UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERÍA EN SISTEMAS INFORMÁTICOS

TEMA: AUDITORÍA INFORMÁTICA A LA EMPRESA ECUA-MAILS

AUTOR: Adrián Patricio Pulgarín Álvarez

TUTOR: Ing, Paul Villavicencio Zambrano, Msc

AÑO: 2016

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, **Ing. Paul Villavicencio Zambrano**, certifico que el señor Adrián Patricio Pulgarín Álvarez con C.I, No. 0103867925 realizó la presente tesis con el título **"AUDITORÍA INFORMÁTICA A LA EMPRESA ECUA-MAILS",** y que es autor intelectual del mismo, que es original, auténtico y personal.

_____

Ing. Paul Villavicencio Zambrano.

CERTIFICADO DE AUTORÍA

El documento de tesis con título: "**AUDITORÍA INFORMÁTICA A LA EMPRESA ECUA-MAILS**", ha sido desarrollado por el señor Adrián Patricio Pulgarín Álvarez con C.I, No. 0103867925 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Adrián Patricio Pulgarín Álvarez

DEDICATORIA

La presente tesis va dedica a Dios quién me ayudo a seguir adelante ante las adversidades, porque sin él no sé dónde estaría ni que sería de mí.

A mis padres Luis y Dunia que confiaron en mí, a mi madre que desde el cielo me ha guiado para alcanzar este objetivo y a mi padre que, a pesar de no contar con los medios económicos suficientes, me apoyo incondicionalmente en el transcurso de esta etapa educativa.

A mi esposa Diana, que con paciencia a soportado cada momento que no he podido pasar y disfrutar a su lado por encontrarme en esta labor, y por ese apoyo incondicional que me brinda para forjar mi futuro y salir adelante.

Y a mis familiares cercanos que de una u otra manera han contribuido para alcanzar esta meta, mención especial a mis Tías: Betty y Rosa, que ha falta de una madre me han apoyado y confiado en mí como si fuese un hijo y esta tesis también es un logro de ellas.

AGRADECIMIENTO

Siempre estaré agradecido a aquellas personas que con su granito de arena forjaron y contribuyeron la realización de este trabajo de grado, a Dios por la vida que me dio y a la vida misma que me forjo como una persona de bien.

Al Ing. Paul Villavicencio y Tannia Mayorga un agradecimiento enorme por su asistencia incondicional en el desarrollo de esta tesis.

RESUMEN

La tesis tiene como objetivo principal la realización de auditoría informática a la empresa Ecua-Mails, dedicada a la importación y distribución de equipos informáticos en la ciudad de Cuenca.

Partiendo de que realizar una auditoría no solo informática sino general en una empresa es fundamental para mejorar la eficacia y eficiencia de la misma, es fácil darnos cuenta del porque se ha elegido este tema de investigación, ya que cada vez más en un mundo tan moderno y competitivo en el que vivimos es necesario implementar nuevas tecnologías y procesos que ayuden a conocer el estado actual de una empresa y por consiguiente mejorarlo.

En la actualidad es indispensable detectar los procesos de la empresa Ecua-Mails para detectar posibles problemas de los mismos y recomendar las posibles soluciones a aquellos problemas para mejorar la eficacia y eficiencia.

Con la clasificación, definición y documentación correspondiente de cada uno de ellos se puede obtener una mejor disposición y una correcta utilización de la información, de esta manera se puede realizar en orden las tareas y definir los responsables de cada una de ellas, lo que conlleva a una mejor ejecución del trabajo y que las tareas pendientes se realicen de la forma más eficiente posible.

Disponiendo de las técnicas y procesos para llevar a cabo una auditoría informática en la empresa, se tienen las herramientas necesarias para tener un análisis completo de la empresa así como las recomendaciones necesarias para mejorar los procesos de la misma, así como también mejorar la imagen de la empresa, generar confianza entre los usuarios sobre los productos ofertados

por la empresa, optimización del clima de trabajo y las relaciones internas de los empleados, generar un reporte de riesgos de TI.

Lo procesos que maneja la empresa están basados en un orden jerárquico siguiendo un organigrama de funciones, para así mantener un respectivo orden.

Para el desarrollo de la Auditoría Informática a la empresa, se recurrió al Framework COBIT que está ampliamente extendido y el cual es una guía de las mejores prácticas para el control y supervisión del TI en la empresa.

La versión de COBIT usada es la 5.0 la última publicada y la cual se basa en COBIT 4.1 pero añade marcos y normas como ITIL y las normas ISO de esta.

Con ello se tendrá un informe de guía que informará las mejores prácticas para la administración de los procesos de TI en la empresa Ecua-Mails

Palabras claves: auditoria, cobit, procesos, informática

ABSTRACT

The main objective of this thesis is to make an informatics audit to the Ecua-Mails company, which dedicates to the importation and distribution of informatics equipment in the city of Cuenca.

Starting with that making a general audit in a company is fundamental to improve its efficacy and efficiency, it is easy to realize why this research topic has been chosen, because in the modern and competitive world in which we live it is necessary to implement new technologies and processes to help finding out the current status of a company and improve it thereafter.

Nowadays it is essential to detect the processes of the Ecua-Mails company to detect possible problems with them and recommend possible solutions to those problems to improve efficacy and efficiency.

With the corresponding classification, definition and documentation of each of them, we can get a better provision and correct use of the information, in this manner the tasks can be done in order and the responsible of each one can be defined, which leads to a better execution of the work and the tasks to be made as efficient as possible.

Counting with the techniques and processes to undertake an informatics audit in the company, we have the necessary tools to make a complete analysis of the company as well as the necessary recommendations to improve its processes, as well as also improving the image of the company, generate thrust amongst the users of the products offered by the company, optimization of the

job environment and internal relationship of the employees, generate an IT risk report.

The processes that the company handles are based on a hierarchical order following a function organigram, to keep the order.

For the development of the informatics audit of the company, we resorted to the COBIT Framework which is widely extended and which is a guide of the best practices for the control and supervision of IT in the company.

The version of COBIT used is 5.0, the latest published, which is based on COBIT 4.1 but adds frames and norms such as ITIL and ISO.

With them we'll have a guide report which will inform on the best practices for the administration of the processes of IT in the Ecua-Mails company.

Keywords: audit, COBIT, processes, IT

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

CAPÍTULO 1

INTRODUCCION

I. Planteamiento del problema

1.1. Definición del problema de investigación

En la empresa Ecua-Mails de la ciudad de Cuenca no existe un control sobre los procesos que se manejan en la empresa, así como un plan para mejorar los mismos. Dicha empresa está conformada por 14 personas distribuidas en diferentes áreas desde la gerencia pasando por el equipo de programación hasta llegar a los ejecutivos de ventas y secretaria. Pero no se sabe con certeza que procesos son los que están fallando ya que de un tiempo para acá han bajado considerablemente la calidad de sus productos informáticos los cuales radican en el desarrollo de software, desarrollo web y el mantenimiento preventivo y correctivo de los equipos informáticos. Todos estos procesos se pretenden analizar para tomar los correctivos necesarios.

Esta empresa se encuentra radicada en la ciudad de Cuenca, en ella se realiza desarrollo de software para empresas de la ciudad, del país y del extranjero, siendo esta última el principal mercado, en ella se enfoca principalmente el desarrollo web, que se lo realiza con herramientas open source y comerciales. Pero de un tiempo para acá se han venido presentando una serie de inconvenientes como por ejemplo retraso en los tiempos de entrega de cierto producto o servicio, así como quejas por parte de los clientes los cuales han manifestado en ocasiones que el producto entregado no es acorde al contrato previamente realizado.

Es por estos motivos principalmente que se necesita realizar dicha auditoría ya que como se comenta los principales clientes se encuentran fuera del país y estas situaciones deterioran la reputación de la empresa repercutiendo en una baja considerable de proyectos a desarrollar.

1.2. Delimitación del problema de investigación

- Límites teóricos

  En los procesos de la Empresa Ecua-mails de la ciudad de Cuenca, se necesita realizar una auditoría informática que permita descubrir que procesos tienen falencias y en base al informe efectuar sugerencias para mejorar el nivel de apoyo a la consecución de dichos objetivos y procesos.

  Disponiendo de las técnicas y procesos para llevar a cabo una auditoría informática en la empresa, se tendrían las herramientas necesarias para tener un análisis completo de la empresa así como las recomendaciones necesarias para mejorar los procesos de la misma, como también mejorar la imagen de la empresa, generar confianza entre los usuarios sobre los productos ofertados por la empresa, optimización del clima de trabajo y las relaciones internas de los empleados, generar un reporte de riesgos de TI.

- Límites temporales

  En lo que respecta al tiempo, 3 meses son suficientes para tener el informe listo, ya que contamos con la directriz de nuestro tutor, así como toda la información contenida en libros e internet para llevar a cabo el tema en cuestión.

- Límites espaciales

  El lugar donde se va a realizar el proyecto de Tesis será la empresa, la misma que ha dado su aprobación para la realización de este proyecto.

II. Objetivos

1.3. Objetivo principal

Realizar una Auditoría Informática en la empresa Ecua-Mails, para obtener un informe que permita conocer las deficiencias en los procesos de TI en la empresa.

1.4. Objetivos secundarios

- Realizar encuestas y entrevistas al personal de la empresa
- Recolectar mediante fichas técnicas la información necesaria de la empresa
- Cumplir con los tiempos establecidos en el plan de trabajo.

III. Justificación de la investigación

1.5. ¿Para qué sirve el trabajo de graduación?

Partiendo de que realizar una auditoría no solo informática sino general en una empresa es fundamental para mejorar la eficacia y eficiencia de la misma, es fácil darnos cuenta del porque se ha elegido este tema de investigación, ya que cada vez más en un mundo tan moderno y competitivo en el que vivimos es

necesario implementar nuevas tecnologías y procesos que ayuden a conocer el estado actual de una empresa y por consiguiente mejorarlo.

Además del aporte a la sociedad que se obtiene, ya que en nuestro país aún no está completamente extendido este proceso y que es de gran importancia para la empresa a implementar. Para ello existen los procesos y técnicas bien definidos para llevar a cabo un buen proceso de auditoria informática, además de contar con la ayuda del tutor encargado, el mismo que nos guiará y nos dará las pautas para concluir con éxito este informe.

1.6. ¿Cuál es la relevancia técnica?

La auditoría se realizará siguiendo las directrices y pasos necesarios para su correcta concepción, con los estándares definidos al realizar este tipo de intervenciones en las empresas, y ayudara a otras empresas a emprender y comprender sobre la gran utilidad y beneficio que tiene desarrollar una auditoría para conocer deficiencias y resolver los problemas encontrados.

1.7. ¿Ayudara a resolver algún problema práctico?

Con el desarrollo de la auditoría se analizarán todos los problemas que tiene la empresa Ecua-Mails para que se puedan tomar decisiones y los correctivos necesarios para tener una eficiencia y eficacia hacia los clientes.

1.8. El tema es de actualidad

Los desarrollos de auditorías se realizan en grandes, medianas y pequeñas empresas de todo el mundo, ya que permiten conocer los problemas que

puedan tener las mismas, ya que tener deficiencias en sus procesos les pueden significar grandes pérdidas de dinero o ser alcanzados o superados por la competencia, este tema está en pleno auge en nuestro país.

IV. Hipótesis

1.9. Hipótesis del trabajo de graduación

Si se realiza una auditoría informática en la Empresa Ecua-Mails, entonces se mejorarán los procesos y objetivos de la empresa en el ámbito informático.

- Variables del trabajo de graduación

Definición conceptual

Auditoría informática a la empresa Ecua-Mails, dedicada a la importación y distribución de equipos informáticos en la ciudad de Cuenca.

Tabla 1: Operacionalización de las variables

Variable	**Dimensión**	**Indicador**
Variable 1: Auditoría Informática a la empresa Ecua-Mails	Se espera completar con éxito al 100% el informe	A la alza
Variable 2: Mejorar los procesos informáticos	Se espera que mejoren en un 70% los procesos en la empresa	A la alza

Variable	Dimensión	Indicador
Variable 3: Reducir costos de TI	Se espera reducir hasta en un 30% los gastos de TI	A la baja
Variable 4: Estudio a la empresa “Ecua-Mails”	Se espera alcanzar un estudio completo al 100%	A la alza

Fuente: “EL autor”

V. Marco de referencia

1.10. Antecedentes teóricos del tema de investigación

Cuando hablamos de un proyecto a desarrollar de auditoría informática, disponemos de varios estudiosos que citan en sus libros varios planteamientos relativos al tema de investigación. Por mencionar a unos cuantos podemos empezar por Mario Piattini, el mismo que afirma que todo lo que conocemos como auditoría nació allá por el año de 1800 en el Reino Unido y Norteamérica, pero no fue sino hasta el auge de las computadoras en el año de 1950 en el área financiera, empieza la denominada “auditoría con el computador” pero mucho cuidado afirma que esto no puede considerarse como una verdadera auditoría informática, sino que utiliza el ordenador como herramienta del auditor financiero.

Ya en la actualidad empresas como ISACA y la Governance Institute, han llevado a la auditoría informática como una herramienta imprescindible para cualquier empresa, y la definen como el proceso de recopilar, agrupar y evaluar

evidencias para establecer si un sistema de información proteje el activo empresarial, conserva la integridad de los datos, lleva a cabo efectivamente los fines de la organización, utiliza eficientemente los recursos, y cumple con las regulaciones y leyes establecidas.

1.11. Marco conceptual

Auditoria Informática: es un examen crítico que se realiza con el fin de evaluar la eficiencia y eficacia de un área, un organismo, una entidad, etc.

Auditoría: proviene del latín auditorius, y de esta se deriva la palabra auditor, que describe a todo aquel que tiene la virtud de oír.

Microsoft Windows: es el nombre de una familia de sistemas operativos desarrollados y comercializados por Microsoft. Microsoft implantó un entorno operativo denominado Windows el 20 de noviembre de 1985 como un complemento para MS-DOS en respuesta al progresivo interés en las interfaces gráficas de usuario (GUI).1 Microsoft Windows llegó a dominar el mercado mundial de PC's ordenadores personales, con más del 90% de la cuota de mercado, superando a Mac OS, que había sido introducido en 1984.

Proceso: es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado. Este término tiene significados diferentes según la rama de la ciencia o la técnica en que se utilice.

Auditor informático: es la persona capacitada para llevar el proceso de Análisis en la empresa a auditar.

Programación: es el proceso de diseñar, codificar, depurar y mantener el código fuente de programas computacionales. El código fuente es escrito en un lenguaje de programación. El propósito de la programación es crear programas que exhiban un comportamiento deseado. El proceso de escribir código requiere frecuentemente conocimientos en varias áreas distintas, además del dominio del lenguaje a utilizar, algoritmos especializados y lógica formal. Programar no involucra necesariamente otras tareas tales como el análisis y diseño de la aplicación (pero sí el diseño del código), aunque sí suelen estar fusionadas en el desarrollo de pequeñas aplicaciones.

Sistema informático: como todo sistema, es el conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico inteligente, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc.

Software: es el equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Hardware: se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Tecnología: es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

.NET: es un Marco de trabajo de Microsoft (framework) que hace un énfasis en la transparencia de redes, sin dependencia de plataforma de hardware y que permita un ágil desarrollo de aplicaciones. Basado en ella, la empresa pretende desarrollar una estrategia horizontal que integre todos sus productos, desde el sistema operativo hasta las herramientas de mercado.

La investigación: es una actividad humana orientada a la obtención de nuevos conocimientos y su aplicación para la solución a problemas o interrogantes de carácter científico.

Análisis de sistemas: es la ciencia encargada del análisis de sistemas grandes y complejos y la interacción entre esos sistemas. Esta área se encuentra muy relacionada con la Investigación de operaciones. También se denomina análisis de sistemas a una de las etapas de construcción de un sistema informático, que consiste en relevar la información actual y proponer los rasgos generales de la solución futura.

Informática: proviene del alemán informatik acuñado por Karl Steinbuch en 1957. Pronto, adaptaciones locales del término aparecieron en francés, italiano, español, rumano, portugués y holandés, entre otras lenguas, refiriéndose a la aplicación de las computadoras para almacenar y procesar la información.

La programación orientada a objetos: o POO (OOP según sus siglas en inglés) es un paradigma de programación que usa los objetos en sus interacciones, para diseñar aplicaciones y programas informáticos. Está basado en varias técnicas, incluyendo herencia, cohesión, abstracción, polimorfismo, acoplamiento y encapsulamiento. Su uso se popularizó a principios de la

década de los años 1990. En la actualidad, existe variedad de lenguajes de programación que soportan la orientación a objetos.

Empresa: Es una organización, institución o industria, dedicada a actividades o persecución de fines económicos y comerciales.

Web: Es un sistema de distribución de información basado en hipertexto enlazados y accesibles a través de internet.

Traducción: es una actividad que radica en comprender el significado de un texto en un determinado idioma, llamado texto origen, para producir un texto con significado equivalente, en otro idioma, llamado texto traducido.

Ingeniería de software: es la aplicación de un enfoque sistemático, disciplinado y cuantificable al desarrollo, operación y mantenimiento de software, y el estudio de estos enfoques, es decir, la aplicación de la ingeniería al software.

1.12. Marco jurídico

CONGRESO NACIONAL

EL PLENARIO DE LAS COMISIONES LEGISLATIVAS

Considerando:

Que la protección de las creaciones intelectuales es un derecho fundamental, así concebido en la Declaración Universal de los Derechos Humanos, aprobada por la Asamblea General de la ONU en 1948;

Que es función del Estado asumir la defensa de los derechos intelectuales;

Que la protección de la propiedad intelectual es vital para el desarrollo tecnológico y económico del País, fomenta inversión en investigación y desarrollo, estimula la producción tecnológica nacional y confiere al Ecuador una ventaja comparativa en el nuevo orden económico mundial; [1]

Que la falta de una adecuada protección a los derechos de propiedad intelectual restringe la libre competencia y obstaculiza el crecimiento económico respecto de la más amplia gama de bienes y servicios que incorporan activos intangibles;

Que la competitividad de la industria y el comercio ecuatorianos en el mercado internacional depende cada vez más de su capacidad de incorporar avances tecnológicos a la producción y comercialización de sus bienes y servicios;

Que la protección de los derechos intelectuales debe responder a los principios de universalidad y armonización internacional;

Que el Ecuador se ha adherido a la Organización Mundial de Comercio y ha ratificado el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC);

Que están vigentes en el Ecuador varias normas de aplicación internacional que implican una reformulación integral de la legislación en materia de Propiedad Intelectual, como la protección a los derechos de autor, especialmente el Convenio de Berna para la Protección de Obras Literarias y Artísticas, Acta de París, la Convención de Roma sobre la Protección de los Artistas; Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, que a pesar de su ratificación en 1963 no fue

[1] http://www.sarime.com/normas.html

reflejada en nuestra legislación, la Convención Universal sobre Derechos de Autor, el Régimen Común sobre Derechos de Autor y Derechos Conexos, regulado en la Decisión Nº 351 de la Comisión del Acuerdo de Cartagena, vigente para todos los países de la Comunidad Andina; y, la protección a la Propiedad Intelectual;

Que el Estado debe optimizar los recursos humanos, tecnológicos y económicos, unificando la aplicación administrativa de las leyes sobre Propiedad Industrial, Obtenciones Vegetales y Derechos de Autor.[2]

1.13. Información de la empresa "ECUA-MAILS"

La empresa Ecua-Mails fue fundada en el año 2006 por un grupo de emprendedores que buscaron dar un servicio efectivo a las necesidades de los consumidores por adquirir su equipo de computación.

Después de un tiempo ampliaron su modelo de negocio incursionando en el desarrollo de software para empresas y el diseño de páginas web, utilizando lenguajes de programación .NET y java, y para entornos web herramientas como Dreamweaver, Joomla y Wordpress.

En la actualidad brindan un completo servicio de distribución, comercialización y mantenimiento de equipos informáticos a personas y empresas de toda la ciudad, así como el desarrollo de aplicaciones para todo tipo de dispositivos basados en PC y Android para todo el Ecuador y empresas de EEUU. Próximamente está previsto el desarrollo para la plataforma IOS para tratar de cumplir con las exigencias de los clientes.

[2] https://www.clubensayos.com/Acontecimientos-Sociales/Ley-De-Propiedad-Intelectual/1437978.html

La Empresa cuenta con 21 empleados distribuidos en las diferentes áreas que van desde la Gerencia a información, y consta de 3 áreas: administrativa, desarrollo y ventas. Por la cantidad de empleados y de los procesos que se manejan es necesaria la realización de una auditoria informática que ayude a identificar problemas entre ellos para poder sacar conclusiones y posibles soluciones a los conflictos.

VI. Metodología

1.14. Métodos generales que se van a utilizar en el trabajo de graduación

Dentro de mi proyecto de tesis se va a utilizar el método Inductivo, en el cual se obtendrá conclusiones generales a partir de las observaciones y las conversaciones con cada uno de los empleados de la empresa. Además, se va a realizar un análisis de las funciones de los procesos que maneja la Empresa Ecua-Mails.

Para luego del desarrollo del sistema que se planea implementar llegar a un proceso de síntesis que se refiere a la "composición de un conjunto de ideas a partir de sus elementos separados en un previo proceso de análisis".

1.15. Técnicas de Investigación que se van aplicar

Dentro de mi proyecto de tesis se van a aplicar las siguientes técnicas:

Observación

Ya que en la Auditoría Informática que se va a realizar a la empresa Ecua-Mails se van a observar los procesos que se desarrollan en ella.

Cuestionarios

Con encuestas y entrevistas relacionados sobre dichos procesos.

Muestreo

A los clientes de la empresa se tomará una muestra para realizar las respectivas encuestas las cuales ayudaran a identificar los problemas e inconvenientes que existe en la ejecución.

CAPÍTULO II

MARCO TEÓRICO

2.1. Auditoría Informática

2.1.1. Introducción

De acuerdo a la organización ISACA y al IT Governance Institute (2014), la Auditoría Informática es el proceso de recopilar, agrupar y evaluar pruebas para comprobar si un sistema de información salvaguarda el activo empresarial, conserva la integridad de los datos, lleva a cabo efectivamente los fines de la organización, utiliza eficientemente los recursos, y cumple con las regulaciones y leyes establecidas. En cuanto a historia se refiere la palabra auditoría proviene del latín auditorius, y de esta se deriva la palabra auditor, que describe a todo aquel que tiene la virtud de oír.

Actualmente en todos los negocios y empresas sin importar el tamaño de sus operaciones y procedimientos dependen de los sistemas informáticos, ya que gracias a ellos las organizaciones pueden efectuar sus operaciones de manera más eficiente para brindar mejores servicios a sus clientes y ser competitivos.

Las bondades que brindan los sistemas informáticos pueden tener como inconveniente hacer más vulnerable la información importante de las organizaciones, por esta razón deben establecer controles para proteger la información y por ende se requiere de auditores especialistas en sistemas informáticos que prueben que estos controles sean efectivos y permiten que la información se procese de manera correcta. En consecuencia, de esta situación se crea la necesidad de realizar habitualmente evaluaciones a los

sistemas, conocidas como auditorías informáticas, con las cuales se pretende identificar y validar los controles implantados en los sistemas y minimizar los riesgos a los cuales las empresas que dependen de los sistemas informáticos se encuentran vulnerables.

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

2.2. Ambiente de control

Basados en el que se define un marco conceptual del control interno común para todas las organizaciones, que satisface las necesidades generalizadas de todos los sectores implicados, se identifica que el marco integrado de control consta de cinco componentes que son:

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

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

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

2.3. El proceso de la auditoría Informática

El proceso de la auditoría informática es similar al de auditoría de estados financieros, en la cual los objetivos principales son, salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales, y la utilización de los recursos con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias. De manera semejante como sucede con la auditoría financiera en la auditoría informática se recogen evidencias, las

cuales se analizan para identificar, la manera en la cual son salvaguardados los activos computarizados, la forma en la que se mantiene la integridad de los datos, como se logran los objetivos de la organización eficazmente y se usan los recursos consumidos eficientemente, pero esto no es un trabajo que se debe realizar de manera desorganizada sino que debe realizarse siguiendo procedimientos ordenados en las siguientes fases:

- Planificación de la Auditoría Informática
- Ejecución de la Auditoría Informática
- Finalización de la Auditoría Informática, las cuales detallaremos más adelante.

Es importante la participación de todas las áreas de la organización durante las fases del proyecto de auditoría puesto que son una pieza fundamental para alcanzar objetivos concernientes a toda la organización como por ejemplo:

- Seguimiento a proyectos relacionados con tecnología informática
- Verificación y aseguramiento del cumplimiento de políticas inherentes a la tecnología informática.
- Aspectos de interés tecnológico para la gerencia.
- Apoyo en la definición, implantación y seguimiento de políticas, controles y procedimientos de auditoría financiera relacionados directa o indirectamente con la tecnología informática.
- Planes de capacitación en el entendimiento y manejo de software de auditoría, herramientas de productividad, bases de datos y equipos de cómputo.

- Identificación de controles de interés para otros tipos de auditoría cuando evalúan áreas del negocio que se apoyan en informática.
- Apoyo en la definición, implantación y seguimiento de políticas, controles, procedimientos y estándares relativos a la administración informática.

2.3.1. Planificación de la auditoría Informática

Como todo proyecto desarrollado dentro de una organización, el proyecto de auditoría informática debe iniciar con una fase de planeación en la cual participen todas las áreas de la organización para determinar los recursos necesarios que permitirá realizar el proyecto, como son, objetivos que se pretenden alcanzar con el proyecto, análisis costo/beneficio, personal humano que intervendrá en el proyecto, marco de referencia de Auditoría Informática que se va a utilizar (p. Ej. COBIT), basándose en varios objetivos fundamentales que son:

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

Se resume en conseguir un conocimiento inicial de la organización a evaluar, con especial interés en sus procesos informáticos fundamentados en evaluaciones administrativas efectuadas a los procesos electrónicos, sistemas y procedimientos, equipos de cómputo, seguridad y confidencialidad de la información, y referencias legales de los sistemas y la información. Una vez que se ha logrado un conocimiento inicial de la organización se procede a implantar metas, programas de trabajo de auditoría, personal que participará en

el proyecto, presupuesto monetario, las fechas y la forma como se presentarán los informes de las actividades de cumplimiento del proyecto, basados en la realidad de la organización evaluada. También dentro del proceso de planificación de la Auditoría Informática se debe incluir y documentar por lo menos los siguientes aspectos:

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

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

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

- Volver a la parte de planificación de la auditoría para rediseñar el trabajo de auditoría debido a que el personal elegido no cuenta con las suficientes capacidades técnicas.
- Proseguir con el desarrollo del Plan de Auditoría basándose en una estrategia de confianza en controles internos para lo cual se deberá revisar que los controles se encuentren adecuadamente implementados y se puedan reducir las pruebas sustantivas.
- Proseguir con el trabajo de auditoría con una estrategia de no confianza en controles debido a que puede ser más eficiente el realizar pruebas sustantivas desde el punto de vista costo-beneficio o que la implantación de controles informáticos produzcan un sobre control cubriendo el mismo ámbito que los controles manuales de usuario.

2.3.2. Ejecución de la auditoría Informática

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

- Entrevistas
- Simulación

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

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

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

La evidencia se clasifica de la siguiente manera:

a. Evidencia documental.

b. Evidencia física.

c. Evidencia analítica.

d. Evidencia testimonial.

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

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

2.3.3. Finalización de la auditoría Informática

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

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

- Debe iniciar con el período de tiempo en el que se ha realizado la evaluación.
- Indicar el equipo de auditoría que ha intervenido en la evaluación.
- Incluir los objetivos que se pretendieron alcanzar con la evaluación de auditoría.
- Posteriormente se debe indicar el Dominio del cual se ha realizado la evaluación de auditoría de acuerdo al marco de trabajo que, utilizado, en este caso COBIT.

- Indicar el criterio sobre el cual se ha realizado la evaluación, en este caso el criterio recomendado por los objetivos de control definidos en COBIT.
- Identificar la condición en la que se encontró a la organización, o también conocida como observación.
- Identificar las causas que provocan la situación observada en la organización.
- Se debe incluir los efectos que puede provocar el hecho que se mantenga la situación actual identificada por los auditores en la organización.
- Incluir las recomendaciones que la administración debería adoptar para cumplir con el criterio de los objetivos de control, que permita reducir la posibilidad de ocurrencia de los efectos anotados anteriormente.
- Por último, se debe incluir el punto de vista de la administración en la que se indique si tomarán en cuenta las recomendaciones emitidas y las fechas en las cuales estas serán adoptadas, lo cual facilitará la ejecución de un seguimiento posterior de la auditoría.

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

2.4. Clasificación de los controles TI

Al momento de realizar un proyecto de auditoría se desarrollan gran variedad de actividades de control para verificar la exactitud, integridad y autorización de las transacciones. Estas actividades pueden agruparse en dos grandes

conjuntos de controles de los sistemas de información, los cuales son, controles de aplicación y los controles generales de la computadora. Sin embargo, estos dos conjuntos de controles se encuentran estrechamente relacionados, puesto que los controles generales de la computadora son normalmente necesarios para soportar el funcionamiento de los controles de aplicación, además que de la efectividad de ambos depende el aseguramiento del procesamiento completo y preciso de información.

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

2.4.1. Controles de Aplicación

La evaluación de los controles de aplicación es una actividad sumamente importante, puesto que la consistencia de la información significativa para la organización depende de la seguridad de los sistemas en los cuales se procesa.

Los controles de aplicación son procedimientos manuales o automatizados que operan típicamente a nivel de los procesos de la organización. Los controles de aplicación pueden ser de naturaleza preventiva o de detección y están diseñados para asegurar la integridad de la información que se procesa en ellos. Debido a lo cual, los controles de aplicación se relacionan con los procedimientos utilizados para iniciar, registrar, procesar e informar las transacciones de la organización. Estas actividades de control ayudan a asegurar que las transacciones ocurridas, estén autorizadas y completamente registradas y procesadas con exactitud. Por ejemplo, podemos incluir los

controles implantados para verificar la validez del ingreso de datos dentro de los sistemas, controles que podemos evaluar mediante el seguimiento manual de los informes de excepción o la corrección en el punto de entrada de datos.

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

- Importancia de las transacciones procesadas.
- Potencial para el riesgo de error incrementado debido a fraude.
- Si el sistema sólo realiza funciones sencillas, como acumular o resumir información o funciones más complejas, como la iniciación y ejecución de transacciones.
- Tamaño y complejidad de los sistemas de aplicación.

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

2.4.2. Controles Generales

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

- Evaluación del diseño de los controles, en la que se determinará que los controles evitan los riesgos para los que fueron diseñados.
- Determinar si los controles se han implementado, lo cual consiste en evaluar si los controles que se han diseñado, se están utilizando durante el tiempo de funcionamiento de la organización.

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

CAPÍTULO III

METODOLOGÍA DE DESARROLLO

3.1 Antecedentes de la empresa

La empresa Ecua-Mails inicia sus actividades en noviembre del año 2006 en la ciudad de Cuenca. La empresa se dedica a la distribución de equipos informáticos en general y al desarrollo de programas informáticos.

3.2 Misión

Brindar las mejores soluciones tecnológicas a nuestros clientes, orientándolos en la adquisición de los productos y servicios que ofrecemos, diferenciándonos de la competencia en distinguir lo que realmente necesita el cliente de acuerdo a sus necesidades.

3.3 Visión

Ubicar a Ecua-Mails como un referente nacional e internacional en soluciones tecnológicas, y que se convierta en la elección número uno de las personas u empresas que necesitan contar con lo último en tecnología.

3.4 Productos y Servicios

- Venta y mantenimiento de equipos informáticos
- Instalación de redes informáticas.
- Desarrollo de aplicaciones corporativas
- Desarrollo Web.
- Help Desk.

3.5 Organigrama de la empresa

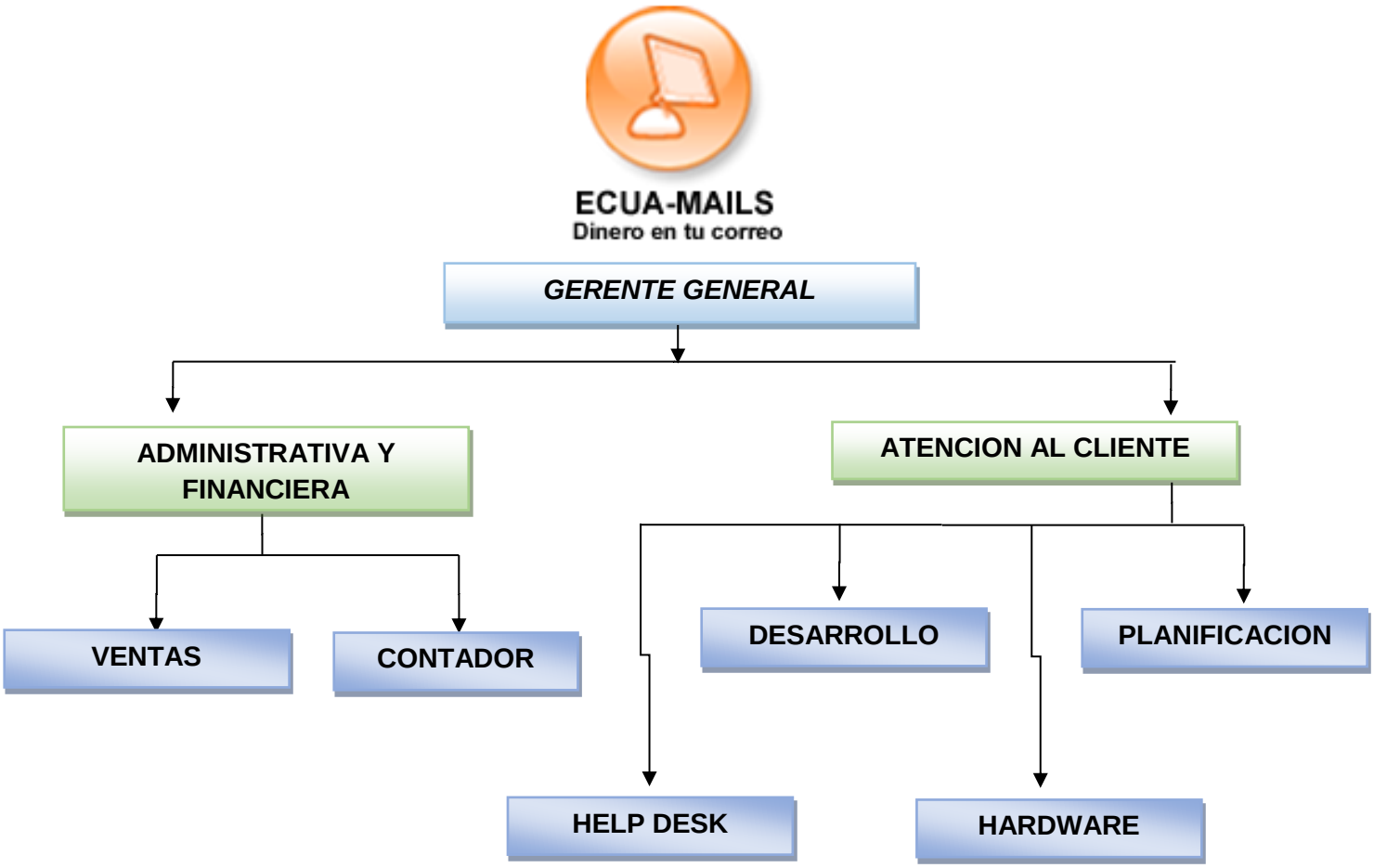


Ilustración 1: Organigrama de la empresa
Fuente: "El autor"

3.6 Programa de auditoría a la empresa

Tabla 2: Programa de auditoría a la empresa

PROGRAMA DE AUDITORIA			
EMPRESA: ECUA-MAILS	FECHA:	DEL 10 DE JUNIO AL 10 DE AGOSTO DE 2014	No hoja. 1
FASE	ACTIVIDAD	DIAS PROGRAMADOS	ENCARGADO
1	Vista Preliminar	4 DIAS	A. PULGARIN
	1.- Solicitud de manuales y documentación.		
	2.- Elaboración de cuestionarios		
	3.- Recopilación de la información		
2	Desarrollo de la Auditoría	15 DIAS	A. PULGARIN
	1.- Aplicación de cuestionario a personal		
	2.- Análisis de claves de acceso, control, seguridad, confiabilidad y respaldos		
	3.- Evaluación de los sistemas. Relevamiento de Hardware y Software, evaluación del diseño lógico		
3	Revisión y Pre-Informe	6 DIAS	A. PULGARIN
	1.- Revisión de los papeles de trabajo		
	2.- Determinación del diagnóstico e implicaciones		
4	Informe	5 DIAS	A. PULGARIN
	1.- Elaboración y presentación del informe.		

Fuente: "El autor"

3.7 Diagrama de Gantt

Partiendo con el tiempo que se dispone para esta investigación se ha realizado una planificación de los pasos a seguir en la elaboración de la auditoria informática a desarrollar para lo cual se ha utilizado el Diagrama de Gantt.

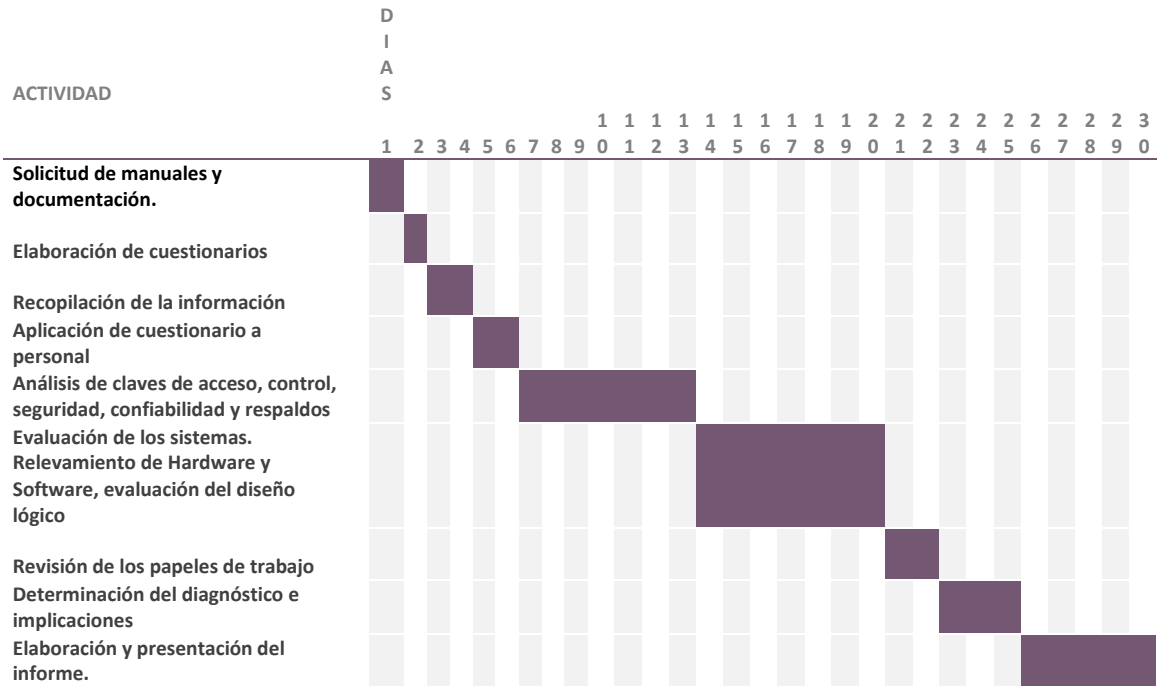


Ilustración 2: Diagrama de Gantt
Fuente: "El autor"

CAPÍTULO IV

RESULTADOS

4.1. Resumen Ejecutivo

La auditoría de sistemas es un examen crítico que debe ser elaborado para evaluar que las áreas responsables del procesamiento de información se encuentren funcionando de manera eficiente y eficaz que conlleven al buen funcionamiento de la empresa y al mejor desempeño de la misma, para brindar una mejor atención a los clientes. Partiendo de este antecedente se ha aprobado y ejecutado el proyecto titulado “REALIZACIÓN DE AUDITORÍA INFORMÁTICA A LA EMPRESA ECUA-MAILS, DEDICADA A LA IMPORTACIÓN Y DISTRIBUCIÓN DE EQUIPOS INFORMÁTICOS EN LA CIUDAD DE CUENCA.”, mediante el cual se realizó la evaluación de los procedimientos que sigue la empresa para dar soporte a los servicios de tecnología que se cumplen en la empresa ECUA-MAILS. A continuación, se especifica un resumen global acerca de la situación actual de la mencionada empresa.

La causa principal de la que nacen varias de las condiciones encontradas, es la falta de conocimiento y conciencia acerca de las mejores prácticas de control interno y auditoría de los sistemas de información por parte de las autoridades de la empresa y del personal que está relacionado con las tecnologías de información y comunicaciones. De acuerdo a lo citado estas condiciones son:

- Las autoridades de la empresa ECUA-MAILS y las unidades de la empresa, en conjunto con los proveedores externos y los usuarios no han realizado un análisis de los servicios de tecnología de la empresa, basados en

sus características básicas, procedimientos que soportan y su nivel de importancia para la empresa, lo cual imposibilita que se definan niveles de servicio que normalicen la disponibilidad y el funcionamiento adecuado de los servicios informáticos brindados por Ecua-Mails.

- El procedimiento de monitoreo del adecuado funcionamiento de los procesos de tecnología brindados por Ecua-Mails y sus proveedores, no se encuentra apropiadamente definido e implementado, puesto que, no se han determinado específicamente personas encargadas de efectuar esta actividad, los parámetros que se han manejado para realizar el monitoreo no son apropiados y entendibles y en los contratos con los proveedores de servicios de tecnología no se incluyen parámetros de disponibilidad de los servicios.

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

- Ecua-Mails no ha considerado la realización de un plan de continuidad de la empresa en el que se incluya análisis de las operaciones y servicios críticos proporcionados, los recursos de hardware y software que permiten la ejecución de estas operaciones, riesgos naturales y tecnológicos que pueden afectar a los mencionados recursos, el personal clave encargado de la ejecución y recuperación de las operaciones, centros alternos de operación. Dentro de este plan se debe considerar la obtención y almacenamiento de

respaldos de la información que permitan la recuperación inmediata de los datos.

4.2. Informe de Auditoría.

"REALIZACIÓN DE AUDITORÍA INFORMÁTICA A LA EMPRESA ECUA-MAILS, DEDICADA A LA IMPORTACIÓN Y DISTRIBUCIÓN DE EQUIPOS INFORMÁTICOS EN LA CIUDAD DE CUENCA."

En conformidad con el Plan del proyecto de tesis, "auditoría informática a la empresa Ecua-Mails, dedicada a la importación y distribución de equipos informáticos en la ciudad de Cuenca", se ha realizado la revisión de los controles referentes al dominio de Entrega de Servicios y Soporte implantados en Tecnología de la Información y Comunicaciones en la empresa, de la que se detalla a continuación las observaciones y recomendaciones resultantes, en base del modelo COBIT.

DS1. DEFINIR NIVELES DE SERVICIO

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

Observación DS1 La Empresa Ecua-Mails no posee niveles de servicio acordados entre sus clientes, la Unidad de Tecnología de la Información y Comunicaciones u otros proveedores de servicios.

Criterio

La alta gerencia deberá implantar un marco de referencia en donde contenga la definición de acuerdos de niveles de servicio formales y determine el contenido mínimo: desempeño, capacidad de crecimiento, confiabilidad, disponibilidad,

niveles de soporte proporcionados al usuario, plan de contingencia/recuperación, restricciones (límites en la cantidad de trabajo), cargos por servicio, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado ,instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

La función de servicios de información y los usuarios deberán contar con un acuerdo escrito que describa el nivel de servicio en términos cuantitativos y cualitativos. El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y la cantidad de servicios ofrecidos y los usuarios deberán ajustar la utilización de los servicios solicitados a los límites acordados.

Condición

- La empresa Ecua-Mails no ha realizado un análisis que sirva para determinar niveles de servicio de tecnología con sus clientes, en los que se indique la calidad, la disponibilidad y el tiempo en el que se prestarán los mencionados servicios.

- Dentro del procedimiento de Soporte Técnico no se ha establecido el tiempo que debe haber transcurrido para que se escale el problema a un área especializada o externa de tecnología.

- El procedimiento de Soporte Técnico no se encuentra correctamente difundido a todos los clientes de la Empresa, puesto que, en lugar de realizar la solicitud de atención de problemas en primera instancia, en varias ocasiones se realiza la solicitudes de solución de problemas a las

unidades especializadas, las que atienden problemas pequeños que podrían ser solucionados en una instancia inferior y que restan productividad a las áreas especializadas.

Causa:

No existen, políticas, acuerdos y análisis basados en la disponibilidad, desempeño, confiabilidad, niveles de soporte proporcionados al usuario, plan de contingencia y capacidad de crecimiento mediante los cuales se puedan definir acuerdos de niveles de servicio con los usuarios.

El procedimiento mediante el cual se brinda soporte técnico a los clientes en el cual se indica que el primer nivel de atención de problemas es el área de Servicio Técnico General, no se encuentra correctamente difundido a todos los clientes.

Efecto:

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

- El no definir límites de tiempo desde el reporte de un problema con los servicios de tecnología hasta el escalamiento del mismo al área especializada de TI, puede provocar que queden requerimientos de usuarios sin atención o en espera indefinida.

- El desconocimiento del procedimiento de reporte de problemas en los servicios de tecnología por los usuarios, provoca que se reporten de manera desorganizada los problemas a cualquier área de Servicio Técnico, teniendo estas que dedicar la mayoría de su tiempo, a resolver problemas menores de soporte técnico que no les corresponden.

Recomendación DS1.-

- El Gerente de la empresa, deberá definir como política institucional el establecimiento de niveles de servicio de TI.

- El Gerente de la empresa, debe elaborar los niveles de servicios de tecnología entre la Unidad de TI y los clientes, en los que se indique el tiempo en el que estos servicios deben estar disponibles, la clasificación de complejidad de los problemas y el tiempo en el que se atenderá cada problema de acuerdo a la complejidad definida. Se capacitará a los clientes acerca de la manera en la que se deben reportar los problemas con los servicios de tecnología de acuerdo al procedimiento de soporte técnico.

DS1.2. Definición de servicios

Observación DS2.- Ecua-Mails no posee un catálogo de productos y servicios en el cual se encuentren definidas las características básicas de los mismos y requerimientos del negocio.

Criterio

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

Condición

No existe un catálogo definido de productos y servicios de TI de la empresa Ecua-Mails, al ser requerido, únicamente fue recibido el catálogo de los equipos informáticos de venta, no existe un catálogo definido para los servicios corporativos ni para los servicios de servicio técnico y mantenimiento.

Causa

Falta de políticas al respecto del mantenimiento de un catálogo de productos y servicios.

Efecto

Deficiencia en los procesos de TI que provocan falta de competitividad.

Recomendación DS2.-

El Gerente de la empresa, durante el primer trimestre del próximo año, deberá desarrollar un catálogo completo de los productos y servicios en el que se indiquen las características completas de dichos productos o servicios.

DS1.3. Procedimientos de Desempeño.

Observación DS3 La empresa Ecua-Mails, no define de manera detallada en los contratos las políticas de desempeño que deberían cumplir sus clientes con la empresa.

Criterio

Deberán definirse procedimientos que afirmen que la forma y las responsabilidades sobre las relaciones que manejan el desempeño (por ejemplo: convenios de confidencialidad) entre todas las partes involucradas sean constituidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

Condición

Se realizó una revisión de varios contratos firmados con proveedores de tecnología, en los que se determinó que no se han definido políticas de desempeño ni tampoco se encuentran definidas sanciones en el caso de incumplimiento con los contratos.

Causa

El formato de los contratos que tiene la empresa Ecua-Mails con sus clientes, tiene un estándar único sin importar el tipo de servicios contratados, en los servicios de tecnología no se consideran cláusulas de calidad y desempeño.

Efecto

No se podría exigir el cumplimiento de los contratos de servicios entre los clientes y la Ecua-Mails para que sean entregados de acuerdo a los requerimientos iniciales de la misma.

Recomendación DS3.-

El gerente de la empresa, dentro del segundo trimestre del próximo año, deberá establecer y poner en ejecución políticas y normatividad e incluir dentro de los contratos, acuerdos de desempeño, cláusulas de confidencialidad y sanciones por incumplimiento de estas cláusulas, deberá contratar a un funcionario encargado de verificar constantemente que estas cláusulas y sanciones se cumplan.

DS1.4. Monitoreo y Reporte

Observación DS4 La empresa Ecua-Mails no tiene una persona responsable de monitorear y reportar el cumplimiento de los procesos del catálogo de productos y servicios que maneja la empresa.

Criterio

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

Condición

- No existe un seguimiento a los procesos de los servicios de tecnología prestados por proveedores externos y por la TI de la empresa; tampoco existe un análisis de los problemas encontrados en dichos procesos para determinar deficiencias u problemas que puedan ocurrir.

- No se realiza un monitoreo continuo de las hojas de control de soporte técnico, que permita detectar la existencia de fallas en el servicio recibido o casos no resueltos.

- No se mantiene un monitoreo continuo de la satisfacción del usuario de los procesos de productos y servicios brindados por Ecua-Mails, no se sabe que siente el cliente y el grado de satisfacción del mismo hacia la empresa.

- No se realiza un monitoreo continuo y un control de los servicios prestados por proveedores externos que permita identificar deficiencias en sus servicios y por lo tanto solicitar las respectivas mejoras.

Causa

La empresa Ecua-Mails no tiene una persona responsable como un Gerente de nivel de servicio encargado de monitorear los procesos de TI.

Efecto

No se conoce la calidad de servicios prestados, errores o fallas en los mismos que permitan aplicar medidas correctivas para mejorar los procesos de tecnología.

Recomendación DS4.-

El gerente de la empresa Ecua-Mails, desde el primer trimestre del próximo año, designará a un Gerente de nivel de servicio, quien será responsable de monitorear y reportar los procesos de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

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

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

Criterio

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

Condición

No existe un proceso de revisión regular de los acuerdos de nivel de servicio y de los contratos de proveedores de acuerdo a los problemas reportados durante el tiempo de duración de los contratos; luego de realizar una revisión de la documentación de los contratos con los diferentes proveedores de servicios de la empresa, no se encontró evidencia de algún procedimiento de revisión regular de acuerdos de servicios y contratos, con la TI, los clientes y los proveedores.

Causa

La empresa, no ha desarrollado políticas y normativas referentes al tema.

Efecto

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

Recomendación DS5.-

El Gerente de la empresa Ecua-Mails, desde el cuarto trimestre del año en curso, debe definir procesos de revisión regular de los acuerdos de nivel de servicio y de los contratos de proveedores de servicios.

DS1.6. Programa de Mejoramiento del Servicio

Observación DS6 No se ha implementado un proceso para asegurar que los clientes y el personal relacionado con los procesos de TI concuerden regularmente en un programa de revisión y mejoramiento de los servicios y los niveles de servicio que los regulan.

Criterio

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

Condición

No se han definido programas de revisión y mejoramiento de los productos y servicios de prestados por la empresa Ecua-Mails.

Causa

Falta de políticas y normatividad al respecto.

Efecto

- Tiempo exagerado por parte del personal de TI en atender problemas presentados con los clientes de la empresa, lo que conlleva a una falta de productividad y a la molestia de los clientes.
- No se tiene una evaluación real del servicio que se está brindado o recibiendo y por tanto no se efectúa la mejora del servicio.

Recomendación DS6.-

El Gerente de la empresa, en el cuarto trimestre del año en curso, debe implementar un proceso para asegurar que los clientes y los encargados del nivel de servicio, concuerden con un programa de mejoramiento del servicio con el fin de dar seguimiento a mejoras al nivel de servicio cuyo costo esté justificado.

DS2. ADMINISTRAR LOS SERVICIOS DE TERCEROS

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

Observación DS7 No se tiene un control con los proveedores.

Criterio

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

Condición

No se tienen los datos suficientes de los proveedores.

Causa

- Desconocimiento de las mejores prácticas de TI.
- No existe conocimiento de procedimientos a seguir en la adquisición de servicios y equipos por parte de las unidades señaladas.

Efecto

No se tiene un control de los proveedores, de sus contratos o del incumplimiento de los mismos.

Recomendación DS7.-

El Gerente de Ecua-Mails, desde el primer trimestre del próximo año, mantendrá un registro actualizado de control de proveedores de tecnologías, en coordinación con el responsable de la unidad de TI.

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

Observación DS 8: No se realizan evaluaciones de los servicios de tecnología con los proveedores externos.

Criterio

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

Condición

- No se mantienen definidas buenas prácticas para asegurar la calidad de las relaciones con los proveedores.
- No se realizan evaluaciones de las relaciones con los proveedores de tecnología, para determinar nuevos acuerdos de los mismos y así garantizar que estén actualizados de acuerdo con las nuevas tendencias en tecnología.
- No se monitorean las relaciones con los proveedores.

Causa

No existen políticas de buenas prácticas en la Unidad de TI.

Efecto

- Falta de competitividad con otras empresas del sector.
- No se detectan posibles deficiencias de los proveedores, lo cual repercute en el rendimiento de los procesos.

Recomendación DS8.-

El Gerente de TI, durante el año en curso, debe definir un procedimiento para establecer relaciones con terceros, a fin de revisar el desempeño actual de los servicios prestados, para luego definir oportunidades de mejora de los servicios de tecnología actuales.

DS2.3. Calificación de Terceros

Observación DS9 No existe una calificación a los posibles proveedores para determinar su capacidad de brindar el servicio.

Criterio

La Gerencia debe asegurar en forma previa a su elección, que los terceros potenciales cuentan con las calificaciones apropiadas a través de una evaluación de su capacidad para proveer los servicios requeridos (due diligence).

Condición

No existe evidencia de calificación a los proveedores de servicios, no existe regulaciones ni políticas en este aspecto.

Causa

No existe una supervisión de las políticas y regulaciones con los proveedores.

Efecto

- Ausencia de garantías al momento de adquirir productos y servicios de los proveedores.
- Falta de eficiencia en tiempos en la entrega de los productos y servicios.

Recomendación DS9.-

El Gerente de la empresa Ecua-Mails, desde el primer trimestre del próximo año, elaborara un procedimiento para asegurar que los proveedores potenciales cumplan con las calificaciones requeridas para brindar un servicio a la empresa.

DS2.4. Continuidad de Servicios

Observación DS10.- No existe un plan para la continuidad de los servicios por parte de terceros, así como determinar riesgos que puedan afectar a la empresa y renegociar contratos en donde se indiquen garantías a Ecua-Mails en relación a sus proveedores.

Criterio

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

Condición

No existe un plan de contingencias sobre la continuidad de los servicios de terceros con la empresa Ecua-Mails.

Causa

No existen definidas normativas y políticas sobre este aspecto.

Efecto

En caso de término intempestivo de un servicio de terceros, puede ocasionar perdida en los procesos que se manejan en el área de TI de la empresa Ecua-Mails.

Recomendación DS10.-

El Gerente de la empresa, durante el año en curso, definirá e implantará políticas y normativas que permitan identificar planes de contingencias sobre los contratos con terceros, además de renegociar los contratos con dichos proveedores.

DS2.5. Relaciones con la Seguridad

Observación DS11.- Dentro de los contratos con los proveedores de servicios, no hay acuerdos de seguridad y de confidencialidad que protejan a la empresa con posibles fugas de información.

Criterio

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

Condición

No se encuentran en los contratos firmados con los proveedores de servicios acuerdos de confidencialidad que protejan a la empresa.

Causa

Falta de políticas y normativas para incluir cláusulas de seguridad y confidencialidad de la información. Desconocimiento de esta buena práctica por parte del personal de la empresa.

Efecto

Eventual fuga de información confidencial e incremento en la vulnerabilidad de los sistemas informáticos de la empresa.

Recomendación DS11.-

El gerente de la empresa Ecua-Mails, durante el cuarto trimestre del año en curso, definirá un procedimiento para asegurar que los acuerdos de seguridad y confidencialidad estén estipulados en los acuerdos con los proveedores de servicios para garantizar la seguridad de la información en la empresa.

DS2.6. Monitoreo

Observación DS12.- No existe un monitoreo continuo de los servicios de los proveedores hacia la empresa.

Criterio

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

Condición

- No existe evidencia de monitoreo realizado a los proveedores de servicios hacia la empresa Ecua-Mails
- No existe un cronograma para definir dicho monitoreo ni se cuenta con una persona para llevar a cabo este proceso

Causa

Desconocimiento sobre esta política por parte de los empleados responsables de TI.

Efecto

No se cumplirían los estándares de calidad al momento de contratar un servicio ya que no se estaría garantizando el cumplimiento de los acuerdos del contrato.

Recomendación DS12.-

El Gerente de la empresa, durante el cuarto trimestre del año en curso, debe definir un procedimiento para efectuar evaluaciones periódicas a los servicios prestados por terceros y de haberlo se tomarán acciones correctivas por parte de los encargados de TI que permitan mejorar los servicios o en su defecto seleccionar a proveedores mejor calificados.

DS3. ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD

DS3.1. Requerimiento de disponibilidad y desempeño

Observación DS13 No se ha realizado un análisis de disponibilidad y desempeño de los servicios de TI.

Criterio

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

Condición

No se ha realizado un análisis de los requerimientos tecnológicos de la empresa que permitan conocer el estado de los recursos tecnológicos en el área de Ti en Ecua-Mails.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- No se cumplen los procesos tecnológicos adecuadamente siguiendo patrones de calidad en los servicios de TI.
- Falta de desarrollo tecnológico en la empresa.

Recomendación DS13.-

El Gerente de la empresa, durante el primer trimestre del próximo año, deberá solicitar la realización de un análisis de requerimientos tecnológicos basado en la disponibilidad y desempeño de los servicios de tecnología, que llevará como resultado el adquirir equipos tecnológicos o desarrollar sistemas de información que garanticen las metas y objetivos trazados por Ecua-mails.

DS3.2. Plan de Disponibilidad

Observación DS14.- No existe evidencia de un plan de disponibilidad que permita monitorear constantemente los servicios tecnológicos que presta Ecua-Mails.

Criterio

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

Condición

No se cuenta con un plan de disponibilidad de servicios de tecnología que se brindan en la empresa Ecua-Mails a sus clientes corporativos, que podría resultar crítico en el impacto en los procesos de TI.

Causa

Falta de políticas y normatividad relativa al tema y desconocimiento de esta práctica.

Efecto

- No se pueden controlar tiempos en los servicios que ofrece la empresa Ecua-Mails, así como la disponibilidad de las mismas.
- No se sabe cuáles son los servicios críticos de la empresa Ecua-Mails y que deben estar disponibles continuamente.

Recomendación DS14.-

El Director de la Unidad de Desarrollo Institucional, dentro del cuarto trimestre del año en curso, en coordinación con el Gerente de TI, definirá dentro de un plan de disponibilidad, el tiempo y las características en las que deben estar disponibles los servicios de tecnología, los riesgos que pueden producirse al no contar con estos servicios de tecnología, los responsables de que los servicios cumplan con estos parámetros y las penalizaciones a los mismos por el incumplimiento con el plan de disponibilidad.

DS3.3. Monitoreo y Reporte

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

Criterio

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

Condición

No se encontraron evidencias de reportes o análisis del desempeño de los recursos de TI.

Causa

Falta de políticas y normativas relativos al tema.

Efecto

Mal desempeño de los recursos tecnológicos de la empresa, los mismos podrían estar defectuosos o dañados. No se realiza correctamente medidas correctivas a los recursos tecnológicos de la empresa que se encuentren defectuosos.

RECOMENDACIÓN DS15.-

El Gerente de la empresa Ecua-Mails, desde el cuarto trimestre del año en curso, implementará un proceso que asegure que el desempeño de los recursos de TI sea continuamente monitoreados y de encontrar deficiencias estas sean reportadas inmediata y oportunamente.

DS3.4. Manejo Proactivo del Desempeño.

Observación DS16.- No se realiza un análisis de los posibles fallos de los sistemas de TI, ya sea de grado de impacto y magnitud de los daños ocasionados.

Criterio

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

Condición

No hay evidencias de monitoreo de los problemas que afectan a los procesos de TI en la empresa Ecua-Mails, antes de que estos afecten los procesos que se manejan en el área de tecnología en la empresa.

Causa

Falta de políticas y normativas relativos al tema.

Efecto

No existe una solución adecuada, rápida y oportuna a alguna falla que pueda presentarse en los servicios de TI de la empresa, así con fallas de los clientes corporativos que disponen páginas web u sistemas desarrollados por Ecua-Mails.

Recomendación DS16.-

El Gerente de la empresa, durante el próximo año, deberá implementar un proceso de administración del desempeño, que incluirá la capacidad de pronóstico, para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño de los sistemas de TI.

Deberán llevarse a cabo análisis de las irregularidades y fallas del sistema en cuanto a frecuencia, magnitud y grado del impacto del daño.

DS3.5. Pronóstico de Carga de Trabajo

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

Criterio

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

Condición

No se ha realizado una planificación para pronosticar la carga de trabajo de los sistemas de TI de la empresa.

Causa

Falta de políticas y normativas relativos al tema.

Efecto

Desconocimiento de la capacidad y desempeño que deben proveer los sistemas de información a los clientes de la empresa Ecua-Mails.

Recomendación DS17.-

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

DS3.6. Administración de Capacidad de Recursos

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

Criterio

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

Condición

No se encontraron evidencias de algún proceso de revisión del desempeño y capacidad de hardware en los procesos tecnológicos de la empresa Ecua-Mails, es más se observó equipos obsoletos en relación a los programas informáticos instalados.

Causa

Falta de políticas y normativas relativos al tema.

Efecto

- Deficiencia en los procesos que se manejan en el área de TI en la empresa.
- Falta de competitividad y demora en los servicios.

Recomendación DS18.-

El Gerente de TI, durante el año en curso, debe establecer un proceso de planeación para la revisión del desempeño y capacidad del hardware, para detectar posibles problemas en relación con el software instalado, para lograr un equilibrio y lograr una cantidad y una calidad de trabajo de eficiencia en los procesos de TI prescritas en los convenios de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

DS4. ASEGURAR EL SERVICIO CONTINUO

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

Observación DS19.- No existe evidencia de un plan de continuidad de negocio en la empresa Ecua-Mails

Criterio

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

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

Condición

La Empresa Ecua-mails no posee un plan de continuidad de negocio, para mantener las operaciones de sus servicios hacia los clientes en caso de ocurrir un desastre, en el cual se incluya un plan de contingencia para llevar a cabo acciones en caso de producirse dicho desastre en la empresa.

Causa

Existe desconocimiento por parte de la Gerencia esta buena práctica.

Efecto

- Posible paralización de los servicios de TI en caso de ocurrir un desastre.
- Posible pérdida de información que se maneja dentro de la empresa.
- Pérdida de tiempo y costo elevado en recuperar nuevamente los servicios en caso de presentarse un desastre.

Recomendación DS19.-

El Gerente de la empresa, en coordinación con los jefes de áreas de la empresa, durante el cuarto trimestre del año en curso, definirá políticas de un plan de continuidad para proveer a la empresa la habilidad de continuar con sus procesos en caso de ocurrir un desastre, a su vez creará un plan de contingencia para mitigar los mismos y que dichos procesos continúen operando aunque no sea con normalidad al menos que no se paralicen.

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

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

Criterio

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

Condición

No existe evidencia de políticas, análisis, marco teórico, metodología o algún procedimiento que se haya realizado por parte de la Gerencia de la empresa Ecua-Mails, que pueda servir de base para el desarrollo del Plan de Continuidad.

Causa

Falta de políticas y normativas relativos al tema.

Efecto

- Existe un riesgo de que se paralicen los procesos en la empresa en caso de ocurrir un desastre.
- Posibles pérdidas de información en caso de ocurrir el desastre y se paralicen los servicios de TI.

Recomendación DS20.-

El Gerente de la empresa, durante el segundo trimestre del próximo año, debe establecer un procedimiento para garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa para validar consistencia.

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

Observación DS21.- No se ha definido los intervalos de tiempo para realizar respaldo de información catalogada como crítica.

Criterio

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

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

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

Condición

Se ha podido verificar que los respaldos que se realizan a la información crítica de la empresa, no se lo hacen con una planificación y continuidad adecuada, existen intervalos de tiempos demasiado distantes lo que provocaría una posible pérdida de información.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

Riesgo de pérdida de información de la empresa y de los clientes corporativos que trabajan con Ecua-Mails.

Recomendación DS21.-

El Gerente de TI, durante el cuarto trimestre del año en curso, deberá implementar políticas y normativas, para garantizar que la información crítica de la empresa sea correctamente respaldada, en función a un tiempo determinado y organizado, siguiendo un nivel de seguridad suficiente, que permita salvaguardar los recursos de respaldo de accesos no autorizados protegiendo la confidencialidad e integridad de la información de la empresa y de sus clientes.

DS5. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

DS5.1. Administrar Medidas de Seguridad

Observación DS22 No se ha definido un plan de seguridad con políticas y normativas en la empresa Ecua-Mails.

Criterio

La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren acorde con los requerimientos de negocio.

Esto incluye: Transportar información sobre evaluación de riesgos a los planes de seguridad de TI, implementar el plan de seguridad de TI, mantener el plan de seguridad de TI para mostrar los cambios en la configuración de TI, valorar el impacto de las solicitudes de cambio en la seguridad de TI, monitorear la implementación del plan de seguridad de TI y alinear los procedimientos de seguridad de TI a otras procedimientos y políticas.

El uso de los recursos y el acceso lógico de TI deberá limitarse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los recursos y los usuarios con las reglas de acceso, para evitar que personal no autorizados, tengan acceso a los recursos de cómputo

La Gerencia deberá establecer procedimientos para asegurar gestiones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberá adicionarse un procedimiento de aprobación formal que indique el propietario del sistema o de los datos que otorga los privilegios de acceso.

La Gerencia deberá contar con un proceso de control establecido para confirmar y revisar periódicamente los derechos de acceso. Se debe llevar a cabo la comparación periódica entre los registros de las cuentas y los recursos para reducir el riesgo de fraudes, errores, alteración no autorizada o accidental.

La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectados, tanto externa como interna y se debe actuar de una manera oportuna.

La Gerencia deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensibilidad, mediante una decisión formal y explícita del dueño de los datos de acuerdo con la estructura de clasificación de datos.

La administración de la función de servicios de información deberá asegurar que la actividad de seguridad y las violaciones sean registradas, reportadas, revisadas y escaladas adecuadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas.

Todo el software y hardware relacionado con seguridad, debe permanecer continuamente protegido contra intromisiones, con el objeto de proteger su integridad y contra divulgación de sus claves secretas.

Con respecto al software malicioso, la Gerencia deberá establecer un marco de referencia adecuado y medidas de control preventivas, detectivas y correctivas para responder y reportar su presencia.

Se deberá contar con Firewalls adecuados para proteger cualquier acceso no autorizado a los recursos internos si existe conexión con Internet u otras redes públicas y contra negación de servicios.

Condición

- No se ha implementado un Plan de Seguridad de TI, que contenga las definiciones de los requisitos de seguridad de la empresa que garanticen la información de los clientes y de la misma empresa.
- No existen políticas de seguridad lógica definidas para el Active Directory, que restrinjan el acceso de personal no autorizado a los sistemas de información.
- No se han elaborado políticas para las cuentas de usuario de la empresa (suspensión, cierre, etc.)
- No existe un procedimiento para realizar revisiones periódicas y oportunas de los derechos de acceso que se les pueda dar a los empleados en los sistemas de TI.

Causa

Falta de políticas y normativas relativos al tema.

Efecto

- Posible pérdida de información al quedar vulnerables los sistemas de la empresa, que pueden ser sustraídos por terceros y que comprometerían la información confidencial de los clientes de Ecua-Mails
- Interrupciones en los procesos de la empresa, al ser estos vulnerados.

- Acceso no autorizado a la información de la empresa.
- Pérdida de confidencialidad de datos y privacidad de los clientes y Ecua-Mails.

Recomendación DS22.-

El Gerente de la empresa, en el cuarto trimestre del año en curso, establecerá políticas y procedimientos, para garantizar la seguridad de los servicios de TI en la empresa, a su vez que implementará políticas de seguridad lógicas en coordinación con el Gerente de TI para que se restrinja a personal no autorizado a los sistemas de información. Además elaborara políticas para las cuentas de usuario de sus empleados y elaborara un plan para la realización de monitoreo continuo de los derechos de acceso que tienen los empleados en los sistemas de TI.

DS6. IDENTIFICAR Y ASIGNAR COSTOS

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

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

Criterio

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

Condición

No existe evidencia de la realización de un análisis costo beneficio, de los servicios de tecnología prestados en los procesos de TI de la empresa

Causa

Falta de políticas y normativas relativo al tema.

Efecto

Desconocimiento y desconfianza en la inversión de TI.

Recomendación DS23.-

El Gerente de la Empresa, desde el cuarto trimestre del año en curso, determinará e implantará políticas y normativa que permita asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los empleados.

DS7. EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS. -

DS7.1. Identificación de necesidades de entrenamiento

Observación DS24 En la empresa Ecua-Mails no existe una planificación de identificación de necesidades de entrenamiento a usuarios

Criterio

La Gerencia deberá implantar y mantener procedimientos para identificar y documentar los requerimientos de entrenamiento del personal que haga uso de los servicios de información.

Condición

- No se ha realizado una evaluación al personal de TI, con respecto al desempeño de sus funciones.
- No se realizan capacitaciones al personal de TI en la empresa en base a sus funciones.
- No existen planes a corto plazo de realizar capacitaciones a los empleados de TI en la empresa Ecua-Mails.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- Que el personal de TI no cumpla sus funciones adecuadamente al no contar con una enseñanza actualizada acorde a las nuevas tecnologías, por lo tanto, se puede hacer un uso inadecuado de los sistemas de información.
- Un servicio defectuoso que puede ocasionar en desastre por parte de los empleados a sus clientes.

Recomendación DS24.-

El Director de la Unidad de Desarrollo Institucional, desde el segundo trimestre del próximo año, establecerá políticas que permitan al personal capacitarse en base a sus procesos en la empresa.

DS8. ASISTENCIA Y APOYO A LOS CLIENTES DE TI

DS8.1. Help Desk

Observación DS25.- No se ha definido un procedimiento adecuado para el reporte y solución de problemas de los clientes.

Criterio

Deberá establecerse un procedimiento de soporte para usuarios dentro de una función de Help Desk, puesto que los usuarios deben contar con una sección dentro de la Unidad de TI, que sirva como contacto para resolver problemas reportados que tienen relación con el uso de los sistemas en aplicación, dificultades en el procesamiento de transacciones inusuales, fallas del hardware, errores en la lógica del sistema de aplicación o problemas de red, para los cuales el área de Help Desk debe registrar el contacto inicial y cualquier acción subsecuente en una bitácora de problemas, lo cual ayuda a la gerencia a monitorear tendencias y estadísticas de problemas de manera tal que se pueda aplicar un enfoque proactivo a la resolución de problemas.

Condición

- No existe una bitácora con los problemas de los clientes, que permitan resolverlos más fácilmente los que son recurrentes.
- No se mantiene un control de incidentes, para saber cuáles ya se solucionaron y cuáles no, existe descoordinación en este tema.
- No hay un personal encargado específico de Help Desk.

Causa

No hay un orden dentro del departamento de TI.

Efecto

- Pérdida de tiempo en resolver los problemas de los clientes.
- Molestia de los clientes al no resolverse un problema en un tiempo determinado.
- Baja calidad en el servicio de TI.

Recomendación DS25.-

El Gerente de la empresa, inmediatamente designará a un encargado específico del área de Soporte Técnico o en su defecto contratarlo. Además, elaborara un registro o bitácora para el control de incidentes recurrentes y se coordinara con el Gerente de TI para elaborar un sistema que permita controlar eficazmente los incidentes que se solucionaron y cuales aún no para mejorar la calidad del servicio prestado por Ecua-Mails.

DS9. ADMINISTRACIÓN DE LA CONFIGURACIÓN

DS9.1. Identificación, mantenimiento y revisión de elementos de configuración

Observación DS26.- No existen procedimientos para realizar mantenimiento a los equipos de sistemas de la empresa Ecua-Mails.

Criterio

La organización debe tener los procedimientos en orden para,

- Determinar elementos de configuración y sus atributos
- Ingresar elementos de configuración nuevos, modificados y eliminados
- Encontrar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones.
- Renovar los elementos de configuración existentes en el repositorio de versiones de configuración
- Impedir la inclusión de software no-autorizado

Estos procedimientos deben brindar un adecuado registro y autorización de todas las acciones.

Verificar y revisar de manera habitual, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar habitualmente contra la política de uso de software, la existencia de cualquier software no autorizado o personal de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Las desviaciones y los errores deben indicarse, atenderse y corregirse.

Condición

No se encontró evidencia de algún documento en el que se registren las configuraciones y nuevas versiones de los sistemas de la Empresa Ecua-Mails.

Además, no se encontró evidencia de registros de la configuración base de los equipos y sus modificaciones, También se ha evidenciado que los equipos de la empresa tienen software pirata en sus sistemas de TI.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- En caso de algún problema en los sistemas es muy probable que estos se paralicen.
- Posibles problemas legales para la empresa por tener instalado software pirata, además se corre el riesgo de que estos programas contengan código malicioso atentando contra la integridad de la información.

Recomendación DS26.-

El gerente de la empresa, en el cuarto trimestre del año en curso, establecerá políticas y normativas para que se registren las configuraciones y nuevas versiones de los sistemas de TI de la empresa, además de establecer políticas para los registros de configuración base, por ultimo deberá hacer un análisis en coordinación con el Gerente de TI sobre el software pirata que pueda contar la empresa para buscar soluciones ya sea adquiriendo sus licencias o buscando alternativas de software libre.

DS10. MANEJO DE PROBLEMAS E INCIDENTES

DS10.1. Escalamiento de problemas. -

Observación DS27.- En la empresa Ecua-Mails no existe un procedimiento de escalamiento de problemas de sus procesos de TI.

Criterio

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

Condición

- En la empresa no existe un personal específico para soporte técnico.
- No existen registros que los problemas son escalados a otras Unidades de la empresa.
- No se realizan monitoreo de los problemas presentados y determinar problemas concurrentes que pueden ser resueltos en un menor tiempo.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- Una mala calidad en el servicio de Soporte técnico a los clientes.

- Mayor tiempo de respuesta al problema presentado.
- Una pérdida de recursos mayor al tratar de resolver un problema.

Recomendación DS27.-

El Gerente de la empresa, desde el primer trimestre del próximo año, establecerá e implantará políticas y normativas de escalamiento de problemas, para resolverlos más rápidamente y contar con un servicio técnico de calidad.

DS11. ADMINISTRACIÓN DE DATOS

DS11.1. Respaldo y restauración

Observación DS28.- En la empresa Ecua-Mails no existe políticas para el respaldo y recuperación de la información.

Criterio

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

Condición

- No se encontró registros de respaldos de la información en la empresa Ecua-Mails que se lo haya hecho recientemente, el ultimo respaldo de la información se pudo verificar que fue hecho hace un año y medio en la empresa, además no se encontró respaldos de las aplicaciones web de

los clientes que la empresa desarrolla, lo que podría ocasionar que esta se pierda.

- No existe un procedimiento definido en caso de recuperar la información.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- Perdida de información de los clientes y de la misma empresa.
- Riesgo de que se paralicen los procesos por un tiempo indefinido.
- Posibles incompatibilidades en las configuraciones de los sistemas al no llevar un registro de los respaldos de las mismas.

Recomendación DS28.-

El Gerente de la empresa, en el último trimestre del año en curso, implementara políticas y normativas que garantizara un correcto respaldo de la información y configuraciones de sus sistemas de TI, a su vez que elaborara una planificación para los mencionados respaldos para así garantizar la seguridad de la información de la empresa y de sus clientes.

DS12. ADMINISTRACIÓN DE INSTALACIONES

DS12.1. Seguridad Física. -

Observación DS 29.- Se ha evidenciado la falta de seguridad física en los equipos de TI.

Criterio

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

Condición

Se ha evidenciado que en las instalaciones de la Empresa Ecua-Mails existen equipos que se encuentran en mal estado, y en algunas partes de la empresa el cableado ya sea de energía o de la red se encuentran en espacios en los que son un riesgo ya que no cuentan con medidas de seguridad que protejan dichas instalaciones, se han hecho añadiduras en las instalaciones de los equipos informáticos sin seguir una planificación ni buenas practicas.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- Posibles daños a los equipos informáticos de la empresa.
- Una posible pérdida de la información de la empresa.

Recomendación DS29.-

El Gerente de la empresa, desde el cuarto trimestre del año en curso, en coordinación con el Gerente de TI, elaborara medidas para garantizar la seguridad de los equipos informáticos de la empresa, realizando un análisis de reestructuración de la ubicación de sus equipos informáticos y el cableado de los mismos.

DS13. ADMINISTRACIÓN DE OPERACIONES

DS13.1 Mantenimiento preventivo del hardware

Observación DS30.- No se han evidenciado procedimientos para el mantenimiento de los equipos informáticos de la empresa.

Criterio

Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

Condición

En la empresa Ecua-Mails no se ha encontrado evidencia de mantenimiento preventivo o correctivo a sus equipos informáticos, se ha observado que algunas de sus computadoras cuentan con unidades ópticas dañadas y otros

accesorios en mal estado, a su vez que dichos equipos no están acordes con las necesidades del software implementado.

Causa

Falta de políticas y normativas relativo al tema.

Efecto

- Perdida de los equipos informáticos de la empresa.
- Una posible pérdida de la información de la empresa en caso de daño de los equipos.
- Bajo rendimiento en los procesos de TI.

Recomendación DS30.-

El Gerente de la empresa, desde el cuarto trimestre del año en curso, en coordinación con el Gerente de TI, definirá e implementara procedimientos para garantizar el mantenimiento oportuno de los equipos informáticos de la empresa y garantizará que estos cumplan con las características requeridas por el software utilizado para brindar un mejor servicio a los clientes y mejorar los procesos de TI.

CONCLUSIONES

Después de haber realizado este trabajo de titulación, se tiene las siguientes conclusiones:

Se concluyó satisfactoriamente con la elaboración del informe final de auditoría, con la revisión de los controles referentes al dominio de Entrega de Servicios y Soporte implantados en Tecnología de la Información y Comunicaciones en la empresa, dicho informe fue entregado al dueño de la empresa.

Se completó satisfactoriamente con el plan de trabajo, cumpliendo los tiempos y expectativas de calidad en base al modelo COBIT.

El modelo COBIT es más completo y sistemático a diferencia de modelos como ITIL.

RECOMENDACIONES

Como recomendación se recalca las ventajas que conlleva un análisis minucioso de los procesos de TI en una empresa, para conocer sus falencias y tomar decisiones al respecto, es recomendable que las empresas adopten como una buena práctica, la realización de ejercicios periódicos de auditoría informática, los cuales además de evaluar los sistemas de información deben hacer un seguimiento de recomendaciones señaladas por consultores externos para mejorar su situación actual.

Bibliografía

4.1, I. F. (s.f.). *ISACA.* Obtenido de http://www.isaca.org/cobit/pages/default.aspx

Antonio., E. G. (2011). *Auditoría informática. México segunda edición.* Mexico.

Audit.org. (2011). *Auditoría Informática.* Obtenido de http://www.audit.gov.tw/ezfiles/0/1000/attach/90/pta_852_2807789_43805.pdf

COBIT, I. F. (2012). *A Business Framework for the Governance and Management of Enterprise IT.* USA.

Emilio, P. V. (2012). *Auditoría informática.* España.

Governance, N. S. (s.f.). Obtenido de http://www.network-sec.com/gobierno-TI/auditoria-COBIT.

Informática, I. a. (2013). *Auditoriasistemas.com .* Obtenido de http://www.auditoríasistemas.com

ITIL, E. O. (s.f.). Obtenido de http://itil.osiatis.es/

ANEXOS

Entrevista

Nombre: _____

Apellido: _____

Cargo: _____

1. **¿Cuantas personas trabajan en la empresa, y que realiza cada una de ellas?**
2. **¿Ecua-Mails que productos y servicios brinda?**
3. **¿Qué medidas de seguridad tiene la empresa en el ámbito de TI?**
4. **¿La empresa maneja información confidencial de los clientes? ¿Cómo la salvaguarda?**
5. **¿Qué sistemas informáticos maneja la empresa?**
6. **¿Podría especificar los pasos a seguir en cuanto un cliente adquiere un producto o servicio de Ecua-Mails?**
7. **¿Existen políticas y normativas de seguridad de la información dentro de su empresa?**
8. **¿La empresa realiza respaldos de la información? Explique su procedimiento.**
9. **¿Qué inconvenientes ha tenido a lo largo de este tiempo relacionado con los procesos de TI de Ecua-Mails?**
10. **¿Se realiza mantenimiento preventivo a los equipos informáticos de la empresa con regularidad? De ser así especifique a cabo de que tiempo se lo realiza y el procedimiento.**

Análisis de resultados a las entrevistas realizadas

1.- ¿Cuantas personas trabajan en la empresa, y que realiza cada una de ellas?

Nos supieron manifestar que actualmente cuentan con 14 personas que laboran en la empresa en las diferentes áreas, distribuidas en las áreas de Administración, Ventas, Desarrollo y Soporte.

2.- ¿Ecua-Mails que productos y servicios brinda?

Se tienen varios productos y servicios entre los que se destacan:

- Venta y mantenimiento de equipos informáticos
- Instalación de redes informáticas.
- Desarrollo de aplicaciones corporativas
- Desarrollo Web.
- Help Desk.

3.- ¿Qué medidas de seguridad tiene la empresa en el ámbito de TI?

Nos indicaron que recién se va a implementar políticas en cuanto a la seguridad en los sistemas de información de la empresa, ya que la misma anteriormente era una empresa pequeña que trabajaba en su totalidad en el ámbito local solamente dedicándose a la comercialización de equipos informáticos, pero recientemente han ido implementado servicios corporativos y desarrollo de software.

4.- ¿La empresa maneja información confidencial de los clientes? ¿Cómo la salvaguarda?

Dicha información es almacenada en un computador al cual sólo gerencia tiene acceso, pero no se la respalda con regularidad y nos indicaron que cuentan

con antivirus instaladas en sus computadoras, pero los mismos no cuentan con licencias originales.

5.- ¿Qué sistemas informáticos maneja la empresa?

Los empleados indican que trabajan con Windows 7 como sistema operativo, manejan el paquete de Office y utilitarios en el área administrativa de la empresa, mientras que en el área de desarrollo trabajan con el paquete de Adobe Master Collection, Netbeans con Java y Visual Studio 2010 para el desarrollo de software y páginas web.

6.- ¿Podría especificar los pasos a seguir en cuanto un cliente adquiere un producto o servicio de Ecua-Mails?

En cuanto el cliente realiza su pedido en el área de ventas, el cual cuenta con personal que orienta al cliente sobre las diferentes alternativas que ofrece Ecua-Mails, es direccionada la orden al departamento indicado ya sea el de soporte, desarrollo o hardware, el mismo que cumpliendo normas de calidad y bajo coordinación con gerencia entregará el producto o servicio en el menor tiempo posible, por último, se direcciona al área de cobranzas para la entrega al cliente.

7.- ¿Existen políticas y normativas de seguridad de la información dentro de su empresa?

No, recién se va a implementar dichas políticas y normativas en el ámbito de TI a la empresa, ya que recién se ha incrementado los productos y servicios ofertados por Ecua-Mails.

8.- ¿La empresa realiza respaldos de la información? Explique su procedimiento.

Se los realiza, pero no constantemente, el ultimo respaldo se lo hizo hace aproximadamente año y medio y dicho respaldo lo hace el gerente de la empresa. El procedimiento es sencillo: se recopila toda la información de cada una de las computadoras en las cuales haya información importante de Ecua-Mails o de sus clientes y la misma es salvaguardada en una computadora central que administra gerencia.

9.- ¿Qué inconvenientes ha tenido a lo largo de este tiempo relacionado con los procesos de TI de Ecua-Mails?

Se han tenido varios inconvenientes con los procesos que maneja la empresa, generalmente se tienen problemas a nivel de hardware de los equipos informáticos ya que al ser antiguos algunas partes se dañan, además han existido problemas con el software por el hecho que se utilizan programas piratas para trabajar y por el uso de memorias usb se contagian de virus y malware que afectan el desempeño de los equipos. Hace aproximadamente 3 años existió un inconveniente muy serio en el cual se perdió información de la empresa al dañarse un disco duro de una de las computadoras, esta información nunca se recuperó.

10.- ¿Se realiza mantenimiento preventivo a los equipos informáticos de la empresa con regularidad? De ser así especifique a cabo de que tiempo se lo realiza y el procedimiento.

Generalmente no, lo que se hace cada mes es solamente realizar un escáner en busca de virus y malware en los equipos informáticos, pero no se realiza un chequeo exhaustivo de los componentes de hardware, tampoco existe un plan para realizar estos mantenimientos.

Cuestionario de la encuesta

Nombre: _____

Apellido: _____

Cargo: _____

1.- **¿La empresa cuenta con un plan estratégico del negocio?**

a.- Si

b.- No

c.- No sé

2.- ¿Sabe usted sobre las políticas y normas de TI y valores empresariales?

a.- Si

b.- No

3.- **¿Existen incentivos para el cumplimiento de los objetivos?**

a.- Si

b.- No

4.- **¿Existen niveles de soporte para atención al usuario o planes de contingencia que garanticen la disponibilidad de dicho soporte?**

a.- Si

b.- No

5.- ¿Se tiene definido el portafolio de productos que ofertan?

a.- Si

b.- No

6.- ¿En la empresa existen acuerdos de confidencialidad para evitar posibles fugas de información?

a.- Si

b.- No

c.- No sé

7.- ¿Existe políticas para analizar y dar seguimiento a los contratos con los proveedores?

a.- Si

b.- No

c.- No sé

8.- ¿Se realizan evaluaciones del servicio a los recursos de TI?

a.- Si

b.- No

9.- ¿Con que frecuencia se realizan los respaldos?

a.- Diario

b.- Semanal

c.- Mensual

d.- Rara vez

e.- Nunca

10.- ¿Se cuenta con una planificación de entrenamiento a los usuarios?

a.- Si

b.- No

11.- ¿Cuándo el cliente reporta un incidente este es atendido?

a.- Se atiende cuando se tiene tiempo

b.- Se atiende con prioridad todo lo que llega

c.- Cuando se vea el mensaje

d.- Se tiene un proceso definido

12.- ¿Con que frecuencia se realizan los mantenimientos a los equipos informáticos?

a.- Nunca

b.- Rara vez

c.- Mensual

d.- Trimestral

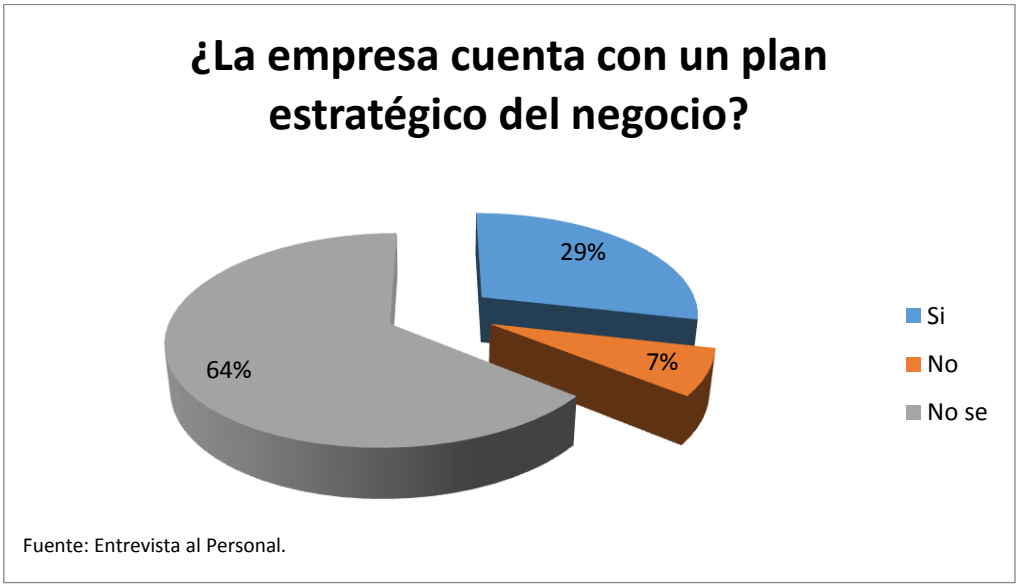
e.- Anual

13.- Existen políticas definidas para

a.- Seguridad

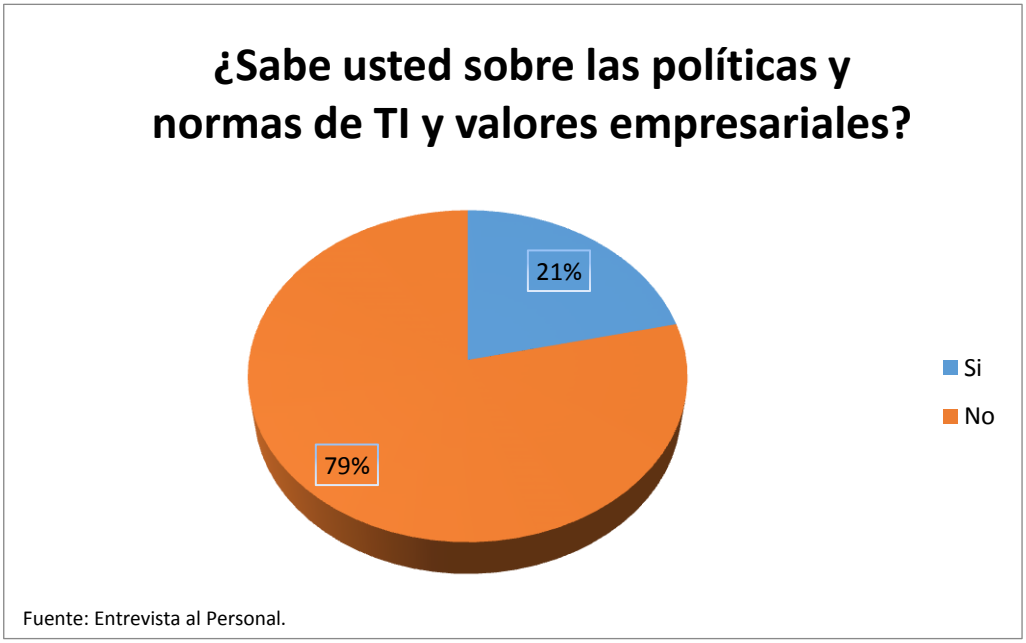
b.- Manejo de incidentes

Resultados de la encuesta



Fuente: Entrevista al Personal.

Se observa de acuerdo a la gráfica que los encuestados respondieron con un 64% que la empresa no cuenta con un plan de negocio definido, el restante 29% reconocieron que la empresa cuenta con un plan de negocio.

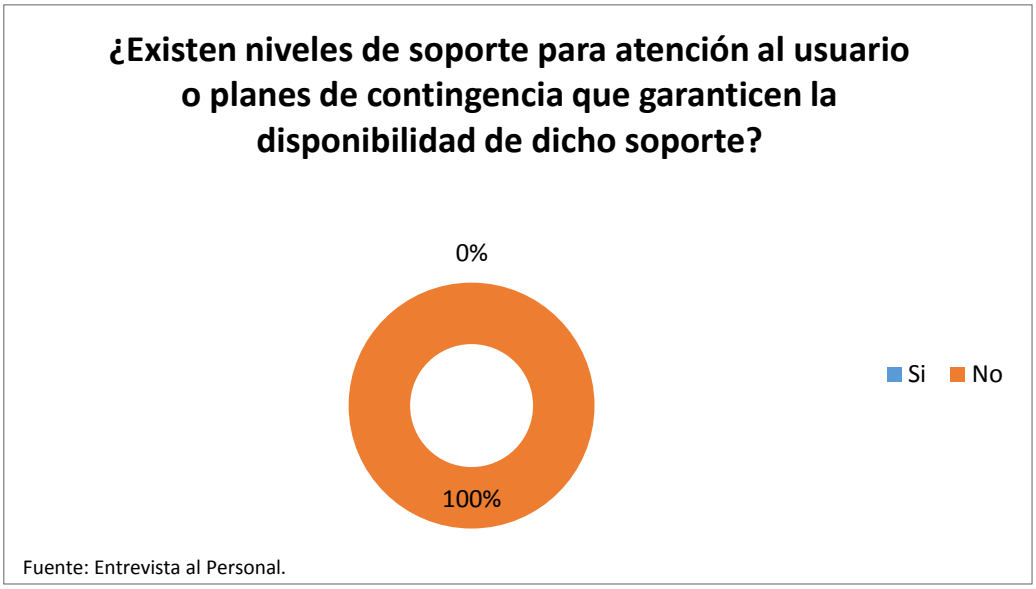


Fuente: Entrevista al Personal.

Se observa que con contundente 79% de los encuestados no conocen sobre las políticas y normas de TI de la empresa para el correcto funcionamiento de los procesos, el 21% restante conocen sobre las políticas de la empresa.

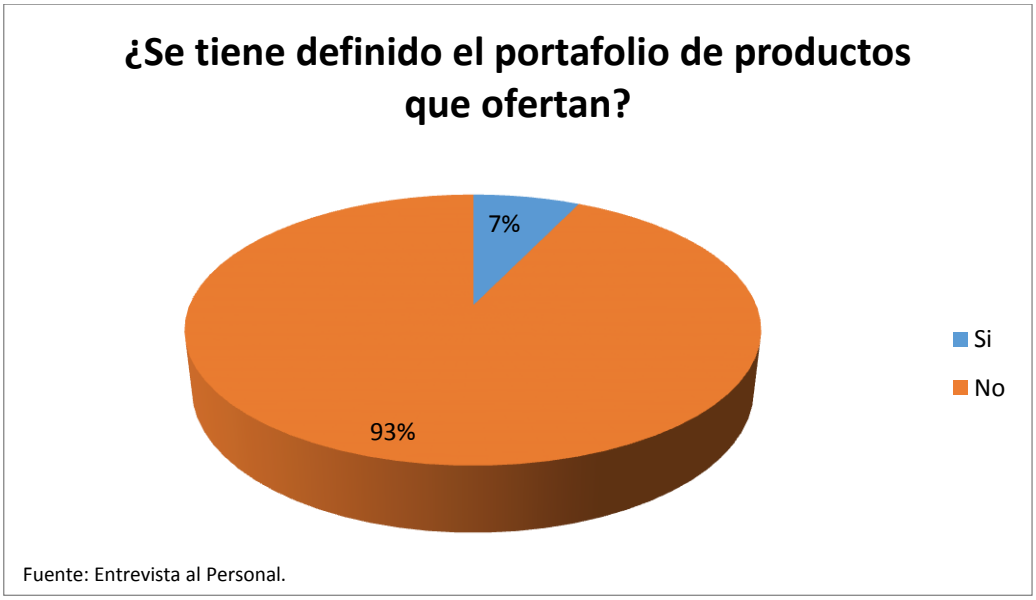
Fuente: Entrevista al Personal.

El 93% del personal encuestado manifestó que no existen incentivos para el cumplimiento de los objetivos en la empresa.



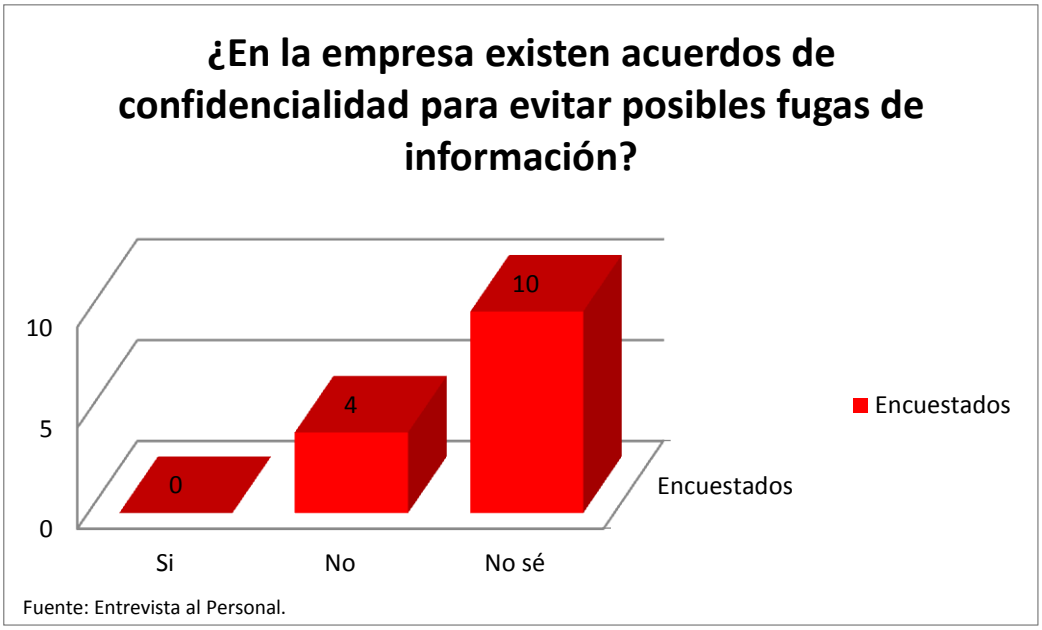
Fuente: Entrevista al Personal.

Un contundente 100% de los encuestados manifestó que en Ecua-Mails no existen niveles de soporte para la atención de incidentes con los usuarios y planes que garanticen la disponibilidad del soporte a dichos usuarios.



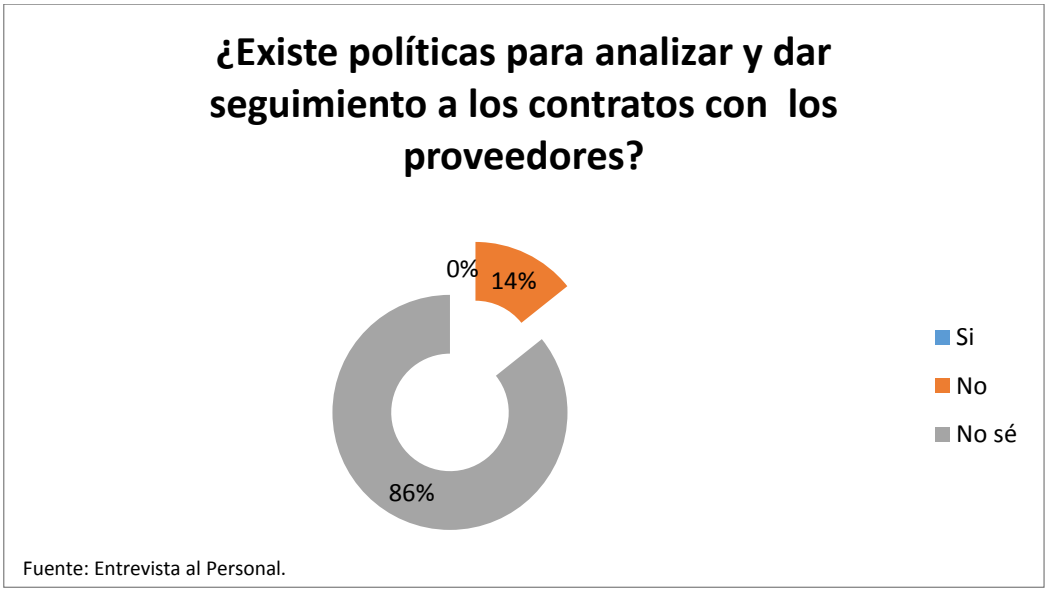
Fuente: Entrevista al Personal.

El 93% del personal manifiesta que no se tiene definido un portafolio de productos y servicios que oferta la empresa Ecua-Mails a sus clientes.



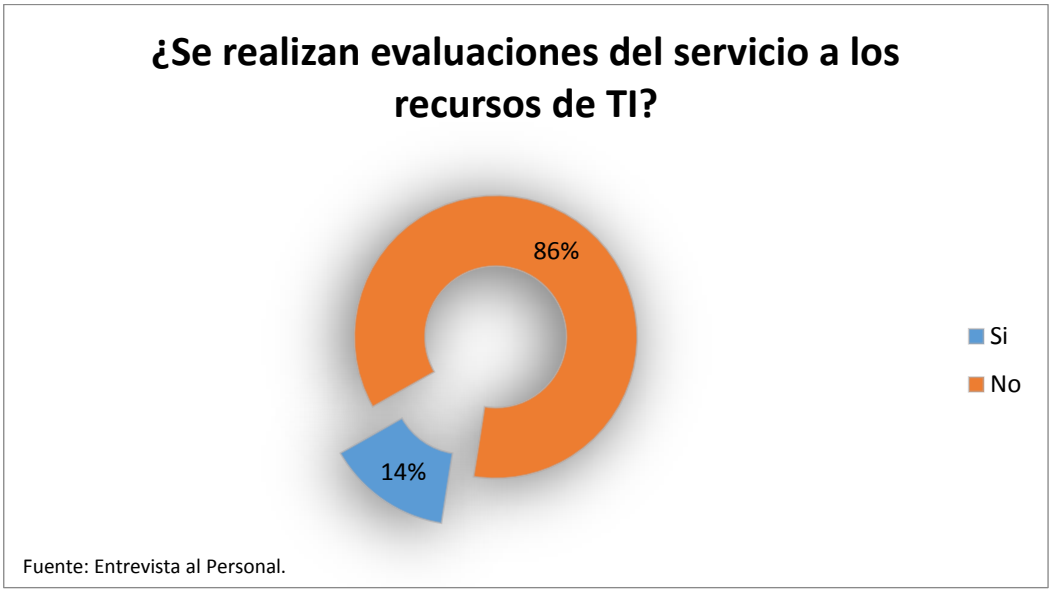
Fuente: Entrevista al Personal.

En base a la gráfica se deduce que en la empresa existe y desconocimiento de políticas de confidencialidad de la información para evitar posibles fugas.



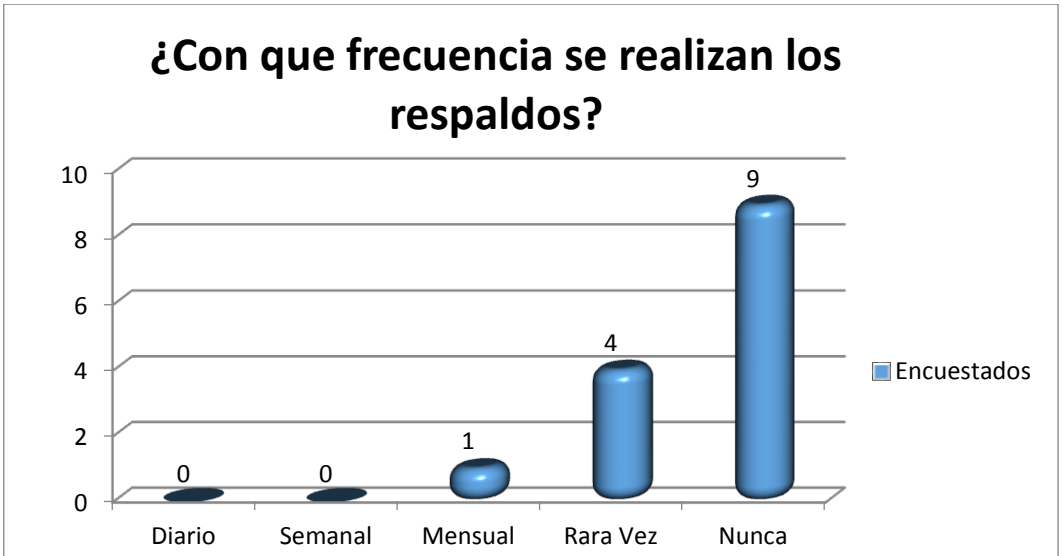
Fuente: Entrevista al Personal.

En relación a las políticas de los contratos con los proveedores externos, el personal tiene un total desconocimiento de dichas políticas.



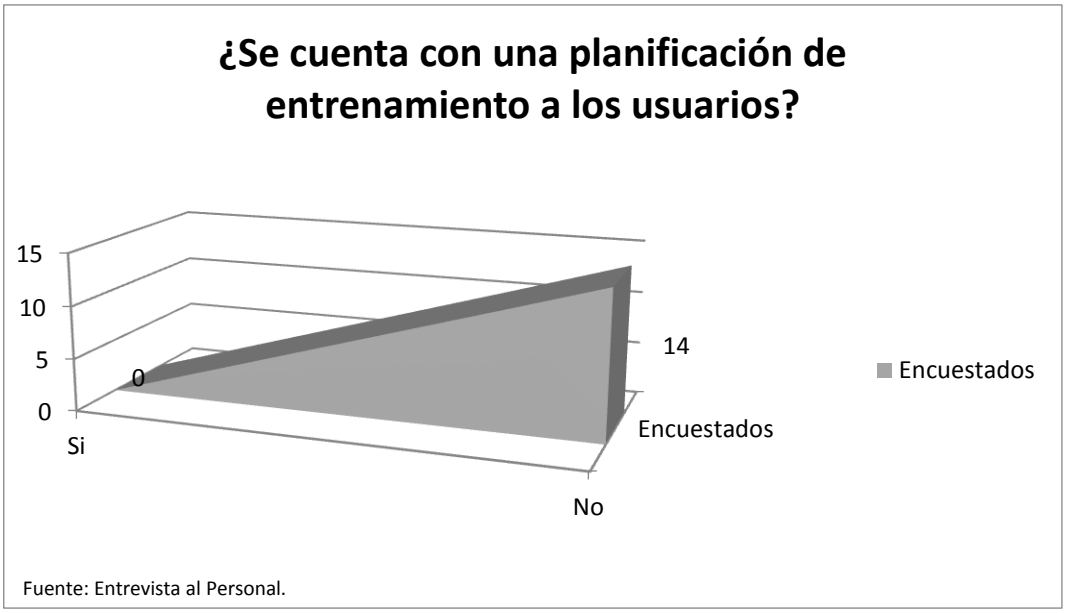
Fuente: Entrevista al Personal.

El 86% del personal encuestados manifestaron que no se realizan evaluaciones a los recursos de Ti de la empresa, un 14% restante manifestó lo contrario.



Fuente: Entrevista al Personal.

La grafica nos demuestra que en la Empresa Ecua-Mails no se realiza frecuentemente respaldos de la información que garanticen la integridad de la misma.

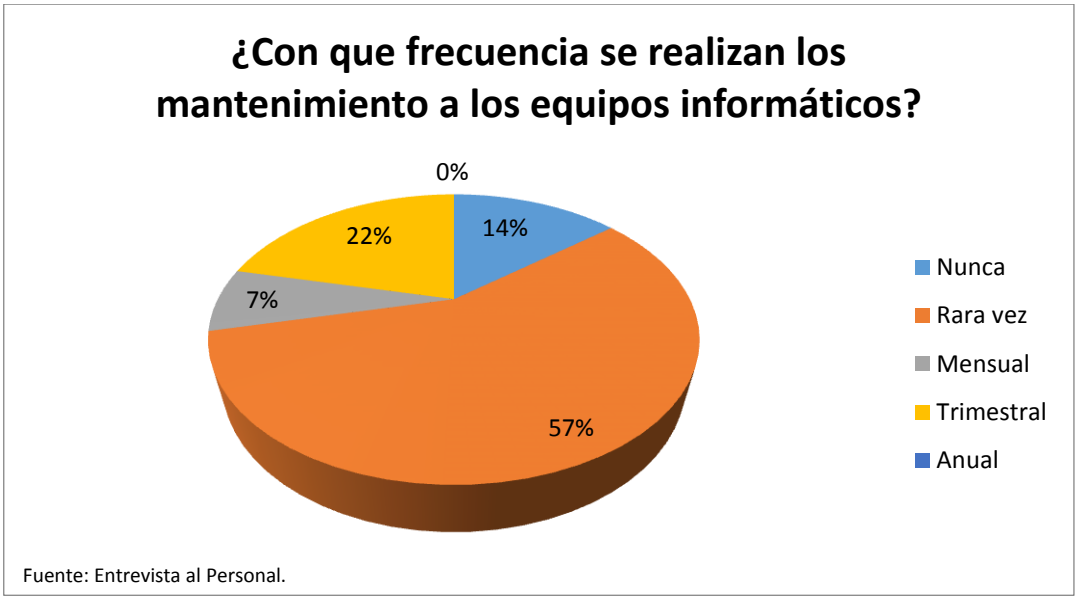


Fuente: Entrevista al Personal.

El total de los encuestados manifestó que en Ecua-Mails no existe una planificación de entrenamiento a los usuarios en los diferentes procesos de TI.

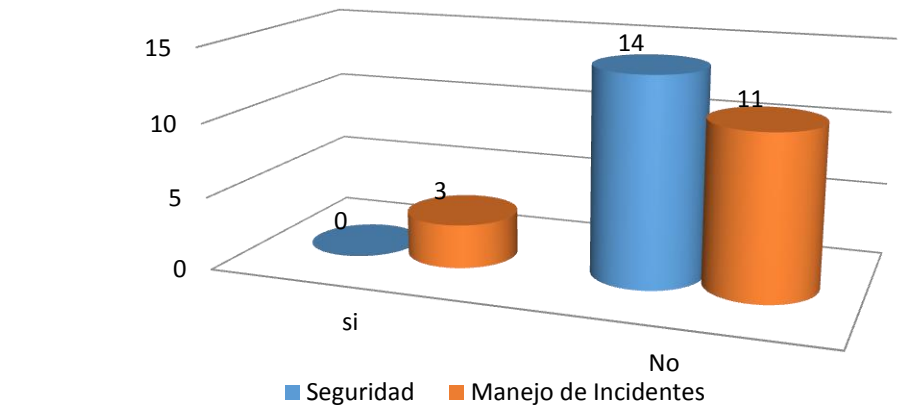
Fuente: Entrevista al Personal.

La gráfica nos demuestra que no se tiene un proceso definido cuando se reporta un incidente por parte de un usuario, se puede observar que existe un proceso desorganizado para atender dichos incidentes.



Fuente: Entrevista al Personal.

Se puede observar que el mantenimiento a los equipos informáticos por el personal encargado no se lo realiza con frecuencia, lo que ocasionaría posibles daños a los equipos informáticos y a los datos que se encuentran en ellos.



Fuente: Entrevista al Personal.

En la gráfica se observa que los encuestados manifiestan que en la empresa no existen políticas definidas tanto para seguridad como para el manejo de incidentes con los usuarios.