV	03-02-2014
Aprobado por:	Fecha:
R.C.	04-02-2014

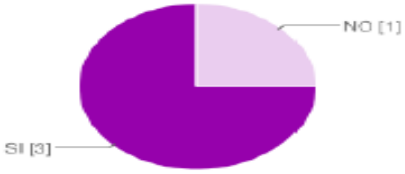
4.1.4. Resultados de las encuestas a los Técnicos Informáticos del Departamento de Informática en relación a Tecnologías de Información y Comunicación.

OBJETIVO: conocer aspectos relacionados a la utilización y aprovechamiento de los recursos informáticos a fin de determinar si los equipos disponibles son actualizados y si existen políticas establecidas para su utilización.

Ilustración 35: Resultados de las encuestas a los Técnicos Informáticos - TIC



6. ¿Existe suficiente mobiliario para los empleados en las actividades diarias de la Empresa?

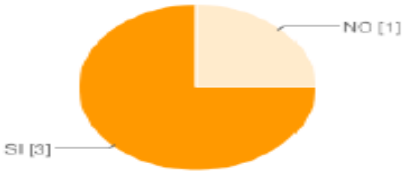


SI	3	75%
NO	1	25%

7. ¿Existen políticas de trabajo definidas sobre el personal que labora dentro de esta área?

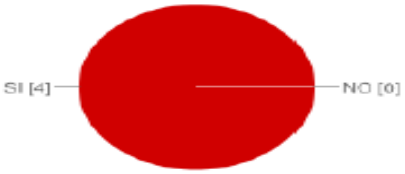
SI	4	100%
NO	0	0%

8. ¿Existe políticas de utilización y uso de las máquinas?



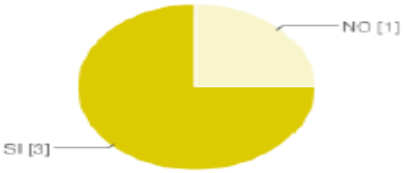
SI	3	75%
NO	1	25%

9. ¿Existe software de producción (programas) que estén disponibles en las maquinas de la empresa y que contribuyan a las actividades diarias de la misma?



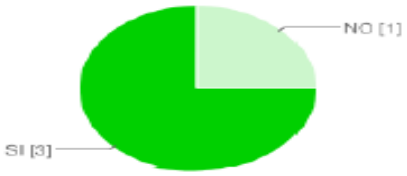
SI	4	100%
NO	0	0%

10. ¿Existe software ofimática actualizado que estén disponibles para los funcionarios de la empresa?



SI	3	75%
NO	1	25%

11. ¿Existe software utilitario que sea de apoyo y que estén disponibles dentro del área?

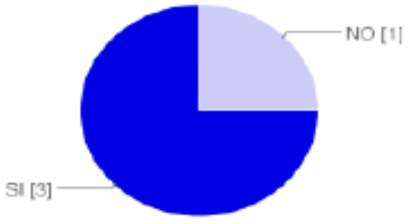


SI	3	75%
NO	1	25%

12. ¿La información de la empresa transmitida por Internet es controlada?

SI	4	100%
NO	0	0%

13. ¿Se elabora normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de Internet, Intranet, correo electrónico y sitio WEB en base a las disposiciones legales?



SI	3	75%
NO	1	25%

14. ¿Se considera el desarrollo de aplicaciones WEB y/o moviles que automaticen los procesos o tramites orientados al uso de instituciones y ciudadanos en general?

SI	4	100%
NO	0	0%

15. ¿Considera que el ancho de banda del servicio de Internet inalámbrico satisface las necesidades de los usuarios?

SI	4	100%
NO	0	0%

16. ¿Se mantiene un registro actualizado de software y hardware que estén bajo la responsabilidad de esta area?

SI	4	100%
NO	0	0%

ANÁLISIS DE RESULTADOS

El ancho de banda del servicio de internet inalámbrico según el personal de tecnologías de información y comunicación satisface las necesidades de los usuarios pero los usuarios del internet mencionan que este servicio es defectuoso. La forma de dar las funciones es a través de memorandos y no existe un manual de funciones debidamente documentado y aprobado. Θ

4.1.5. Resultados de las encuestas a los Técnicos Informáticos del Departamento de Informática en relación a la Gestión Informática.

OBJETIVO: conocer aspectos relacionados sobre la gestión que desempeña el personal del departamento de informática.

Ilustración 36: Resultados de las encuestas a los Técnicos Informáticos - Gestión Informática

4 respuestas

Ver todas las respuestas Publicar análisis

Resumen

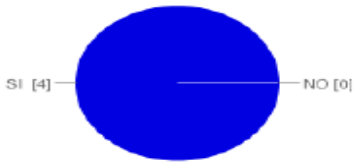
Cargo:

ASISTENTE INFORMÁTICO PROGRAMADOR INFORMÁTICO ASISTENTE DE CATASTRO

Departamento:

DEPARTAMENTO DE INFORMÁTICA

1. ¿Los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área?

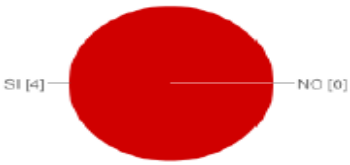


SI	4	100%
NO	0	0%

2. Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la:

SI	4	100%
NO	0	0%

3. ¿El área tiene delimitadas con claridad sus responsabilidades?

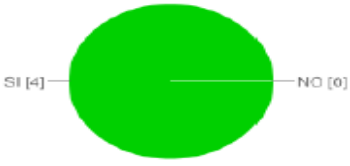


SI	4	100%
NO	0	0%

4. ¿Los puestos actuales son adecuados a las necesidades que tiene el área para llevar a cabo sus funciones?

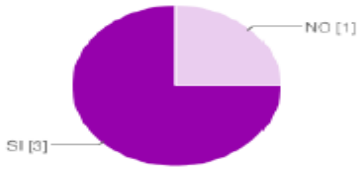
SI	4	100%
NO	0	0%

5. ¿El numero de empleados que trabajan actualmente es adecuado para cumplir con las funciones encomendadas?



SI	4	100%
NO	0	0%

6. ¿Consta en algún documento las funciones del área?



SI	3	75%
NO	1	25%

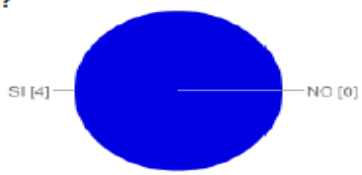
7. ¿Cuál es la forma de dar a conocer las funciones?

PROCESOS DEPARTAMENTALES | VERBAL Y ESCRITO | MEDIANTE MEMORANDO O INFORME DE ACTIVIDADES | INFORME

8. ¿Quién elaboró las funciones?

DEPARTAMENTO DE RECURSOS HUMANOS - JEFE INMEDIATO | RECURSOS HUMANOS Y JEFE DE INFORMÁTICA

9. ¿Las funciones están encaminadas a la consecución de los objetivos de la empresa?

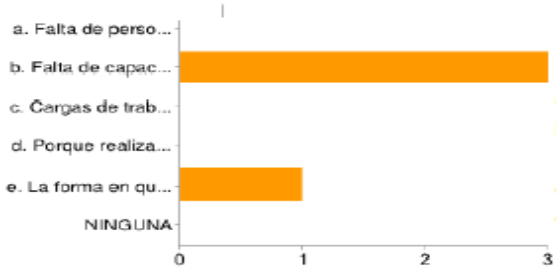


SI	4	100%
NO	0	0%

10. ¿Cuáles son sus principales limitaciones?

FALTA DE HERRAMIENTAS , LOS RECURSOS | NO SE CUENTA CON SUFICIENTES HERRAMIENTAS | NINGUNA

11. La falta de cumplimiento de sus funciones es por:



a. Falta de personal	0	0%
b. Falta de capacitación del personal	3	75%
c. Cargas de trabajo excesivas	0	0%
d. Porque realiza otras actividades	0	0%
e. La forma en que las ordena	1	25%
NINGUNA	0	0%

12. ¿Tienen programas y tareas encomendadas?

SI	3	75%
NO	1	25%

13. ¿Quién es el responsable de ordenar que se ejecuten las actividades?

ING. ANDRÉS YÉPEZ, JEFE DE INFORMÁTICA | JEFE INMEDIATO | ING. ANDRES YÉPEZ JEFE DE INFORMÁTICA | ING. ANDRES YÉPEZ, JEFE DE IN FORMÁTICA

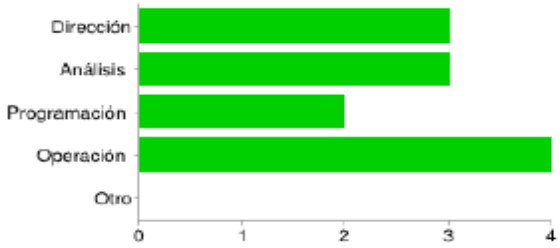
14. En caso de no encontrarse el jefe inmediato, ¿quién lo reemplaza para que se ejecuten las actividades del deparatamento de informática?

ING. HENRY VILLA | ING. HENRY VILLA O EL ING. FABRICIO

15. ¿Para cumplir con sus funciones requiere de apoyo de otras áreas de la empresa?

SI	4	100%
NO	0	0%

16. Los programas de capacitación incluyen al personal de:



Dirección	3	25%
Análisis	3	25%
Programación	2	17%
Operación	4	33%
Otro	0	0%

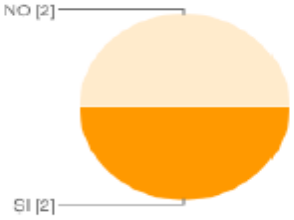
17. ¿Se han identificado las necesidades actuales y futuras de capacitación del personal del área?

SI	3	75%
NO	1	25%

18. ¿Se desarrollan programas de capacitación para el personal del área?

SI	3	75%
NO	1	25%

19. ¿Los resultados de los programas de capacitación son debidamente evaluados?



SI	2	50%
NO	2	50%

20. ¿Cómo se lleva a cabo la supervisión del personal?

. INFORMES

21. ¿Cómo se controla el ausentismo y los retardos del personal?

RELÓJ BIOMÉTRICO RELÓJ BAROMÉTRICO

22. ¿Cómo se evalúa el desempeño del personal?

ESCRITO . PLANIFICACIÓN DEL AÑO INFORME DE ACTIVIDADES

23. ¿Cuál es la finalidad de la evaluación del personal?

. MEJORA DEL RENDIMIENTO CONTROL DE ERRORES CUMPLIR EXPECTATIVAS

24. ¿En términos generales, ¿se adapta el personal al mejoramiento administrativo (resistencia al cambio)?

SI	4	100%
NO	0	0%

25. ¿Cuál es el grado de disciplina del personal?

Total	4	100%
Parcial	0	0%

26. ¿Cuál es el grado de asistencia y puntualidad del personal?

Total	4	100%
Parcial	0	0%

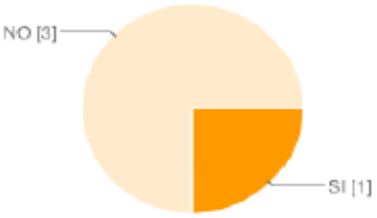
27. ¿Existe una política uniforme y consistente para sancionar la indisciplina del personal?

SI	3	75%
NO	1	25%

28. ¿Puede el personal presentar quejas y/o sugerencias?

SI	4	100%
NO	0	0%

29. ¿Existen políticas de incentivos y ascensos salariales?



SI	1	25%
NO	3	75%

30. ¿Cómo se otorga los ascensos, promociones y aumentos salariales?

CONSEJO DE TRABAJADORES EP-EMAPAR | CONSEJO O DIRECTORIO

31. ¿Cuáles son las principales causas de faltas y ausentismos?

ENFERMEDAD, CALAMIDAD DOMÉSTICA | ENFERMEDAD

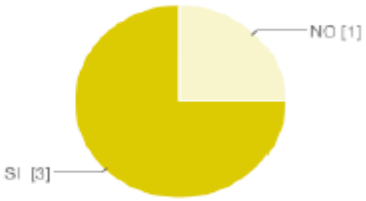
32. ¿Cómo se realiza la motivación del personal del área?

. | REUNIONES Y CONVERSACIONES | MEDIANTE CHARLAS | VERBAL

33. ¿Existen valores corporativos y personales dentro del área de informática?

SI	4	100%
NO	0	0%

34. ¿Existe planes de contingencia dentro del área?



SI	3	75%
NO	1	25%

35. ¿Los objetivos operativos/actividades están adecuadamente relacionados con los objetivos generales de la empresa?

SI	3	75%
NO	1	25%

36. ¿Existe un cronograma de cumplimiento de metas?

SI	3	75%
NO	1	25%

37. ¿Existen políticas definidas sobre la autorización de inversiones en activo fijo, y que estén a cargo de determinadas personas o comités?

SI	4	100%
NO	0	0%

ANÁLISIS DE RESULTADOS

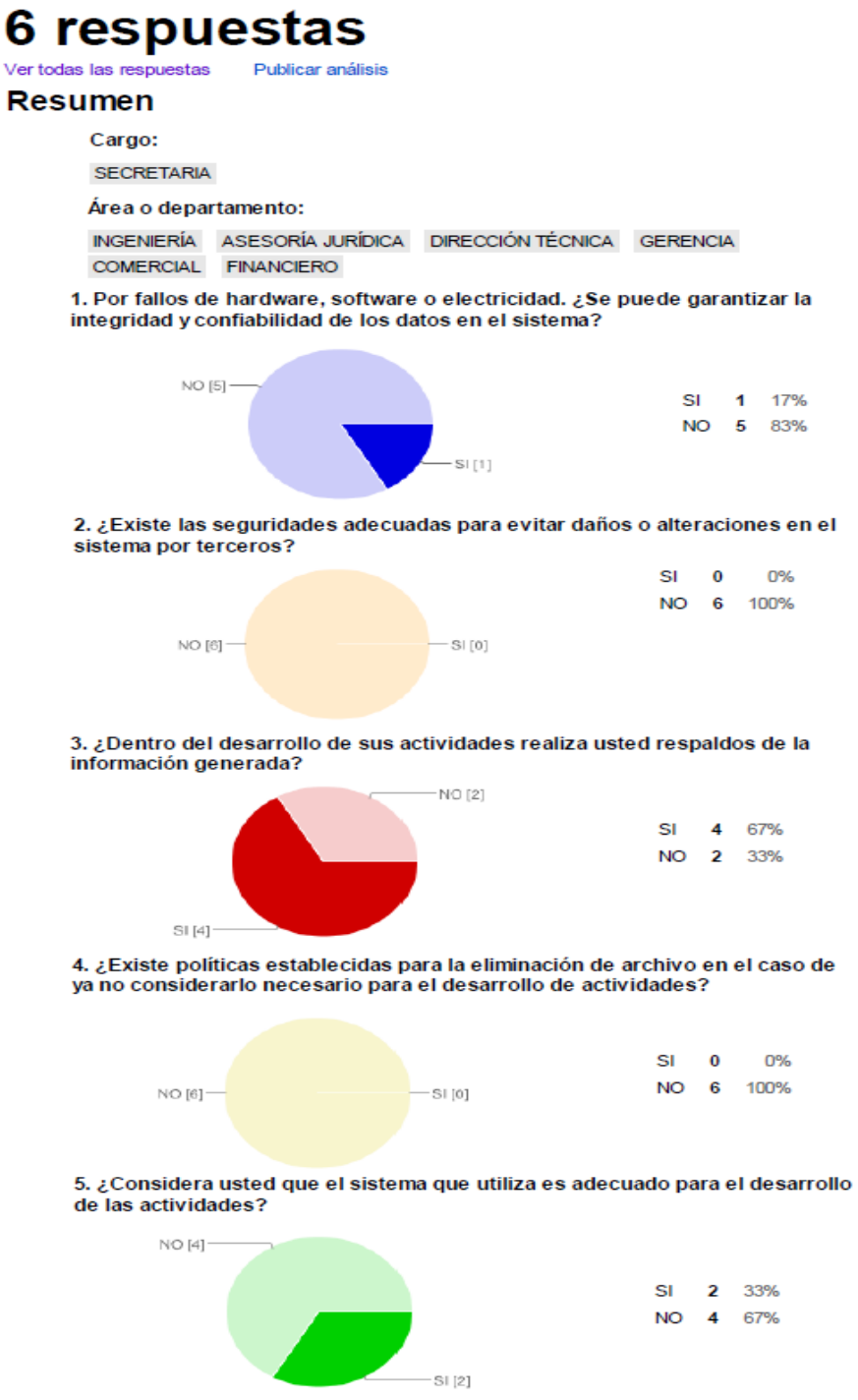
Los funcionarios del departamento de sistemas de la EP EMAPAR no tienen en claro cuál es la forma de dar a conocer sus funciones. Dentro de las principales limitaciones que tienen los empleados del departamento de informática de la empresa son: la falta de herramientas y los recursos económicos **Θ**. La falta de cumplimiento de las funciones se debe a que no existen capacitaciones permanentes a todo el personal y las formas que las ordena el jefe inmediato es decir estas órdenes no son claras **Θ**. Los resultados de las capacitaciones que se da parcialmente no son evaluados. No existen políticas de incentivos y ascensos del personal de área de informática. Existe un cronograma de cumplimiento de metas pero no es aprobado por el gerente ya que se está realizando actualmente el trámite para dicha aprobación.

Elaborado por:	Fecha:
WRPV	03-02-2014
Aprobado por:	Fecha:
R.C.	04-02-2014

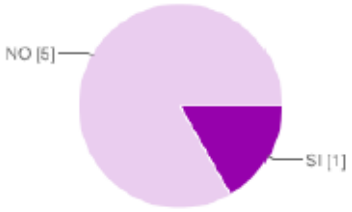
4.1.6. Resultados de encuestas aplicadas al personal administrativo (secretarias)

OBJETIVO: conocer aspectos relacionados en el ámbito administrativo respecto a las actividades, políticas establecidas para la utilización del sistema informático y correo electrónico.

Ilustración 37: Resultados de las encuestas al personal administrativo - Secretarias



6. ¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado período de tiempo en lo referente a sistema operativo, correo electrónico, sistema informático?



SI	1	17%
NO	5	83%

7. En el caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, principalmente durante un determinado período de tiempo por motivos de seguridad?

SI	6	100%
NO	0	0%

ANÁLISIS DE RESULTADOS

Dentro del área administrativa específicamente en las secretarias de toda la empresa se determina lo siguiente: no se puede garantizar la integridad y confiabilidad de los datos del sistema que maneja la empresa por fallos de hardware, software o electricidad, no existen las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas, no se realiza respaldos de la información generada de manera permanente, no existen políticas establecidas para la eliminación de archivo en el caso de ya no considerarlo necesario para el desarrollo de actividades **Θ**, el sistema que se utiliza no es el adecuado para el desarrollo de las actividades diarias de la empresa, no se tiene establecido políticas de cambio de claves de acceso al sistema informático, sistema operativo, correo electrónico que se utiliza en las actividades diarias de la empresa se menciona que existe una sola clave para toda la empresa **Θ**.

El personal de secretaría considera muy necesario e importante realizar el cambio de claves de acceso al sistema, principalmente durante un determinado periodo de tiempo por motivos de estricta seguridad.

Tabla 38: Matriz de Riesgo.

REF PT	DETALLE	CAUSA	EFECTO	Riesgo Inherente	Riesgo de Control	Riesgo de Detección	ACCIONES RECOMENDADAS	NORMA RELACIONADA
FE 4	Ausencia de política de cambio de claves de acceso a los sistemas de información, LOTUS, correo electrónico, sistema operativo.	No existe una comunicación formal por parte de los técnicos informáticos de la empresa para realizar dichos cambios.	Alteraciones en el sistema informático al ingresar con una sola clave y no se realicen los cambios pertinentes.	Medio	Bajo	Bajo	A los técnicos informáticos deberían comunicar de manera formal la importancia que implica el realizar cambios periódicos en claves de acceso para mayor seguridad	410-04 Políticas y procedimientos.
FE 5	Falta de medidas de seguridad para proteger y salvaguardar los bienes informáticos especialmente los del departamento de informática de la empresa.	No existen medidas de seguridad adecuada como el control de acceso físico a la unidad de informática en la protección de los bienes informáticos de la empresa.	Pérdida y fugas de los bienes informáticos y la información que se proceda mediante sistemas informáticos dentro de la empresa.	Medio	Bajo	Bajo	La unidad de tecnologías de información y comunicación, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas de los medios físicos y la información que se procesa mediante sistemas informáticos.	410-10. Seguridad de tecnologías de información.
FE 5	No en todos los departamentos cuentan con elementos de seguridad como: extintores, alarmas, espacio físico adecuado, sistema de ventilación, salidas de emergencia debidamente señalizadas.	No existe disponibilidad de estos medios por tanto no se ha adquirido oportunamente dentro del plan operativo.	Directamente a los usuarios de tecnologías de información y comunicación dentro de la empresa	Bajo	Bajo	Bajo	Se instale en todas las unidades de la empresa estos dispositivos y equipos especializados con el fin de monitorear la seguridad, pruebas periódicas y acciones correctivas sobre vulnerabilidades o incidentes.	410-10. Seguridad de tecnologías de información

REF PT	DETALLE	CAUSA	EFECTO	Riesgo Inherente	Riesgo de Control	Riesgo de Detección	ACCIONES RECOMENDADAS	NORMA RELACIONADA
FP 4	No son claramente definidas las funciones y responsabilidades del personal de tecnología de información.	No existe una adecuada segregación de funciones y responsabilidades del personal de tecnología de información.	Existencia de funciones incompatibles.	Bajo	Medio	Medio	Las funciones y responsabilidades del personal de tecnología de información deberán ser claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente Autoridad y respaldo.	410-03 Segregación de Funciones
FE 2	Falta de recursos necesarios y primordiales para un adecuado desarrollo de la gestión informática de la empresa.	No se especifica un plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos los recursos necesarios para un adecuado desarrollo de la gestión informática de la empresa.	Pérdida de tiempo por parte del personal de tecnologías de información al momento de solucionar un problema.	Medio	Bajo	Medio	La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.	410-03 Plan informático estratégico de tecnología.
FE 2	No existe un plan de contingencias.	La unidad de informática no ha diseñado un plan de contingencia que describa acciones a tomar en caso de una emergencia.	Pérdida de la información que no ha sido respaldada oportunamente.	Alto	Bajo	Medio	La unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.	410-11 Plan de contingencias.

REF PT	DETALLE	CAUSA	EFECTO	Riesgo Inherente	Riesgo de Control	Riesgo de Detección	ACCIONES RECOMENDADAS	NORMA RELACIONADA
FE 3 ½	Falta de políticas para el desecho y eliminación de información cuando ya no se considere necesario su uso.	La unidad de informática no ha definido, documentado y socializado políticas y estándares en la eliminación de un archivo.	Eliminación accidental por desconocimiento de archivos informáticos que provoquen pérdidas de tiempo a la empresa.	Medio	Bajo	Medio	La unidad de tecnología de información definirá, documentará y difundirá las políticas de eliminación de un archivo informático.	410-04 Políticas y procedimientos.
FE 2	Ausencia de inventario de bienes de Equipos, Sistemas y Paquetes informáticos.	Situación producida por falta de gestión de parte del Gerente Administrativo Financiero y Responsable de Bodega.	Ocasiona que no cuente con un saldo real y presente inconsistencias.	Medio	Alto	Bajo	El responsable de bodega y control de activos fijos deberá elaborar el inventario en coordinación con la contadora.	Art. 77 de la LOCGE. Máximas Autoridades, Titulares y Responsables.
FE 6 GI 1 2/6	Falta de capacitación identificada tanto para el personal de tecnologías como para los usuarios que utilizan los servicios de información.	Falta de coordinación por parte de la unidad de tecnologías de información como a unidad de talento humano de la empresa.	Desconocimiento por parte del personal de tecnologías como los usuarios de la información en temas de tecnologías de información y comunicación.	Medio	Medio	Medio	Coordinar la unidad de informática con la unidad de talento humano capacitaciones identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático.	410-15 Capacitación Informática

Elaborado por: El Autor
Fuente: Investigación

HA

TERCERA ETAPA: DETERMINACIÓN DE HALLAZGOS

PROGRAMA DE AUDITORIA

Entidad: Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba.
Área: Departamento de Informática de la EP- EMAPAR
Tipo de Auditoria: Auditoria Informática.
Fase: Determinación de hallazgos
Objetivo: Determinar hallazgos en base a las encuestas aplicadas, análisis de resultados y entrevistas realizadas.

N°	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA.
	PROCEDIMIENTOS			
1	Realice la determinación de los hallazgos en base a los resultados obtenidos.	HA	WRPV	23/02/2014

Elaborado por:	Fecha:
WRPV	24/02/2014
Aprobado por:	Fecha:
RC	25/02/2014

HA 1/8

TÍTULO 1: FALTA DE ACTUALIZACIÓN PERIÓDICA DE LAS CLAVES DE ACCESO A LOS SISTEMAS DE INFORMACIÓN.

CONDICIÓN: Los usuarios de los sistemas de información no realizan cambios periódicos en sus claves de acceso o contraseñas, en lo referente al ingreso al sistema LOTUS, correo electrónico y sistema operativo, por lo tanto no existe políticas establecidas de cambio de claves de acceso.

CRITERIO: debe existir una política de cambio de claves de acceso de al menos cada tres meses a todos los usuarios de los sistemas de información y a la vez comunicar de manera formal la importancia que implica el realizar cambios periódicos en claves de acceso para mayor seguridad.

La Norma de Control Interno 410-04, "*Políticas y procedimientos*", que en su parte pertinente indica:

"…Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir…"

CAUSA: situación producida por falta de comunicación formal por parte de los técnicos informáticos de la empresa para realizar dichos cambios.

EFECTO: Existencia de alteraciones en el sistema informático al ingresar con una sola clave y no se realicen los cambios pertinentes.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 2/8

TÍTULO 2: FALTA DE MEDIDAS DE SEGURIDAD PARA PROTEGER Y SALVAGUARDAR LOS BIENES INFORMÁTICOS.

CONDICIÓN: No existen medidas de seguridad adecuada como el control de acceso físico a la unidad de informática en la protección de los bienes informáticos de la empresa.

CRITERIO: La unidad de tecnologías de información y comunicación, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas de los medios físicos y la información que se procesa mediante sistemas informáticos.

La Norma de Control Interno *410-10,* "*Seguridad de tecnologías de información*", que en su parte pertinente indica:

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

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

CAUSA: Inexistencia de un control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y mantenimiento; los mismos que no reposan en una planificación adecuada para la adquisición de medidas de seguridad.

EFECTO: Pérdida y fugas de los bienes informáticos y la información que se proceda mediante sistemas informáticos dentro de la empresa.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 3/8

TÍTULO 3: INADECUADA SEGREGACIÓN DE FUNCIONES

CONDICIÓN: No existe una adecuada segregación de funciones y responsabilidades del personal de tecnología de información.

CRITERIO: Las funciones y responsabilidades del personal de tecnología de información deberán ser claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente Autoridad y respaldo. *410-02*

La Norma de Control Interno *410-02*, "*Segregación de funciones*", que en su parte pertinente indica:

"…La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave".

CAUSA: No se ha diseñado una manual de funciones por parte de la unidad de tecnología de información.

EFECTO: Funciones del personal de informática incompatibles e inconsistentes.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 4/8

TÍTULO 4: FALTA DE RECURSOS NECESARIOS Y PRIMORDIALES PARA UN ADECUADO DESARROLLO DE LA GESTIÓN INFORMÁTICA DE LA EMPRESA.

CONDICIÓN: No se especifica un plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos los recursos necesarios para un adecuado desarrollo de la gestión informática de la empresa.

CRITERIO: La unidad de tecnología de la información elaborara e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

La Norma de Control Interno *410-03,* "*Plan informático estratégico de tecnología*", que en su parte pertinente indica:

"La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, (...), Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico"

CAUSA: No se toma en cuenta los materiales y herramientas necesarias por parte de las Autoridades y por cuanto exista algún daño se solucione oportunamente.

EFECTO: Pérdida de tiempo por parte del personal de tecnologías de información al momento de solucionar un problema. La obsolescencia de máquinas equipos y tecnología.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 5/8

TÍTULO 5: FALTA DE UN PLAN DE CONTINGENCIAS.

CONDICIÓN: La unidad de tecnología de información y comunicación de la empresa no ha definido, aprobado e implementado un plan de contingencias que describa acciones a tomas en caso de una emergencia.

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

La Norma de Control Interno *410-11*, "*Plan de contingencias*", que en su parte pertinente indica:

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

CAUSA: La unidad de informática por descuido no ha diseñado un plan de contingencia que describa acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información.

EFECTO: Pérdida de la información que no ha sido respaldada oportunamente.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 6/8

TÍTULO 6: FALTA DE POLÍTICAS PARA EL DESECHO Y ELIMINACIÓN DE INFORMACIÓN

CONDICIÓN: La unidad de tecnología de información y comunicación no definió, documentó y difundió políticas de eliminación de un archivo informático.

CRITERIO: La unidad de tecnología de información definirá, documentará y difundirá las políticas de eliminación de un archivo informático.

La Norma de Control Interno *410-04,* "*Políticas y procedimientos*", que en su parte pertinente indica:

"La máxima Autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria…

…Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros…".

CAUSA: La unidad de informática por descuido no ha definido, documentado y socializado políticas y estándares en la eliminación de un archivo.

EFECTO: Eliminación accidental por desconocimiento de archivos informáticos importantes que provoquen pérdidas de tiempo a la empresa.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 7/8

TÍTULO 7: AUSENCIA DE INVENTARIO DE BIENES DE EQUIPOS, SISTEMAS Y PAQUETES INFORMÁTICOS.

CONDICIÓN: No existe un inventario sobre los bienes de equipos, sistemas y paquetes informáticos.

CRITERIO: El responsable de bodega y control de activos fijos deberá elaborar el inventario en coordinación con la contadora.

Incumpliendo el Artículo 77 numeral 3, de la Ley Orgánica de la Contraloría General del Estado que señala entre las atribuciones y obligaciones de las Autoridades de la Unidad Financiera y servidores:

> *"…a) Organizar, dirigir, controlar todas las actividades de administración financiera de la entidad, organismo o empresa del sector público.- d) Adoptar medidas para el funcionamiento del sistema de administración financiera…".*

Artículo 3 del Reglamento Sustitutivo para el Manejo y Administración de Bienes del Sector Público.- "Del procedimiento y cuidado", señala en su parte pertinente:

> "*…El Guardalmacén de Bienes o quién haga sus veces sin perjuicio de los registros propios de la contabilidad de la entidad debe tener información sobre los bienes y mantener un inventario actualizado…"*

y el artículo 12 del Reglamento Sustitutivo para el Manejo y Administración de Bienes del Sector Público.- "Obligatoriedad de Inventarios", que señala:

> *"…El Guardalmacén de Bienes o quién haga sus veces, al menos una vez al año, en el último trimestre, procederá a efectuar la toma de inventario, a fin de actualizarlo y tener la información correcta…"*

CAUSA: Situación producida por falta de gestión de parte del Gerente Administrativo Financiero y Responsable de Bodega.

EFECTO: Ocasiona que no cuente con un saldo real y presente inconsistencias.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

HA 8/8

TÍTULO 8: NO EXISTE CAPACITACIÓN INFORMÁTICA.

CONDICIÓN: Falta de capacitación identificada tanto para el personal de tecnologías como para los usuarios que utilizan los servicios de información que no ha sido coordinado por parte de la unidad de informática con la unidad de talento humano.

CRITERIO: la unidad de informática debe coordinar con la unidad de talento humano capacitaciones identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático.

La Norma de Control Interno *410-15*, "*Capacitación informática*", que en su parte pertinente indica:

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

CAUSA: Falta de coordinación por parte de la unidad de tecnologías de información como a unidad de talento humano de la empresa.

EFECTO: Desconocimiento por parte del personal de tecnologías como los usuarios de la información en temas de tecnologías de información y comunicación.

Elaborado por:	Fecha:
WRPV	23/02/2014
Aprobado por:	Fecha:
RC	24/02/2014

FCR

CUARTA ETAPA: COMUNICACIÓN DE RESULTADOS.

PROGRAMA DE AUDITORIA

Entidad: Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba.
Área: Departamento de Informática de la EP- EMAPAR
Tipo de Auditoria: Auditoria Informática.
Fase: Comunicación de resultados
Objetivo: Dar a conocer los hallazgos encontrados durante la evaluación en los aspectos de seguridades tanto físicas como lógicas, utilización y aprovechamiento de tecnologías de información, comunicación y gestión informática.

N°	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA.
	PROCEDIMIENTOS			
1	Elabore la Carta de Presentación.		WRPV	28/02/2014
2	Elabore el Informe de Auditoria		WRPV	28/02/2014
3	Elabore el Acta de Convocatoria		WRPV	10/03/2014
4	Realice la Convocatoria		WRPV	11/03/2014
5	Realice el Archivo Correspondiente		WRPV	31/03/2014

Elaborado por:	Fecha:
WRPV	31/03/2014
Aprobado por:	Fecha:
RC	01/04/2014

CARTA DE PRESENTACIÓN

Riobamba, 11 de marzo del 2014

Ingeniero

Víctor Méndez

GERENTE GENERAL DE LA EP-EMAPAR

Presente,

De mi consideración:

Hemos realizado la Auditoría Informática a la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba por el período comprendido Enero – Diciembre 2012.

El análisis se realizó de acuerdo con las Normas de Control Interno emitidas por la Contraloría General del Estado en lo referente a tecnologías de información y comunicación. La evaluación incluye el análisis y estudio de seguridad lógica, seguridad física, utilización y aprovechamiento de tecnologías de información y comunicación Tics y gestión informática.

Debida a la naturaleza de estudio y de los componentes evaluados, los resultados de la auditoria se encuentran en las conclusiones y recomendaciones del presente informe.

Atentamente,

Rolando Peralta

AUDITOR

INFORME CONFIDENCIAL

Riobamba, 11 de marzo del 2014

Emisión del informe de auditoría informática.

1. Al Gerente General de la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, por el período comprendido enero – diciembre 2012, en cuanto a seguridad lógica, seguridad física, aprovechamiento y correcta utilización de las Tecnologías de información y comunicación, y gestión de la informática, la responsabilidad consiste en expresar una opinión sobre los mismos en base a la práctica de la auditoría.

2. El análisis se realizó de acuerdo con las Normas de Control Interno emitidas por la Contraloría General del Estado grupo 410 en lo referente a tecnologías de información y comunicación. La gran mayoría de los síntomas percibidos a lo largo de la auditoría informática obedecen a la falta de políticas establecidas que indiquen de manera documentada y debidamente aprobada, el cambio de claves de acceso a los sistemas de información como de correo electrónico y sistema operativo con una periodicidad de tiempo establecida y formalmente comunicada, también políticas de eliminación de archivos que ya no se usan; la falta de medidas de seguridad adecuadas para proteger y salvaguardar los bienes en especial los que están a disposición del Departamento de Informática, la falta de recursos necesarios para desarrollar una mejor gestión informática cuando se presentan daños o desperfectos en los equipos que reposan en las diferentes unidades de la empresa, la ausencia de un inventario físico de bienes de equipos, sistemas y paquetes informáticos, la falta de un plan de contingencia en caso de alguna eventualidad emergente, la ausencia de capacitaciones tanto para los usuarios del sistema como para el personal del área de informática. Se considera que este estudio proporciona una base razonable para expresar la opinión en base a los parámetros establecidos.
3. En nuestra opinión, los aspectos mencionados en el párrafo anterior son inconsistencias que se deben mejorar a través de la toma de decisiones en base a las recomendaciones emitidas en el presente informe.

Rolando Peralta.
AUDITOR

INFORME DE AUDITORÍA INFORMÁTICA

CAPÍTULO I

Motivo del examen.

El trabajo se realizó por la razón que en la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba no se ha realizado una Auditoria Informática que evalué los aspectos de seguridad lógica, seguridad física, correcta utilización de la Tecnologías de Información y Comunicación y la gestión informática.

Objetivo General

Realizar la Auditoría Informática a la Empresa Pública-Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012, para medir el grado de cumplimiento de las Normas de Control Interno sobre Tecnologías de la Información.

Objetivos específicos

- Analizar los documentos de soporte que sustentan la propiedad, veracidad y legalidad de las operaciones de gestión informática.
- Evaluar el sistema de control existente para el uso, control y resguardo de los Equipos, Sistemas y Paquetes Informáticos.
- Determinar el cumplimiento de la normativa legal vigente como son las Normas de Control Interno emitidas por la Contraloría General del Estado.

Alcance del Examen

El examen comprendió el análisis a "Seguridad física, Seguridad Lógica, uso adecuado de Tecnologías de Información y Comunicación y la Gestión Informática", de la Empresa Pública – Empresa Municipal de Agua potable y Alcantarillado de Riobamba, del período 2012-01-01 al 2012-12-31.

Base Legal

"La Empresa Municipal de Agua Potable y Alcantarillado del Cantón Riobamba, fundamenta su actividad en la Ordenanza No.010-2004, aprobada en sesiones realizadas por el I. Concejo Municipal de Riobamba del 26 de julio y 20 de septiembre del 2004 y publicado en el Registro Oficial No. 442 del 14 octubre del 2004. Cuyas siglas son EMAPAR, y por ello, con este nombre se identificará actuará en todos los actos públicos, privados, judiciales, extrajudiciales y administrativos, normada sus actividades por las Leyes, Disposiciones, Reglamentos, Resoluciones y Ordenanzas para los organismos del sector Público".

La Empresa Pública Empresa Municipal de Agua Potable y Alcantarillado de Riobamba EP-EMAPAR se rige principalmente por la Ley Orgánica de Régimen Municipal, la Ley Orgánica de Empresas Públicas, y la Ordenanza 001-2010 que regula la prestación de los servicios públicos de Agua Potable y Alcantarillado, las disposiciones de los Reglamentos Internos Generales y Específicos que se expidan y demás normas jurídicas aplicables, la Constitución de la República del Ecuador Cap. 4, el Código Territorial, la Ordenanza de la Creación de la Empresa, el Reglamento Orgánico Estructural, el Reglamento Orgánico Funcional, Reglamento de Servicios, Reglamento Interno para la LOSCCA, Reglamento Interno para el Código de Trabajo, Reglamento de Funcionamiento del Directorio. Conforme a la ley orgánica de empresas públicas, la EP- EMAPAR es una persona jurídica de derecho público con patrimonio propio, dotada de autonomía presupuestaria, financiera, económica, administrativa y de gestión. De conformidad con el Art. 4 de la Ley Orgánica de Empresas Públicas podrá establecer empresas subsidiarias, empresas filiales, agencias o unidades de negocios.

Estructura Orgánica

Para el cumplimiento de sus funciones, EP-EMAPAR, observará el correspondiente orgánico funcional aprobado por su Directorio, con los siguientes niveles jerárquicos:

a) Nivel Directivo.- Conformado por el Directorio.
b) Nivel ejecutivo.- Conformado por la Gerencia General.
c) Nivel asesor.- Conformado por Asesoría Jurídica y Auditoría Interna.
d) Nivel de apoyo.- Conformado por las Direcciones Administrativa y Financiera;
e) Nivel operativo.- Conformado por las Direcciones: De Ingeniería, Técnica y Comercial. Y las demás unidades técnico- administrativas que se contemplaren en los manuales Orgánico- Funcional y de Procesos.

Cultura Organizacional.

Misión

"Somos una empresa pública que dota de servicio de agua potable y saneamiento ambiental, con responsabilidad social, contribuyendo al mejoramiento de la calidad de vida de los habitantes del cantón Riobamba"

Visión

"la EP-EMAPAR será una empresa eficiente que dotará de servicio de agua potable y saneamiento ambiental de forma permanente, con talento humano capacitado, insumos y tecnología de calidad"

Objetivos

- ✓ Garantizar Eficiencia y Sostenibilidad
- ✓ Mejorar continuamente los servicios a nuestros usuarios.
- ✓ Implementar un sistema de Comunicación e Integración.

Capitulo II

RESULTADO DEL EXAMEN

SEGURIDAD LÓGICA

Falta de actualización periódica de las claves de acceso de los usuarios.

CONCLUSIÓN: Dentro de la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba no se cuenta con políticas establecidas para cabios periódicos de las claves de acceso al sistema informático.

RECOMENDACIÓN DIRIGIDA AL GERENTE, JEFE DE INFORMÁTICA Y TÉCNICOS INFORMÁTICOS.

1. Definir políticas para establecer contraseñas fuertes y hacer renovación de claves de acceso a los sistemas de manera periódica. Establecer un sistema de caducidad de claves de acceso en el sistema informático que indique notificaciones de que se debe realizar dicho cambio cuando cumpla con el período de tiempo establecido. Implementar controles a través del sistema informático por parte de los técnicos para realizar la verificación de claves de acceso y determinar si estas cumplen con las condiciones estipuladas en el tiempo previsto.

Falta de políticas para el desecho y eliminación de información cuando ya no se considere necesario su uso.

CONCLUSIÓN: La unidad de informática no ha definido, documentado y socializado las políticas y estándares en la eliminación de un archivo.

RECOMENDACIÓN DIRIGIDA AL GERENTE, JEFE DE INFORMÁTICA Y TÉCNICOS INFORMÁTICOS.

2. Definir las políticas de acceso a los archivos confidenciales y eliminación de los mismos cuando estos ya no sean necesarios su uso.
   Definir mecanismos de control para asegurar el buen proceso de eliminación de un archivo que no pueda afectar ni alterar la información confidencial de la empresa.

SEGURIDAD FÍSICA

Falta de medidas de seguridad para proteger y salvaguardar los bienes informáticos especialmente los del departamento de informática de la empresa.

CONCLUSIÓN: el departamento de informática de la empresa no cuenta con las medidas de seguridad adecuadas para mantener un mejor control de los bienes.

RECOMENDACIÓN DIRIGIDA AL JEFE DE INFORMÁTICA Y TÉCNICOS INFORMÁTICOS.

3. Realizar un registro físico y documentado que sirva de control para las personas que ingresan a la unidad de informática.
   Implementar un circuito cerrado de cámaras de vigilancia.
   Disponer de un espacio adecuado para el mantenimiento y reparación de equipos.
   Contratar a una persona que se encargue de la seguridad de la unidad de informática es decir un recepcionista que a la vez cumpla la función del llenado del registro físico de acceso al mismo, para así evitar fugas de la información y bienes informáticos.

Inexistencia de un Plan de Contingencias.

CONCLUSIÓN: no existen disponibilidad de los elementos principales de seguridad por lo tanto no se ha adquirido oportunamente dentro del plan operativo.

AL GERENTE, JEFE DE INFORMÁTICA Y TÉCNICOS INFORMÁTICOS.

4. Diseñar, aprobar e implementar un plan de contingencias con el fin de evitar pérdidas significativas de la información o daños mayores a los equipos informáticos.
   Implementar salidas de emergencia señalizada en cada uno de los departamentos de la empresa, extintores, ventilación, alarmas de seguridad contra robos e incendio; disponer de un espacio adecuado para el mantenimiento y reparación de equipos.

GESTIÓN INFORMÁTICA

Falta de recursos necesarios y primordiales para un adecuado desarrollo de la gestión informática.

CONCLUSIÓN: No se especifica un plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos los recursos necesarios para un adecuado desarrollo de la gestión informática de la empresa.

AL GERENTE, JEFE DE INFORMÁTICA Y TÉCNICOS INFORMÁTICOS.

5. Elaborar e implementar un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

Falta de una adecuada segregación de funciones del personal del área de informática

CONCLUSIÓN: no existe una adecuada segregación de funciones y responsabilidades dentro del área de informática.

AL GERENTE, JEFE DE INFORMÁTICA Y TÉCNICOS INFORMÁTICOS.

6. Elaborarán un manual de funciones claramente definidas y debidamente aprobadas por la máxima Autoridad para el personal de tecnologías de información, con la finalidad de que no exista funciones incompatibles.

Ausencia de Inventario de Bienes, Equipos, Sistemas y Paquetes Informáticos.

CONCLUSIÓN: la empresa no cuenta con inventarios de bienes de Equipos, Sistemas y Paquetes Informáticos.

AL RESPONSABLE DE BODEGA Y CONTROL DE ACTIVOS FIJOS

7. Elaborará el inventario en coordinación con la Contadora, con la finalidad de obtener en forma oportuna el saldo correspondiente y su descomposición, facilitando además las labores de control posterior.

Falta de capacitación informática

CONCLUSIÓN: falta de capacitación informática programada para los técnicos informáticos y usuarios del parque informático de la empresa

AL DIRECTOR DE RECURSOS HUMANOS, JEFE DE INFORMÁTICA Y TÉCNICOS DE INFORMÁTICA

8. Planificar periódicamente capacitación para el personal del área de informática y usuarios de los sistemas de información y comunicación, con la finalidad de fomentar la automotivación y autoaprendizaje en el talento humano de la empresa en temas de Tecnologías de Información y Comunicación.

Convocatoria de conferencia final

Ingeniero
Víctor Méndez
GERENTE GENERAL DE LA EP-EMAPAR
De mi consideración:

De conformidad con lo dispuesto en los artículos 90 de la Ley Orgánica de la Contraloría General del Estado y 23 de su reglamento convoco a usted a la conferencia final de comunicación de resultados mediante la lectura del borrador del informe de la Auditoría Informática a la Empresa Pública - Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012 mediante orden de trabajo 001 de fecha veinte y cuatro de enero del dos mil catorce.
La diligencia se llevará a cabo en la sala de sesiones de la empresa el día catorce de abril del 2014. En caso de no poder asistir personalmente agradeceré notificar por escrito, indicando los nombres, apellidos y número de cédula de ciudadanía de la persona que actuará en su representación.

Atentamente

Sr. Rolando Peralta.

ACTA DE CONFERENCIA FINAL DE COMUNICACIÓN DE RESULTADOS CONTENIDOS EN EL BORRADOR DEL INFORME DE LA AUDITORÍA INFORMÁTICA A LA EMPRESA PÚBLICA – EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA, PERIODO 2012.

En la ciudad de Riobamba, provincia de Chimborazo, a los catorce días del mes de abril del dos mil catorce, a las 15 horas, el suscrito: Sr. Rolando Peralta, se constituyen en la sala de sesiones de la Empresa, con el objeto de dejar constancia de la lectura del Borrador del Informe de Auditoría Informática a la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012 que realizado de conformidad a la carta a gerencia enviada.

Se convocó mediante oficio a los funcionarios, para que asistan a la presente diligencia.

Al efecto, en presencia de los abajo firmantes, se procedió a la lectura del borrador del informe, se analizaron y discutieron los resultados de la Auditoría, constantes en los comentarios, conclusiones y recomendaciones.

Para constancia de lo actuado, las personas asistentes suscriben la presente acta en dos ejemplares de igual tenor.

NOMBRES Y APELLIDOS	CARGO	N° DE CÉDULA	FIRMA
Ing. Víctor Méndez	Gerente de la EP-EMAPAR		
Ing. Andrés Yépez	Jefe de Informática		
Ing. Henry Villa	Técnico Informático		
Ing. Fabricio Carbajal	Técnico informático		
Ing. Walter Parra	Técnico Informático		
Ing. Hugo Trujillo	Técnico Informático		

4.2. Verificación de la Hipótesis

Dentro de la hipótesis planteada en el presente trabajo "Al realizar la Auditoría informática, a la Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012, permitirá cumplir las Normas de Control Interno del grupo 410 emitidos por la Contraloría General del Estado". Acordando que en la encuesta aplicadas a Gerente, Directores, Jefes y demás empleados usuarios del parque informático de la empresa, al responder la pregunta N° 5 acerca de la consideración necesaria que se realice una Auditoría Informática en la empresa, el 100% dice que sí, justificando de esta manera la necesidad de presentar la Auditoría.

De acuerdo a las encuestas realizadas al Gerente, Directores, Jefes y demás empleados usuarios del parque informático de la empresa, en la pregunta N°. 6, el 44% afirma que mediante la Auditoría informática permitirá cumplir con las Normas de Control Interno grupo 410 en Tecnologías de Información.

CONCLUSIONES

- ✓ Se diagnosticó los aspectos generales sobre el grado de cumplimiento de las Normas de Control Interno emitidos por la Contraloría General del Estado donde se determinó que existen más debilidades que fortalezas en lo referente a tecnologías de información.

- ✓ Se ejecutó la Auditoría Informática mediante la elaboración de un plan de trabajo para obtención de evidencias suficientes y pertinentes.

- ✓ Se emitió un informe final proponiendo mejoras y soluciones sobre la utilización más eficiente y segura de la información para una adecuada toma de decisiones.

- ✓ La empresa no cuenta con políticas en la actualización periódica de las claves de acceso de los usuarios al sistema de información así como también políticas para el desecho y eliminación de información cuando ya no se considere necesario su uso.

- ✓ La empresa no cuenta con medidas de seguridad física adecuadas para proteger y salvaguardar los bienes informáticos especialmente los del departamento de informática de la empresa.

- ✓ Inconsistencias en la segregación de funciones del personal del área de informática debido a que no se ha diseñado un manual de funciones y responsabilidades.

- ✓ Falta de capacitación informática debido a que no se ha realizado un plan de capacitación de manera periódica y que sea planificado por la unidad de informática como la unidad de talento humano.

RECOMENDACIONES

- ✓ Aplicar las normas de control interno emitidas por la Contraloría General del Estado del grupo 410, en lo referente a Tecnologías de Información y Comunicación para que existan mejoras en la gestión informática

- ✓ Definir políticas en la actualización periódica de las claves de acceso de los usuarios al sistema de información así como también políticas para el desecho y eliminación de información cuando ya no se considere necesario su uso y así mejorar eficientemente los procesos tecnológicos.

- ✓ Establecer medidas de seguridad física adecuadas para proteger y salvaguardar los bienes informáticos especialmente los del departamento de informática de la empresa para evitar posibles robos, fuga de información y sabotajes.

- ✓ Diseñar un manual de funciones y responsabilidades para que exista una adecuada segregación de funciones.

- ✓ Planificar las capacitaciones informáticas periódicas diseñando un plan de capacitación, que sea planificado por la unidad de informática como la unidad de talento humano.

- ✓ Aplicar Auditorías Informáticas anuales que permitan el buen cumplimiento de las Normas de Control Interno emitidas por la Contraloría General del Estado, tomando ampliamente como referencia no solo las NCI de la CGE sino las TICs y modelo COBIT.

BIBLIOGRAFÍA

- ✓ EcheniqueG., J. A. (2008). Auditoría en informática. En J. A. García, *Auditoría en Informática* (págs. 26-27). México: Mc GRAW-HILL/INTERAMERICANA EDITORES, S.A. de C.V.
- ✓ Mario Piattini Velthuis, Emilio del Peso Navarro, & Mar del Peso Ruiz. (2008). *Auditoría de Tecnologías y Sistemas de Información.* México D.F.: C. 2008 Alfaomega Grupo Editor, S.A. de C.V.
- ✓ Muñoz Razo , C. (2002. P.). *Auditoría en Sistemas Computacionales.* Juárez - México: D.R. C. 2002 por Pearson Educación México, S.A. de C.V.
- ✓ Vandama N., Lescay M., & García F. . (2002). *Auditoría Informática en ETECSA.* Obtenido de http://espejos.unesco.org.uy/simplac2002/Ponencias/Segurm%E1tica/VIR024.doc
- ✓ Normas de Control Interno Grupo 410 referente a tecnologías de información, emitidas por la Contraloría General del Estado. (2009) http://www.contraloria.gob.ec/normatividad_vigente.asp

ANEXOS

Anexo 1: Papeles de Trabajo

PAPELES DE TRABAJO

EMPRESA PÚBLICA - EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA

FE 2

*Obligatorio

ÁREA: DEPARTAMENTO DE INFORMÁTICA
COMPONENTE: GESTIÓN INFORMÁTICA
FASE: EJECUCIÓN

MOTIVO DEL EXAMEN: Conocer aspectos relacionados sobre el desempeño del departamento de informática.

1. ¿Los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área? *
- SI
- A VECES
- NO

2. ¿Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la: *

	SI	A VECES	NO
a. Operación?	◉	○	○
b. Supervisión?	◉	○	○
c. Comunicación ascendente?	◉	○	○
d. Comunicación descendente?	◉	○	○
e. Toma de decisiones?	◉	○	○

3. ¿La Unidad de Informática, está posicionada dentro de la estructura orgánica de la entidad en un nivel que le permita, efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias? *
- SI
- NO

4. ¿Considera que debe revisarse la estructura orgánica actual, a fin de hacerla más eficiente? *
- SI
- NO

5. ¿Los puestos actuales son adecuados a las necesidades que tiene el área para llevar a cabo sus funciones? *
- SI
- NO

6. ¿Están las funciones del Departamento de Informática en forma empírica? *
- SI
- NO

7. ¿Existen conflictos por las cargas de trabajo desequilibradas? *
- SI
- NO

8. ¿La asignación de funciones y sus respectivas responsabilidades garantizan una adecuada segregación, evitando funciones incompatibles? *
- SI
- NO

9. ¿Se realiza dentro del Departamento de Informática la supervisión de roles y funciones del personal, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal? *
- SI
- NO

10. ¿Está documentado y aprobado los puestos de trabajo que conforman la Unidad de Informática? *
- SI
- NO

11. ¿Se elabora un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos de la Empresa? *
- SI
- NO

12. ¿Se definió, documentó y difundió las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones dentro de la Empresa? *
- SI
- NO

13. Se consideran dentro de las políticas y procedimientos temas como: *
Puede seleccionar varias.
- [x] Calidad
- [x] Seguridad
- [x] Confidencialidad
- [ ] Controles Internos
- [ ] Propiedad Intelectual
- [ ] Firmas Electrónicas
- [ ] Mensajería de datos
- [ ] Legalidad del Software
- [ ] Otros:

14. ¿Se promueve y establece convenios con otras organizaciones o terceros a fin de promover y visibilizar el intercambio de información interinstitucional? *
- SI
- NO

15. ¿Se regula en la Unidad de Informática los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos? *
- SI
- NO

16. ¿Se elabora manuales técnicos, de instalación y configuración; así como de usuario, los cuales son debidamente difundidos, publicados y actualizados de forma permanente? *
410-07
- SI
- NO

17. ¿Están alineadas las adquisiciones tecnológicas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios? *
410-08 1
- SI
- NO

18. ¿Cuales son las principales limitaciones que existen en el departamento de informática que impidan el normal desarrollo de las actividades? *

NO EXISTIR DISPONIBILIDAD ECONÓMICA
INESTABILIDAD DE PUESTOS DIRECTIVOS CAMBIANTES

19. ¿Se elabora un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentando en revisiones periódicas y monitoreo en función de las necesidades organizacionales? *
- SI
- NO

20. ¿Se mantiene el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables? *
- SI
- NO

21. ¿El mantenimiento de los bienes que se encuentran en garantía es proporcionado por el proveedor, sin costo adicional para la empresa? *
- SI
- NO

22. ¿Los servidores se encuentran en una ubicación adecuada? *
- SI
- NO

23. ¿Se lleva un control de acceso físico a la unidad de informática en especial en el área de los servidores? *
- SI
- NO

24. ¿Se realiza respaldos de la información, en función a un cronograma definido y aprobado? *
- SI
- NO

25. ¿Existe instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego? *
- SI
- NO

26. ¿Se definió, aprobó e implementó un plan de contingencias que describa las acciones a tomar en caso de una emergencia? *
- SI
- NO

27. ¿Se designó un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia? *
- SI
- NO

28. ¿Se presenta informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados? *
- SI
- NO

29. ¿Se considera el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general? *
- SI
- NO

30. ¿Se realiza capacitaciones identificadas tanto para el personal del departamento de informática como para los usuarios que utilizan los servicios informáticos, las cuales constan en un plan de capacitación informático, que sea formulado conjuntamente con la unidad de talento humano? *
- SI
- NO

Enviar

Nunca envíes contraseñas a través de Formularios de Google.

100 %: ¡Lo lograste!

FE 4

EMPRESA PÚBLICA – EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA
DEPARTAMENTO DE INFORMÁTICA

OBJETIVO: verificar si se establecen cambios de claves de acceso al sistema y correo electrónico durante un determinado período de tiempo.

USUARIO	¿Se tienen establecidas políticas de cambio de claves de acceso a los usuarios del sistema informático, correo electrónico u otro?		¿Cada qué tiempo se lo realiza?					Las contraseñas para el ingreso al sistema de información, correo entre otros se considera un sistema de seguridad:			¿El sistema informático de la empresa permite que las claves de acceso tengan caducidad y por tanto notificar al usuario que debe realizar dichos cambios?		OBSERVACIONES
	SI	NO	30 d	90 d	180 d	Año	Nunca	Alta	Media	Baja	SI	NO	
Secretaria de Gerente		✓					✓		✓			✓	Todos tienen lo mismo otros
Secretaria General		✓					✓		✓			✓	
Secretaria del Dep Tecnico		✓					✓			✓		✓	
Secretaria del Dep Financiero		✓					✓		✓			✓	
Secretaria de Juridico		✓					✓		✓		✓		
Secretaria Financiero		✓					✓			✓		✓	

Elaborado por:	Fecha:
W R P V	03-02-2014
Aprobado por:	Fecha:
R C	04-02-2014

FE 5

EMPRESA PÚBLICA – EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA
DEPARTAMENTO DE INFORMÁTICA
VERIFICACIÓN DE MEDIDAS DE SEGURIDAD FÍSICA

CARACTERÍSTICAS	DETALLE	CUMPLE		OBSERVACIÓN
		SI	NO	
La seguridad	Existe un circuito cerrado de cámaras en los laboratorios		✓	está realizando el proceso
	Existe una persona encargada de la seguridad "guardia" que custodie los bienes del departamento de informática	✓		
	El departamento de informática está en un lugar seguro.	✓		
	Posee puertas metálicas de protección.	✓		
	Existe salidas de emergencia		✓	
	Existe extintores de incendio	✓		
	Posee alarma		✓	
Los accesos	Existe un control físico adecuado del acceso a los servidores		✓	no existe en el departamento
	Se restringe el acceso a personas extrañas		✓	
El cableado	El cableado en toda la empresa se encuentra oculta		✓	
	Existe UPS que solvente la perdida de energía	✓		
Otros	Existe espacio exclusivo para servidores	✓		
	La unidad de informática cuenta con una empresa aseguradora		✓	no existe presupuesto
	Existe un lugar adecuado para el mantenimiento de los equipos	✓		
	Dispone de un sitio seguro para el almacenamiento de licencias de software	✓		

Elaborado por:	Fecha:
WRPY	03-02-2014
Aprobado por:	Fecha:
RC	04-02-2014

FE 6

EMPRESA PÚBLICA – EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA

DEPARTAMENTO DE INFORMÁTICA
CONDICIONES DE LOS SERVIDORES

Descripción	SI	NO	Observaciones
¿Funcionan todos los puntos de iluminación?	✓		
¿Independencia del interruptor eléctrico?	✓		
¿Adecuado nivel de luz eléctrica?	✓		
¿Existe Sistema de ventilación que mantenga una temperatura adecuada?	✓		
¿Ingresa polvo por las ventanas?	✓		
¿Afecta a los usuarios la temperatura?	✓		
¿Existe un registro de control de acceso físico?		✓	
¿Los servidores están libres de golpes?		✓	
¿Dispone de protección contra posibles sabotajes o virus?	✓		
¿Está exenta de ataques por internet?	✓		
¿Están en un espacio seguro?	✓		
¿Existen fallos en el diseño de la infraestructura tecnológica?	✓		

Elaborado por:	Fecha:
WRPV	04/02/2014
Aprobado por:	Fecha:
RC	05/02/2014

FE 7

AUDITORIA INFORMÁTICA A LA EMPRESA PÚBLICA – EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA
SOFTWARE DISPONIBLES EN LOS DEPARTAMENTOS - PERÍODO 2012

DIRECCIÓN O DEPARTAMENTO	NOMBRE DEL SOFTWARE	TIPO	LICENCIA	OBSERVACIONES
GERENCIA	LOTUS		SI	Todo el área
	Microsoft Office 2010		SI	"
	Adobe Reader X1			"
	OPEN OFFICE.ORG 3.4.			"
	Microsoft Project	Libre		"
	Kaspersky		SI	"
COMERCIAL	LOTUS		SI	Todo el área
	Microsoft office 2010		SI	Todo el área
	kaspersky		SI	Todo el área
	Adobe Reader X1		SI	"
	Exploradores de Internet			"
	Microsoft Project	Libre		"
TÉCNICA	LOTUS		SI	Todo el área
	Microsoft office 2010		SI	"
	Open office.org 3.1		SI	"
	Microsoft project	Libre		"
	kaspersky			"
	Microsoft project			"
	Adobe Reader X1		SI	"
JURIDICO	LOTUS		SI	Todo el área
	Microsoft office 2010		SI	"
	Microsoft project	Libre		"
	MS-office	Libre		"
	kaspersky		SI	"
	Microsoft project.			"
FINANCIERO/ ADMINISTRATIVO	LOTUS		SI	Todo el área
	Microsoft office 2010		SI	Todo el área
	SQL-SERVER	Libre		Dep Informática
	MySQL	Libre		"
	PHP	Libre		"
	Kaspersky		SI	Todo el área
	ASP	Libre		Dep Informática
INGENIERÍA	LOTUS		SI	Todo el área
	Microsoft office 2010		SI	"
	kaspersky		SI	"
	Autocad	Libre		"

Elaborado por:	Fecha:
WRPV	10/02/2014
Aprobado por:	Fecha:
RC	11/02/2014

FE 13

AUDITORIA INFORMÁTICA A LA EMPRESA PÚBLICA – EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA PERIODO 2012.

HOJA DE CUMPLIMIENTO DE CARACTERÍSTICAS DE SOFTWARE Y HARDWARE DE LOS DEPARTAMENTOS DE LA EMPRESA

N° de Máquina	PROCESADOR		DISCO DURO		MEMORIA RAM		SOFTWARE BASE		SOFTWARE DE ACUERDO A LOS DEPARTAMENTOS		ACCESO A INTERNET		PERIFÉRICOS	
IP	Cumple	No cumple	Cumple	No cumple	Cumple	No cumple	Cumple	No cumple	Cumple	No cumple	Cumple	No cumple	Cumple	No cumple
						GERENCIA								
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓		✓		✓	
						JURIDICO								
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓		✓		✓	
						COMERCIAL								
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓			✓	✓	
	✓		✓		✓		✓		✓		✓		✓	
						INGENIERÍA								
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓			✓	✓	
						FINANCIERA								
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓		✓		✓	
						TECNICA								
	✓		✓		✓		✓		✓		✓		✓	
	✓		✓		✓		✓		✓		✓		✓	

OBSERVACIONES: Se observo que en el departamento o dirección comercial en recaudación no disponen de internet, de igual forma en el dirección de ingeniería

Elaborado por:	Fecha:
WRPV	10-02-2014
Aprobado por:	Fecha:
RC	11-02-2014

Anexo 2: Funciones del Jefe de Sistemas

Art.15.- Del/a Jefe/a de Sistemas

a) Dirigir la implementación de proyectos informáticos en la EP-EMAPAR.
b) Coordinar la presentación de proyectos de innovación tecnológica para la Institución
c) Liderar la administración que permita mantener la operatividad y seguridad de los sistemas informáticos de la institución.
d) Formular y supervisar el cumplimiento de las normas de seguridad en los procesos informáticos correspondientes.
e) Brindar asistencia especializada en tecnología a todos los niveles y dependencias institucionales.
f) Generar políticas de administración de las cuentas y perfiles de usuarios de la red central institucional.

e) Autorizar la movilización interna o externa (con otras dependencias de la empresa) de los equipos de la EP-EMAPAR; e informar al Director Financiero, para el registro de la unidad encargada de Activos Fijos.
f) Autorizar la movilización fuera de predios de la empresa de los equipos de la institución solo cuando se trate de realizar reparaciones, que no se puedan realizar en el Departamento de Informática, SIG y Catastros, o en casos de suma exclusividad.

Anexo 3: Principales funciones y procedimientos de la Unidad de Tecnologías.

RESOLUCIÓN ADMINISTRATIVA

Ing. Carlos Velarde Humanante, Gerente General de la EP-EMAPAR, en uso de sus atribuciones legales.

CONSIDERANDO:

Que, la EP-EMAPAR ha experimentado un acelerado crecimiento informático que ha ocasionado un desarrollo heterogéneo de las dependencias de la empresa en cuanto a sus sistemas automatizados y sus equipos informáticos.

Que, el Departamento de Informática, SIG y Catastros, se encuentra desarrollando proyectos integrales tendientes a la modernización y mejoramiento de servicios que facilitarán el desarrollo de sistemas de información, a fin de responder a los retos de la tecnología, orientar los esfuerzos de información y optimizar el uso de los recursos informáticos, la racionalización de procesos, de fuentes de información, de equipos de computación y software de aplicación en las dependencias de la empresa.

Que, los niveles Ejecutivo y Operativo deben contar con herramientas de gestión, operación y control adecuadas que redunden en la optimización de los servicios internos y externos.

Que, es necesario reglamentar la administración y control de equipos, productos y servicios informáticos.

EXPIDE

LA SIGUIENTE RESOLUCIÓN ADMINISTRATIVA PARA LA ADMINISTRACIÓN Y CONTROL DE EQUIPOS, PRODUCTOS Y SERVICIOS INFORMÁTICOS, HARDWARE Y SOFTWARE

AMBITO DE APLICACIÓN

Art.1**.-** La presente resolución administrativa se la aplicará en las dependencias de la EP-EMAPAR, por parte de todos los funcionarios, empleados y obreros.

Art.2.- La ejecución y cumplimiento de la presente Resolución administrativa, será supervisado por los técnicos del Departamento de Informática, SIG y Catastros.

ESTANDARIZACIÓN DE SOFTWARE O PRODUCTOS DE APLICACIÓN

Art. 3.- Los productos informáticos existentes en el Mercado, que se han seleccionado y que constituyen el **estándar institucional son:**

DESCRIPCIÓN	PRODUCTO
Sistema Operativo de Red	√ Windows Server y/o Linux
Sistema Operativo de Estaciones de Trabajo	√ Windows x y/o Linux
Herramientas de Escritorio Ms-office 97 en adelante	Microsoft Office, como alternativa Open Office, y equivalentes en Software Libre
Las Dependencias que requieran para intercambio de información interinstitucional	√ Ms-office, equivalentes en Software Libre
Herramientas de Desarrollo Institucional Manejador de Bases de Datos Lenguaje de Programación	Postgres, SQL-SERVER, MySQL, equivalentes en Software Libre PHP, ASP, equivalentes en Software Libre
Manejador de Proyectos	√ Microsoft Project equivalentes en Software Libre
Antivirus y utilitarios	√ Kaspersky
Diagramador de Flujos	√ Visio y/o equivalentes en Software Libre
Graficador	√ Software Libre
Publicidad	√ Software Libre
Digitalización	√ ArcGis, ArchiCad, Autocad y/o equivalentes en Software Libre

Se entenderá como "Software Libre", programas informáticos de código abierto, el uso de programas de estándares abiertos y basados en trabajo comunitario.

a) Si alguna dependencia necesita incorporar productos de aplicación informáticos de uso específico que no hayan sido considerados en los estándares antes referidos, comunicará su requerimiento al Departamento de Informática, SIG y Catastros para su análisis y aprobación y/o recomendación; igual criterio se aplicará con el software de distribución gratuita, incluyendo aquellos que se obtienen a través de Internet, se propenderá al uso de Software Libre (no licenciado), guiados en el Decreto Presidencial No. 1014 de 10 de abril del 2008..

b) Para el tratamiento de la información de uso Institucional se utilizarán los sistemas de información existentes en el computador central y de no existir la aplicación específica requerida, se solicitará la intervención del Departamento de Informática, SIG y Catastros a fin de planificar su desarrollo o viabilizar su adquisición; y,

c) Toda adquisición o renta de software, contratación de servicios y soluciones informáticas o proyectos especiales relacionados al tema, deberán contar con la aprobación del Departamento de Informática, SIG y Catastros.

DE LAS ADQUISICIONES

Art.4.- El Departamento de Informática, SIG y Catastros será la unidad responsable de analizar los requerimientos de equipos o productos de aplicación informáticos, tanto de hardware como de software de las dependencias de la empresa, y someterlos a la aprobación por parte del Señor Gerente General. Las adquisiciones podrán ser:

a) ADQUISICIONES PLANIFICADAS: Aquellas que deberán constar en el presupuesto de cada año como resultado de la elaboración del plan anual de adquisiciones aprobado dentro del Plan Operativo del Departamento de Informática, SIG y Catastros, en el que se recogerán los requerimientos formulados por las dependencias de la empresa y su análisis correspondiente.

Para generar el Plan Anual de Adquisiciones, los pedidos deberán estar dirigidos al Departamento de Informática, SIG y Catastros hasta el mes de septiembre de cada año, para el análisis y elaboración del Informe Técnico correspondiente.

b) ADQUISICIONES NO PLANIFICADAS: Aquellas solicitudes de requerimientos que se enmarcan en proyectos especiales o necesidades que no fueron incluidas en el Plan Operativo Anual. El Departamento de Informática, SIG y Catastros elaborará los informes y enviará para el trámite correspondiente.

Art.5.- El Departamento de Informática, SIG y Catastros sustentará sus informes en la realización de un análisis operativo que determinará la factibilidad o no de compra, renta y/o renovación de hardware y software, que serán puestos en consideración de la Dirección de Ingeniería.

Art.7.- El Departamento de Informática, SIG y Catastros será quien emita los informes de verificación de características técnicas de los equipos recibidos en bodega frente a las características técnicas solicitadas, procedimiento que debe hacerlo a los equipos y/o dispositivos adquiridos, previo a su pago y distribución.

ANÁLISIS TÉCNICO OPERATIVO

Art.8.- El Departamento de Informática, SIG y Catastros será el responsable de realizar análisis operativos de las dependencias de la empresa y elaborar el informe técnico, previo a la provisión de equipos, dispositivos y/o productos de aplicación informáticos.

Los parámetros que se aplicarán en el análisis técnico operativo serán los siguientes:

a) El número de equipos instalados y sus características técnicas.
b) Las funciones de los usuarios requirentes.
c) Los productos de aplicación instaladas en cada uno de los equipos.
d) Los volúmenes, frecuencia y carga de trabajo.
e) El cumplimiento de normas y procedimientos estándar en vigencia.
f) El nivel y las frecuencias de uso de las herramientas y sistemas operativos instalados.
g) Las capacidades de memoria y de almacenamiento requeridos para cada uno de los equipos en función de las tareas que se desarrollan.

g) Los niveles de seguridad en el manejo de equipos y/o información, las seguridades de acceso, las instalaciones físicas y los procedimientos de respaldo.
h) Los requerimientos no satisfechos en equipos, en productos de aplicación y en seguridades.

REDISTRIBUCIÓN DE EQUIPOS Y RACIONALIZACIÓN DE PRODUCTOS

Art.9.- Si el informe del análisis técnico determina que existen equipos subutilizados o equipos que requieren de mayor capacidad para desarrollar las actividades de una área o tarea específica. El Departamento de Informática, SIG y Catastros procederá con la redistribución de equipos o racionalización de los productos instalados o adquiridos de acuerdo a su necesidad.

Art.10.- El Departamento de Informática, SIG y Catastros estará facultado para realizar la **REDISTRIBUCIÓN INTERNA O EXTERNA (**con otras dependencias de la empresa) de los equipos y la racionalización de productos determinada en el informe técnico.

Art.11.- La **REDISTRIBUCIÓN** de equipos podrá realizarse antes y/o después de la provisión o renovación de equipos.

DE LAS REDES

Art l2**.-** El Departamento de Informática, SIG y Catastros efectuará la evaluación respectiva en cada una de las unidades administrativas a fin de:

a) Construir redes locales en cada una de las dependencias de la empresa e integrarlas a la Intranet institucional.

b) Implementar el software de aplicación necesario para el buen funcionamiento de las redes locales y la comunicación con las demás redes de la institución.
c) Incorporar a la red institucional los servidores y software de aplicación necesaria para implementar los servicios considerados de uso general en la EP-EMAPAR tales como, Internet y Correo Electrónico.
d) Incorporar en lo posible al Backbone Central los servidores existentes en otras dependencias de la empresa.
e) Proporcionar a los usuarios de las redes locales los servicios de Internet, Correo Electrónico y cuando el caso lo amerite, integrarlas a los servicios de la red del Computador Central, aplicando las seguridades necesarias a fin de proteger la información de la EP-EMAPAR.

DEL SERVICIO DE CORREO ELECTRÓNICO

Art. 13.- El personal de la EP-EMAPAR en todos los niveles, están obligados a utilizar sus cuentas de correo electrónico institucional para realizar la comunicación interna, y/o el sistema documental oficial que se encuentra en la empresa.

DE LA PROPIEDAD INTELECTUAL EP-EMAPAR

Art.17.- Es de propiedad intelectual de la EP-EMAPAR los sistemas de información, aplicaciones (programas ejecutables) y los componentes derivados de su desarrollo (programas fuentes), efectuados por el personal de la institución durante el ejercicio de sus funciones, utilizando los recursos informáticos instalados en las dependencias de la empresa, así como, toda la documentación y manuales generada para el efecto.

DE LAS PROHIBICIONES

Art.18.- Se prohíbe a los funcionarios, empleados, obreros; responsables de los recursos informáticos de la EP-EMAPAR:

a) Instalar o usar productos de aplicación sin licencia de uso certificada (documento original) para la EP-EMAPAR.
b) Permitir el uso de los equipos a personas extrañas a la EP-EMAPAR.
c) Utilizar los equipos en actividades no relacionadas con las inherentes a la EP-EMAPAR.
d) Reproducir, duplicar, copiar o utilizar sistemas de propiedad EP-EMAPAR o productos de aplicación instalados en los servidores y estaciones de trabajo de las dependencias de la empresa.
e) Movilizar fuera del departamento, unidad o de la institución los equipos y/o dispositivos de computación, productos de aplicación y sistemas de información e informáticos de propiedad de la EP-EMAPAR.
f) Realizar trámites de adquisición de equipos y/o suministros informáticos sin la Autorización del Departamento de Informática, SIG y Catastros.
g) Instalar y utilizar juegos en los equipos de computación de la EP-EMAPAR.
h) Ceder o dar a conocer a segundas personas, las claves registradas para el acceso a equipos y/o software informático perteneciente a la EP-EMAPAR, ya que las claves utilizadas son personales e intransferibles, para uso de personal no Autorizado.

DE LAS SANCIONES

Art 19**.-** El incumplimiento de las disposiciones contenidas en la presente Resolución Administrativa, por parte de los funcionarios, empleados, obreros; responsables de los recursos informáticos de la EP-EMAPAR, será sancionado aplicando los artículos del Capítulo VIII correspondiente al Régimen Disciplinario de la Ley de Servicio Civil y Carrera Administrativa, de acuerdo a la gravedad de la falta cometida.

Art.20.- Se aplicarán las sanciones de AMONESTACIÓN ESCRITA de acuerdo al Artículo 62 de la Ley de Servicio Civil y Carrera Administrativa, por cualquiera de las siguientes causales:

a) Utilizar los equipos de computación o productos de aplicación en actividades no relacionadas con las inherentes a la EP-EMAPAR;
b) No apagar los equipos computacionales luego de cumplir con la jornada de trabajo;
c) Sacar de la institución documentación e información relacionada con productos de aplicación informática sin la Autorización respectiva.

d) Ceder de forma deliberada claves personales.
e) Instalar y utilizar juegos en los equipos de computación de la EP-EMAPAR.

Art. 21.- Será sancionado con MULTA de acuerdo al Artículo 62, de la Ley de Servicio Civil y Carrera Administrativa, el servidor que incurra en cualquiera de las siguientes faltas:

a) Instalar o usar productos de aplicación sin licencia de uso certificada para la EP-EMAPAR.; y
b) Reincidir en las faltas enumeradas en el artículo anterior.

Art.22.- Se impondrá la sanción de SUSPENSIÓN TEMPORAL de acuerdo al Artículo 62 de la Ley de Servicio Civil y Carrera Administrativa, en los siguientes casos:

a) Reproducir, duplicar, copiar o utilizar sistemas informáticos o productos de aplicación instalados en los servidores o estaciones de trabajo de las dependencias de la empresa para uso personal, no relacionado con las actividades de la institución;
b) Acción u omisión de las responsabilidades establecidas en el presente reglamento que perjudique la prestación de los servicios públicos institucionales que brinda la EP-EMAPAR.
c) Movilizar fuera del Departamento o Predios Institucionales equipos electrónicos o dispositivos computacionales de propiedad de la EP-EMAPAR y que estén se encuentren con daños por ésta causa.
d) Reincidir en las faltas enumeradas en el artículo anterior.
e) Incapacidad, negligencia o falta de probidad en el desempeño de la responsabilidades asignadas en el manejo de los recursos informáticos de acuerdo a la presente Resolución Administrativa, debidamente comprobadas;
a) Ocasionar daños intencionales a los equipos computacionales y/o equipo electrónico de la EP-EMAPAR.
b) Reincidir en una infracción de la presente Resolución Administrativa sancionada con suspensión temporal

DE LA DIFUSIÓN DE LA PRESENTE RESOLUCIÓN ADMINISTRATIVA

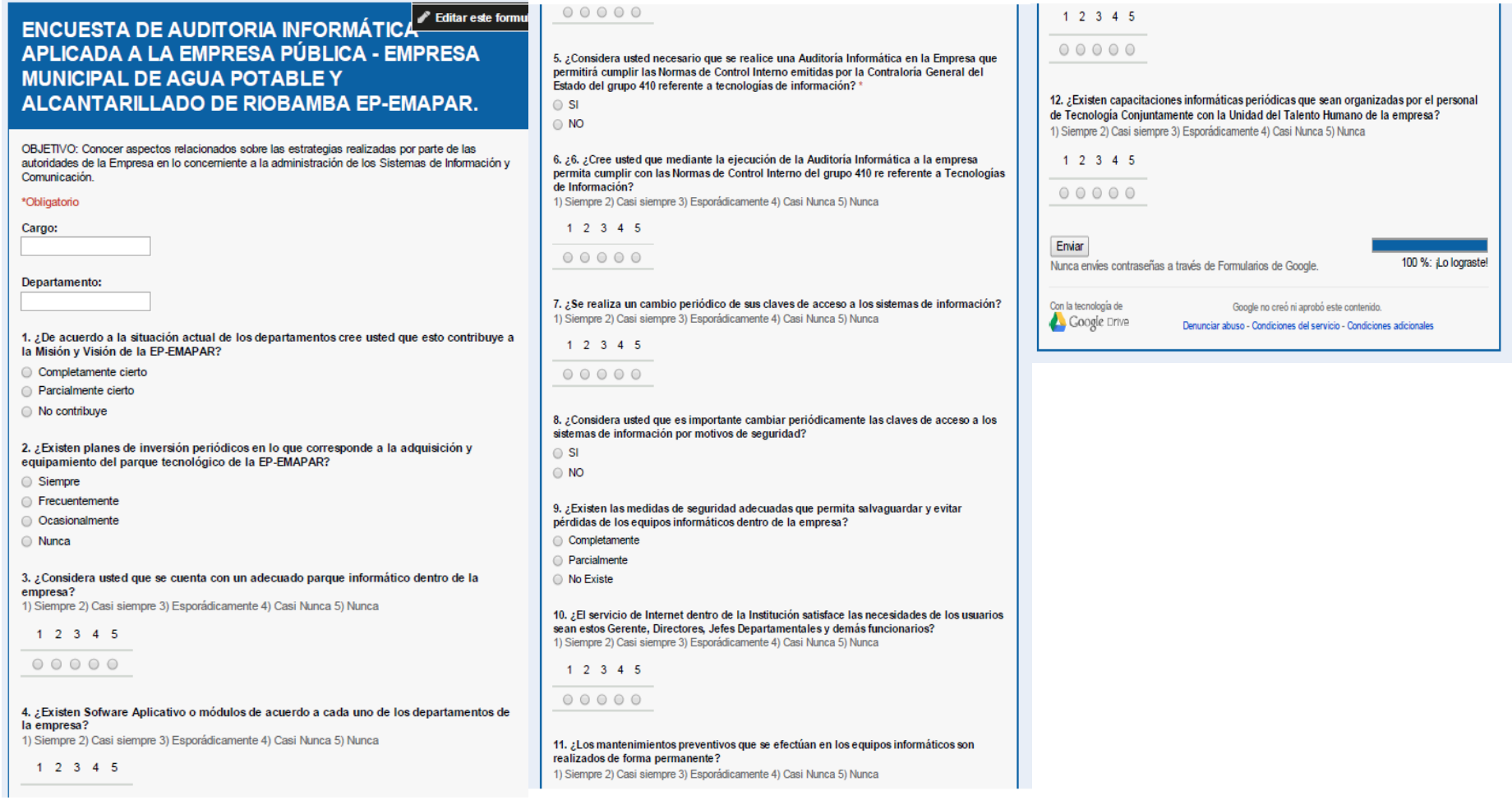
Art.24**.-** Con el objeto de garantizar la aplicación y cumplimiento de la presente Resolución Administrativa, se encargará al Departamento de Informática, SIG y Catastros y a la Jefatura de Personal los mismos que harán conocer a los funcionarios, empleados y obreros de todas las dependencias de la empresa.

COMUNIQUESE:

Riobamba, 3 de octubre de 2012

Ing. Carlos Velarde Humanante
GERENTE GENERAL DE LA EP-EMAPAR

Anexo 4: Modelo de escueta para el análisis FODA aplicada a Gerente, Directores, Jefes y demás usuarios del parque informático



ENCUESTA DE AUDITORIA INFORMÁTICA APLICADA A LA EMPRESA PÚBLICA - EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA EP-EMAPAR.

Editar este formu

OBJETIVO: Conocer aspectos relacionados sobre las estrategias realizadas por parte de las autoridades de la Empresa en lo concerniente a la administración de los Sistemas de Información y Comunicación.

*Obligatorio

Cargo:

Departamento:

1. ¿De acuerdo a la situación actual de los departamentos cree usted que esto contribuye a la Misión y Visión de la EP-EMAPAR?
- Completamente cierto
- Parcialmente cierto
- No contribuye

2. ¿Existen planes de inversión periódicos en lo que corresponde a la adquisición y equipamiento del parque tecnológico de la EP-EMAPAR?
- Siempre
- Frecuentemente
- Ocasionalmente
- Nunca

3. ¿Considera usted que se cuenta con un adecuado parque informático dentro de la empresa?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

4. ¿Existen Sofware Aplicativo o módulos de acuerdo a cada uno de los departamentos de la empresa?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

5. ¿Considera usted necesario que se realice una Auditoría Informática en la Empresa que permitirá cumplir las Normas de Control Interno emitidas por la Contraloría General del Estado del grupo 410 referente a tecnologías de información? *
- SI
- NO

6. ¿6. ¿Cree usted que mediante la ejecución de la Auditoría Informática a la empresa permita cumplir con las Normas de Control Interno del grupo 410 re referente a Tecnologías de Información?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

7. ¿Se realiza un cambio periódico de sus claves de acceso a los sistemas de información?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

8. ¿Considera usted que es importante cambiar periódicamente las claves de acceso a los sistemas de información por motivos de seguridad?
- SI
- NO

9. ¿Existen las medidas de seguridad adecuadas que permita salvaguardar y evitar pérdidas de los equipos informáticos dentro de la empresa?
- Completamente
- Parcialmente
- No Existe

10. ¿El servicio de Internet dentro de la Institución satisface las necesidades de los usuarios sean estos Gerente, Directores, Jefes Departamentales y demás funcionarios?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

11. ¿Los mantenimientos preventivos que se efectúan en los equipos informáticos son realizados de forma permanente?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

12. ¿Existen capacitaciones informáticas periódicas que sean organizadas por el personal de Tecnología Conjuntamente con la Unidad del Talento Humano de la empresa?
1) Siempre 2) Casi siempre 3) Esporádicamente 4) Casi Nunca 5) Nunca

1 2 3 4 5

Enviar

Nunca envíes contraseñas a través de Formularios de Google.

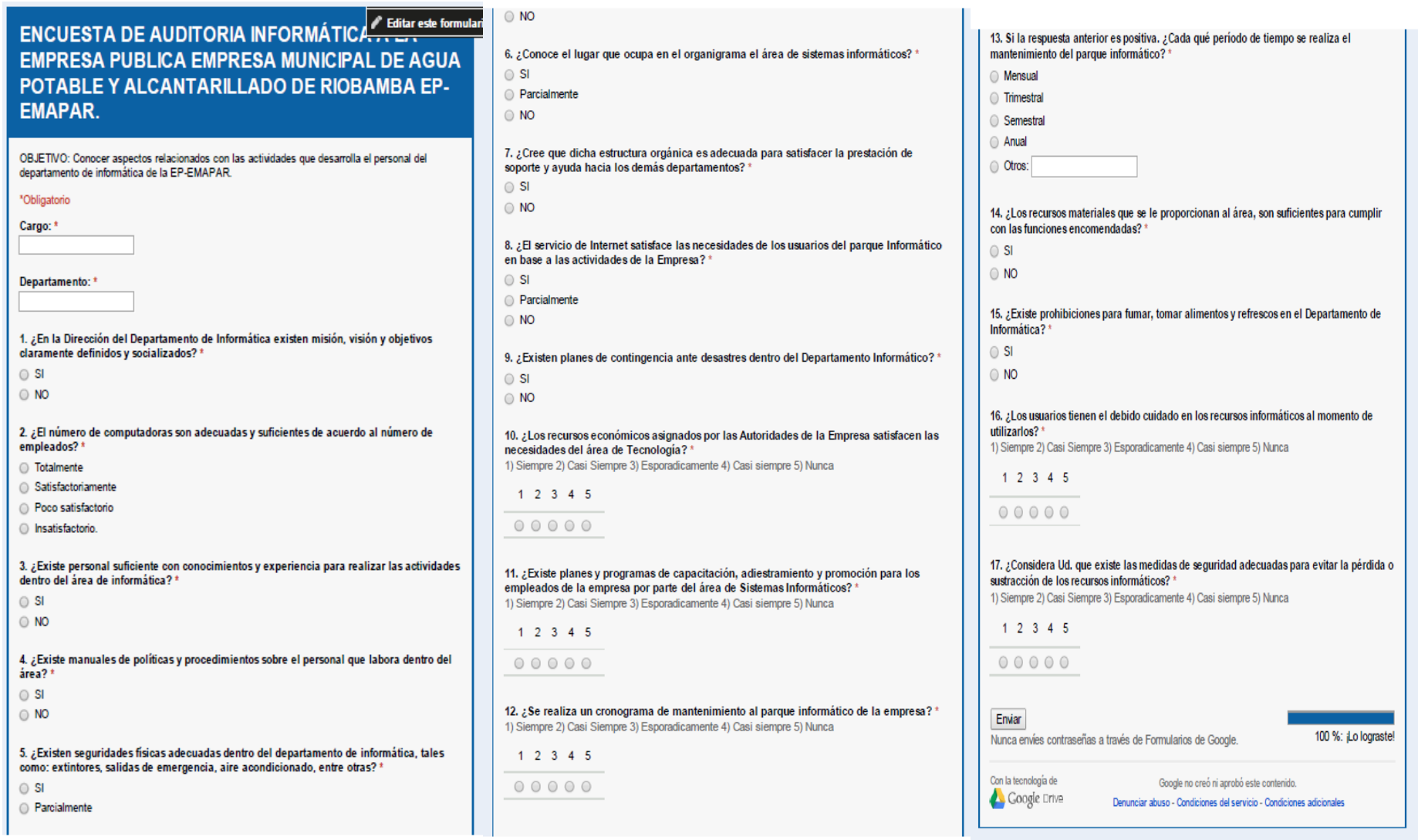
100 %: ¡Lo lograste!

Con la tecnología de Google Drive

Google no creó ni aprobó este contenido.

Denunciar abuso - Condiciones del servicio - Condiciones adicionales

Anexo 5: Modelo de encuestas para el análisis FODA aplicada a los funcionarios del departamento de Informática.



Editar este formulario

ENCUESTA DE AUDITORIA INFORMÁTICA A LA EMPRESA PUBLICA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA EP-EMAPAR.

OBJETIVO: Conocer aspectos relacionados con las actividades que desarrolla el personal del departamento de informática de la EP-EMAPAR.

*Obligatorio

Cargo: *

Departamento: *

1. ¿En la Dirección del Departamento de Informática existen misión, visión y objetivos claramente definidos y socializados? *
- SI
- NO

2. ¿El número de computadoras son adecuadas y suficientes de acuerdo al número de empleados? *
- Totalmente
- Satisfactoriamente
- Poco satisfactorio
- Insatisfactorio.

3. ¿Existe personal suficiente con conocimientos y experiencia para realizar las actividades dentro del área de informática? *
- SI
- NO

4. ¿Existe manuales de políticas y procedimientos sobre el personal que labora dentro del área? *
- SI
- NO

5. ¿Existen seguridades físicas adecuadas dentro del departamento de informática, tales como: extintores, salidas de emergencia, aire acondicionado, entre otras? *
- SI
- Parcialmente
- NO

6. ¿Conoce el lugar que ocupa en el organigrama el área de sistemas informáticos? *
- SI
- Parcialmente
- NO

7. ¿Cree que dicha estructura orgánica es adecuada para satisfacer la prestación de soporte y ayuda hacia los demás departamentos? *
- SI
- NO

8. ¿El servicio de Internet satisface las necesidades de los usuarios del parque Informático en base a las actividades de la Empresa? *
- SI
- Parcialmente
- NO

9. ¿Existen planes de contingencia ante desastres dentro del Departamento Informático? *
- SI
- NO

10. ¿Los recursos económicos asignados por las Autoridades de la Empresa satisfacen las necesidades del área de Tecnología? *
1) Siempre 2) Casi Siempre 3) Esporadicamente 4) Casi siempre 5) Nunca

1 2 3 4 5

11. ¿Existe planes y programas de capacitación, adiestramiento y promoción para los empleados de la empresa por parte del área de Sistemas Informáticos? *
1) Siempre 2) Casi Siempre 3) Esporadicamente 4) Casi siempre 5) Nunca

1 2 3 4 5

12. ¿Se realiza un cronograma de mantenimiento al parque informático de la empresa? *
1) Siempre 2) Casi Siempre 3) Esporadicamente 4) Casi siempre 5) Nunca

1 2 3 4 5

13. Si la respuesta anterior es positiva. ¿Cada qué período de tiempo se realiza el mantenimiento del parque informático? *
- Mensual
- Trimestral
- Semestral
- Anual
- Otros:

14. ¿Los recursos materiales que se le proporcionan al área, son suficientes para cumplir con las funciones encomendadas? *
- SI
- NO

15. ¿Existe prohibiciones para fumar, tomar alimentos y refrescos en el Departamento de Informática? *
- SI
- NO

16. ¿Los usuarios tienen el debido cuidado en los recursos informáticos al momento de utilizarlos? *
1) Siempre 2) Casi Siempre 3) Esporadicamente 4) Casi siempre 5) Nunca

1 2 3 4 5

17. ¿Considera Ud. que existe las medidas de seguridad adecuadas para evitar la pérdida o sustracción de los recursos informáticos? *
1) Siempre 2) Casi Siempre 3) Esporadicamente 4) Casi siempre 5) Nunca

1 2 3 4 5

Enviar

100 %: ¡Lo lograste!

Nunca envíes contraseñas a través de Formularios de Google.

Con la tecnología de Google Drive

Google no creó ni aprobó este contenido.

Denunciar abuso - Condiciones del servicio - Condiciones adicionales

ANEXO 6: ARTÍCULO DE LA INVESTIGACIÓN

"AUDITORÍA INFORMÁTICA A LA EMPRESA PÚBLICA- EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE RIOBAMBA, PERÍODO 2012".

Washigton Rolando Peralta Villacrés,
rolando_auditor@hotmail.com,

RESUMEN

La presente investigación es una "Auditoria Informática a la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012". Encaminada en el desarrollo y análisis de Seguridad Lógica, Seguridad Física, Utilización y aprovechamiento de Tecnologías de Información y Comunicación y Gestión Informática. Antes de realizar la auditoria se realizó un análisis previo a la empresa, en donde se obtuvo un conocimiento de la misma. Con este análisis previo se elaboró una planificación adecuada, permitiendo integrar los programas correspondientes a las diferentes áreas de análisis; en donde se aplicó técnicas y procedimientos de auditoría prevista en el marco teórico, considerando las Normas de Control Interno grupo 410, emitidas por la Contraloría General del Estado. Como resultado de la Auditoria Informática tenemos la falta de políticas sobre actualización periódica de claves de acceso a los sistemas y eliminación de archivos, ausencia de medidas adecuadas de seguridad física en la Unidad de Informática, falta de capacitación informática, inadecuada segregación de funciones. Recomendando a la EP-EMAPAR tomar en cuenta los aspectos estipulados en el informe de Auditoría. Y aplicar cada año una auditoria Informática, para medir el grado de cumplimiento de las Normas de Control Interno emitidas por la CGE.

ABSTRACT

This research work is a "Computer Processes Audit done to the Public Municipal Water Supply and Sewerage Company of Riobamba (EP-EMAPAR- acronym for the Spanish Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba) during 2012." It is aimed to promote the development and analysis of logical security, physical security, procedure and good use of information and communication technologies, and computer systems management. Before doing the audit, a previous analysis was carried out in the enterprise in order to get acquainted with it. With this previous analysis, an adequate planning was done by integrating the corresponding programs in the different analyzed areas. Here, different techniques and produces described in the theoretical framework were applied considering the Internal Control Regulations group 410 given by General State Comptroller. As a result of this Computer Process Audit, it can be seen there is lack of policies about changing password periodically and file deleting; there is also, lack of adequate physical security in the Computer Systems Unit; there is lack of computer use training, and inadequate duties segregation. It is recommended that EP-EMAPAR consider the different aspects prescribed in the audit report and do a yearly computer processes audit to see the degree of compliance they have of the Internal Control Regulations given by the General State Comptroller.

INTRODUCCIÓN

A partir de los años 50, la informática se convierte en una herramienta muy importante en las labores de auditoría, que permite llevar a cabo, de forma rápida y precisa, operaciones que manualmente consumirían demasiados recursos. En los años 60 ya se comete el primer delito con la computadora por tal motivo ya se inicia con la auditoría del ordenador. Actualmente la información a más de ser ya un activo principal es el centro de estrategias productivas más importante en las instituciones tanto públicas como privadas, por ello en la Empresa Pública – Empresa Municipal de Agua Potable y Alcantarillado de Riobamba no se ha realizado una auditoria informática que mida el grado de cumplimiento de las normas de control interno sobre Tecnologías de Información, del grupo 410 emitidas por la

Contraloría General del Estado. Generando así un nivel de perplejidad en el cumplimiento de dichas normas.

Auditoría Informática: Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y de más componentes. (Muñoz Razo , 2002. P., pág. 23).

Dentro del marco hipotético se determina que al realizar la Auditoría informática, a la Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Riobamba, período 2012, permitirá el cumplimiento de las Normas de Control Interno del grupo 410 emitidos por la Contraloría General del Estado.

Se desarrolla un diagnóstico de los aspectos generales de la empresa en base a estos se ejecuta la auditoria informatica iniciando en un plan de trabajo para la obtencion de evidencias suficientes y pertinenetes y por ultimo se emitió un informe final proponiendo mejoras y soluciones a los hallazgos encontrados sobre la utilizacion eficiente y segura de la infromacion para una adecuada toma de decisiones.

INSTRUMENTOS DE RECOPILACIÓN DE INFORMACIÓN DENTRO DE AUDITORÍA INFORMÁTICA.

El auditor debe aprovechar las técnicas de Inspección como un contacto inicial y especifico de las áreas de análisis, Revisión Documental del control interno de la empresa y análisis FODA donde se hizo un análisis minucioso de los medios internos y los medios externos traducido en Fortalezas, Oportunidades, Debilidades y Amenazas. Procedimientos y herramientas tradicionales de auditoría aplicables en la auditoría informática; el propósito es que se diseñó y se utilizó para hacer una evaluación correcta del funcionamiento de dicha área, de la operación del propio sistema o de su gestión informática, beneficiándose con ello debido a la ya aprobada eficiencia y eficacia en otros tipos de auditoría entre las cuales tenemos los siguientes instrumentos:

- ✓ Entrevistas.- se realizó al Gerente, Directores departamentales y Jefe de Informática.
- ✓ Cuestionarios.- se hizo una lista de preguntas donde se seleccionaron las más adecuadas para el tratamiento de la auditoría.
- ✓ Encuestas.- se aplicó en temas de seguridad física, seguridad lógica, Tecnologías de Información y Comunicación y Gestión Informática.
- ✓ Observación.- se aplicó en la verificación de las instalaciones de la institución en temas relacionados con mobiliario, estado de los equipos periféricos, funciones de los empleados entre otros.
- ✓ Inventarios.- se trató de verificar el listado de equipos periféricos en toda la empresa.

CONCLUSIÓN

En la investigación se realizó un análisis previo a la empresa donde se obtuvo un conocimiento del área crítica motivo de análisis. En base al análisis FODA que arrojó como resultado el 2,36 indica que existen más debilidades de fortalezas dando la base necesaria y justificación para el desarrollo y aplicación de la auditoria informática. Cabe resaltar en el ámbito de medios externos tiene un promedio del 2,86 indica que la empresa tiene más oportunidades que amenazas lo cual podría beneficiarse disponiendo de software de acuerdo a los diferentes departamentos, de manera que pueda contribuir a mejorar la calidad de las actividades de la empresa.

Como resultado de la Auditoria Informática tenemos la falta de políticas sobre actualización periódica de claves de acceso a los sistemas y eliminación de archivos, ausencia de medidas adecuadas de seguridad física en la Unidad de Informática, falta de capacitación informática, inadecuada segregación de funciones. Ausencia de un inventario donde se determine el saldo real de los equipos informáticos periféricos.

RECOMENDACIONES

- ✓ Aplicar las normas de control interno emitidas por la Contraloría General del Estado del grupo 410, en lo referente a Tecnologías de Información y Comunicación para que existan mejoras en la gestión informática.
- ✓ Definir políticas en la actualización periódica de las claves de acceso de los usuarios al sistema de información así como también políticas para el desecho y eliminación de información cuando ya no se considere necesario su uso y así mejorar eficientemente los procesos tecnológicos.
- ✓ Establecer medidas de seguridad física adecuadas para proteger y salvaguardar los bienes informáticos especialmente los del departamento de informática de la empresa para evitar posibles robos, fuga de información y sabotajes.
- ✓ Aplicar Auditorías Informáticas anuales que permitan el buen cumplimiento de las Normas de Control Interno emitidas por la Contraloría General del Estado, tomando ampliamente como referencia no solo las NCI de la CGE sino las TICs y modelo COBIT.

REFERENCIAS

- ✓ EcheniqueG., J. A. (2008). Auditoría en informática. En J. A. García, *Auditoría en Informática* (págs. 26-27). México: Mc GRAW-HILL/INTERAMERICANA EDITORES, S.A. de C.V.
- ✓ Mario Piattini Velthuis, Emilio del Peso Navarro, & Mar del Peso Ruiz. (2008). *Auditoría de Tecnologías y Sistemas de Información.* México D.F.: C. 2008 Alfaomega Grupo Editor, S.A. de C.V.
- ✓ Muñoz Razo , C. (2002. P.). *Auditoría en Sistemas Computacionales.* Juárez - México: D.R. C. 2002 por Pearson Educación México, S.A. de C.V.
- ✓ Vandama N., Lescay M., & García F. . (2002). *Auditoría Informática en ETECSA.* Obtenido de http://espejos.unesco.org.uy/simplac2002/Ponencias/Segurm%E1tica/VIR024.doc
- ✓ Normas de Control Interno Grupo 410 referente a tecnologías de información, emitidas por la Contraloría General del Estado. (2009) http://www.contraloria.gob.ec/normatividad_vigente.asp