UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROPUESTA TECNOLÓGICA

"AUDITORÍA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN LA EMPRESA ROSAS DEL CORAZÓN"

AUTOR:

DIEGO ARMANDO QUILLUPANGUI TOAPANTA

TUTOR:

MGS. JORGE BLADIMIR RUBIO PEÑAHERRERA

LATACUNGA – ECUADOR

Febrero 2019

DECLARACIÓN DE AUTORÍA

Yo DIEGO ARMANDO QUILLUPANGUI TOAPANTA declaro ser autor de la presente Propuesta Tecnológica: "AUDITORIA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN EL EMPRESA ROSAS DEL CORAZÓN", Ing. JORGE BLADIMIR RUBIO PEÑAHERRERA siendo tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

DIEGO ARMANDO QUILLUPANGUI TOAPANTA
CI. 172176299-3

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:

"AUDITORIA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN EL EMPRESA ROSAS DEL CORAZÓN", de QUILLUPANGUI TOAPANTA DIEGO ARMANDO, de la carrera INGENIERIA INFORMATICA Y SISTEMAS COMPUTACIONALES, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, febrero, 2019

Mgs. JORGE RUBIO
CC. 050222229-2
TUTOR

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS; por cuanto, el postulante: QUILLUPANGUI TOAPANTA DIEGO ARMANDO con el título de Proyecto de titulación: "AUDITORÍA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN LA EMPRESA ROSAS DEL CORAZÓN" han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, Febrero 2019

Para constancia firman:

Lector 1 (Presidente)
ING. JOSÉ CADENA
CC: 0501552798

Lector 2
ING. SILVIA BRAVO
CC: 0502437122

Lector 3
ING. GUSTAVO RODRÍGUEZ
CC: 1757001357

AVAL APROBACIÓN EMPRESA ROSAS DEL CORAZÓN

Rosas del Corazón

Rosas del Corazón Cía. Ltda.
Panamericana Sur Km 41, lote San Antonio
Teléfonos: 2316368/ 23957584
Machachi – Ecuador

CERTIFICADO

Yo, Orlando Tapia, con CI. 180163205-8, en calidad de GERENTE ADMINISTRATIVO de la Empresa Rosas del Corazón, certifico que el Sr. DIEGO ARMANDO QUILLUPANGUI TOAPANTA, con cedula de identidad 172176299-3, egresado de la Universidad Técnica de Cotopaxi, de la Carrera de Ingeniería en Informática y Sistemas Computacionales, ha concluido satisfactoriamente la **AUDITORIA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN LA EMPRESA ROSAS DEL CORAZÓN.** Dicho trabajo ha sido entregado y aprobado, sujeto a los parámetros establecidos al principio de la misma.

Es todo cuanto puedo certificar, autorizo al interesado hacer uso lícito del presente documento como lo estime conveniente.

Machachi, Enero 2019

ROSAS DEL CORAZÓN
GERENCIA
ADMINISTRATIVA

Ing. Orlando Tapia
GERENTE ADMINISTRATIVO RDC

AGRADECIMIENTO

Desde que entendí que creer en Dios no es una religión, he podido vivir creyendo en una Palabra que me ha dado aliento día tras día durante todo este trayecto de mi vida. "Esfuérzate y se valiente, no desmayes porque Dios está contigo", he entendido que habrán problemas pero no debo desmayar. Agradezco de manera infinita a Dios por su gran misericordia.

Agradezco a mi madre (+) quien siempre fue un pilar fundamental en mi vida, a mi padre que me ha apoyado de distintas maneras, a mi hermana que nunca se ha descuidado de mí, a mi hermano que ha estado respaldando y cuidando de mí, a mi pastor que después de Dios ha formado parte fundamental y que ha sido un mentor en mi vida.

Agradezco a mis tías que a pesar de la distancia siempre están apoyándome, a mis sobrinos, a mis cuñados, a mis primos y primas.

Agradezco grandemente a todas aquellas personas que estuvieron apoyándome, guiándome, dándome una palabra de ánimo para culminar con este escalón en mi vida.

Diego

DEDICATORIA

Este trabajo se lo dedico a Dios quien me da su Palabra, que me va ayudando cada día a cumplir mi propósito en mi vida, que me inspira a seguir adelante y luchar en medio de toda dificultad.

Se lo dedico a mi madre (+), quien durante toda su vida fue un pilar fundamental en mi vida y me dejo enseñanzas fuertemente inscritas en mi corazón y que día a día me inspiran a luchar y seguir alcanzando mis metas.

A mi padre, mis hermanos, a mis tías y a todas aquellas personas que me ayudaron con una palabra de ánimo, de lucha, de esperanza y de amor.

Diego

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TEMA: "AUDITORIA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN LA EMPRESA ROSAS DEL CORAZÓN"

AUTOR:
Quillupangui Toapanta Diego Armando

RESUMEN

El presente proyecto describe la ejecución de la auditoria informática aplicada a la Empresa Rosas del Corazón, ubicada en la ciudad de Machachi, provincia de Pichincha, la cual se dedica a la producción y exportación de flor de calidad; la empresa utiliza recursos informáticos para llevar a cabo su objetivo de negocio sistematizando sus procesos internos que ayudan a cumplir su trabajo de manera eficiente.

La auditoría se basa en los lineamientos de COBIT 5.0, el cual es un marco de negocio para el gobierno y la gestión de las Tecnologías de la Información (TI) que permiten el desarrollo de políticas claras y buenas prácticas para el control de TI. Esta metodología también ofrece métodos y métricas pero no impone procedimientos detallados, no es radical, sino, tolerante e incluso recomienda otras normas o marcos internacionales.

Actualmente, nos encontramos con muchas empresas que sufren ataques cibernéticos o incidentes en donde se violenta la seguridad física o lógica del área informática. La empresa Rosas del Corazón no se encuentra exenta de este tipo de sucesos. Es por eso que se considera necesario una evaluación de las debilidades y fortalezas del área informática. Durante la ejecución de este proyecto se detallan los objetivos y alcances del presente estudio debidamente justificados, además se exponen algunos conceptos y parámetros que definen a la auditoría y la seguridad informática.

La ejecución de la auditoria constituye la recopilación de la mayor cantidad de información como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI, para ello se utilizaron técnicas de recolección de datos como son entrevistas y cuestionarios.

Luego del análisis de la información recopilada se presenta un informe y resultados del caso práctico describiendo las debidas conclusiones y recomendaciones. Está investigación fue de gran aporte para la empresa, ya que se pudo señalar los inconvenientes existentes lo cual beneficiará a la empresa para aumentar la seguridad en el área informática.

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

THEME: "INFORMATIC AUDIT THROUGH COBIT 5 FOR THE COMPUTING AREA IN ROSAS DEL CORAZÓN ENTERPRISE"

AUTHOR:
Quillupangui Toapanta Diego Armando

ABSTRACT

This project describes the execution of the informatics audit applied in Rosas del Corazon Enterprise, located in the Machachi city, Pichincha province, which is dedicated to the production and exportation of quality flower. The enterprise uses computer resources to carry out its business objectives by systematizing its internal processes that help it to fulfill its work efficiently. The audit is based on the guidelines of COBIT 5.0, which is a business framework for the government and management of Information Technologies (IT) that allows the development of clear policies and good practices for IT control. This methodology also offers methods and metrics but it does not impose detailed procedures, it is not radical, on the contrary, it is tolerant and even recommends other standards or international frameworks. Currently, there are lots of enterprises that suffer cyber-attacks or incidents where the physical or logical security of the IT is violated. The Rosas del Corazon enterprise is not exempt from this type of events. Due to this fact, it is considered necessary an evaluation of the company's weaknesses and strengths of computing area. During the execution of this project, the reach and objectives of this research are properly justified, in addition, some concepts and parameters that define the audit and information security are exposed. The execution of the audit constitutes the compilation of the most information such as documents and evidence that allow the auditor to base their comments, suggestions and recommendations regarding to the management and administration of IT, for this purpose, data collection techniques were used such as interviews and questionnaires. After the analysis of the information collected, a report and results of the practice case are presented by describing the appropriate conclusions and recommendations. This research was a great contribution to the company, since it was possible to point out the existing inconveniences which will benefit the enterprise to increase in the computing area.

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal CERTIFICO que: La traducción del resumen de tesis al Idioma Inglés presentado por el señor Egresado de la Carrera Ingeniería en Informática y Sistemas Computacionales de la Facultad de Ciencias de La Ingeniería y Aplicadas: **QUILLUPANGUI TOAPANTA DIEGO ARMANDO,** portador de la cedula de ciudadanía 172176299-3 cuyo título versa **"AUDITORIA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN LA EMPRESA ROSAS DEL CORAZÓN"**, lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente certificado de la manera ética que estimaren conveniente.

Latacunga, enero 22 del 2019

Atentamente,

.....

Mg. Carolina Cisneros
DOCENTE INGLÉS CI-UTC
C.C. 050276643-9

CENTRO DE IDIOMAS

1. INFORMACIÓN BÁSICA

Propuesto por:

Diego Armando Quillupangui Toapanta

Tema aprobado:

Auditoria informática mediante COBIT 5 para el área informática en la empresa Rosas del Corazón.

Carrera:

Ingeniería en Informática y Sistemas Computaciones

Director del proyecto de titulación:

Mgs. Jorge Bladimir Rubio Peñaherrera

Equipo de trabajo:

PhD. Gustavo Rodríguez, Mgs. Jorge Rubio (Asesores técnico y metodológico)

Lugar de ejecución:

Provincia pichincha, Cantón Mejía, Parroquia de Machachi, Panamericana Sur. Km 41. La Avanzada. Empresa Rosas del Corazón

Tiempo de duración de la propuesta:

Octubre 2018 – Febrero 2019

Fecha de entrega:

Enero 2019

Línea(s) y sublíneas de investigación:

Diseño implementación y configuración de redes y seguridad computacional aplicando normas y estándares internacionales.

Línea de investigación: sublinea de investigación de la carrera:

Tecnologías de la Información y Comunicación (TICs) y Diseño Gráfico.

Tipo de propuesta:

Se aplica una metodología para realizar la evaluación y control de TI en la empresa

2. DISEÑO INVESTIGATIVO

2.1. Título de la propuesta tecnológica

AUDITORÍA INFORMÁTICA MEDIANTE COBIT 5 PARA EL ÁREA INFORMÁTICA EN LA EMPRESA ROSAS DEL CORAZÓN

2.2. Tipo de propuesta alcance

Evaluación y auditoría del ambiente informático del área informática de la empresa Rosas del Corazón, profundizando conceptos de control interno y procedimientos que se ejecutan. Los módulos en los que se ejecuta este proyecto, abarcan los siguientes aspectos:

Identificación de Soluciones Automatizadas: donde se utilizaran criterios de información sobre efectividad y eficiencia en los procesos requeridos en el área Informática, así satisfacer los requerimientos de los usuarios. Las prácticas de control que se utilizan en este módulo están directamente involucradas con los recursos de TI (Tecnologías de la Información).

2.3. Área de conocimiento

En conformidad a la clasificación Internacional Normalizada de la Educación CINE-UNESCO, el área es Ciencia, y la sub área Informática.

2.4. Sinopsis de la propuesta tecnológica

En la actualidad la tecnología informática es una herramienta fundamental en el desenvolvimiento diario de la actividad empresarial; por ello, hay normas y estándares informáticos que deben estar alineados e implementados en el área de Sistemas de la organización. El presente proyecto, trata sobre un examen que permite recoger, agrupar, medir y controlar el uso de las tecnologías de información, esta evaluación ayudará a aumentar la integridad de los datos.

La evaluación aplicada al área informática de la empresa Rosas del Corazón, ayudará a analizar, monitorizar, optimizar los servicios informáticos que se manejan en la empresa. Ayudando así a agilizar los procesos y subprocesos que se realizar diariamente con la ayuda de la tecnología.

En el presente proyecto se aplica la metodología COBIT, la cual será de fundamento para realizar la auditoria en el área informática de la empresa.

Toda la información es importante para la empresa y se ha visto en la necesidad de mantener un equilibrio, para lo cual se trata de identificar las principales falencias y fortalezas que tiene la empresa en la actualidad para disminuir los riesgos de pérdida de información.

El Marco Referencial de COBIT proporciona herramientas al propietario de procesos de negocio (administrador de TI) que facilitan el cumplimiento de esta responsabilidad, aumentando la seguridad en la información y disminuyendo los riesgos de manera integral cubriendo todas las áreas funcionales y de negocios, considerando los intereses relacionados con las tecnologías informáticas.

2.5. Objeto de estudio y campo de acción

2.5.1. Objeto de estudio

Proceso de gestión de seguridad de la información en área de TI.

2.5.2. Campo de acción

Herramienta de auditoría informática que permite ayudar en la administración de las TI.

2.6. Situación problemática y problema

2.6.1. Situación problemática

A nivel mundial la sociedad está envuelta en la Tecnología Informática que ha sobrepasado todos los antecedentes tecnológicos, es algo que no se percibía que llegaría tan lejos y en tan corto tiempo, es por ello que las empresas a nivel mundial han implementado nuevas tecnologías que les permita administrar de mejor manera su información. La falta de una buena gestión y control de las tecnologías de información puede ocasionar graves pérdidas o robos de la información de la empresa.

El uso de la tecnología en el Ecuador, ha permitido identificar que se necesita optimizar y actualizar las políticas para la administración de la información a nivel gubernamental, a nivel empresarial y a nivel educativo, ya que al igual que las organizaciones a nivel mundial todas las entidades administran información valiosa que deben mantenerla segura, alejando o minimizado el riesgo de atacantes informáticos, es por ello que se realizar una auditoria informática al área informática de la empresa Rosas del Corazón.

En la empresa Rosas del Corazón se gestiona la información de campo, del personal operativo, la contabilidad, registro, control de procesos y subprocesos en la producción y venta de flor de exportación; un análisis previo de la situación actual del Área de TI, ha

permitido identificar debilidades en cuanto a la seguridad informática, gestión y administración de las TIC en la empresa.

2.6.1. Problema

Actualmente en la Empresa no se considera este enfoque básico y necesario para poder mantener segura la información ya que un descuido en las TIC implicaría estar vulnerable a los ataques de delincuentes informáticos y desde luego la información estaría vulnerable a cualquier ataque.

Por lo cual se debe aplicar una auditoria informática para identificar las principales debilidades y fortalezas que presenta el área informática de la empresa. Y al final emitir un informe de la auditoria al administrador de la empresa.

2.7. Objetivos

2.7.1. Objetivo general

Realizar una auditoria informática a partir de los preceptos de COBIT 5 para el Área informática en la Empresa Rosas del Corazón, a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos en la organización.

2.7.2. Objetivos específicos

- Recopilar la información sobre la situación actual de las tecnologías de información en la empresa Rosas del Corazón, enfocándose en la infraestructura tecnológica que contribuyen al logro de los objetivos de TI.
- Determinar el cumplimiento de los procesos según el marco de referencia COBIT 5 aplicando una evaluación a la gestión y control del área informática de la empresa Rosas del Corazón.
- Elaborar un informe de auditoría que permita ver los resultados de la evaluación, en base a un estudio y aplicación de metodologías a los procesos informáticos.

2.8. Descripción de las actividades y tareas propuestas con los objetivos establecidos

- Utilizar herramientas y técnicas para la recolección de información sobre la situación actual de la empresa Rosas del Corazón, solicitando información necesaria acerca del área informática de la empresa.
- Realizar la recopilación bibliográfica sobre auditoria aplicando la metodología COBIT 5, identificando cada uno de los procesos que indica la guía de referencia, emparejando los objetivos de la metodología y los objetivos de la empresa.

- En base a los resultados obtenidos en la auditoria, presentar un informe a la administración de la empresa, describiendo los hallazgos y recomendaciones de la auditoria.

3. MARCO TEÓRICO

3.1. Antecedentes

En la actualidad nos encontramos rodeados de la tecnología que inunda nuestras vidas y también cumplen un papel muy importante y necesario en las organizaciones públicas y privadas, podemos identificar como en la actualidad las organizaciones han logrado integrar las TI en las empresas ayudando así a disminuir la relación espacio y tiempo [1].

En la empresa Rosas del Corazón, se utiliza las TI como una herramienta prioritaria para realizar los procesos de producción de rosas como son las fumigación, cosecha, postcosecha, emboche, empaque, entre otros procesos que se registran en el sistema informático, que ayudan a llevar un estricto control de los proceso de producción de rosas.

Con el paso del tiempo cada empresa utiliza la tecnología para manipular su información de manera permanente, por lo cual se requiere ajustar la utilización de estándares y prácticas para garantizar la seguridad de su información y la utilidad de su red. La creciente adopción de mejores prácticas de Tecnologías de la Información, explica porque se requiere mejorar la administración de la calidad y la confiabilidad de TI en los negocios y para responder a una creciente demanda de requerimiento en cuanto a administración de TI.

La información institucional, se ha convertido en un activo fijo real invaluable de la empresa, y esto hace que ante inconvenientes en la red o en la infraestructura física de las TI, el personal tome alternativas rápidas para ganar tiempo, afectando de esta manera la calidad de servicio que presta y en muchos casos obstaculizando otros procesos o dejándolos en pendiente.

En la actualidad se utiliza la tecnología para realizar todos los procesos y subprocesos de producción de flor, pero según una indagación previa se pudo observar que no lleva un control, gestión y gobernabilidad de las TI, esto podría ocasionar que sufran ataques, pérdidas de información, retrasos de producción, errores en la infraestructura de red interna y red de internet.

Es así como cada empresa ha optado por la necesidad de aplicar un modelo de seguridad a las tecnologías de información, pero aun así en la actualidad no se puede confirmar la eficiencia de las seguridades.

Para que se pueda mejorar la utilización de las TI en una empresa se requiere tomar medidas que ayuden a sobrellevar, organizar y administrar cada parte de las TI, según [2] indica que las organizaciones deben tomar cinco tipos de decisiones correspondientes a la arquitectura de las TI, infraestructura de las TI, aplicaciones de negocio, priorización e inversiones en TI, así como también tomar muy en cuenta que las TI forman parte de los activos de la empresa y son un eje fundamental para que la empresa cumpla con sus funciones y lleve a cabo sus objetivos organizacionales.

El uso de la tecnología de la información ha impulsado que los procesos se lleven a cabo en tiempo real [1], y esto exige que la administración y control también se lo realice en tiempo real, es por ello que se busca mejorar la gestión de TI y elevar la eficacia en las actividades lo cual es fundamental para mantener el éxito de la empresa. Además constituyen un marco de referencia para la gestión de políticas, controles internos y prácticas definidas, así como muchas otras ventajas, incluyendo ganancias y beneficios, menor dependencia de expertos, menos errores y mejora de la confianza de los trabajadores al manejar la información que refleja el proceso de su trabajo.

3.1.1. Seguridad informática

En la actualidad las TI han formado parte de la empresas ya que [3] "La sociedad de la información es el producto de una revolución tecnológica sin precedentes, basada en las telecomunicaciones"

Al hablar de las tecnologías de la información, se puede fomentar que forman parte de la empresa ya que transmiten, guardan, gestionan la información de la empresa. Se puede decir que las TIC [3] "constituyen, en consecuencia, uno de los elementos críticos para cualquier entidad. Su flexibilidad funcional y operativa, su soporte a los requerimientos organizacionales y sus capacidades de evolución son, entre otros, factores clave de éxito para el posicionamiento de cualquier institución."

Esto quiere decir que son parte fundamental de la empresa, y al mismo tiempo llevan información crítica de la empresa que debe ser cuidada y llevada bajo estricto control.

> *"la gestión de la seguridad de la información debe ser revisada (¿complementada?) para no solamente cubrir las fallas de seguridad, sino para comprender la manera estructural y sistemática las tensiones entre los elementos que componen el sistema de gestión de la seguridad. En este sentido, consecuente con las tendencias internacionales y la realidad de un mundo global, la seguridad de la información se convierte en un elemento activo y estratégico para las empresas del siglo XXI" [4]*

La seguridad informática se refiere, en sentido amplio, a la confianza en la información y los servicios informáticos disponibles en una red no puedan ser accedidos por usuarios no autorizados.

En [5] se expone que la protección de la información es importante y debe cumplir con los siguientes principios básicos:

- Integridad: La información debe ser oportuna, exacta, completa y consistente.
- Disponibilidad: la información debe estar lista y disponible en cualquier momento que sea requerida, es decir que los recursos se encuentran libre de interrupciones en el servicio.
- Confidencialidad: la información debe ser conocida solamente por su propietario o por quienes el usuario desea compartirla, es decir que no exista acceso no autorizados a los recursos computacionales.

3.2. Red informática

Al referirnos a una red informática, se puede decir que "Una red de ordenadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello es necesario contar, además de los ordenadores correspondientes, con las tarjetas de red, los cables de conexión, los dispositivos periféricos y el software conveniente." [6]

Según el fundamento teórico, una red constituye un conjunto de elementos interconectados entre sí, que sirven para compartir recursos como: impresoras, archivos, mensajes, discos duros locales, extraíbles, internet, etc.

3.2.1. Administración y gestión de las redes LAN

Todas las redes deben ser gestionadas y administradas, lo que implica configurar y controlar los componentes, con el objetivo de proporcionar prestaciones óptimas, tiempos mínimos de caída, seguridad adecuada y flexibilidad. La gestión de la red se realiza mediante sistemas diseñados para mejorar las prestaciones y monitorizar el comportamiento de la red.

"La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio". [7]

Para mantener una red en buen estado se requiere [8] "la gestión de red extiende sus bases sobre la planificación, organización y el control de los elementos comunicacionales que

garanticen una adecuada calidad de servicio sobre un determinado costo; éste busca mejorar la disponibilidad, rendimiento y efectividad de los sistemas".

Al referirnos a la gestión de redes informáticas, se refiere a la administración y continuo monitoreo de la misma, con la finalidad de mejorar los servicios de red, las comunicaciones entre dispositivos logrando una efectividad y control para garantizar un óptimo nivel de operatividad y acceso, en todos los servicios que la red informática ofrece a sus usuarios.

3.2.2. Gestión de seguridad

En el libro de Seguridad Informática [9] se describe que "La seguridad Informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable."

Al momento de gestionar seguridad informática, se define la forma de proteger el activo más importante de la organización que corresponde a la información que se genera cada día. Se encarga además de proteger los equipos que permiten la comunicación, brindar seguridad a la información y estaciones de trabajo con la finalidad de prevenir ataques y mantener la integridad de las TI. Algunas de las funciones y tareas son:

- "Monitorear la red o el sistema frente ataques.
- Encriptado de la información.
- Establecimiento de procedimientos de autentificación.
- Implementación de medidas de seguridad.
- Mantenimiento de la información de seguridad.
- Control de acceso a los recursos" [10]

Según el autor [10] "Algunos ataques que pueden ser perpetrados hacia el software y el hardware durante la gestión de seguridad son: interrupción, intercepción y modificación."

3.2.3. Problemática en la entrega de los servicios TIC

Para que exista una entrega de servicios tecnológicos de calidad, hay que tomar en cuenta la amplitud de conocimiento que se debe tener y los requerimientos tan variados de los usuarios.

Existen estándares que permiten analizar e identificar la problemática que se suscita al momento de hablar de las TIC.

Entre ellos podemos definir:

- La mala utilización de los servicios tecnológicos
- Se considera a TI como un gasto y no como una inversión

- No se puede administrar proyectos
- Ocasionalmente no se considera un área tan importante en la empresa
- No existe proceso de control
- Lentitud en la atención de requerimientos
- Excesivos cambios de la tecnología
- Expectativas erróneas de los usuarios respecto a las TI
- Servicios de TI de mala calidad

3.2.4. Falta de alineamiento estratégico para las iniciativas en la entrega de los servicios TIC

En muchas ocasiones este problema representa uno de los de mayor importancia, ya que se ha podido identificar que en muchas organizaciones públicas o privadas el área de TI va por un camino que no está determinado en el plan estratégico institucional.

Este problema se da por diversas causas, especialmente debido a la falta de visión que tienen los directivos del área, ya que únicamente privilegian la tecnología y no a la mejora y administración de los procesos de negocio con TI.

3.2.5. Falta de compromiso y apoyo de las autoridades

La falta de atención de las autoridades administrativas de las empresas hacia la iniciativa de innovación de las áreas de TIC es un problema de mucha relevancia, esto generalmente ocurre en empresas que consideran que la tecnología es únicamente el proveedor de equipo y el manejo de internet.

Esto representa en muchas organizaciones una falta de atención de parte de la gerencia y generalmente no apoyan las iniciativas de TI.

3.2.6. Gestión de servicios tecnológicos inoportuna

En las empresas la infraestructura tecnológica se orienta a satisfacer las necesidades de los requerimientos del procesamiento de la información institucional.

Esta meta está orientada a ser proporcionada con calidad y oportunamente, tomando en cuenta que es la principal función del área de TI.

En la actualidad se ha podido ver que esta meta no se cumple de acuerdo a los requerimientos necesarios ya que en la mayoría de empresas públicas o privadas tiene un pobre nivel de aceptación.

3.3. Definición auditoría

Para centralizarnos en el tema concreto como es la auditoria informática vamos a tomar de definición de Castello que dice que la "Auditoría de sistemas es un término con varias aceptaciones: en este trabajo entendemos por ella a las actividades de evaluación y control de los sistemas de información de una organización." [11]

Según [11] se considera que la auditoria es la actividad de evaluar y controlar las tecnologías de la Información de una empresa, esta actividad ayudará a administrar y gestionar las TI de mejor manera.

3.3.1. Importancia de la auditoria

Luego de identificar la fundamentación teórica para realizar una auditoría, nos centramos en "La importancia de las auditorías informáticas radica en que permiten determinar las fortalezas y debilidades del sistema de información de las organizaciones." [12]

Ya que se puede deducir que todo ha ido cambiando en torno a la tecnología, esto ha hecho que la información, y los procesos llevados a cabo por las TI, sufran minuciosos ataques, que pueden causar daños o pérdida de la información de la empresa según [12].

> *"Así como la tecnología ha ido evolucionando, los fraudes y delitos informáticos han ido a la par, a tal punto que en la actualidad un delincuente informático puede sustraer recursos económicos de una organización desde la comodidad de su hogar, sin dejar rastro alguno, o estructurar grandes delitos desde el interior de la organización." [12]*

Para realizar una auditoria debemos basarnos en una metodología o modelo que nos permita gestionar el proceso de auditoría que este fundamentado en bases teóricas y buenas practicas que proporcionen confiabilidad y respaldo antes, durante y luego de la auditoria.
Para la cual se ha basado en una metodología que ha ayudado en la gestión de TI en las entidades a nivel mundial.

3.3.2. Auditoría informática

Con el auge de las nuevas tecnologías, los temas relativos a la auditoría informática cobran cada vez más relevancia, tanto a nivel nacional como internacional, debido a que la información se ha convertido en el activo más importante de las empresas, representando su principal ventaja estratégica, por lo que éstas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información con el fin de obtener la mayor productividad y calidad posibles.

Según [13] define que “la auditoría se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información en la organización, se llevan a cabo de una manera oportuna y eficiente“.

La auditoría informática permite la aplicación de un conjunto de procesos para evaluar y garantizar que las herramientas y los recursos tecnológicos funcionen de acuerdo con las necesidades de la empresa brindando un ambiente de seguridad para que la información este presente de manera íntegra, confiable y exacta.

3.3.3. Objetivos de la auditoria informática

La auditoría informática consiste en el examen crítico y sistemático de las políticas, normas, prácticas y procedimientos para dictaminar respecto a la economía, eficiencia, eficacia, la efectividad del sistema de control interno asociado a las TI.

Según [13] aclara que es sumamente importante que toda empresa posea un tipo de mecanismo que permita controlar, y al mismo tiempo permita identificar los riesgos en las TI a los que están expuestos.

La práctica de la auditoría informática es de vital importancia para el desempeño de los sistemas de información, pues proporcionan los controles necesarios para que los sistemas sean confiables y alcancen elevados niveles de seguridad. Se evalúan los sistemas de cómputo y los sistemas de información en general incluyendo sus entradas, procedimientos, controles, archivos y obtención de información.

Como objetivo de la auditoria informática podemos decir que:

- Sirve para protección de los activos fijos de la empresa, la base para lograr este objetivo es tener una información actualizada de apoyo para la planificación y control de los activos y las funciones que realiza la empresa.
- Se debe alinear la información de las áreas críticas del negocio, de esta manera alcanzar los objetivos de la empresa.

3.3.4. Importancia de la auditoria informática

Todo el proceso de la auditoria debe ser llevado con sumo cuidado, la evaluación de actividades, funciones específicas, resultados u operaciones de la empresa, para que al final se logre obtener una correcta evaluación, al mismo tiempo debe evitar cualquier influencia en cuanto a los resultados de la misma.

3.3.5. Tipos de auditoria

a) **Auditoria de gestión:** es la contratación de bienes y servicios, documentación de programas, etc.

b) **Auditoria legal del reglamento de protección de datos:** cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

c) **Auditoria de datos:** Clasificación de los datos, estudio de las aplicaciones y flujogramas.

d) **Auditoria de base de datos:** Controles de acceso, de actualización, de integridad y de calidad de Datos.

e) **Auditoria de seguridad:** Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación.

f) **Auditoria de la seguridad Física:** Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no relevando la situación física de esta. También referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.).

g) **Auditoria de la seguridad Lógica:** comprende los métodos de autenticación de los sistemas de Información.

h) **Auditoria de las comunicaciones:** se refiere a la auditoria de los procesos de autenticación de los sistemas de comunicaciones de la empresa.

3.3.6. El Proceso de la auditoría informática

Según [14] "El proceso de la auditoría informática es similar al que se lleva a cabo a los de estados financieros, en el cual, los objetivos principales son: salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias."

Muchos de los componentes de la pirámide nacen de un proceso de auditoría, el cual se detalla a continuación y al cual se divide en 3 etapas:

- Planificación de la auditoría Informática
- Ejecución de la auditoría Informática

- Finalización de la auditoría Informática

3.4. Planificación de la auditoría informática

En esta fase se establecen las relaciones entre auditores y colaboradores de la organización, para determinar el alcance y objetivos. Se hace un bosquejo de la situación de la entidad, acerca de su organización, sistema contable, controles internos, estrategias y demás elementos que le permitan al auditor elaborar el programa de auditoría que se llevará a efecto.

Elementos Principales de esta Fase:

1. Conocimiento y comprensión de la entidad
2. Objetivos y alcance de la auditoría
3. Análisis preliminar del control interno
4. Análisis de los riesgos
5. Planeación específica de la auditoría
6. Elaboración de programas de auditoría

3.4.1. Conocimiento y comprensión de la entidad a auditar

Previo a la elaboración del plan de auditoría, se debe investigar y analizar todo lo relacionado con la entidad a auditar, para poder elaborar el plan en forma objetiva. Este análisis debe contemplar: su naturaleza operativa, su estructura organizacional, giro del negocio, capital, estatutos de constitución, disposiciones legales que la rigen, sistema contable que utiliza, volumen de sus ventas y, todo aquello que sirva para comprender exactamente cómo funciona la organización.

Para el logro del conocimiento y comprensión adecuados de la entidad, se deben establecer diferentes mecanismos o técnicas que el auditor deberá dominar, siendo entre otras:

a) Visitas al lugar

b) Entrevistas y encuestas

c) Análisis comparativos de Estados Financieros

d) Análisis FODA (Fortalezas, oportunidades, debilidades, amenazas)

e) Análisis Causa-Efecto

f) Árbol de Objetivos.- Desdoblamiento de Complejidad.

g) Árbol de Problemas

3.4.2. Objetivos y alcance de la auditoría

Los objetivos indican el propósito para el cual es contratada la firma de auditoría, qué se persigue con el examen, para qué y por qué. Si es con el objetivo de informar a la gerencia sobre el estado real de la empresa, o si es por cumplimiento de los estatutos que mandan efectuar auditorías anualmente, en todo caso, siempre se cumple con el objetivo de informar a los socios, a la gerencia y resto de interesados sobre la situación encontrada para que sirvan de base para la toma de decisiones.

El alcance de una auditoría ha de definir con precisión el entorno y los límites, en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. Por otro lado, el alcance también puede estar referido al período a examinar: puede ser de un año, de un mes, de una semana y, podría ser hasta de varios años

3.4.3. Análisis preliminar del control interno

Este análisis es de vital importancia en esta etapa, porque de su resultado se comprenderá la naturaleza y extensión del plan de auditoría, la valoración y oportunidad de los procedimientos a utilizarse durante el examen.

3.4.4. Análisis de los riesgos

El Riesgo en auditoría, representa la posibilidad de que el auditor exprese una opinión errada en su informe, debido a que los estados actuales de la información suministrada a él estén afectados por una distorsión material o normativa.

En auditoría se conocen tres tipos de riesgo: Inherente, de control y de detección. El riesgo inherente, es la posibilidad de que existan errores significativos en la información auditada, al margen de la efectividad del control interno relacionado con errores que no se pueden prever.

El riesgo de control, está relacionado con la posibilidad de que los controles internos imperantes no prevean o detecten fallas que se están dando en sus sistemas y que se pueden remediar con controles internos más efectivos.

El riesgo de detección, está relacionado con el trabajo del auditor y, es que éste en la utilización de los procedimientos de auditoría, no detecte errores en la información que le suministran.

3.4.5. Planeación específica de la auditoría

Para cada auditoría que se va a practicar, se debe elaborar un plan. Esto lo contemplan las Normas para la ejecución. Este plan debe ser técnico y administrativo. El plan administrativo debe contemplar todo lo referente a cálculos monetarios a cobrar, personal que conformarán los equipos de auditoría, horas hombres, etc.

3.4.6. Elaboración de Programa de Auditoría

Todo el equipo de auditoría, debe tener conocimiento, el programa completo de los objetivos y procedimientos de la auditoría, objeto de su examen.

Esto quiere decir, que debe existir un programa de auditoría para cada proceso. De esto se deduce que un programa de auditoría debe contener dos aspectos fundamentales: Objetivos de la auditoría y Procedimientos a aplicar durante el examen de auditoría. También se pueden elaborar programas de auditoría no por áreas específicas, sino por ciclos transaccionales.

3.4.7. Ejecución de la auditoría informática

La ejecución de la auditoría informática, constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI.

Para la recolección de información, se pueden aplicar las siguientes técnicas:

- 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

Toda la información entra luego en un proceso de análisis, el cual debe ser realizado utilizando un criterio profesional por parte de los auditores y el equipo a cargo del proceso de Auditoría, toda la información recopilada debe ser clasificada de manera que nos permita ubicarla fácilmente, para luego del análisis respectivo justificar de manera correcta las recomendaciones.

La evidencia se clasifica de la siguiente manera:

a) Evidencia documental.

b) Evidencia física.

c) Evidencia analítica.

d) Evidencia testimonial.

Una vez que tenemos información real y confiable, procedemos a evaluar y probar la manera en la que han sido diseñados los controles en la organización, para el mejoramiento continuo de la misma, para esto el equipo de Auditoría utilizara medios informáticos y electrónicos que permitan obtener resultados reales.

El equipo de auditores, para poder dar una opinión sobre un sistema o proceso informático, debe comprobar el funcionamiento de los sistemas de aplicación y efectuar una revisión completa de los equipos de cómputo. [15]

3.5. Normas, estándares y procedimientos de auditoría

La influencia de las TI ha propiciado que comiencen a ser parte fundamental en la operación y desarrollo de las empresas. Debido a esto, la administración efectiva de la información y de las tecnologías relacionadas se ha vuelto un factor crítico para la supervivencia y éxito en las organizaciones.

Los procedimientos de auditoría que se basan en el empleo de normas y estándares garantizan el control de las tecnologías de la información. Algunos de los estándares más conocidos son:

Objetivos de Control para Tecnologías de Información y relacionadas, es un conjunto de mejores prácticas para el manejo de la información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA, en inglés Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (IT Governance Institute).

ISACA lanzó el 10 de abril de 2012 la nueva edición de este marco de referencia. COBIT 5 es la última edición del framework mundialmente aceptado, el cual proporciona una visión empresarial del gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

Para la realización de la auditoría se han definido 3 fases:

- Diseño del procedimiento de auditoría

En esta fase se seleccionan los procesos que se van a auditar y se desarrollan a partir de la integración de COBIT 5, ITIL e ISO/IEC 27002. Esto permitirá al auditor elaborar un programa de auditoría, determinando el alcance y los objetivos.

- Ejecución de la auditoría

El objetivo de esta etapa es obtener toda la información de los procesos que se auditarán, con el fin de adquirir evidencia suficiente, competente y relevante, que permita al auditor establecer conclusiones.

- Informe y plan de acción

En esta fase se analizará el resultado de la aplicación de la auditoría efectuada por los auditores, expresando por escrito su opinión sobre el área, proceso y actividad auditada en relación con los objetivos fijados. Se señalan las debilidades de control interno, si las hubo, y se formulan las recomendaciones necesarias para contribuir al mejoramiento de la seguridad de la red LAN.

3.5.1. ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La norma ISO le proporciona la metodología y el marco que le ayuda a gestionar su ITSM.

La gestión de servicios de tecnologías de la información (en inglés IT Service Management, ITSM) es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final.

3.6. COBIT

COBIT puede ayudar a las empresas a reducir sus perfiles de riesgo a través de la adecuada administración de la seguridad. La información específica y las tecnologías relacionadas son cada vez más esenciales para las organizaciones, pero la seguridad de la información es esencial para la confianza de los accionistas.

3.6.1. COBIT 5

COBIT 5 fue creado para ayudar a la alta dirección a garantizar el logro de objetivos de la empresa, mediante la dirección y control de las TI, la aplicación de COBIT 5 debería ser realizada en todos los niveles organizativos de la empresa y no tan solo concentrarse en la tecnología de la información. COBIT 5 ofrece las principales matrices jerárquicas que permitan el control de la tecnología de información aplicada a la empresa.

Según el comité directivo de COBIT 5 (2012) dice que "COBIT 5 está orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas."

En el año 2012 en mes de junio, ISACA lanzó COBIT 5 para la seguridad de la información, actualizando la última versión de su marco con fin de proporcionar una guía práctica en la seguridad de la empresa, en todos sus niveles prácticos.

COBIT 5 está basado en marcos de referencia establecidos, tales como el Modelo de Capacidad y Madurez (CMM, en inglés: Capability Maturity Model) del Instituto de Ingeniería de Software (SEI, en inglés: Software Engineering Institute); sin embargo, no incluye tareas y pasos de procesos, aunque está orientado a procesos de TI. Es un marco de referencia para gestión y control y no un marco de referencia para procesos centrado en lo que la empresa necesita hacer y no cómo lo debe hacer.

La audiencia objetiva es:

- Alta gerencia: Para lograr un balance entre los riesgos y las inversiones en un ambiente de TI.
- Gerentes funcionales: Para obtener garantía en cuanto a la seguridad y control de los servicios de TI proporcionados internamente o por terceros.
- Gerentes de TI: Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada.
- Auditores: Para respaldar sus opiniones y proporcionar asesoría a la gerencia sobre controles internos.

COBIT 5 otorga especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos.

COBIT 5 para seguridad de la información puede ayudar a las empresas a reducir sus perfiles de riesgo a través de la adecuada administración de la seguridad. La información específica y las tecnologías relacionadas son cada vez más esenciales para las organizaciones, pero la seguridad de la información es esencial para la empresa.

Los sistemas informáticos, están integrados a la gestión empresarial; por ello, las normas y estándares informáticos deben estar alineados e implantados previa la aprobación de la dirección de sistemas de la organización, misma que se encargará de la implementación de controles de acceso a la información, que se maneja en los diversos procesos del departamento encargado de las TI en consecuencia, se debe destacar que, las organizaciones

informáticas forman parte de la gestión de la empresa y se constituyen en un elemento de apoyo en la toma de decisiones.

La evaluación de los sistemas de información, deberá cubrir aspectos de planificación, organización, procesos, ejecución de proyectos, seguridades, equipos, redes y comunicaciones, con el objeto de determinar los riesgos a los que se encuentran expuesto dichos sistemas con respecto a la información.

3.6.2. Beneficios COBIT 5

Permite que la información y la tecnología relacionada sean gobernadas y gestionadas de manera integral para toda la empresa (entidad), abarcando de principio a fin el negocio y áreas funcionales, teniendo en cuenta los intereses de las partes interesadas internas y externas.

- Optimizar los servicios el coste de las TI y la tecnología
- Gestión de nuevas tecnologías de información
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas

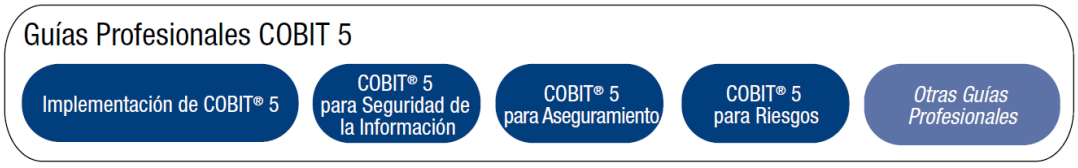


Gráfico 3.1. Guías referenciales – COBIT 5
Fuente: Manual COBIT 5 (IT Governance Institute)

3.7. Clasificación de los controles de TI

Al momento de realizar un proyecto de auditoría, se desarrollan una 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 de la efectividad de ambos depende el aseguramiento del procesamiento completo y preciso de la información.

El principal objetivo de la Auditoría de Sistemas es la revisión del estado de los controles internos que han sido definidos por la organización para lograr una mayor certeza de que la Gestión de las Tecnologías de la Información soportará efectiva y eficientemente los objetivos de negocios. Los controles son variados, a veces impuestos por la forma de trabajo de la

organización, a veces establecidos a través de la Gerencia General y la Gerencia de Informática. En algunas organizaciones, especialmente las financieras, los controles son requeridos por las normativas regulatorias del país.

3.8. Hipótesis

Si se realiza una auditoria en el área informática de la empresa Rosas del Corazón, se podrá minimizar las vulnerabilidades y riesgos de ataque y mejorar la administración y gestión de las TIC.

4. METODOLOGÍA

Según [16] dice: de acuerdo con el tipo de investigación que se pretenda realizar: los estudios de investigación pueden clasificarse:

4.1. Investigación de campo

Según [17] en su libro argumenta que "La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos".

En el presente proyecto se utilizará la investigación de campo para recabar información del lugar de trabajo, para poder interactuar directamente en el área de TIC de la empresa, ya que la información brindada por las personas proporcionará datos relevantes para alcanzar los objetivos planteados.

4.1.1. Método científico

El método científico de investigación es la forma de abordar la realidad, de estudiar la naturaleza, la sociedad y el pensamiento, con el propósito de descubrir su esencia y sus relaciones.

Al aplicar este método en el presente proyecto, ayudará a identificar la veracidad o no de la hipótesis, ya que será de mucha ayuda para obtener resultados orientados a la realidad basados en estudios prácticos.

En la presente investigación se aplicaran los siguientes métodos:

4.1.2. Método inductivo-deductivo

Según [18] "con este método y siguiendo reglas lógicas de deducción se llega a nuevos conocimientos y predicciones, las que posteriormente son sometidas a verificaciones empíricas".

En el desarrollo del presente proyecto se empleara para realizar la recolección de la información, se analizara la información de acuerdo con los hechos suscitados en tiempo real,

lo que permite deducir los resultados basados en experiencias, lo cual ayuda a elevar el grado de conocimiento sobre el tema.

4.1.3. Método analítico-sintético

En [18] este método también argumenta que Por medio de la abstracción el objeto es analizado en el pensamiento y descompuesto en conceptos abstractos, la formulación de dichos conceptos es la forma de lograr un nuevo conocimiento concreto. El hombre en el proceso del conocimiento de los fenómenos, al realizar la división de los mismos en sus partes ejecuta el análisis del objeto.

Durante la investigación se hallaran datos que estarán dispersos o separados, al aplicar este método se podrá reunir los distintos elementos, o partes de un todo, así se podrá gestionar de mejor manera con la información recolectada.

4.1.4. Método de observación

Según [18] la observación científica es la percepción planificada dirigida a un fin y relativamente prolongada de un hecho o fenómeno. Es el instrumento universal del científico, se realiza de forma consciente y orientada a un objetivo determinado.

En toda investigación es necesaria la observación, y en este caso no es la excepción, ya que ayuda a recopilar información que a simple vista es compleja de entender o de obtener, la observación permite conocer la realidad mediante la percepción directa de los objetos.

4.1.5. Método no experimental:

Es no experimental porque los datos de interés son recogidos en forma directa de la realidad para hacer un análisis sistémico del problema, con la finalidad de interpretarlo, explicar su causa y efecto y recomendar una solución.

En el presente trabajo de investigación se utilizarás las siguientes técnicas de investigación:

4.2. Técnicas de investigación

4.2.1. La entrevista

En [19] nos dice que “La entrevista, desde el punto de vista del método, es una forma específica de interacción social que tiene por objeto recolectar datos para una indagación. El investigador formula preguntas a las personas capaces de aportarle datos de interés, estableciendo un diálogo peculiar, asimétrico, donde una de las partes busca recoger informaciones y la otra es la fuente de esas informaciones.”

Al aplicar la entrevista se podrá recolectar información relevante que será de gran utilidad, ya que los datos vendrán de fuentes confiables de personas conocedoras del tema o que utilizan los servicios TIC de manera directa.

A. Tipos de entrevistas

- *Entrevistas libres:* son las entrevistas en las que se sigue un guion básico para obtener la información, pero la participación del entrevistado es libre y sin ninguna atadura. El propósito es tener mayor intimidad en la plática para que la información sea más verídica.
- *Entrevistas dirigidas:* este tipo de entrevista siempre se dirigen las opiniones del entrevistado, forzando sus respuestas dentro de un parámetro o guion establecido.
- *Entrevista de exploración:* Este tipo de entrevista permite que el primer contacto con los auditados se a través de este tipo de entrevistas, por lo general son de carácter libre.
- *Entrevistas de comprobación:* este tipo de entrevista se utiliza para comprobar la veracidad de la información recopilada durante la evaluación y permiten corroborar o rectificar los datos recolectados sobre las observaciones encontradas.
- *Entrevistas de información:* este tipo de entrevista permite al auditor comente cada una de las desviaciones que reporta en su informe y sirve para rectificar o ratificar las situaciones que está informando.
- *Entrevistas informales:* este tipo de entrevista ayuda al auditor a conocer algún tipo de problemática que solo se expresa cuando no existe la presión de una entrevista formal.

B. Tipos de preguntas

Así como existen tipos de entrevistas, existen también tipo de preguntas que se realizan de acuerdo con las necesidades y características de cada entrevista que se las describe a continuación:

- *Preguntas abiertas: s*on entrevistas realizadas con este tipo de preguntas, donde el entrevistado tiene la libertad absoluta para expresar su opinión sin ningún límite, aunque a veces se salga del tema planteado.

- *Preguntas cerradas:* son preguntas cerras o concretas que se realizan con el propósito de centras las preguntas del auditado hacia el objetivo de la entrevistas sin dejarlo salir del tema.

C. Formas de realizar una entrevista para la auditoria informática

- *Entrevistas tipo embudo:* son preguntas de carácter general (abiertas), y conforme avanza la plática va haciendo preguntas más concretas.
- *Entrevistas tipo pirámide:* son fundamentadas para recopilar información en la auditoria, pero se encuentra de forma inversa a la anterior. Inicia con preguntas cerras y termina con preguntas abiertas.
- *Entrevistas tipo diamante:* este tipo de entrevistas inicia con preguntas cerradas y conforme avanza la plática se realizar preguntas más abiertas, preguntas generales, y de acuerdo a la necesidad vuelve hacer preguntas cerradas para enfocarse al tema de interés.
- *Entrevistas tipo reloj de arena:* este tipo de preguntas inicia con preguntas de carácter general, conforme avanza la plática, va realizando preguntas más concretas, enfocadas hacia temas de su interesa, y finaliza con preguntas abiertas, buscando que el entrevistado proporcione la mayor cantidad de información.

4.2.2. La observación

Según [19] la observación es la percepción directa, atenta racional, planificada del fenómeno de estudio. Percepción porque se la realiza a través de los órganos de los sentidos: visión, audición, especialmente directa porque se la realiza sin intermediarios y en el lugar mismo de los hechos. Atenta, en el sentido de no dejar escapar ningún detalle por más insignificante que parezca, en muchas ocasiones ese detalle es la clave para la comprensión de una parte del proceso investigativo racional porque trata de unir los diferentes aspectos del fenómeno observado en un todo integro e integral, que explique las variable, su relación, las hipótesis y otros aspectos de la investigación.

4.2.3. Cuestionarios

Es la recopilación de datos mediante preguntas impresas en cedulas o fichas, en las que el encuestado responde con su criterio, de esta manera el autor obtiene información útil que pueda concentrar, clasificar e interpretar por medio de su tabulación y análisis.

4.3. Marco metodológico COBIT 5

"COBIT se ha convertido en el standard de la industria para todos aquellos que buscan adoptar un marco de gobierno en el manejo de tecnología de la información. Este marco de referencia incluye guías de negocio simples de usar y sensibles a todas las realidades que tenemos en las empresas de esta región", comentó Salomón Rico, CISA, CISM, CGEIT, miembro del comité de Guías y prácticas de ISACA.

4.3.1. COBIT 5

Al tomar una guía para realizar un marco de referencia nos dice que "COBIT 5 se puede adaptar a todos los tamaños de empresa (inclusive a las Pymes), a todos los modelos de negocios, entornos de tecnología, industrias, lugares y culturas corporativas. Y se puede aplicar a:" [20]

- Seguridad de la información
- Gestión de riesgo
- Gobierno y administración de TI en la empresa
- Actividades de aseguramiento
- Cumplimiento legislativo y regulador

Se utilizará el estándar COBIT 5.0, para la evaluación y auditoría del ambiente informático de la empresa "Rosas del Corazón", aplicando conceptos de control interno y procedimientos.

Identificación de Soluciones Automatizadas: donde se utilizaran criterios de información sobre efectividad y eficiencia en los procesos del negocio, requeridos para la empresa Rosas del Corazón de esta manera satisfacer los requerimientos de los usuarios.

4.3.2. Metodologías COBIT 5

Según [21] indica que se realiza una guía para que las entrevistas y cuestionamiento se las realice a las personas que laboran en el área de TIC con la finalidad de reunir los datos necesarios para el análisis de la situación actual de la empresa y efectuar los diagnósticos necesarios.

COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas, tal y como se muestra en el gráfico 4.2.

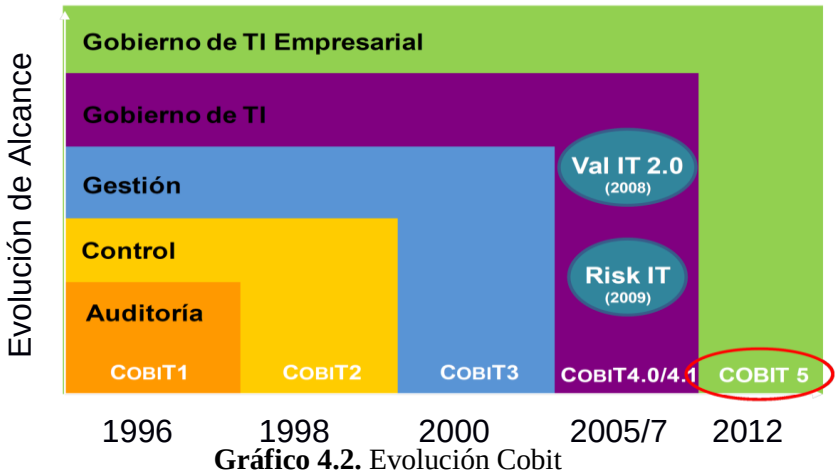


Gráfico 4.2. Evolución Cobit
Fuente: Documentación COBIT 5 (www.isaca.org/cobit)

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones y responsables de TI. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

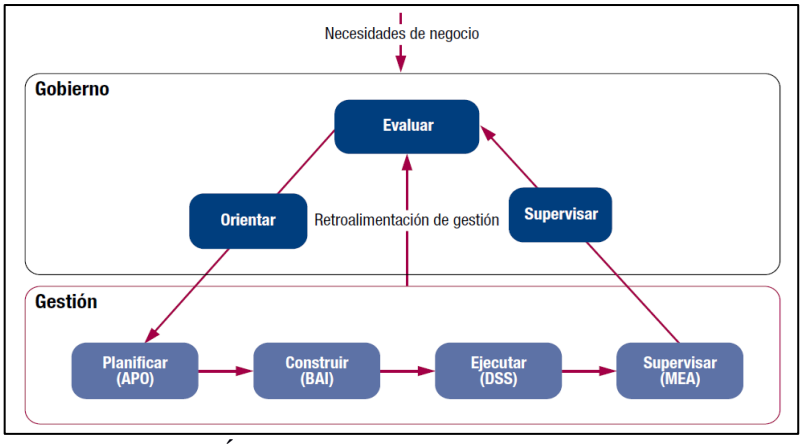


Gráfico 4.3 Áreas clave de gobierno y gestión COBIT 5
Fuente: Manual COBIT 5 (IT Governance Institute)

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI, es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- **Gobierno:** Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).
- **Gestión:** Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM).

El modelo de referencia de procesos de COBIT 5 es el sucesor del modelo de procesos de COBIT 4.1 e integra también los modelos de procesos de Risk IT y Val IT. La Figura Nº 4 muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5. Los detalles de todos los procesos de acuerdo con el modelo de proceso anteriormente descrito, están recogidos en la guía COBIT 5: Procesos Catalizadores

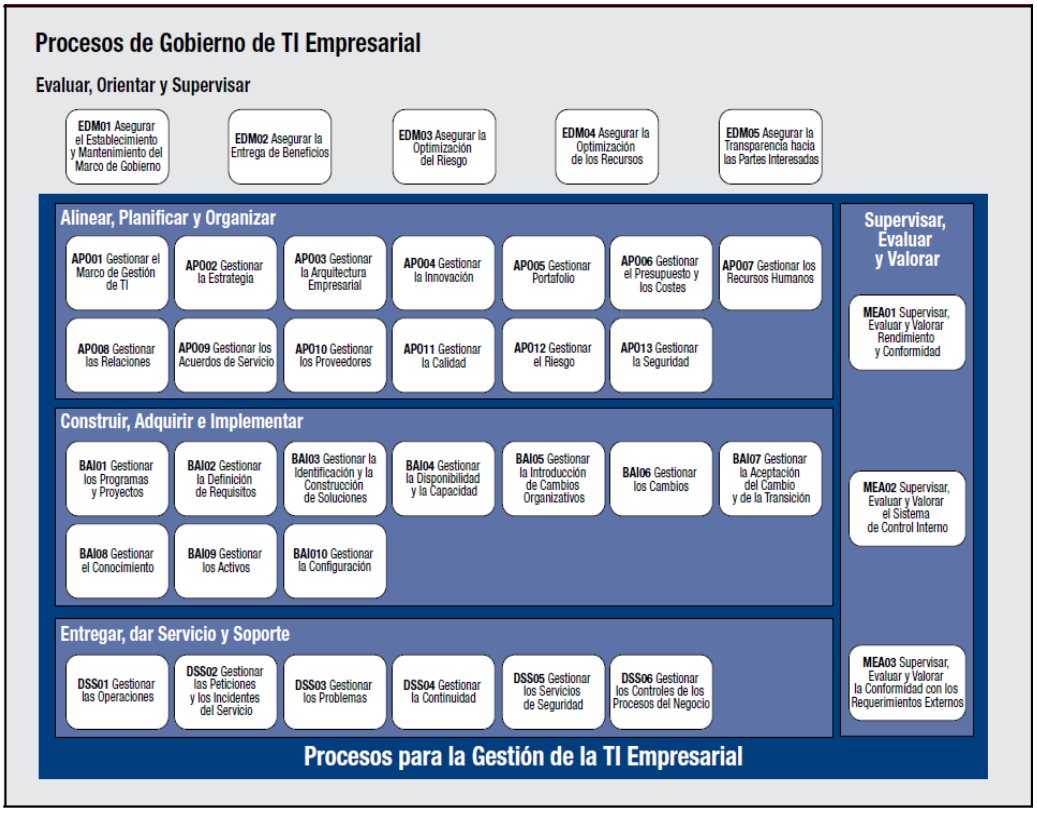


Gráfico 4.4. Modelo de referencia de procesos – COBIT 5
Fuente: Manual COBIT 5 (IT Governance Institute)

El marco de gobierno y gestión de TI de COBIT 5, tiene como principal objetivo obtener información de alta calidad lo que redundará en crear valor al negocio y alcanzar niveles de calidad y excelencia en su operación, con la consecuencia de ahorrar cosas, cumplir con las normas adecuadas.

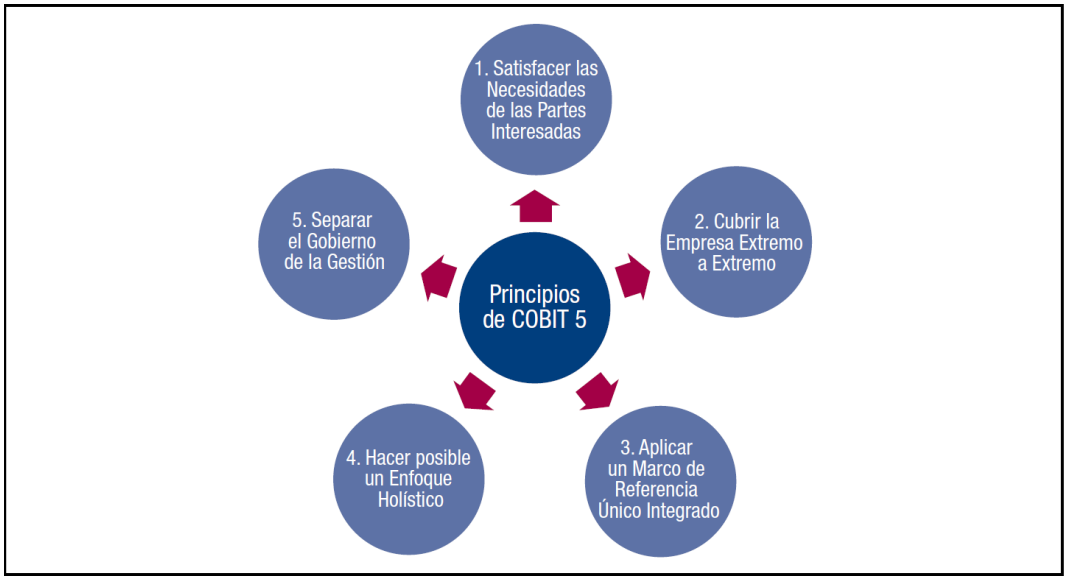


Gráfico 4.5. Principios COBIT 5
Fuente: Manual COBIT 5 (IT Governance Institute)

COBIT 5 se fundamente en cinco principios:

1. Satisfacer las necesidades de las partes interesadas
2. Cubrir la empresas de extremo a extremo
3. Aplicar un marco de referencia único integrado
4. Hacer posible un enfoque holístico
5. Separar el gobierno de la gestión

A lo largo del tiempo, el ciclo de vida debería seguirse de modo iterativo, al tiempo que se construye un modelo sostenible de gobierno y gestión de TI corporativa.

4.4. Satisface las necesidades de las partes interesadas

Uno de los cinco principios de COBIT 5, ayuda entender y direccionar de mejor manera los objetivos de una empresa, es así que este objetivo nos permite entender que las empresas existen para crear valor para sus accionistas.

4.5. Cascada de metas de COBIT 5

Según [22] “Cada empresa opera en un contexto diferente, este contexto está definido en factores internos y factores externos y requiere un sistema de gobierno y gestión personalizado”.

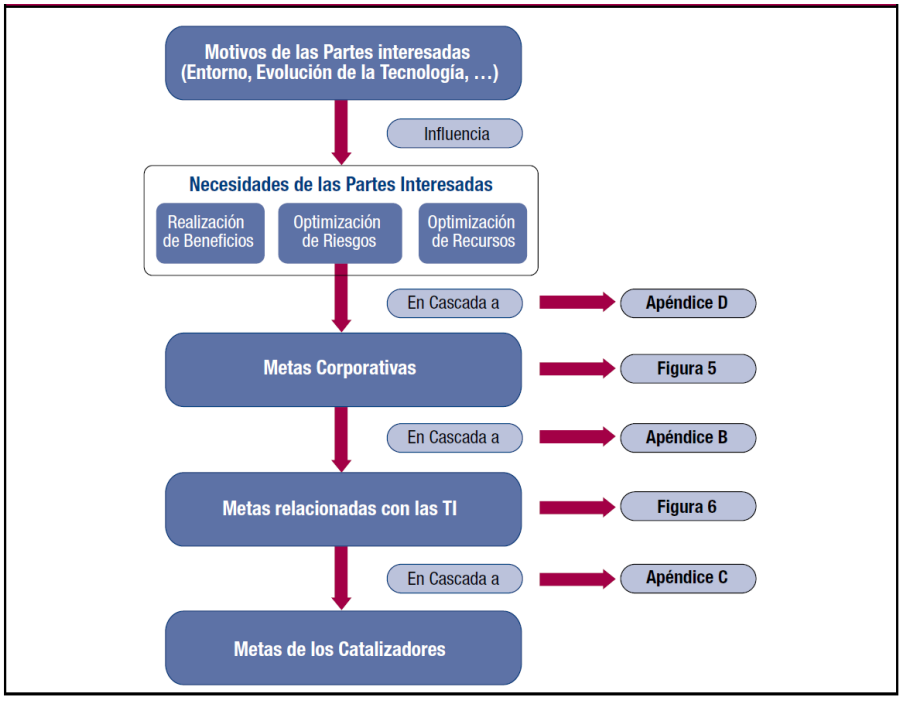


Gráfico 4.6. Cascada de metas de COBIT 5
Fuente: Manual COBIT 5 (IT Governance Institute)

La cascada de metas COBIT es un mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI.

1. Motivos de las partes interesadas influye en las necesidades de las partes interesadas: las partes interesadas están influenciadas por diferentes motivos, entre ellos cambios de estrategias, nuevas tecnologías en un entorno cambiante [22].
2. Las necesidades de las partes interesadas desencadenan metas empresariales: Estas necesidades pueden estar relacionadas con un conjunto de metas empresariales genéricas, en [22] presenta una lista de objetivos comúnmente usados con los que se los puede relacionar fácilmente con la mayoría de metas corporativas de una empresa.
3. Cascada de Metas de empresa a metas relacionadas con las TI: El logro de las metas empresariales requiere un número de resultados relacionados con las TI, que están representados por las metas relacionadas con las TI.
4. Cascada de metas relacionadas con las TI hacia metas catalizadoras: alcanzar las metas relacionadas con las TI requiere la aplicación satisfactoria y el uso de varios catalizadores, los catalizadores incluyen procesos, estructuras organizativas e información.

4.6. Procesos de seguridad de la información seleccionados

En base al gráfico 4.4, se realiza un análisis para identificar claramente los dominios, procesos y prácticas de gestión aplicables [23] en base al mapeo entre las metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI.

Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Gráfico 4.7. Metas relacionadas con las TI
Fuente: Manual COBIT 5 (IT Governance Institute)

Dimensión del CMI	Meta Corporativa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Gráfico 4.8. Metas corporativas de COBIT 5
Fuente: Manual COBIT 5 (IT Governance Institute)

Al utilizar la cascada de Metas de COBIT 5 permite definir las prioridades de implementación, mejora y aseguramiento del gobierno de las TI de la empresa, que se basa en las metas corporativas de la empresa y el riesgo relacionado.

Según [22] las metas en cascada relacionada entre las metas empresariales con la TI y entre las metas relacionales con la TI y catalizadores de COBIT, no son una verdad universal, sino que sirven como una guía, ya que cada empresa establece sus objetivos con distintas prioridades, y estas prioridades pueden cambiar en el tiempo.

Esto quiere decir que para la presente auditoria se puede ajustar COBIT a los requerimientos de la empresa.

			Meta corporativa																
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		Meta relacionada con las TI	Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Gráfico 4.9. Mapeo entre las metas corporativas de COBIT 5 y las metas relacionadas con las TI.
Fuente: Manual COBIT 5 (IT Governance Institute)

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de los costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Cómo se consigue valor mediante el uso de TI? ¿ Está el usuario final satisfecho con la calidad del servicio de TI?	■	■				■	■						■			■	■
¿Cómo se gestiona el rendimiento de TI?		■			■				■	■	■	■		■			
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?	■	■						■					■			■	■
¿Cómo puedo construir y estructurar mejor mi departamento de TI?								■		■	■	■		■	■	■	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?			■	■						■							
¿Cuáles son los requisitos (de control) para la información?				■					■						■		
¿He contemplado todo los riesgos relacionados con TI?			■				■		■						■		
¿Estoy ejecutando una operación de TI eficiente y robusta?					■		■										
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?										■		■		■			

Gráfico 4.10. Mapeo entre las metas corporativas de COBIT 5 y las preguntas del gobierno y la gestión

Fuente: Manual COBIT 5 (IT Governance Institute)

Para orientarse de mejor manera se utiliza una serie de preguntas para que sean relacionadas con el objetivo de TI empresarial. Como se muestra en el Gráfico 4.11. Son las preguntas que servirán de guía que ofrece COBIT 5, para realizar un mapeo con las metas relacionadas con las TI, como se muestra en los gráficos anteriores, esto ayudará a fomentar de mejor manera las preguntas durante el desarrollo de la auditoria, tomando en cuenta que el modelo COBT 5, sugiere que se puede relacionarlas con las metas corporativas, lo cual permitirá que pueden ser resueltas con efectividad.

Partes Interesadas Internas	Preguntas de las Partes Interesadas Internas
• Consejo de Administración • Director general ejecutivo (CEO) • Director financiero (CFO) • Director de sistemas de información (CIO) • Responsable de riesgos • Ejecutivos del negocio • Propietarios de los procesos del negocio • Responsables del negocio • Responsables de riesgos • Responsables de seguridad • Responsables del servicio • Responsables de recursos humanos • Auditoría interna • Responsables de privacidad • Usuarios de TI • Gerentes de TI • Etc.	• ¿Cómo consigo valor del uso de TI? ¿Están los usuarios finales satisfechos con la calidad del servicio de TI? • ¿Cómo gestiono el rendimiento de TI? • ¿Cómo puedo explotar mejor las nuevas tecnologías para nuevas oportunidades de negocio? • ¿Cómo construyo y estructuro mejor mi departamento de TI? • ¿Cuánto dependo de los proveedores externos? ¿Estoy gestionando bien los contratos de externalización de TI? • ¿Cómo obtengo aseguramiento sobre los proveedores externos? • ¿Cuáles son los requisitos (de control) para la información? • ¿Considero todos los riesgos relativos a TI? • ¿Estoy realizando una operación de TI eficiente y resiliente? • ¿Cómo controlo el coste de TI? ¿Cómo utilizo los recursos de TI de la manera más efectiva y eficiente? • ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes? • ¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento? • ¿Cómo consigo aseguramiento sobre TI? • ¿Está bien asegurada la información que se está procesando? • ¿Cómo puedo mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible? • ¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué? ¿Está siendo TI un obstáculo para ejecutar la estrategia de negocio? • ¿Cuán críticas son las TI para la sostenibilidad de la empresa? ¿Qué haría si las TI no estuvieran disponibles? • ¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio? • ¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI? • ¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio? • ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos? • ¿Cuánto se tarda en la toma de decisiones importantes de TI? • ¿Son transparentes el esfuerzo y las inversiones totales en TI? • ¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?
Partes Interesadas Externas	**Preguntas de las Partes Interesadas Externas**
• Aliados del negocio • Proveedores • Accionistas • Reguladores/gobierno • Usuarios externos • Clientes • Organizaciones de estandarización • Auditores externos • Consultores • Etc.	• ¿Cómo sé que las operaciones de mi aliado de negocio son seguras y fiables? • ¿Cómo sé que la empresa cumple con las normativas y regulaciones aplicables? • ¿Cómo sé que la empresa está manteniendo un sistema efectivo de control interno? • ¿Los aliados del negocio mantienen bajo control la cadena de información entre ellos?

Gráfico 4.11. Cuestiones sobre las TI de gobierno y dirección
Fuente: Manual COBIT 5 (IT Governance Institute)

Todas estas preguntas están relacionadas con la gestión y administración de las TI en una entidad, COBIT nos ayuda a aplicar estas preguntas con la finalidad de relacionar los objetivos de TI con los objetivos de la empresa. Recordando que COBIT es una guía y se pueden realizar los ajustes necesarios según el requerimiento de la auditoria.

5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

5.1 Análisis de la encuesta aplicada al personal de la empresa Rosas del Corazón

Objetivo: obtener información fundamental para evaluar los controles de las seguridades informáticas dentro de la Empresa Rosas del Corazón.

1. ¿La empresa cuenta con un Departamento informático?

Tabla 5.1. Departamento Informático

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	15	100%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

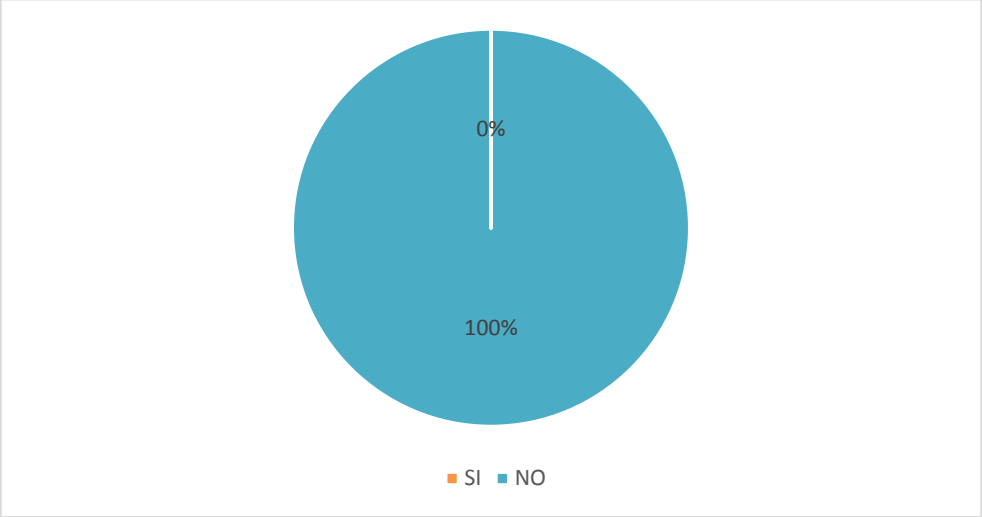


Gráfico 5.12. Departamento Informático
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas encuestadas en el área administrativa de Rosas del Corazón las 15 personas representan al 100%, manifiestan que existe una persona que realiza el mantenimiento a los equipos informáticos, también se encarga del soporte y ayuda inmediata.

Los usuarios manifiestan que no existe un departamento de TI, y la persona que da mantenimiento cumple con parte de estas funciones, pero necesitan a alguien a tiempo completo.

2. ¿Se efectúan respaldos planificados de la información de la empresa?

Tabla 5.2. Respaldos de la información

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	5	33%
NO	10	67%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

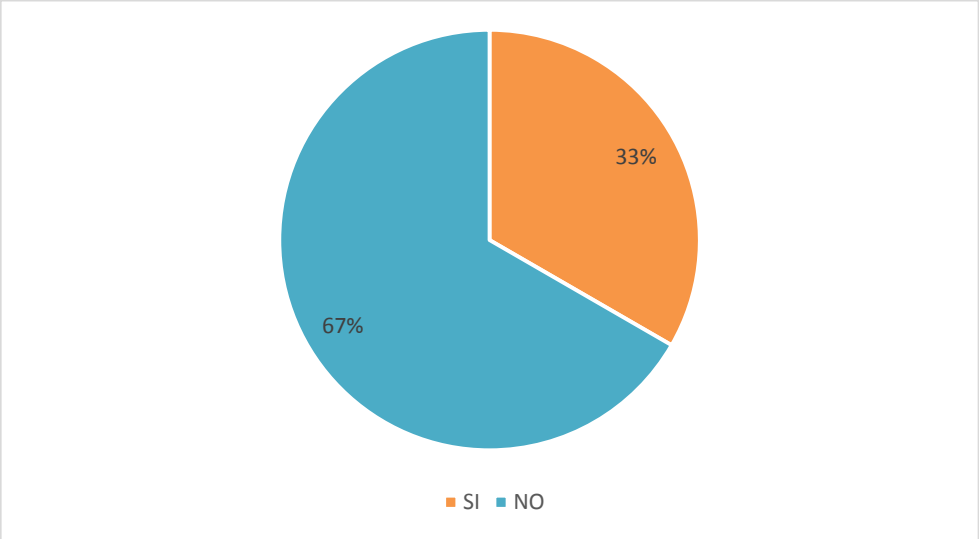


Gráfico 5.13. Respaldos de la información
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas encuestadas en el área administrativa de Rosas del Corazón 5 personas que representan al 33.3% manifiestan que los respaldos de la información son realizados de manera organizada, mientras que el 67% del personal administrativo asegura que no se realiza un respaldo planificado.

Este tema inquieta mucho a las personas que dependen de esta información ya que hace poco tiempo la empresa sufrió de un ataque cibernético. Favorablemente se logró recuperar %100 de la información de la empresa, y se logró restablecer el servidor de manera eficiente.

3. ¿Se ejerce un control del sistema informático?

Tabla 5.3. Control sistema informático

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	8	53%
NO	7	47%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

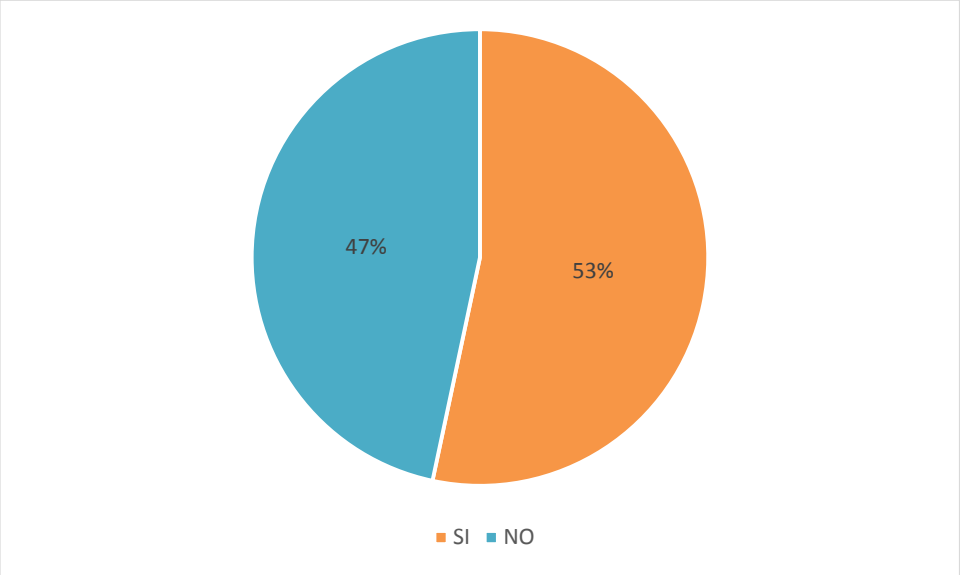


Gráfico 5.14. Control sistema informático
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan los equipos informáticos, 8 personas que representan el 53%, indican que si existe un control del sistema informático en cuanto al control y configuración del software que manejan en la empresa, en cambio 7 personas que representan el 47% indican que no existe un control.

Como resultado de estos sucesos los usuarios ocasionalmente han sufrido algún tipo de desperfecto al momento de usar el sistema informático ya sea de manera física o en cuanto al software y en ocasiones hasta problemas graves en cuanto a las conexiones de la red interna de la empresa.

4. ¿Utiliza usuario y contraseña para acceder a su equipo de trabajo?

Tabla 5.4. Acceso al equipo

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	12	80%
NO	3	20%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

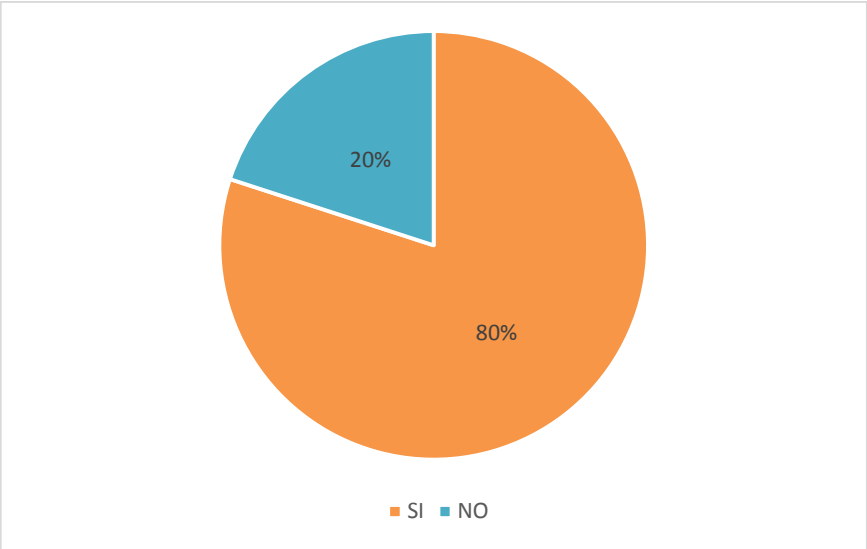


Gráfico 5.15. Acceso al equipo
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan los equipos informáticos, 12 personas que representan el 80%, indican que si utilizan un usuario y su respectiva contraseña para iniciar su sesión en el computador de trabajo, por lo cual esto hace más seguro el uso del equipo de cómputo, en cambio 3 personas que representan el 20% indican que no disponen de un usuario y contraseña.

La ausencia de usuario y contraseña en la sesión del computador representa un peligro para el control de acceso a la información que maneja cada usuario. Esto pone en riesgo la información.

5. ¿El sistema cuenta con claves de seguridad?

Tabla 5.5. Uso de claves de seguridad

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	15	100%
NO	0	0%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Gráfico 5.16. Uso de claves de seguridad
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas encuestadas, 15 personas que representan el 100%, afirman que el sistema informático que se maneja en la empresa Rosas del Corazón UNOSOF y SOFIA requiere de clave para acceder a su cuenta.

La existencia de un usuario y clave para acceder al software de la empresa representa una mayor seguridad para la información y mayor confianza para el usuario que utiliza el recurso informático.

6. ¿El sistema cuenta con personal técnico que ayude cuando se producen inconvenientes?

Tabla 5.6. Ayuda y soporte del sistema

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	8	53%
NO	7	47%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

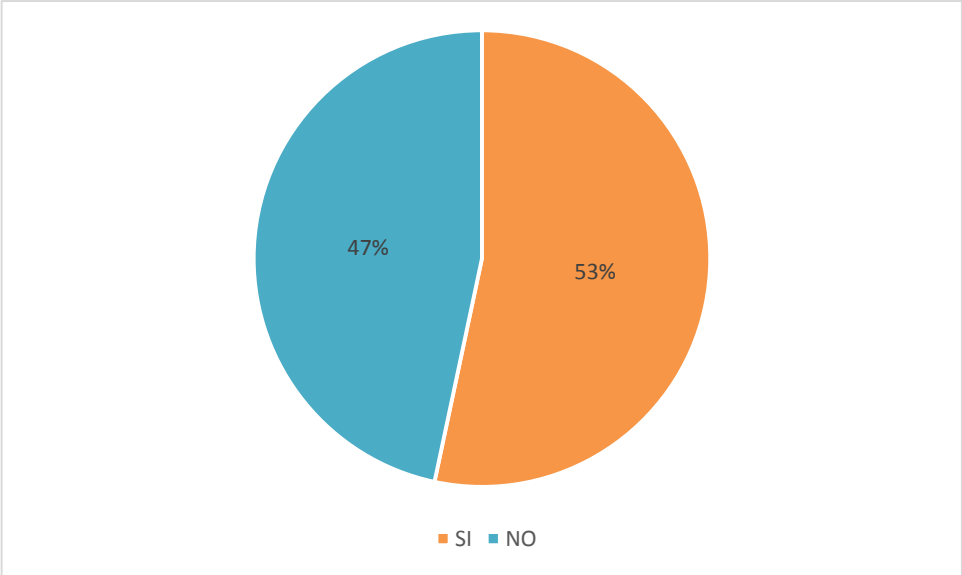


Gráfico 5.17. Ayuda y soporte del sistema
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan los equipos informáticos, 8 personas encuestadas representan el 53%, indican que si existe personal de soporte técnico al momento de tener algún tipo de dificultad con el sistema informático, mientras que 7 personas que representa el 47% indica que no existe una persona que ayude cuando se producen inconvenientes en el sistema informático.

Los usuarios afirman que no existe una persona como tal, ya que deben llamar por teléfono a soporte técnico del software para que resuelvan el inconveniente de manera remota o gestionando la ayuda a través de la llamada telefónica. Esto causa molestias y en ocasiones retraso en el trabajo, ya que no existe una ayuda inmediata.

7. ¿Existe un instructivo en el uso del software?

Tabla 5.7. Instructivo de uso de software

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	1	7%
NO	14	93%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

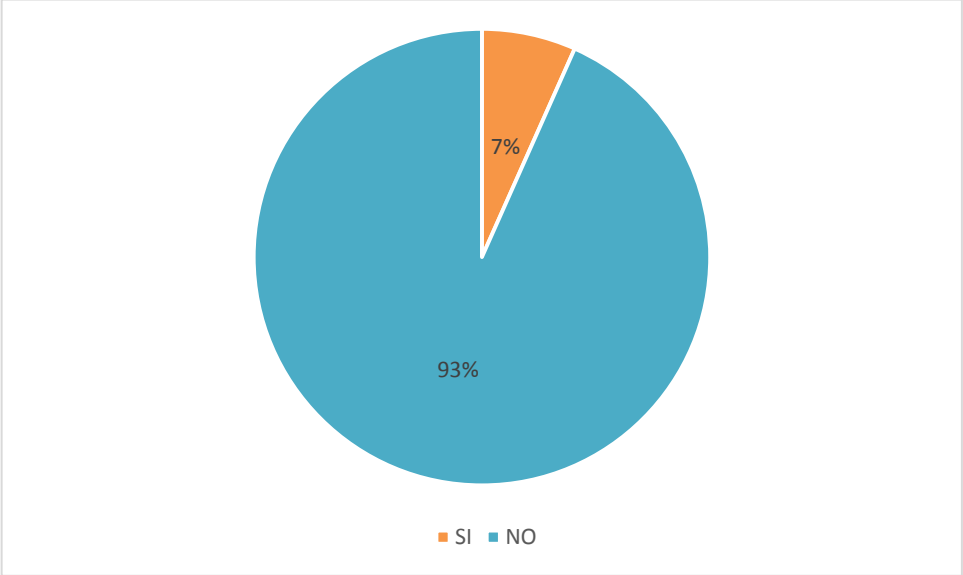


Gráfico 5.18. Instructivo de uso de software
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan el sistema informático, 1 persona que representa el 7%, indican que si existe un instructivo o manual para el uso del software de la empresa, mientras 14 personas que representan el 93% afirman que no existe un manual o instructivo para el uso de software de la empresa.

Al no existir un manual se han creado inconvenientes, muchas de las veces esto ha causado retraso en el registro de la información. También afirman que existió una capacitación en la fase de pruebas durante el desarrollo del sistema. Pero los usuarios afirman que no es suficiente.

8. ¿Existen políticas para la seguridad para el uso del equipo informático?

Tabla 5.8. Políticas de seguridad

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	15	100%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

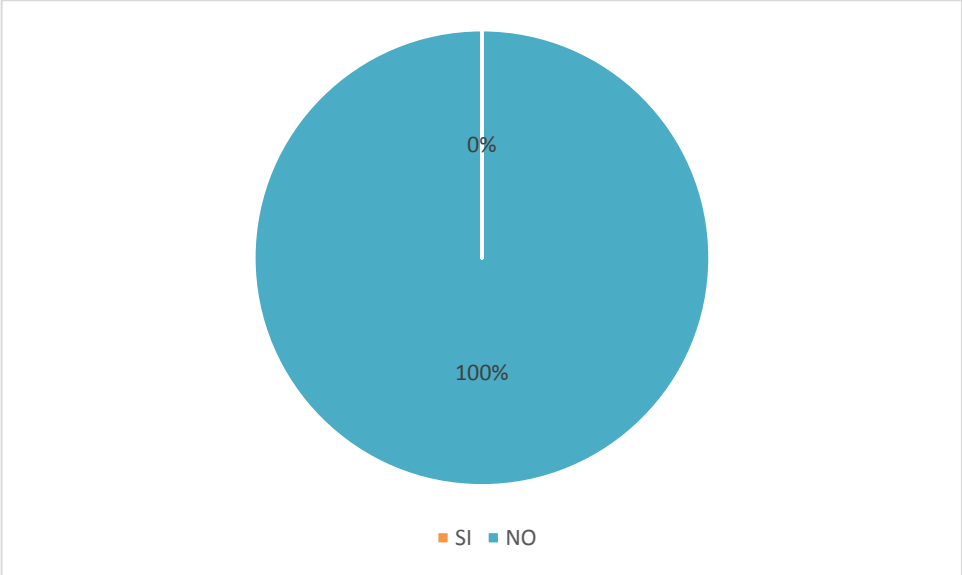


Gráfico 5.19. Políticas de seguridad
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan el equipo informático, las 15 representan el 100% de las personas encuestadas, afirman que en la empresa Rosas del Corazón no existen políticas de seguridad sobre el equipo informático.

Los usuarios indican que deberían existir políticas de seguridad implantadas, seria de mucha ayuda conocer algunas normas de uso del equipo, normas de acceso a la información, pero actualmente no conocen políticas escritas que ratifiquen la seguridad o el uso de los equipos.

9. ¿Los equipos servidores están en un área segura?

Tabla 5.9. Seguridad de los servidores

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	1	7%
NO	14	93%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

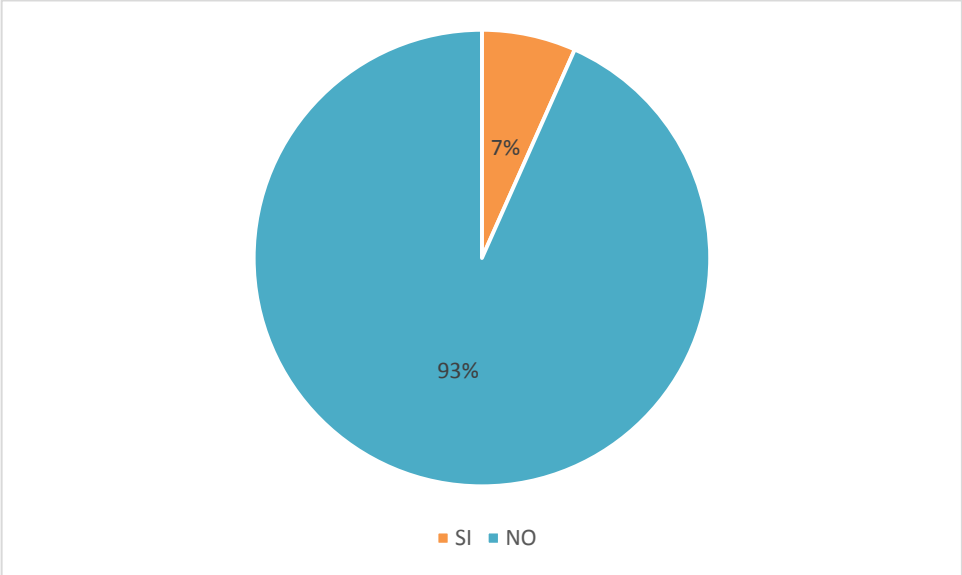


Gráfico 5.20. Seguridad de los servidores
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan el equipo informático, 1 persona que representa el 7% de las personas encuestadas, indica que los equipos servidores están en un área segura, ya que cuenta con un guardia, y con cámaras de seguridad, mientras que el 93% que son 14 personas afirman que los servidores no están en un área segura.

Los usuarios afirman que existe un fácil acceso al área de servidores, y que la infraestructura física no es la adecuada, ya que están a la vista de todos y se encuentra en un área que no tiene seguridades en las ventanas ni en las puertas.

10. ¿Cree que el computador tiene las seguridades necesarias?

Tabla 5.10. Seguridad en los equipos

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	7	47%
NO	8	53%
TOTAL	**15**	**100%**

Fuente: Personal empresa
Elaborado por: Diego Quillupangui

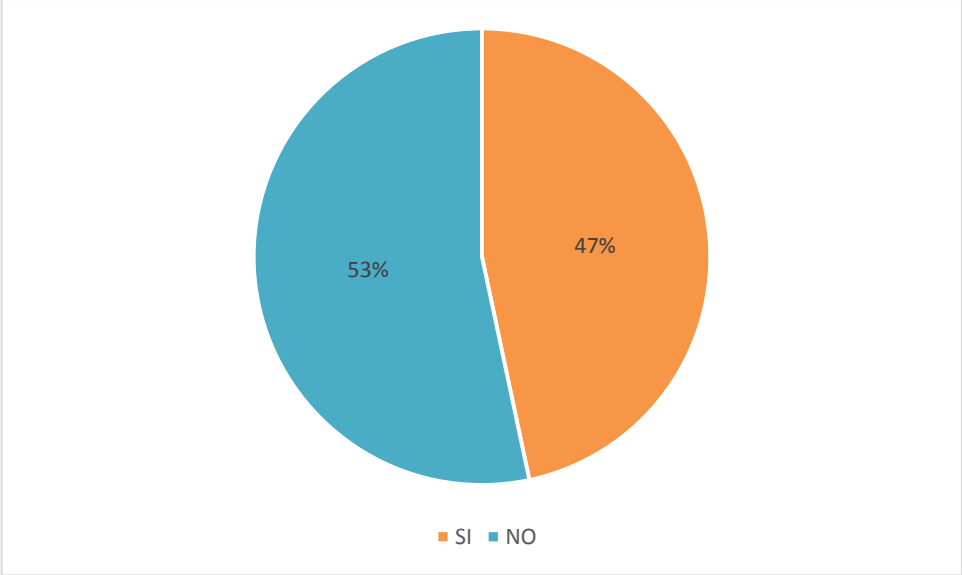


Gráfico 5.21. Seguridad en los equipos
Fuente: Personal empresa
Elaborado por: Diego Quillupangui

Análisis e interpretación

De las 15 personas que manejan el equipo informático, 7 personas representan el 47% de las personas encuestadas, los usuarios indican que los equipos de cómputo si tienen las seguridades de hardware y de software, en cambio el 53% de las personas encuestadas afirman que los computadores no tienes seguridades en el hardware y el software.

Los usuarios afirman que si existen seguridades ya que identifican que continuamente se actualiza el antivirus y el antimalware de sus computadores, así como también otros aplicativos.

5.2. Análisis de resultados de la entrevista aplicada al administrador de la empresa Rosas del Corazón

Objetivo: Recopilar la información que permita conocer más a fondo la empresa y los detalles menores en cuanto al área de TI

1. ¿Se ha realizado algún tipo de auditoria en el área informática?

En administrador de la empresa manifiesta que no se han realizado auditorias aplicadas al área informática.

2. ¿El área Informática cuenta con una planificación estratégica?

El administrador manifiesta que es de mucha importancia contar con una planificación estrategia, pero al momento no cuenta con una, pero que cuentan con una programación para gestión de la empresa.

3. ¿Existen políticas informáticas internas que conozca y se estén aplicando?

El administrador de la empresa notifica que al momento no cuentan con políticas informáticas escritas.

4. ¿Estas políticas son importantes?

El administrador explica que las políticas son importantes, ya que con la ayuda de estas políticas podrían trabajar en la planificación, y podrían tener una mejor estructura del área informática de la empresa.

5. ¿Quiénes están autorizados a acceder a los archivos y programas de la empresa?

Según el administrador asegura que en la actualidad tiene personas específicas que tienen acceso a estos archivos. Son personas de mucha confianza. No tienen roles por escrito.

6. ¿Todos los usuarios tienen usuario y contraseña para acceder a sus equipos de trabajo?

El administrador de la empresa manifiesta que este tema es de su conocimiento y él ha verificado que sim, que todos los computadores tiene usuario y contraseña

7. ¿Qué medidas de seguridad existen en Rosas del Corazón?

El administrador afirma que las medidas de seguridad: son copias de los archivos, tener bloqueos suficientes para limitar las inseguridades ante ataque informáticos. Los cuales actualmente están activos

8. ¿Es importante implementar un plan de contingencia?

El administrador de la empresa detalla que si es conveniente tener un plan de contingencia en el área informática, ya que es un área la cual está expuesta constantemente, ya que la tecnología va mejorando y también se van actualizando los ataques informáticos, y es importante estar actualizados y estar preparados antes este tipo de ataque

9. ¿El personal está preparado para un ataque informático?

El administrador expone que el personal de Rosas del Corazón actualmente no estaría preparado ante un ataque informático.

10. ¿El lugar de los servidores cuenta con todas las seguridades físicas?

El administrador explica que tienen seguridades en las puertas, sensores de humo, cámaras de seguridad, y también disponen de alarmas que ayuda a tener seguros los equipos servidores.

11. ¿Hay alguna planificación en cuanto a la inversión anual para el área de TI?

El administrador de la empresa describe que actualmente no dispone de una planificación, las inversiones se las realiza de acuerdo a las necesidades de la empresa.

12. ¿Cuán importante son las TI para la empresa?

El administrador explica que en la actualidad son muy importantes las TI, ya que toda la operación de la empresa está basada en la informática, es muy importante actualizarse, tener un mantenimiento constante, para un desenvolvimiento eficiente en las labores del día a día.

13. ¿Actualmente cómo se controlan las tecnologías de la información en la empresa?

El administrador manifiesta que si existe una persona que continuamente realiza soporte y mantenimiento en cuanto a los equipos.

14. ¿Existe un plan para restablecer operaciones en caso de un fallo en la TI?

El administrador de la empresa manifiesta que actualmente si dispone de este plan. Ya que cuenta con los respaldos que son realizados constantemente.

15. ¿La empresa usa software libre?

El administrador manifiesta que toda la empresa maneja sistema operativo Windows. Software con licencia.

16. ¿Se dispone a las contraseñas administrables para los servidores de la empresa?

El administrador de la empresa manifiesta que sí disponen de las contraseñas de los equipos, que actualmente manejan dos sistemas informáticos que son SOFIA y UNOSOF. Los dos sistemas son realizados por terceros, entonces ellos también disponen de acceso a los servidores para que puedan administrar los sistemas.

17. ¿Quiénes tiene acceso a la red WIFI y bajo que parámetros?

Según el administrador explica que no todas las personas tienen acceso a la red, las personas que administran las contraseñas de la red wifi son la persona que realiza el mantenimiento y la gerencia administrativa. Existen parámetros para acceder, ya sea en casos urgentes, para no saturar la red.

18. ¿Alguna vez han tratado de hackear su red o el equipo informático y cuál fue su primera acción?

El administrador expone que la primera acción que tomaron fue buscar los respaldos para tratar de restaurar los servicios de los sistemas informáticos, cambiar las claves de seguridad.

19. ¿Existen un plan de acción en caso de un fallo en la red?

El administrador de la empresa manifiesta que no existe un plan de acción o manual ante algún fallo en la red.

20. ¿Quién toma decisiones en cuanto a los cambios de red?

El administrador relata que para modificar la red interna, las decisiones las toman directamente las gerencias, y las toman de acuerdo a los fallos que puedan ocurrir en la empresa. De acuerdo a las necesidades del caso.

21. ¿Cada que tiempo se realiza las actualizaciones de seguridades del sistema operativo?

El administrador explica que no existe ninguna planificación para realizar actualizaciones de los sistemas operativos. Las medidas actualmente se toman bajo los requerimientos y necesidades de la empresa.

22. ¿Poseen los usuarios restricciones de uso de su computador? En cuanto a uso a programas.

El administrador de la empresa da a conocer que cada computador tiene limitaciones para que no puedan utilizar programas que no corresponden, tienen restricciones, tienen bloqueos en la red, para que no puedan descargarse información que no es necesaria.

23. ¿Tienen una bodega para los equipos informáticos nuevos o descompuestos, partes y piezas?

Actualmente se dispone de una bodega para almacenar los equipos informáticos, y los equipos dañados tienen el trato correspondiente, ya que se tiene conocimiento que pueden perjudicar al medio ambiente y se buscan gestores ambientales.

24. ¿Existe un plan para tratar los equipos dañados?

El administrador manifiesta que si existe un plan, un proceso a seguir. Tiene un plazo para darle de baja, o esperar que tenga solución.

25. ¿Existen acuerdos con proveedores de equipos informáticos?

El administrador explica que existen acuerdos verbales con empresas proveedores de equipos informáticos.

26. ¿Cuál es el proveedor de internet?

El administrador manifiesta que la empresa proveedora de internet es TELCONET, ya que prestan un buen servicio, última tecnología, y son más viables para tener su servicio en la empresa.

27. ¿Los usuarios tiene acceso a internet libremente?

Los usuarios tienen acceso limitado al internet.

28. ¿Tienen un presupuesto asignado al mantenimiento?

No existe un presupuesto planificado para mantenimiento informático.

29. ¿La empresa está preparada ante un ataque cibernético?

El administrador explica que continuamente se cambia las claves de los sistemas, de los equipos y de los servicios de internet.

30. ¿Desde su punto de vista es importante desarrollar políticas de seguridad informática y socializarlas con el personal?

El administrador manifiesta que actualmente sería muy importante tener políticas de seguridad informática.

6. ESTUDIO DEL MODELO COBIT EN LA EMPRESA ROSAS DEL CORAZÓN

6.1. Situación actual de la empresa

Rosas del Corazón, es una empresa que nació en el año de 1993, con la finalidad de satisfacer a los clientes más exigentes como son: Rusia, Ucrania, Europa, Caribe, Asia y EEUU.

Rosas del Corazón, trabaja acorde a la naturaleza, ya que tiene el privilegio de estar situado a una altitud ideal para la producción y el cultivo de rosas. En la actualidad la empresa cuenta con dos sucursales que son centros productores de flor para la exportación.

La calidad es un tema importante para la empresa, así que constantemente innovan sus controles de calidad y el servicio al cliente:

- Ofrecen la variedad de rosas más populares
- Larga vida en florero
- Tallos de entre 50-120 cm
- Botones de gran tamaño
- Colores intensos y de alta saturación
- Producción estable a lo largo del año de rosas de alta calidad
- Cajas de tamaños óptimos para el transporte
- Controles estrictos de calidad antes de salir de finca y previa al vuelo realizadas por High Control®.
- Trabajo en conjunto con los breeders para actualizar constantemente la variedad de clase Premium.

En la actualidad la empresa controla todos estos procesos de producción y de gestión administrativa utilizando las TI, las cuales ayudan en gran manera para gestionar y controlar el proceso de producción de la flor, y controlar la administración de personal (horas extras, faltas, atrasos, asistencia, compra de insumos, fertilizantes, abonos, etc.), de esta manera la empresa se cerciora que el producto final sea de buena calidad.

En los últimos años ha sido acreedor a reconocimientos internacionales en diferentes variedades (especies) que se cultivan en la empresa. Lo cual ha sido de mucha influencia para las personas que trabajan en la parte obrera de la empresa y para la parte administrativa, influenciándolos así a realizar un mejor trabajo.

6.1.1. Ubicación geográfica

La empresa Rosas del Corazón, está ubicada en la Provincia de Pichincha, Cantón Mejía, a unos 2 kilómetros de la ciudad de Machachi, sector la Avanzada. Km $41^{1}/2$. Tiene vías de fácil acceso a la planta de producción, a pocos metros de la Panamericana Sur. Es muy concurrida por turistas que visitan para conocer sobre el proceso de producción de flor.

6.1.2. Conocimiento y comprensión de las actividades de la empresa

La empresa Rosas del Corazón realiza las siguientes operaciones:

Al encontrarse en un área geográfica fría, la empresa se dedica a la producción de rosas. Las cuales pasan por un riguroso control de calidad, en cada uno de sus procesos: siembra, fumigación, cosecha, postcosecha, corte, embonche, empaque y como parte del proceso de producción, la rosa sale a exportación.

En la actualidad la empresa cuenta con una página web (www.rosasdelcorazon.com), la cual permite la comunicación entre los clientes y la empresa, dando a conocer las principales variedades que ofrece a sus principales clientes. La página da a conocer de manera general la información básica de la empresa

La página web también muestra la información acerca de los reconocimientos internacionales (premios obtenidos), por cumplir con un alto nivel de calidad en las ferias realizadas en los países europeos, algunas variedades de flor han sido premiadas

Actualmente en la empresa se manejan dos sistemas informáticos, uno de ellos fue implementado en el último año.

SOFIA: sistema de control de los diferentes procesos de las principales actividades que desempeña la empresa internamente (el área de compra de insumos, gestión de personal, asistencia, la parte contable).

UNOSOF: sistema web que gestiona las actividades internas de la empresa (aplicación que ayuda al control y gestión de la producción de la empresa, como son siembra, fumigación, cosecha, postcosecha, corte, embonche, empaque). La empresa cuenta con personal que desempeñan funciones administrativas en la empresa, consta de los siguientes departamentos:

- Administración
- Recursos humanos (RRHH)
- Recepción

- Contabilidad
- Compras
- Ventas
- Logística y trasporte
- Seguridad y salud ocupacional
- Trabajo Social
- Departamento Medico

También cuenta con personal que desempeñan funciones en el área operativa, en el cual se maneja el sistema de gestión de procesos de producción:

- Técnico de procesos
- Recepción de flor
- Postcosecha
- Empaque
- Transferencia entre fincas

En el área operativa existen subprocesos de producción que hacen que la flor cumpla con altos controles de calidad, ya que la flor es monitoreada desde su siembra hasta su cosecha luego de tres meses.

6.1.3. Descripción de funciones del nivel directivo de la empresa

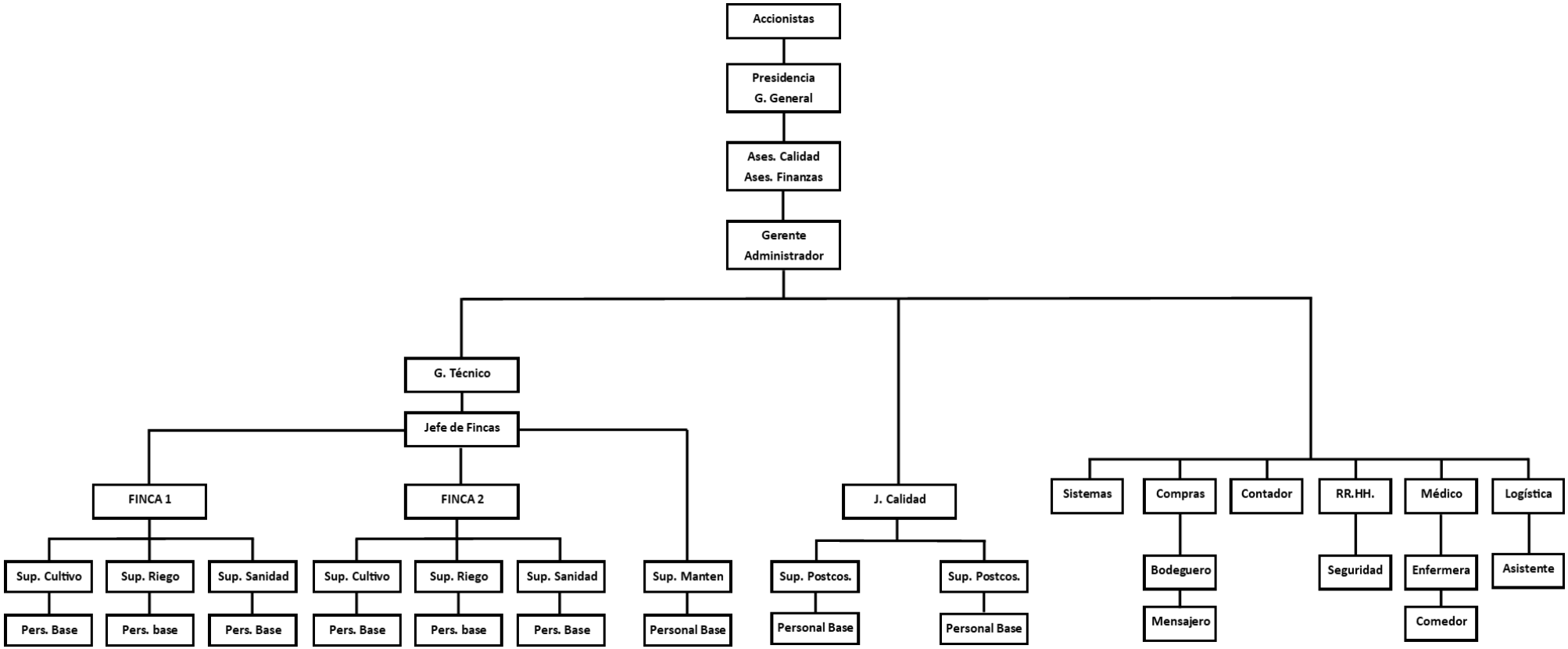


Gráfico 6.22. Organigrama funcional de la empresa
Fuente: Empresa Rosas del Corazón

La Estructura organizacional de la empresa Rosas del Corazón, está conformada por áreas.

6.1.4. Áreas ocupacionales

Estos son los conjuntos de actividades afines que constituyen las relaciones laborales.
Área administrativa
Área operativa

6.1.5. Grupos ocupacionales

Son ocupaciones de naturaleza similar, de acuerdo al tipo de funciones, responsabilidades y requerimientos para el cumplimiento de su ocupación.

6.1.6. Descripción de funciones

A continuación se describirá las principales funciones del personal de la empresa Rosas del Corazón.

- Gerente general:
    - Cumplir y hacer cumplir con las disipaciones de código de trabajo y demás leyes laborales que controlan la legislación del Ecuador.
    - Presentar para aprobación del consejo de administración el plan estratégico, el plan operativo y el presupuesto empresarial.
    - Representar jurídicamente a la empresa.
    - Se encarga de la organización, planificación, evaluación y control de las metas planteadas de la empresa.
    - Responder por la gestión administrativa y financiera de la empresa
    - Actualizar y mantener bajo custodia los inventarios de bienes y valores de la empresa.
    - Contratar, remover, sancionar, de acuerdo a las políticas que fije el consejo de administración a los empleados de la empresa.
    - Suministrar la información que soliciten los socios, representantes, órganos internos y su impacto en el patrimonio, cumplimiento del plan estratégico y sobre todo que sean solicitados, así como el plan anual de gestión.
    - Informar al consejo de administración sobre la situación financiera de la empresa, de riesgos y su impacto en el patrimonio, cumplimiento del plan estratégico y sobre otros que sean solicitados, así como el informe anual de gestión.
    - Mantener los controles y procedimientos adecuados para asegurar el control interno.

- Delegar o evocar delegaciones conferidas a otros funcionarios de la empresa, previa información al consejo de administración, sin que ello implique exonerarse de la responsabilidad legar.
- Analizar y aprobar las estrategias de mercadeo de productos y servicios de la empresa.
- Aprobar la adquisición de bienes y servicios requeridos para la gestión de la empresa de acuerdo a lo establecido en el manual de adquisición.
- Realizar el reclutamiento y selección de personal.

- Recepción
  - Se encarga de recibir a los clientes que acuden a las oficinas de Rosas del Corazón, dando una atención eficaz y oportuna, de esta manera satisfacer la necesidad del cliente.
  - Asistir a los diferentes departamentos de la empresa.
  - Intercomunicar a los demás departamentos por medio de la extensión telefónica del departamento correspondiente.
  - Recibir y hacer llamadas a los clientes, proveedores con el fin de tener una comunicación efectiva.
  - Archivar documentación pertinente de acuerdo a las necesidades de la empresa de manera organizada, en orden cronológico, alfabético con el fin de tener una fuente de consulta y fácil acceso cuando sea necesario.
- Departamento técnicos de procesos de producción
  - Cumplir y hacer cumplir con la planificación de la producción con el fin de cumplir con la producción anual establecida en Rosas del Corazón.
  - Solicitar con antelación la materia prima, los insumos de siembra y fumigación, y así evitar retrasos en la producción.
  - Sugerir posibles mejoras en el proceso de producción, de esta manera fomentar una buena comunicación organizacional.
  - Hacer un seguimiento durante todo el proceso de producción de Flor, de esta manera corroborar con las fechas planificadas.
  - Notificar cualquier situación anormal, positiva y negativa a los superiores.
- Departamento de contabilidad.
  - Realiza el control y gestión de los estados financieros.
  - Revisar la documentación contable antes de su registro.
  - Elabora los estados financieros de la empresa.

- Analiza y elabora un informe sobre la situación económica y financiera de la empresa.
- Toma decisiones en el área contable.
- Notifica sobre cualquier situación a los superiores.
- Realiza transferencias para pago de proveedores y servicios de la empresa.
- Recepta facturas de los proveedores y realiza el respectivo registro en el sistema contable.
- Emite facturas por venta de productos a distribuidos nacionales.
- Gestiona toda la parte contable, relacionándose con plataformas web bancarias, y plataformas de gobierno (SRI).
- Gestión sobre proveedores en el sistema SOFIA.

- Departamento de Compras
  - Se encarga de comunicarse con los proveedores para solicitar insumos y materiales necesarios para la producción.
  - Se encarga de mantener en stock, los implementos necesarios para la producción de flor.
  - Llevar a cargo la bodega de insumos agrarios e insumos de oficina en correcto orden, con un registro de todos los productos que se expiden desde bodega.
  - Monitorear el consumo adecuado de los insumos expedidos desde bodega.
  - Registra en el sistema SOFIA sobre proveedores, y productos en bodega
  - Comunicar con anticipación de la falta de productos o problemas con los proveedores a los superiores de la empresa.
- Recursos humanos
  - Tener una estrecha comunicación con el personal que labora en el área operativa (cosecha, postcosecha)
  - Estar actualizado de las normas y reglamentos que exige el ministerio de trabajo tanto para el patrono como para el empleado.
  - Cumplir y hacer cumplir las leyes y obligaciones al personal operativo de la empresa.
  - Manejo del sistema del módulo de RRHH, para registro de horas de trabajo, horas extras, sanciones a los empleados, etc.
  - Gestión con las principales plataformas web de gobierno (SRI, IESS, Ministerio de trabajo), plataformas bancarias.
  - Dar a conocer a la gerencia sobre situaciones anormales en el desempeño de sus obligaciones

- Registra las horas extras en el sistema SOFIA, y genera roles de pagos según BD de horas de ingreso, horas de trabajo mensuales.

- Departamento de Ventas
  - Gestiona las ventas de rosas a nivel internacional.
  - Gestión en el sistema UNOSOF sobre el registro de ventas de productos en stock.
  - Gestiona la comunicación con clientes internacionales y nacionales, acerca de pagos, transferencias, transporte de productos.
  - Constante comunicación con los departamentos de producción: postcosecha y empaque.
  - Dar a conocer a la gerencia sobre anomalías en la ejecución de sus funciones.
- Logística y trasporte
  - Gestionar con los medios de transporte de flor.
  - Gestión y comunicación con las empresas cargueras.
  - Comunicación constante con el departamento de empaque, para agilizar él envió del producto empacado a tiempo a las cargueras.
  - Registro en el sistema UNOSOF sobre los paquetes vendidos y gestiona los productos en Stock para futuras ventas.
  - Dar a conocer a la gerencia de los acontecimientos suscitados en este departamento.
- Seguridad y salud ocupacional
  - Se encarga de la gestión de seguridad en el sitio de trabajo.
  - Cumple y hace cumplir con las normativas de seguridad internas de la empresa.
  - Gestiona y administra los sistemas de seguridad y salud ocupacional dentro de la empresa
  - Se encarga de las capacitaciones del personal en el área de seguridad laboral, equipamiento, pruebas de reconocimiento.
  - Se encarga de realizar pruebas a las personas en el área laboral en el que se encuentran para identificar si son aptas o no para el puesto de trabajo.

- Cumple y hace cumplir las normas y reglamentos internos, que el ministerio de trabajo norma para las empresas privadas
- Constante actualización de conocimientos en el área de seguridad, para reforzar y monitorear la seguridad laboral en la empresa.
- Realizar un informe mensual a la gerencia sobre los trabajos desempeñados en esta área.

- Trabajo Social
  - Comunicar a la parte operativa de la empresa sobre sus funciones y afianzar la relación entre empleados.
  - Crear planes estratégicos para fomentar la seguridad intrafamiliar de los empleados de la empresa.
  - Charlas y capacitaciones al personal obrero en los diferentes temas sociales (sexualidad, relaciones personales, relaciones familiares, relaciones en el trabajo etc.).
- Departamento Medico
  - Administrar el departamento médico.
  - Gestiona citas médicas externas con el IESS.
  - Suministra medicamentos a los pacientes.
  - Gestiona permisos en caso de ser necesarios dando a conocer a RRHH.
  - Crear un informe mensual de las actividades realizadas en este departamento.
  - Gestión y planificación de campañas medicas con el fin de resguardar la salud de los empleados administrativos y operativos.
  - Control de enfermedades, brotes, infecciones, en el área de trabajo, conjuntamente con el Departamento de Salud y Seguridad Ocupacional
- Área de informática y tecnología
  - Administrar y asegurar los recursos informáticos, la infraestructura tecnológica de la empresa.
  - Elaborar o actualizar el plan de contingencia.
  - Planificación, seguimiento y monitoreo de los mantenimientos de las redes WAN, LAN (remotas, locales) y del sistema UNOSOF y SOFIA.
  - Instalación y configuración de software de ofimática.

- Asesorar a gerencia general de las nuevas herramientas informáticas.
- Planificación, seguimiento y monitoreo de las actividades asignadas al área de TIC.
- Gestionar las principales eventualidades con los proveedores de servicios (ISP) y recursos (hardware, software).
- Realizar un informe anual de los recursos de TI en la empresa
- Presentar un informe mensual sobre las acciones tomadas por el encargado de TI

6.2. Recursos informáticos

6.2.1 Departamentos administrativos de la empresa Rosas del Corazón

- Administración de Rosas del Corazón

  La persona que se encuentra a cargo de la administración de la empresa es el Ing. Orlando Tapia, en este departamento se ubica un punto red, que permite la conexión a internet, también está al alcance la red WIFI.

- Recursos humanos (RRHH)

  Este departamento se encuentra a cargo la Ing. Marisol Flores, aquí se ubica un punto de red, una impresora compartida con el departamento de contabilidad.

- Contabilidad

  Este departamento se encuentra a cargo de la Srta. Pamela Salazar, encargada de la parte contable de la empresa. Para la conectividad del equipo de trabajo está al alcance la señal de la red WIFI.

- Compras

  Este departamento se encuentra a cargo del Sr. Cesar Jaguaco, en este departamento se ubica un punto de red, aquí se ubica una impresora matricial y una impresora multifunción a tinta continúa.

- Recepción y auxiliar RRHH

  En esta área desempeña sus funciones la Sra. Nataly Sánchez, en esta área de trabajo se encuentra disponible un punto de red.

- Ventas

  Este departamento se encuentra a cargo de la Ing. Verónica Cruz, aquí se encuentra un punto de red, también utiliza una impresora compartida.

- Logística y transporte

  Este departamento está a cargo de la Sra. Carolina Vera, aquí se ubica un punto de red y una impresora.

- Seguridad y salud ocupacional

  Este departamento se encuentra a cargo de la Dra. Patricia Paredes, aquí se encuentra un punto de red, también se ubica una impresora.
- Trabajo Social

  Este departamento se encuentra a cargo de la Lcda. Jenny Guaigua, en este departamento se encuentra un punto de red.
- Departamento Medico

  Se encuentra a cargo de la Srta. Mariela Calero, en este departamento se ubica un punto de red.
- Técnico de procesos

  Este departamento se encuentra a cargo de la Sra. Mayra Flores, aquí se puede observar una punto de red y el uso de una impresora compartida desde el departamento de compras.
- Recepción de flor

  Este lugar de trabajo se encuentra a cargo la Sra. Erica Monta, cabe recalcar que esta estación de trabajo es usada por otras personas, que ejercen la función de registrar la flor que llega de la cosecha.
- Postcosecha

  En esta estación de trabajo se encuentra a cargo de la Ing. Mónica Puruncajas, se puede identificar que este computador lo manipulan varias personas ya que requieren subir información relevante de sus funciones (procesos, cortes, embonche, etiquetado)
- Empaque

  En este departamento se encuentra la parte operativa de la Empresa, quienes registran en empaque de las flores en sus cajas de exportación, junto a la computadora de transferencia de flor.
- Transferencia de flor

  En está computadora es usada por la parte operativa de la empresa, que gestionan los cambios de flor, empaque de flor entre las dos estaciones que dispone la empresa, también se realiza el registro de flor para la venta nacional.

A continuación se detalla el último inventario realizado por el encargado del área informática de la empresa, en el cual se muestran los detalles físicos y lógicos de los equipos que se encuentran ubicados en cada área de trabajo:

Tabla 6.11. Inventario equipos empresa

ÁREA	DETALLE	MOUSE TECLADO	REG. VOLTAJE -UPS	IMPRESORA / VARIOS
Contabilidad	Intel Core i3-6100 CPU @ 3.70GHz- 8Gb Ram - 2 TB Disco Duro. MOTHERBOARD ALASKA - 1072009	SI	Altek model 1072KA	NO
RR.HH	Intel Core i3-3240 3.40 Ghz - Mainboard Intel DH61CR - 4Gb Ram - 500 Gb Disco Duro	SI	Altek model 1072KA	Samsung M2875FD
Logística y transporte	Intel Core i3-4160 CPU @ 3.60GHz Mainboard H81MLV3 - 8Gb Ram - 1Tb Disco Duro.	SI	UPS – CDP	Samsung SCX-3405F
Ventas	Intel Core i3 3.70 Ghz - Mainboard Asus H81M-A - 4Gb Ram - 1Tb Disco Duro.	SI	NiveLine 600 STSI	NO
Recepción	Intel (R) Core i3-6100 CPU a 3.70GHz, 8Gb Ram, 500Gb Disco Duro	SI	Apex AVR 1600PS	NO
Seguridad y Salud Ocupacional	Intel Core i3-3240 3.40 Ghz - Mainboard Intel DH61CR - 4Gb Ram - 500 Gb Disco Duro.	SI	Apex AVR 1600PS	Samsung M2070Fw
Trabajo Social	Intel Celeron J1800 2.41 Ghz - Mainboard Biostar J1800NH2 - 4Gb Ram - 1Tb Disco Duro.	SI	Apex AVR1500 m	NO
Compras	Intel Core i3-3240 3.40 Ghz - Mainboard Intel DH61CR - 4Gb Ram - 500 Gb Disco Duro.	SI	Tripp Lite BC2405	- EPSON LX-300+II - EPSON L210

Departamento Médico	Intel Celeron(R) CPU G1610 @ 2.60GHz - 6GbRam - 500Gb Disco Duro.	SI	CDP R2C-AVR1008	NO
Departamento Técnico producción	Intel Core i3-4150 3.50Ghz - Mainboard Gigabyte GA-H81M-H - 6Gb Ram - 1Tb Disco Duro	SI	Apex AVR 1600PS	NO
Postcosecha	Intel Core i3-7100 CPU @ 3.90GHz - Mainboard Biostar J1800NH2 - 4Gb Ram - 1Tb Disco Duro.	SI	Apex AVR 1600PS	Zebra LP2844
Recepción Flor	Intel Pentium Dual-Core CPU E5500 @ 2.80GHz. 4Gb Ram - 1TB Disco Duro.	SI	UPS CDP	- Samsung M2020 - Lector de Código de Barras MS837-U Motorola
Empaque	Intel Core i3 3.70 Ghz - Mainboard Asus All Series - 8Gb Ram - 1Tb Disco Duro.	SI	CDP R2C-AVR1008	Lector de Código de Barras inalámbrico Honeywell
Transferencia entre fincas	Intel Core i3-7100 CPU @ 3.90GHz - Mainboard Biostar J1800NH2 - 4Gb Ram - 1Tb Disco Duro	SI	CDP R2C-AVR1008	Lector de Código de Barras Motorola Li2208

Fuente: Área de informática empresa

La tabla anterior muestra los departamentos adecuados en la empresa, según el organigrama funcional de la empresa Rosas del Corazón.

6.3. Características de los sistemas y ambiente computarizado

SOFIA: sistema de gestión de fincas

El sistema SOFIA, es un sistema especializado para manejo de fincas en toda el área contable y el área administrativa de la misma.

SOFIA en un sistema multiusuario, multiempresa, y multibodega. Esta desarrollado con el Front End Power Builder, la base de datos INFORMIX bajo la plataforma Windows en todas sus versiones.

Los módulos son los siguientes:

- Financiero
- Nómina
- Florícola
- Seguridades

Módulo financiero

Contiene los siguientes submódulos: contabilidad, tesorería, inventario de productos (bodega), cuentas por cobrar, cuentas por pagar, anexos transaccionales, activos fijos y facturación electrónica.

Módulo de nomina

Este módulo se puede gestionar Datos del personal como módulo de control de asistencia, faltas, atrasos, horas extras, manejo de horarios, registro a través de código de barras.

Módulo florícola

Proyecciones de producción. Ingreso de aplicaciones fitosanitarias y fertilización, generación de salidas de bodega, reportes y estadísticas semanales, mensuales, anuales, monitoreo de enfermedades, control fitosanitario, productividad planta.

El sistema también permite gestionar: el inventario de flor, facturación de flor, control de empaques, seguridades de acceso al sistema.

Módulo Seguridad

El sistema permite gestionar el ingreso al sistema mediante el uso de usuario y contraseña.

6.4. Base de datos de la empresa

La empresa Rosas del Corazón cuenta con sus servidores propios adecuados en un lugar remoto y también dentro de las instalaciones de la Empresa.

La base de datos del software SOFIA trabaja con la BD Informix y bajo la plataforma Windows en todas sus versiones.

También se maneja una BD de los servidores de UNOSOF, que es un software orientado directamente al control de producción de flor, el servidor que maneja esta base de datos es un software desarrollado para la plataforma web, que la empresa hace uso para gestionar los procesos de producción de rosas.

6.5. Servidores de la empresa Rosas del Corazón

La empresa cuenta con 3 servidores, 1 servidor de datos y 2 servidores de aplicaciones:

Tabla 6.12. Servidores de la empresa Rosas del Corazón

Servidor de Control de Producción	**Detalles**
Nombre del Host	UNOSOFT-APP
Dirección IP	192.168.2.10
Servidor de BD control de producción	
Nombre del Host	UNOSOFT-DB
Dirección IP	192.168.2.12
Servidor de control administrativo y de personal	
Nombre del Host	SOFIA
Dirección IP	192.168.2.18

Fuente: Diego Quillupangui

El servidor UNOSOFT-APP, es un servidor gestionado por los administradores del sistema, este soporte lo realizan de forma remota.

El servidor de BD de UNOSOF, es un servidor que maneja los datos de la empresa del software antes mencionado.

El servidor que maneja los datos de control de producción de rosas, maneja y controla los productos a la venta. A este servidor se accede de forma remota desde otras sucursales que realizan la venta de rosas a nivel internacional.

El servidor SOFIA es un software de control administrativo y de personal, que ayuda a la gestión de pagos, registrar horas extras, control de inventario, bodega entre otras acciones internas que requiere la empresa.

6.6. RED

La empresa cuenta con dos Rack de comunicaciones (Rack de piso), en el primer rack existe un Switch TP-Link de 16 puertos al cual están ubicados los servidores de aplicaciones y de base de datos y en el segundo rack están los equipos de red LAN y WAN.

El ISP es TELCONET, es una empresa dedicada a brindar soporte en cuanto al área de comunicaciones a nivel nacional, ellos son quiere prestan el servicio de internet con una compartición 1-1, utilizando el medio de transmisión de Fibra óptica que fue implementado directamente para la empresa, ya que por motivos de distancia, los proveedores no suministraban este servicio.

Dispone de un equipo de red Router CISCO RV130, que permite la conexión entre el internet y la red LAN, este Router está distribuido de la siguiente manera:

Puerto 1: es utilizado para conectar el Switch de servidores.

Puerto 2: es utilizado para la conexión del Switch D-Link de 32 puertos a 100 Mbps, que controla los puntos de red de la red LAN.

Puerto 3. Es utilizado para la conexión de punto de acceso inalámbrico para compartir internet con dispositivos que permiten comunicación WIFI (Invitados, visitas, personal administrativo).

En cuanto a la distribución de los puntos de red LAN, estos han sido realizados mediante cableado tipo par trenzado UTP Cat 5e.

Para mayor seguridad de los equipos ubicados en el rack de comunicaciones existe dos UPS, un UPS de 3KVA línea alta, que suministra energía a los servidores de datos y de aplicación de UNOSOF, y en el otro rack de 2KVA para proporcionar energía a los elementos activos de la red de la empresa.

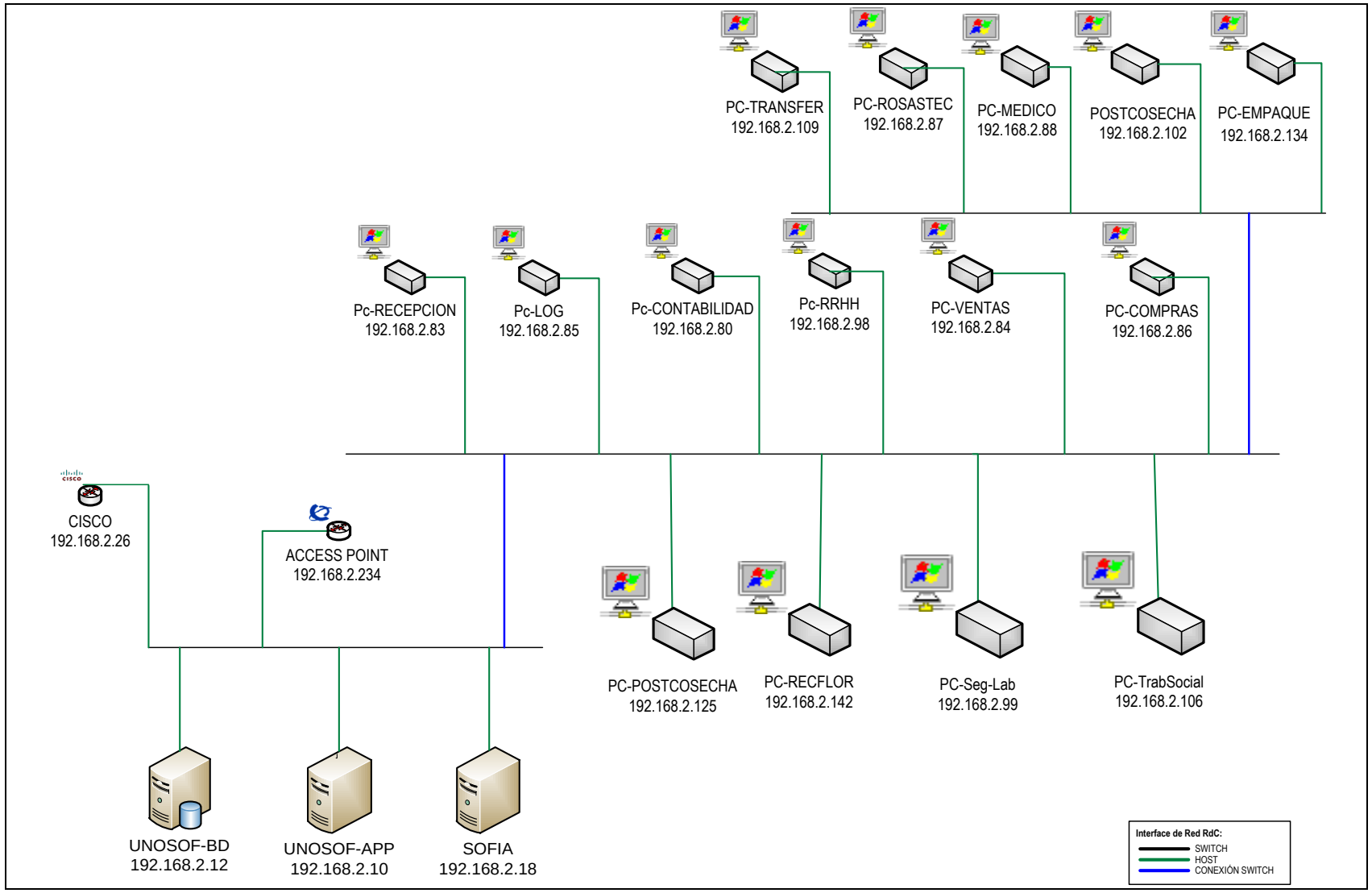


Gráfico 6.23. Esquema de red LAN de la empresa
Fuente: Empresa Rosas del Corazón

La empresa Rosas del Corazón también cuenta con un sistema de seguridad de CCTV, para monitoreo de zonas de mucho riesgo en la empresa, son lugares específicos requeridos para controlar los procesos de producción y de activos de la empresa.

Este sistema de seguridad es administrado por el administrador de la empresa.

6.7. Funciones principales del área informática

- Proponer alternativas tecnológicas, para las distintas áreas que permitan mejorar los procesos operativos y administrativos de la empresa.
- Administrar y mantener operativos todos los sistemas informáticos, disponiendo del recurso humano y utilizando los medios técnicos necesarios.
- Brindar un mantenimiento preventivo y correctivo del equipamiento tecnológico, al mismo tiempo dar soporte técnico y asesoramiento inmediato necesario a cada departamento de la empresa.
- Configuración y soporte de los equipos tecnológicos que se maneja en cada departamento, siendo de prioridad todos y cada uno de los departamentos.
- Gestión y monitoreo de la adquisición de nueva infraestructura tecnológica necesaria con los proveedores de servicios y proveedores de hardware.
- Supervisar el uso correcto de las TI en los departamentos de la empresa.

6.8. Diagnóstico de la situación actual de la empresa

Para realizar la auditoria se realiza un análisis FODA de la empresa a auditar, según los parámetros a seguir de auditoria informática.

En los siguientes puntos se procede a analizar las principales variables que intervienen en la empresa.

6.8.1. Análisis macro ambiente

En este punto se analizan aquellos factores que la empresa no puede controlar, el cambio o modificación en uno estos factores ocasionaría graves consecuencias, cabe recalcar que está compuesto por las fuerzas que dan forma a las oportunidades o presentan una amenaza para la empresa.

- **Factor tecnológico**

Al hablar de la tecnología, en la actualidad es un factor determinante para el desarrollo de un país, de una nación, de una empresa; el avance tecnológico constituye una **oportunidad** para el área informática, ya que implementar la tecnología en la empresa, le obliga a actualizar los conocimientos y actualizar sus procesos de producción y esto hace que el uso de la tecnología optimiza los recursos de la empresa. Pero al mismo tiempo se genera una **amenaza** con respecto a la seguridad cibernética lo que se refiere a los virus, a las **amenazas** de intrusos o aumentar el riesgo de robo de la información.

- **Factor político**

Para el desarrollo de una nación se necesita de una estabilidad política de un país es por ello que la estabilidad política de nuestro país genera una **oportunidad** que crea oportunidad y planes de crecimiento, genera una confianza para los inversionistas, considerando cumplir y mantener la visión empresarial a mediano y largo plazo.

- **Factor legal**

Al ser una empresa privada se rige a varios entes públicos como son el Ministerio de trabajo, Servicio de Rentas Internas y demás entes gubernamentales, que exigen la aplicación de leyes, normas, reglamentos, estatutos, esta es una **amenaza** para la empresa, pues la recaudación de tributos obliga a las empresas privadas a que transparenten sus ingresos y así asegurar el presupuesto de la empresa pública.

- **Factor geográfico**

El factor geográfico comprende la naturaleza, la cantidad, y la disponibilidad de los recursos naturales, condiciones geográficas y climáticas que puede presentarse en el área de trabajo.

Actualmente la empresa se encuentra ubicada en un área alta de la sierra, las condiciones climáticas de este lugar son una **oportunidad**, ya que el clima es perfecto para el crecimiento de la flor, en las distintas épocas del año, sin embargo al ser un lugar un poco alejado del centro y respecto a las condiciones climáticas de la sierra ecuatoriana se presentan tormentas eléctricas, esto representa una **amenaza** para la empresa, ya que las descargas eléctricas ocasionan daños graves a los equipos informáticos.

6.8.2. Análisis microambiente

Aquí se evalúa el ambiente interno y los recursos internos de la empresa, para así detectar sus fortalezas y debilidades en el desarrollo de sus operaciones diarias.

En este proceso se identifica los factores internos positivos que impulsan positivamente a la empresa, este tipo de recursos pueden controlar capacidades y habilidades, actividades que se desarrollan positivamente, y también los obstáculos o los inconvenientes que impiden el correcto desempeño de las actividades que desarrolla la empresa en su diaria labor.

- **Talento humano**

La empresa Rosas del Corazón cuenta con 140 personas en el área operativa y 15 personas en el área administrativa que utilizan computadores, quienes están distribuidos en las diferentes áreas de la empresa, también se agregan 2 personas que regularmente visitan y realiza labores administrativas en la empresa, cada persona está capacitada para realizar sus laboras de manera eficiente, tienen conocimiento del software que manejan, y conocen las herramientas que dispone el computador para trabajar y hacer su trabajo más efectivo. Este aspecto representa una **fortaleza** en la empresa.

- **Infraestructura**

La infraestructura física de la red LAN es deficiente, ya que no tiene un plan de mantenimiento preventivo, y su cableado de datos tiene muchos años desde su instalación, esto representa una **debilidad** para la empresa considerando que no tiene un mantenimiento adecuado y parte del cableado está expuesto a la intemperie climática.

- **Tecnología**

La empresa cuenta con equipos de cómputo y de comunicación, los cuales en su mayoría han sido modificados, se ha realizado la actualización del hardware y otros han sido adquiridos nuevos en los últimos dos años, se ha presentado un trato adecuado y se ha realizado el respectivo mantenimiento preventivo, esto representa una **fortaleza** para la empresa.

- **Cliente**

La empresa brinda servicios a sus clientes, los cuales se comunican mediante línea telefónica o utilizando las redes sociales, también otra gran parte de atención a los clientes se lo realiza en las instalaciones que brindan la empresa, y el personal administrativo está actualizado y capacitado para dar una buena atención a los clientes. Esto representa una **fortaleza** para la empresa.

- **Proveedores**

La empresa Rosas del Corazón al ser una institución privada y tener años de experiencia en el área de producción de flor, se ha ganado el reconocimiento y confianza de los principales proveedores de los diferentes insumos que requiere la empresa, esto representa una **fortaleza** para la empresa.

6.9. Análisis FODA

Las fortalezas como las debilidades son internas en la empresa, por lo que se puede actuar directamente sobre ellas. En cambio al hablar de las oportunidades y amenazas se refiere que son causales externos que no resulta fácil poder modificarlos y no se puede ejercer control sobre ellas.

En el proceso de auditoria se procedió a aplicar entrevistas, encuestas con el personal de la empresa, interviniendo en sus labores diarias con preguntas que nos ayudan a obtener información para el desarrollo de este trabajo. Para continuar con el presente trabajo a continuación se muestra una tabla detallada del análisis FODA.

Tabla 6.13. Análisis FODA

FORTALEZAS	**DEBILIDADES**
- Personal capacitado en el uso del Sistema Informático - Trabajo en equipo de todas las áreas - Equipo informático actualizado - Buena atención a los clientes - Buena reputación con los proveedores	- Infraestructura de red deficiente - Carencia de un plan de contingencia - Carencia un plan estratégico del área Informática - Falta de coordinación en la toma de decisiones en el área informática
OPORTUNIDADES	**AMENAZAS**
- Desarrollo tecnológico - La estabilidad política permite la creación de planes de crecimiento - Ubicación geográfica adecuada para la producción de flor	- Intervención de entes gubernamentales - Ataques cibernéticos - Robo de información - Las frecuentes lluvias ocasionan problemas con el servicio eléctrico.

Fuente: Diego Quillupangui

En esta etapa del proyecto en base a la información de las necesidades de la administración de la empresa, la información recopilada nos ayuda al proceso de auditoría, ya que es de vital importancia para la seguridad de la empresa. De acuerdo a [23] el modelo de referencia de procesos COBIT 5, proporcionan una guía acerca de cómo definir, operar y monitorizar el sistema para la gestión de Seguridad informática. De acuerdo a los datos obtenidos se asume que la Seguridad de la información se encuentra presente a lo largo de toda la organización, es aquí donde COBIT proporciona una guía para el gobierno y la gestión corporativa de la seguridad de la información.

6.10. Aplicación del mapeo de metas en la empresa Rosas del Corazón

6.10.1. Selección de preguntas de gobierno de TI

Para llegar a este proceso de selección se realizó un análisis exhaustivo basado en las preguntas del Gráfico 4.11, 4 preguntas son consideradas como importantes, relevantes.

1. ¿Tengo suficiente personal para TI?
2. ¿Está bien asegurada la información que se está procesando?
3. ¿Cuán críticas son las TI para la sostenibilidad de la empresa?
4. ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de la empresa requeridos

6.10.2. Mapeo de las metas corporativas de COBIT y las preguntas de gobierno y gestión

A continuación se realiza un mapeo de las metas corporativas de COBIT y las preguntas de gobierno y gestión, este proceso ayudará a conocer cuáles son los objetivos de la empresa y cuáles son las preocupaciones de las partes interesadas definidas por parte de la empresa. Esto establece una relación con las metas corporativas.

En la siguiente tabla se puede apreciar los procesos seleccionados para evaluar la seguridad de la información en la empresa Rosas del Corazón, en la que se indica los procesos principales (P) y secundario (S).

Tabla 6.14. Mapeo entre las metas corporativas de COBIT 5 y las preocupaciones de las partes interesadas

Mapeo entre las metas Corporativas de COBIT 5 y las Preguntas de Gobierno y Gestión																
NECESIDADES DE LAS PARTES INTERESADAS	Valor para los interesados de las inversiones de negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas agiles a un entorno de negocio cambiante	Toma estratégica de decisiones basada en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

¿Tengo suficiente personal para TI?																	
¿Está bien asegurada la información que se está procesando?																	
¿Cuán críticas son las TI para la sostenibilidad de la empresa?																	
¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de la empresa requeridos																	

Fuente: Diego Quillupangui

Como resultado de esta actividad se han definido las metas corporativas.

3. Riesgos de negocio gestionados (salvaguarda de activos)
6. Cultura de servicio orientada al cliente
7. Continuidad y disponibilidad del servicio de negocio
9. Toma estratégica de decisiones basada en información
14. Productividad operacional de los empleados
17. Cultura de innovación de producto y negocio

Como siguiente procedimiento tenemos el mapeo entre las metas corporativas y las metas relacionadas con TI, con la ayuda de las metas corporativas obtenidas en la actividad anterior.

En la tabla 6.5. se identifica las relaciones con las letras P (primario) y S (secundario), las cuales establecen un valor cuantitativo, con el objeto de definir la priorización se le asigna a P el valor de 3 por considerarse de mayor prioridad y a S el valor de 1.

Tabla 6.15. Mapeo entre metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI

Mapeo entre metas corporativas de COBIT 5 y las metas relacionadas con las TI														
		Meta corporativa						**PONDERACIÓN**						**TOTAL**
		Riesgos de negocio gestionados (salvaguarda de activos)	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Toma estratégica de decisiones basada en información	Productividad operacional de los empleados	Cultura de innovación de producto y negocio							
Metas relacionadas con las TI		3	6	7	9	14	17							
01	Alineamiento de TI y estrategia de negocio	S	S	S		S	S	1	1	1		1	1	5
02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	S	P		S		S	1	3		1		1	6
03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		S	S		S	P		1	1		1	3	6
04	Riesgos de negocio relacionados con las TI gestionados	P	S	P	S	P	P	3	1	3	1	3	3	14
05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI													0
06	Transparencia de los costes, beneficios y riesgos de las TI	S		P			P	1		3			3	7
07	Entrega de servicios de TI de acuerdo a los requisitos del negocio		S	S	P				1	1	3			5
08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	P	S	S	S	P	P	3	1	1	1	3	3	12
09	Agilidad de las TI			S		P	S			1		3	1	5
10	Seguridad de la información,	P	P	P	P	P	P	3	3	3	3	3	3	18

	infraestructura de procesamiento y aplicaciones													
11	Optimización de activos, recursos y capacidades de las TI			S		S	S			1		1	1	3
12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio			S			S			1			1	2
13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.			S			S			1			1	2
14	Disponibilidad de información útil y fiable para la toma de decisiones		S	S		S			1	1		1		3
15	Cumplimiento de las políticas internas por parte de las TI	S				P		1				3		4
16	Personal del negocio y de las TI competente y motivado					P						3		3
17	Conocimiento, experiencia e iniciativas para la innovación de negocio			P		S	S			3		1	1	5

Fuente: Diego Quillupangui

Como resultado de la tabla 6.15, se selecciona las metas relacionadas con la TI con la ponderación más alta como resultado tenemos lo siguiente:

Tabla 6.16. Metas relacionadas con TI resultantes

Metas relacionadas con TI		**Ponderación**
04	Riesgos de negocio relacionados con las TI gestionados	14
08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	12
10	Seguridad de la información, infraestructura de procesamiento y aplicaciones	18

Fuente: Diego Quillupangui

Continuando con los procedimientos definidos en COBIT 5, a continuación se realiza un mapeo entre las metas relacionadas con las TI resultantes y los procesos catalizadores. Como

muestra en la tabla 6.17, como resultado de esta actividad se obtendrá los procesos catalizadores. La relación se establece con la letra P (primario) y S (secundario), para establecer un valor cuantitativo y definir su prioridad se asigna a P el valor de 3 y S el valor de 1.

Tabla 6.17. Mapeo entre las metas relacionadas con las TI y los procesos catalizadores

Mapeo entre las metas relacionadas con las TI y los procesos catalizadores								
		Meta corporativa			**PONDERACIÓN**			**TOTAL**
		Riesgos de negocio relacionados con las TI gestionados	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Seguridad de la información, infraestructura de procesamiento y aplicaciones				
Procesos de COBIT 5		4	8	10				
EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S			1			1
EDM02	Asegurar la entrega de beneficios							0
EDM03	Asegurar la optimización del riesgo	S	S	P	1	1	3	5
EDM04	Asegurar la optimización de los Recursos	S		P	1		3	4
EDM05	Asegurar la transparencia hacia las partes interesadas	S	S	S	1	1	1	3
APO01	Gestionar el Marco de Gestión de TI	S	S		1	1		2
APO02	Gestionar la estrategia	S			1			1
APO03	Gestionar la arquitectura empresarial							0
APO04	Gestionar la innovación		S	S		1	1	2

APO05	Gestionar portafolio							0
APO06	Gestionar el presupuesto y los costes							0
APO07	Gestionar los recursos humanos			S			1	1
APO08	Gestionar las relaciones							0
APO09	Gestionar los acuerdos de servicio	S	P	S	1	3	1	5
APO10	Gestionar los proveedores	S	P	P	1	3	3	7
APO11	Gestionar la calidad	S		S	1		1	2
APO12	Gestionar el riesgo	S	S	P	1	1	3	5
APO13	Gestionar la seguridad	S	P	S	1	3	1	5
BAI01	Gestionar los programas y proyectos		S			1		1
BAI02	Gestionar la definición de requisitos							0
BAI03	Gestionar la identificación y la construcción de soluciones	S			1			1
BAI04	Gestionar la disponibilidad y la capacidad	P	P	P	3	3	3	9
BAI05	Gestionar la introducción de cambios organizativos							0
BAI06	Gestionar los cambios	S	S		1	1		2

BAI07	Gestionar la aceptación del cambio y de la transición	S			1			1
BAI08	Gestionar el conocimiento		S	P		1	3	4
BAI09	Gestionar los activos	P	S	P	3	1	3	7
BAI10	Gestionar la configuración	S	S	S	1	1	1	3
DSS01	Gestionar las operaciones	P	P	P	3	3	3	9
DSS02	Gestionar las peticiones y los incidentes del servicio	P	P	P	3	3	3	9
DSS03	Gestionar los problemas	S	P	S	1	3	1	5
DSS04	Gestionar la continuidad	P	P	S	1	3	1	7
DSS05	Gestionar los servicios de seguridad	P	P	P	3	3	3	9
DSS06	Gestionar los controles de los procesos del negocio	P	S	S	3	1	1	5
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad	S		S	1		1	2
MEA02	Supervisar, evaluar y valores el sistema de control interno	S		S	1		1	2
MEA03	Supervisar, evaluar y valorar la conformidad de los requisitos externos		S			1		1

Fuente: Diego Quillupangui

Como resultado del mapeo entre las metas relacionadas con las TI y los procesos catalizadores se obtiene los siguientes procesos a aplicarse en el presente trabajo, como se muestra en la siguiente tabla:

Tabla 6.18. Procesos catalizadores prioritarios

Procesos catalizadores prioritarios	Ponderación
BAI04 Gestionar la disponibilidad y la capacidad	9
BAI09 Gestionar los activos	7
APO10 Gestionar los proveedores	7
DSS01 Gestionar las operaciones	9
DSS02 Gestionar las peticiones y los incidentes de servicio	9
DSS04 Gestionar la continuidad	7
DSS05 Gestionar los Servicios de Seguridad	9

Fuente: Diego Quillupangui

Los datos presentados en la Tabla 6.18 son los procesos que serán aplicados en la auditoria a la seguridad informática de la empresa Rosas del Corazón.

6.11. Alcance

La siguiente propuesta tecnológica está orientado a la auditoria Informática aplicada a la seguridad Informática en la Empresa Rosas del Corazón, ubicada en la ciudad de Machachi, para lo cual se va a utilizar los preceptos de COBIT 5.0, para la evaluación del ambiente informático, durante el periodo octubre 2018 – febrero 2019.

6.11.1. Justificación

En la actualidad la confidencialidad de la información de las empresas es cada vez más importante, ya que se enfoca en la protección de los datos de los usuarios o información de las empresas, la infraestructura y todo lo relacionado con el área informática. Es por eso que la auditoría informática se constituye una gran herramienta que gestiona las TI, aplicando normas, estándares, leyes, manuales, reglas para minimizar los posibles riesgos de seguridad en los recursos informáticos.

Es por ello que se toma como marco de referencia COBIT 5.0, el cual es un marco de gobernabilidad de TI que sirve como guía con un conjunto de herramientas de ayuda, que permite a los administradores, tener en cuenta y asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgo del negocio.

Este conjunto de las mejores prácticas permiten evaluar la seguridad, calidad, eficacia y eficiencia de tecnologías de la información en la empresa Rosas del Corazón. Mediante este procedimiento se determinan los riesgos y amenazas, para permitirán emitir recomendaciones para tener una gestión efectiva de los recursos de TI, medir el desempeño y cumplimiento de los objetivos de la empresa.

Además la ejecución de una auditoria a la seguridad física, permite una evaluación objetiva de la seguridad de los recursos tecnológicos. Es por eso que resulta conveniente realizar una auditoría a la seguridad física del área informática de la empresa Rosas del Corazón, ya que permite evaluar el estado actual de los equipos informáticos, identificar los posibles riesgos, emitir recomendaciones para mejorar la gestión de las TI y aumentar la seguridad de los equipos tecnológicos, del personal que labora salvaguardando la información.

Ante tal virtud, la empresa Rosas del Corazón consciente que los procesos que se realizan diariamente son de vital importancia para la gestión de los procesos internos y que la protección de las TI son imprescindibles, es por ello que se lleva a cabo la auditoria informática en la empresa Rosas del Corazón.

6.11.2. Objetivo general de la auditoria

Realizar una auditoria informática a la seguridad física de la empresa Rosas del Corazón, aplicando dominios, procesos y prácticas de control según el marco de referencia COBIT 5, con la finalidad de resguardar los activos útiles de la empresa a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos.

6.11.3. Objetivos específicos

- Levantamiento de la información en base al marco de referencia COBIT 5.
- Determinar los hallazgos para la elaboración de la estructura de un informe a presentar.
- Establecer conclusiones y recomendación que permitan aumentar la seguridad de la información y disminuir los riesgos de TI de la empresa por medio de un informe de auditoría.

6.12. Plan de auditoria

En la siguiente tabla se seleccionan los recursos de TI a ser auditados en la empresa Rosas del Corazón, basándose en los resultados de la Tabla 6.18.

Tabla 6.19. Plan de auditoria

Área a auditar	Objetivos	Componentes	Riesgo
Seguridad lógica	Comprobar la existencia de normativas y	1. Acceso de los usuarios a sistemas, sistemas operativos y bases de datos. 2. Acceso a los usuarios a programas y	Alto Alto

	procedimientos que resguarden el acceso a los datos y los permisos de acceso al personal autorizado	archivos 3. Disposición de sistemas alternos en caso de fallos 4. Existencia de software de protección (Antivirus, firewall) 5. Control de accesos de los usuarios a los servicios de internet	Alto Alto Medio
Seguridad física	Evaluar la protección de datos, programas, instalaciones, equipos, red y personal de la empresa	1. Control de accesos de los usuarios a los equipos 2. Informes de accesos y visitas a las instalaciones. 3. Inventario de equipos y software. 4. Revisión de la red (Factor: ambiental, físico, humano) 5. Controles para la instalación de dispositivos externos	Alto Alto Medio Alto Alto
Respaldos y plan de contingencia	Verificar la existencia de respaldos de la información vital para el funcionamiento de la empresa, tanto físico como digital y que cumplan los requisitos adecuados	1. Respaldo de la información importante de la empresa 2. Plan de continuidad 3- Plan de contingencia 4. Plan de mantenimiento de Software y Hardware	Alto Alto Alto Medio
Documentación de software y hardware	Corroborar la existencia de documentación de todo lo adquirido por la empresa en materia de informática, manuales, facturas, contrato, además de documentación detallada de los sistemas que la empresa ha adquirido	1. Existe licenciamiento de los aplicativos instalados en el equipo informático. 2. Existencia de documentos de adquisición de equipos y Software, contrato legal de proveedor de Internet (ISP) 3. Documentación de los sistemas utilizados para los servicios de la empresa	Medio Alto Medio

Fuente: Diego Quillupangui

6.12.1. Adecuación

Para ejecutar la presente auditoria se utiliza diferentes técnicas para recopilar la información necesaria y el posterior procesamiento y análisis de la misma nos ayudará a obtener los resultados que se correlacionen con los objetivos de este proyecto.

Entre las técnicas a aplicar tenemos las siguientes:

- Cuestionarios
- Entrevistas
- Observación.
- Hoja de procesamiento de información

Las áreas en las que se va aplicar la auditoria fueron analizadas mediante la metodología COBIT 5.0, la cual establece cinco dominios. Debido a los objetivos planteados para la presente propuesta a aplicarse a la empresa Rosas del Corazón, el análisis de esta auditoría se basara en los siguientes dominios: Alinear, Planificar y Organizar (APO), Construir, adquirir e implementar (BAI), Entregar, dar Servicio y Soporte (DSS), cabe recalcar que para la siguiente auditoria no se aplicaran todas las prácticas clave de Gobierno.

6.13. Guías de auditoria

1. Componente: Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.

Tabla 6.20. Guía de auditoria (Componente 1)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de seguridad
Práctica	DSS05.4: Gestionar la identidad del Usuario y el acceso lógico
Objetivos de Control	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio
N°	**Procedimiento**
1	Solicitar al encargado del área el listado de las definiciones de roles y responsabilidades relacionadas con TI
2	Aplicar una encuesta para identificar si todos los usuarios tienen su usuario y contraseña respectivas
3	Pedir información sobre la existencia de claves de acceso al sistema informático y BDD.

Fuente: Diego Quillupangui

2. Componente: Acceso de los usuarios a programas y archivos.

Tabla 6.21. Guía de auditoria (Componente 2)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.6: Gestionar Documentos Sensibles y dispositivos de Salida
Objetivos de Control	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario de activos de TI sensibles.
N°	**Procedimiento**
1	Solicitar al encargado del área información sobre el acceso a archivos (información) de la empresa, su uso y eliminación de dichos archivos.
2	Mediante la observación, identificar si los usuarios tienen acceso a la información almacenada sin restricción.
3	Identificar si existen medidas de control a los usuarios en el uso de aplicaciones ajenas al giro de negocio.

Fuente: Diego Quillupangui

3. Componente: Disposición de sistemas alternos en caso de fallos

Tabla 6.22. Guía de auditoria (Componente 3)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS02: Gestionar los servicios de Seguridad
Práctica	DSS02.5: Resolver y recuperarse ante incidentes
Objetivos de Control	Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI.
N°	**Procedimiento**
1	Solicitar al encargado del área el registro de errores frecuentes u ocasionales que ocurren en TI
2	Identificar si existe un servidor alterno donde se almacene la información de clientes y gestiones diarias
3	Aplicar una entrevista al encargado del área para conocer qué tipos de medidas cuentan en caso de fallar uno de los sistemas

Fuente: Diego Quillupangui

4. Componente: Existencia de software de protección (antivirus, firewall)

Tabla 6.23. Guía de auditoria (Componente 4)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.1: Proteger contra software malicioso (malware)
Objetivos de Control	Implementar y mantener efectivas medidas preventivas de detección y correctivas (parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (virus, gusanos, software espía, etc.)
N°	**Procedimiento**
1	Verificar mediante la observación directa la existencia de software de protección en cada uno de los computadores
2	Verificar por medio de la observación si existe una continua actualización de parches de seguridad del Sistema Operativo
3	Verificar si están activados los filtros de correo no deseado del correo electrónico de cada usuario

Fuente: Diego Quillupangui

5. Componente: Control de acceso de los usuarios a los servicios de internet

Tabla 6.24. Guía de auditoria (Componente 5)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.2: Gestionar la seguridad de la red y las conexiones
Objetivos de Control	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión
N°	**Procedimiento**
1	Verificar por medio de una entrevista al encargado del área para saber si existe un reglamento de control de accesibilidad para el uso del servicio de internet Wifi
2	Verificar si las reglas son correctas para el uso óptimo del servicio de internet

Fuente: Diego Quillupangui

6. Componente: Control de accesos de los usuarios a los equipos

Tabla 6.25. Guía de auditoria (Componente 6)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Objetivos de Control	Asegurar los puestos de usuario final (portátil, equipo sobremesa, servidor y otros dispositivos), verificar las normativas de uso y acceso a los equipos
N°	**Procedimiento**
1	Solicitar al encargado del área la lista de equipos que se usan, cuantos usuarios las usan y cuantas horas al día son usados los equipos informáticos.
2	Verificar por medio de una entrevista la existencia de políticas de seguridad para dispositivos de usuario final

Fuente: Diego Quillupangui

7. Componente: Informes de accesos y visitas a las instalaciones

Tabla 6.26. Guía de auditoria (Componente 7)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.5: Gestionar el acceso físico a los activos de TI
Objetivos de Control	Definir e implementar procedimiento para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias
N°	**Procedimiento**
1	Verificar por medio de la observación si todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles de negocio
2	Verificar por medio de la observación directa los mecanismos de seguridad sobre el ingreso al área de servidores, y área de operaciones.

Fuente: Diego Quillupangui

8. Componente: Inventario de equipos y software

Tabla 6.27. Guía de auditoria (Componente 8)

Guía de Auditoria	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI09: Gestionar los activos
Práctica	BAI09.1: Identificar y registrar activos actuales
Objetivos de Control	Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad de TI.
N°	**Procedimiento**
1	Aplicar una entrevista al encargado del área para conocer la existencia de inventario de equipos y software de respaldo en caso de un fallo.
2	En caso de que exista un inventario, verificar su existencia visitando el lugar de almacenamiento (Bodega).

Fuente: Diego Quillupangui

9. Componente: Revisión de la Red (Factor ambiental, físico y humano)

Tabla 6.28. Guía de auditoria (Componente 9)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.2: Gestionar la seguridad de la red y las conexiones
Objetivos de Control	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión en el área de TI de la entidad
N°	**Procedimiento**
1	Por medio de la observación directa verificar que las instalaciones de la red interna y los equipos de cómputo esta implementada de forma correcta
2	Aplicar una encuesta al personal a cargo sobre las seguridades que cuenta el cuarto de comunicaciones y su accesibilidad.

Fuente: Diego Quillupangui

10. Componente: Controles para la instalación y uso de dispositivos externos

Tabla 6.29. Guía de auditoria (Componente 10)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Objetivos de Control	Verificar si existe algún tipo de control para el uso de periféricos, restricciones y su alcance
N°	**Procedimiento**
1	Aplicar una entrevista al encargado del área para identificar si utilizan algún método para restringir la instalación y uso de dispositivos externos (USB, HDD)

Fuente: Diego Quillupangui

11. Componente: Respaldo de información crítica

Tabla 6.30. Guía de auditoria (Componente 11)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad
Práctica	DSS04.7: Gestionar acuerdos de respaldo
Objetivos de Control	Mantener la disponibilidad de la información crítica de la empresa
N°	**Procedimiento**
1	Aplicar una entrevista al encargado del área para conocer la existencia de respaldos de la información importante de la empresa
2	Verificar si los respaldos son digitales (HDD, Flash, dispositivos externos)
3	Mediante una entrevista verificar si existe un plan de respaldo de información

Fuente: Diego Quillupangui

12. Componente: Plan de continuidad

Tabla 6.31. Guía de auditoria (Componente 12)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad
Práctica	DSS04.1: Definir la política de continuidad del negocio, objetivos y alcance
Objetivos de Control	Definir y Documentar los objetivos y el alcance de las políticas de continuidad del negocio en casos de desastres naturales o incidentes provocados que puedan afectar las operaciones totales o parciales de TI
N°	**Procedimiento**
1	Realizar una entrevista al encargado del área para conocer la existencia de un plan de continuidad ante un desastre natural o provocado
2	Solicitar detalles del plan de continuidad y los pasos que se realizan al momento de surgir un desastre natural o incidentes provocados en la empresa

Fuente: Diego Quillupangui

13. Componente: Plan de contingencia

Tabla 6.32. Guía de auditoria (Componente 13)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS02: Gestionar las peticiones y los Incidentes de Servicio
Práctica	DSS02.5: Resolver y recuperarse de incidentes
Objetivos de Control	Documentar, solicitar y aprobar soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio de TI
N°	**Procedimiento**
1	Realizar una entrevista al encargado del área para conocer la existencia de un plan de contingencia al momento de una fallo
2	Solicitar detalles del plan de contingencia de los pasos a seguir al momento de ocurrir un fallo que detenga las actividades de la empresa

Fuente: Diego Quillupangui

14. Componente: Plan de mantenimiento de Hardware y Software

Tabla 6.33. Guía de auditoria (Componente 14)

Guía de Auditoria	
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS01: Gestionar las Operaciones
Práctica	DSS01.3: Supervisar la infraestructura de TI
Objetivos de Control	Supervisar la infraestructura de TI y los eventos relacionados. Almacenar los registros cronológicamente de las operaciones de mantenimiento de Hardware y Software
N°	**Procedimiento**
1	Aplicar una entrevista para identificar la existencia de un plan de mantenimiento de TI
2	Identificar que el plan de mantenimiento de tecnologías de información, supervisar los registros de eventos sobre el mantenimiento de Hardware y Software

Fuente: Diego Quillupangui

15: Componente: Existe licenciamiento de los aplicativos instalados en el equipo informático

Tabla 6.34. Guía de auditoria (Componente 15)

Guía de Auditoria	
Dominio	Construir, adquirir e Implementar (BAI)
Proceso	BAI09: Gestionar los Activos
Práctica	BAI09.5: Administrar licencias
Objetivos de Control	Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos del negocio
N°	**Procedimiento**
1	Solicitar al encargado del área los detalles de las licencias de los aplicativos instalados en las computadoras de la empresa
2	Revisar las condiciones de licenciamiento de software que se están utilizando en la empresa

Fuente: Diego Quillupangui

16. Componente: Existencia de documentos de adquisición de equipos y software, contrato legal de proveedor de internet (ISP)

Tabla 6.35. Guía de auditoria (Componente 16)

Guía de Auditoria	
Dominio	Alinear, Planificar y Organizar (APO)
Proceso	APO10: Gestionar los Proveedores
Práctica	APO10.3: Gestionar contratos y relaciones con proveedores
Objetivos de Control	Seleccionar proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos
N°	**Procedimiento**
1	Solicitar al encargado del área el registro y respaldo de facturas donde demuestre la adquisición de equipos, software y servicio de Internet
2	Evaluar la eficiencia de la relación con los proveedores e identificar las mejoras necesarias

Fuente: Diego Quillupangui

17. Componente: Documentación de los sistemas utilizados para los servicios de la empresa

Tabla 6.36. Guía de auditoria (Componente 17)

Guía de Auditoria	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI04: Gestionar la Disponibilidad y Capacidad
Práctica	BAI04.4: Supervisar y revisar la Disponibilidad y la Capacidad
Objetivos de Control	Determinar la existencia de la documentación de los sistemas adquiridos por la empresa y si esta documentación posee todos los datos necesarios para dar mantenimiento al sistema en caso necesario
N°	**Procedimiento**
1	Solicitar al personal a cargo sobre la documentación (diagramas, arquitectura, código) de los sistemas adquiridos por la empresa

Fuente: Diego Quillupangui

6.14. Formalización

El proceso de esta auditoria se acordó de manera formal con el administrador de la empresa Rosas del Corazón, en una reunión donde se convino entre el gerente y el auditor, el área a auditar, los límites y alcances, visitas y tiempo de evaluación.

6.14.1. Desarrollo

Luego de aplicar las técnicas y herramientas durante la auditoria de seguridad informática se evidencio los siguientes detalles:

Seguridad lógica

Al evaluar cada uno de los componentes expresados con anterioridad, se obtuvieron los siguientes detalles que se describen a continuación:

Componentes:

1. **Acceso de los usuarios a sistemas, sistemas operativos y bases de datos**

En el apartado de acceso de los usuarios a sistemas, sistemas operativos y bases de datos. Se aplica una entrevista al responsable del área, se pudo evidenciar que no existe el listado de definiciones de los roles y responsabilidades relacionadas con las TI.

Durante el desarrollo de esta etapa del trabajo se evidencio que no existe un departamento de TI como tal, y se manifiesta que existe una persona que realiza soporte técnico a los equipos, monitorea la red interna de la empresa y lleva el control del área informática de la empresa.

Luego de aplicar la encuesta al administrador de la empresa Rosas del Corazón y aplicando la observación directa se pudo constatar que todos los equipos informáticos disponen de usuario y contraseña respectiva para acceder a cada computadora.

En cuanto al acceso de los usuarios a sistemas se encontró que en la empresa se emplean dos sistemas de información, luego de comunicarse con el administrador del sistema (SOFIA) que maneja la empresa se evidencio que cada aplicación requiere de usuario y contraseña para poder acceder a gestionar cada proceso. SOFIA es un software de gestión de empleados, horas de trabajo, facturación electrónica, el cual requiere una conexión a internet para trabajar o también se puede trabajar en la LAN, el servidor se encuentra alojado en las mismas instalaciones de la empresa. Este sistema requiere usuario y contraseña para el acceso, administración, y gestión de información. En la empresa existe el personal que administra las

TI y tiene su usuario y contraseña para acceder al servidor para gestionar los respaldos de la BDD.

Al mismo tiempo el administrador del Sistema SOFIA es el encargado de gestionar, administrar, actualizar servicios que requiere el sistema para su correcto funcionamiento. Cabe aclarar que este sistema no es propiedad de la empresa, pertenece a una empresa la cual presta este servicio. En la empresa Rosas del Corazón existen ocho usuarios que disponen de usuario y contraseña para acceder a distintos servicios que gestiona SOFIA.

También existe el sistema UNOSOF, el cual ayuda a la gestión de procesos de producción de flor, este sistema fue adquirido a terceros. Y ellos son los encargados de administrar, gestionar el sistema y las BDD, luego de la entrevista con el gerente de la empresa se evidencio que para acceder a este sistema se necesita usuario y contraseña, según la información obtenida cada empleado en las distintas áreas de producción de flor tiene acceso al sistema. Indicó asimismo que son 10 usuarios que usan el sistema.

Los controles de acceso a los sistemas informáticos son muy importantes, ya que así se aumenta la seguridad e integridad de la información, se disminuye el riesgo de fraude o alteración, esto beneficia enormemente a la empresa, ya que la información está segura y bien administrada.

2. Acceso de los usuarios a programas y archivos

Con respecto al manejo de la información sensible de la empresa, su uso y su eliminación, se pudo identificar por medio de la entrevista que la información tiene acceso restringido para las personas de la empresa, y que solo son manipuladas por personas específicas de confianza, y las decisiones se las toma en la gerencia administrativa.

Se pudo observar que la información se encuentra vulnerable ante el acceso a personas, ya que algunas carpetas no se encuentran protegidas, aunque no se ha podido acceder a la información sensible de la empresa, cabe recalcar que si hubiera una persona con fines fraudulentos podría acceder fácilmente.

También se evidenció que en ocasiones algunos computadores son usados por más de una persona en la misma sesión.

Luego de aplicar una entrevista al personal responsable del área, en este caso al gerente administrativo de la empresa, supo manifestar que si existen reglamentos en cuanto a permisos de acceso para que los usuarios únicamente tengan acceso a ciertos programas, se ha

podido observar que utilizan los programas de ofimática, Outlook, Incredimail, OperaMail para uso del correo institucional, exploradores de internet (Internet Explorer, Mozilla Firefox, Google Chrome) para acceder a páginas de la empresa y de gobierno (IESS, SRI), Skype para la comunicación interna compartir recursos (fotografías, capturas, documentos). Y tiene prohibido el uso de programas ajenos a la función de cada empleado.

Estas prohibiciones son informadas de manera verbal a los empleados, por medio de la gerencia administrativa. También se pudo constatar que no existen rótulos visibles que indiquen los reglamentos de uso de TI.

Este control es muy importante ya que el empleador deja claro a los empleados cuáles son sus responsabilidades, derechos y restricciones en cuanto al uso de TI en la empresa.

3. Disposición de sistemas alternos en caso de fallos

En cuanto a la disposición de sistemas alternos en caso de fallos, se solicitó la documentación necesaria pero no se encontró información sobre estos registros de fallos frecuentes u ocasionales. También admitió que no se tiene un control de los fallos que ocurren en la empresa, generalmente ante fallos graves en los equipos de cómputo o servidores se emite un informe con los datos del incidente y la solución dada al caso.

Por otra parte se pudo constatar que no existe un servidor alterno que almacene la información de la empresa en tiempo real. Solamente existe un respaldo de la información de contabilidad, de empleados, registro de horarios que se la realiza periódicamente en el mismo servidor y luego se lo sube a una nube de Google Drive manualmente.

Luego de una entrevista para obtener información acerca de las medidas de seguridad que cuenta en caso de fallar uno de los sistemas, se pudo constatar que no existen medidas de seguridad en caso de fallo. El administrador expresa que ante un fallo cuenta únicamente con la información respaldada en el servidor y las acciones que se toman son acorde a las necesidades del caso.

La falta de sistemas alternos para la prevención de caídas, o pérdida de servicios es una falencia muy grave, ya que ante algún inconveniente la empresa podría detener parcial o totalmente sus actividades, y esto ocasionaría pérdida de recursos (tiempo, recurso humano), estas pérdidas pueden ser cuantiosas para la empresa.

4. **Existencia de software de protección (Antivirus, firewall)**

Al verificar la existencia de software de protección se obtuvo que cada computadora cuenta con el antivirus Panda Cloud con licencia por un año, la contratación de este servicio lo hace de manera directa la gerencia administrativa de la empresa. También se pudo observar que se utiliza el firewall del sistema operativo.

Durante este proceso se pudo constatar lo expuesto en la entrevista, que las actualizaciones de los parches de seguridad del sistema operativo no se actualizan regularmente, que todo es según las necesidades de la empresa.

Asimismo se evidencio que están desactivados los filtros de correo electrónico no deseado, esto quiere decir que generalmente todos los correos son aceptados sin ayuda de ninguna seguridad que garantice la veracidad del contenido del correo electrónico.

La existencia de un software se seguridad, parches de sistema operativo actualizados y filtro de correo electrónico no deseado es indispensable para la integridad y manejo de la información de la empresa. Este tipo de seguridad, permite proteger en gran manera la información digital de la empresa, así como mantenerse seguro ante ataques de software malicioso o virus que merodean la red WAN.

5. **Control de acceso de los usuarios a los servicios de internet**

Luego de aplicar la entrevista al administrador de la empresa se confirmó que no existe un reglamento de control de acceso para el uso del servicio a internet, también nos supo manifestar que la red está protegida por la clave de seguridad del Wifi, y que las personas que tienen acceso a internet son limitadas para no congestionar la red interna.

En la empresa se hace un control de acceso a internet por medio de la restricción de IP, configurados desde el router principal de la empresa, el cual está divido para el área administrativa y la parte activa de la empresa. El área administrativa puede acceder a todas la paginas de internet, mientras que la parte operativa solo puede acceder a sitios de uso exclusivo de trabajo, páginas de la empresa y la gestión de correo electrónico.

Mantener el control de los permisos de acceso a internet y utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información permite que disminuya los riesgos que puedan afectar la integridad de la información, y garantizar la comunicación efectiva y ágil a través de este medio de comunicación.

Seguridad física

A continuación se describe los datos obtenidos al evaluar los componentes descritos como seguridad física en la empresa Rosas del Corazón:

Componentes

6. **Control de acceso de los usuarios a los equipos**

Al solicitar información sobre el control de acceso de los usuarios a los equipos informáticos se evidencio que existe un control de los equipos y su ubicación por cada departamento con su respectivo equipamiento, pero no se halló un registro de las horas de trabajo de cada equipo, asimismo se evidenció que no existe un registro de los equipos que dejaron de funcionar, también no se encontró un registro de control de acceso a los servidores

Luego de aplicar la entrevista se comprobó que no existen políticas de seguridad para dispositivos de usuario final, cabe aclarar que el administrador de la empresa afirma que las políticas son importantes y necesarias, ya que sirven para tener una mejor estructura dentro del área informática.

El uso de controles de acceso a equipos asegura los puestos de usuario final, aplicar estas normativas evita riesgos provocados por accidentes o acciones mal intencionadas, dando así mayores garantías de disponibilidad e integridad de la información.

7. **Informes de accesos y visitas a las instalaciones**

En la empresa Rosas del Corazón si existe una garita a la entrada de la plantación, también existen informes de acceso y visitas, las notificaciones de ingreso se hacen de manera verbal por un radio de comunicaciones interno de la empresa y se pide la autorización al área administrativa. Según sea el caso. También se solicita un documento de identificación a que área se dirigen y si tiene cita o no.

Cuando es personal de soporte técnico de equipos especiales como es el caso de impresoras de etiquetas o pistolas lectoras de código o instalación de nuevo equipamiento informático se los identifica por el nombre de la empresa, se los registra en la garita, pero no hay un registro en una hoja de actividades en el área de TI, el encargado del área de TI emite un informe al administrador de la empresa con las actividades realizadas.

Se pudo observar la existencia de un sistema de seguridad en el área de servidores que permite monitorear por medio de cámaras, se pudo constatar también que no existe un área de operaciones como tal, no existe un departamento de sistemas físico.

Mantener un control de visitas y control de presencia de personal externo en la organización es de vital importancia, porque de esta forma se mantiene un ambiente seguro para el personal que labora en la empresa, así también se mantienen seguros los activos de la empresa y permite la operación normal de los trabajos en la empresa.

8. Inventario de equipos y software

Al momento de aplicar la entrevista se pudo constatar que si existe un inventario de equipos y software, la empresa no cuenta con un almacén donde se encuentran solo las computadoras y equipos electrónicos, actualmente utilizan una bodega donde se almacenan todos los equipos sin ningún tipo de registro.

Existe un registro manual de los equipos que están es cada área, con su impresora, regulador de voltaje o UPS, modelo del procesador, disco duro, RAM.

Existe un computador donde se realizan las operaciones internas del área informática, donde se realizan informes, se realizan pruebas de hardware y software, es un área compartida en una oficina junto al departamento de compras.

Este computador es un equipo básico que es compartido con el área de Trabajo Social que generalmente ocupa la computadora dos veces por semana.

Es importante tener el inventario de hardware y software actualizado, así como también un área de trabajo independiente, es de mucha importancia disponer de un lugar donde almacenen las TI, esto permite a la empresa tener un control directo sobre sus activos, asimismo ayuda a identificar de manera eficiente lo que debe adquirir en caso de alguna modificación en el equipamiento informático.

9. Revisión de la red (factor ambiental, físico y humano)

La red informática está compuesta por un cableado plano, el proveedor de servicios de Internet (ISP) es Telconet que proporciona una conectividad con fibra óptica compartición 1:1, que cuenta con equipos de conversión de fibra óptica a UTP cat 5e, también cuenta con un router Cisco que sirve de puerta de enlace para el servicio de internet; del lado de la empresa se conecta con un cable UTP con un router Cisco RV130, que permite la configuración de restricciones y que trabaja como un equipo firewall de la red.

Se observó que el router se encuentra en un rack de piso de 42UR, junto con un Switch de 32 puertos, también se encuentra el dispositivo de comunicaciones para las líneas telefónicas IP, el servidor SOFIA y el equipo DVR para la seguridad de las cámaras. Cada punto de red de

datos se dirige por medio de canaletas que cubren la mayor parte del recorrido del cable hasta su respectiva toma de datos ubicado en cada sitio de trabajo, se utiliza un solo estándar para cableado estructurado que cumple con el proceso de transmisión de datos es EIA/TIA 568-B, también se observó que los equipos de comunicaciones no cuentan con las condiciones ambientales y condiciones físicas establecidas por los estándares. Existe un segundo rack de comunicaciones de 42UR donde se ubican los servidores de UNOSOF con un Switch de comunicaciones de 16 puertos 10/100, también se observa un UPS de torre de gran capacidad (3000VA).

Los rack de comunicaciones están ubicados en la oficina de Bienestar, seguridad y salud ocupacional de la empresa. Esto evidencia que no cuenta con un cuarto de comunicaciones como tal. Cabe destacar que en lo referente a seguridad, esta oficina cuenta con detector de humo, alarma, seguridad en las puertas, monitoreo mediante cámaras de seguridad.

La seguridad de la red es un factor muy importante dentro del área informática, ya que se debe garantizar una buena seguridad de los datos que son transmitidos a través del medio, sea físico o inalámbrico. Así que para asegurar la red de datos se debe tomar en cuenta todos los aspectos que incorpora la red para realizar una revisión o mantenimiento, la cual debe realizarse bajo una planificación, y según los tiempos que se considere internamente en la empresa.

10. Controles para la instalación y uso de dispositivos externos

En lo que se refiere a los controles de instalación y uso de dispositivos externos, se identificó que la empresa no tiene una política de restricciones en cuanto al uso de dispositivos externos, esto ha ocasionado serias complicaciones al momento de realizar un inventario de equipos, también el uso libre de dispositivos pone en riesgo la información de la empresa.

Los controles para la instalación de hardware o software impiden que personas no autorizadas conecten dispositivos externos, y puedan copiar la información confidencial de la empresa o que puedan instalar aplicaciones que son necesarias para el flujo normal de la empresa, evitando también la reproducción o copia de virus o archivos maliciosos.

Respaldos y planes de contingencia

Al evaluar los componentes descritos en este punto, se identificaron los hallazgos que se muestran a continuación:

Componentes:

11. Respaldo de información crítica

Luego de la entrevista aplicada al administrador de la empresa, se pudo constatar que si existen respaldos de la información importante de la empresa, estos respaldos se los realiza en el mismo servidor, y posteriormente son subidos a la nube. También se pudo constatar que no existe una planificación de respaldo de información, únicamente se realiza un respaldo periódico sin ningún control o supervisión de parte del administrador de la empresa.

El administrador supo manifestar que las personas encargadas de realizar el respaldo de la información son la persona encargada del área de TI, y los administradores de sistema UNOSOF quienes realizar un respaldo de forma remota.

El respaldo de la información crítica, es lo más importante de TI en una empresa, es necesario salvaguardar la información de la empresa, las personas responsables de esta información deben ser muy cautelosas, para asegurar que sus operaciones no sean afectadas por desastres o accidentes, ya que la existencia de respaldos actualizados de la información puede ser de gran ayuda para una pronta recuperación en caso de un incidente informático.

12. Plan de continuidad

Luego de realizar una entrevista al administrador de la empresa se constató que no existe un plan de continuidad ante un desastre natural o provocado, también supo manifestar que en un momento dado ya se presentó un ataque provocado, y que el primer punto a seguir fue levantar nuevamente el servidor, acceder a los respaldos de la información, cambiar claves de seguridad para limitar accesos.

El plan de continuidad es necesario, y al mismo tiempo debe ser funcional en una entidad ya que si ocurriera un desastre natural o provocado, la empresa enfocada en asegurar la continuidad del negocio, no quedaría fuera de operaciones por largos periodos de tiempo y no tendría pérdidas económicas representativas.

13. Plan de contingencia

Luego de la entrevista aplicada al administrador de la empresa se constató que en caso de fallos de los sistemas de información la empresa no cuenta con un plan de contingencia, ya que si ocurriera algún problema se llamaría a las personas respectivas que puedan dar solución inmediata a los problemas, en ocasiones el servicio de luz eléctrica ha sido muy fluctuante en la temporada invernal, y se ha tenido que tomar medidas precautelares, tales

como, revisar las instalaciones eléctricas de manera general, para prevenir esto hace pocos meses se instaló un generador de luz.

En el área de producción de flor tienen planes de contingencia para sobrellevar la información de manera física en fichas o libretas de apuntes, y esto hace que la información no se pierda y se espere hasta que se restablezca el sistema y puedan ser registrados en el sistema informático.

Un plan de contingencia actualizado es muy importante ya que ante algún fallo en el sistema, se tomaría procedimientos y acciones de respuesta inmediata para afrontar de manera oportuna y efectiva la eventualidad tratando de disminuir el impacto que puede causar el incidente.

14. Plan de mantenimiento de hardware y software

Al realizar la entrevista se encontró que una persona realiza el soporte y mantenimiento de equipos de cómputo, esta persona va continuamente a la empresa y realiza el mantenimiento preventivo y correctivo de los equipos, existe una planificación anual de mantenimiento, la cual no se ha podido cumplir a cabalidad, puesto que los equipos informáticos la mayor parte del tiempo están siendo utilizados.

El mantenimiento de software UNOSOF y SOFIA es realizado por los propios propietarios de los sistemas, en caso de actualización o modificaciones, parches de seguridad, actualización de módulos.

Es necesaria la existencia de un plan de mantenimiento, puesto que en un supuesto caso exista algún cambio de personal en la empresa, la nueva persona estaría al tanto de los procedimientos a seguir sin tener ningún tipo de sorpresas futuras.

Documentación de hardware y software

Al evaluar los componentes descritos en la documentación de Hardware y Software, se han encontrado los siguientes hallazgos que se detallan a continuación:

Componentes:

15. Existe licenciamiento de los aplicativos instalados en el equipo informático

Luego de obtener la información adecuada se pudo constatar que si existen licencias en cuanto a programas antivirus, cuenta con el programa Panda Cloud con licencia para un año.
En cuanto a lo que tiene que ver con los programas de ofimática y los sistemas operativos en cada computador de la empresa si cuenta con licenciamiento, este licenciamiento es aplicado

por medio de parches o crack al momento de la instalación. Es un tipo de licencia no autorizada por el desarrollador del programa. Las computadoras de la empresa utilizan software no original, salvo el caso de los servidores UNOSOF y las laptop del personal administrativo.

Para el licenciamiento del antivirus Panda Cloud se pudo constatar que es un licenciamiento para un número ilimitado de computadoras, la renovación la realiza la gerencia administrativa de la empresa.

La instalación de programas con licencia legal garantiza el funcionamiento correcto de los productos, y al mismo tiempo los programas no tienen ningún tipo de inconvenientes, a su vez el usuario podría disfrutar de características adicionales y beneficiarse con las últimas actualizaciones del software y recibir soporte técnico.

16. Existencia de documentos de adquisición de equipos y software, contratos legal de proveedores de Internet (ISP)

Al comprobar la existencia de documentos de adquisición de equipos y software y contratos legales de proveedores de internet, se encontró que la empresa tiene un contrato legal, resguardados por el área contable, no se puede acceder a él físicamente pero la contadora aseguró la existencia del mismo.

En cuanto al proveedor de equipos de cómputo se identifica que la empresa trabaja con dos proveedores con los cuales solo se tiene un contrato verbal, y que hasta ahora ha existido una comunicación eficiente y fluida.

Se explicó también que existe un contrato con una empresa aseguradora del equipo de cómputo que se llama Seguros Equinoccial, las cláusulas de dicho contrato cubren daños por eventos naturales. Se evidencio que hace un tiempo atrás pudieron aplicar este seguro y se lo realizo de manera eficiente. Está póliza de seguro debe ser renovada cada año.

La implementación de un control de proveedores en la empresa es muy importante, es necesario que la empresa posea documentación que ratifique los convenios con los proveedores, dando a conocer cláusulas de convenio que den legitimidad y veracidad de sus servicios.

17. Documentación de los sistemas utilizados para los servicios de la empresa

En cuanto a la información de los sistemas utilizados por la empresa se constató que no posee la documentación de los programas que utiliza, ya que son programas comprados y desarrollados por terceros.

Cabe aclarar que la compra de los sistemas como tal es solo para uso, y que no se han comprado los derechos de modificación de código fuente.

La única documentación obtenida por parte de los administradores de los sistemas son los manuales de usuario, pero según la encuesta aplicada este manual no es de conocimiento para el personal que utiliza estos sistemas, solamente tuvieron capacitaciones para su uso.

La falta de documentos o la falta de socialización de los mismos, ocasiona que los sistemas puedan convertirse en una carga para la empresa, ya que no existiría un manejo eficiente de los sistemas, y no se podría explotar la máxima capacidad del software.

6.15. Informe de auditoria

6.15.1. Objetivo

Realizar la valoración de los resultados obtenidos en el proceso de auditoría a la seguridad Informática en la empresa Rosas del Corazón.

6.16. Alcance

La auditoría a la seguridad Informática se llevó a cabo en la Empresa Rosas del Corazón en un periodo de 40 días laborables (dos meses) para la recolección de datos, y 40 días laborables para el análisis de la información, conclusiones y recomendaciones de la auditoria, en el cual se abordó la evaluación del área informática de la empresa y dentro de esta evaluación se seleccionó las siguientes áreas de TI: seguridad física, seguridad lógica, respaldos de datos, planes de mantenimiento, contingencia y continuidad, y la documentación general y específica sobre equipos, sistemas y software utilizados en la empresa.

Debido a los parámetros acordados previos a la auditoria, la gerencia administrativa no permitiría el acceso a la información valiosa y confidencial de la empresa (contabilidad), es por ello que se aplicaron técnicas de recolección de datos como son: entrevistas, cuestionarios y la observación directa, que permitieron verificar el cumplimiento de las normas de seguridad en el área de TI de la empresa.

6.17. Situación observada (hallazgos) y recomendaciones

Durante la auditoria se recolectaron datos muy importantes sobre la gestión y control de las tecnologías de información, hasta este punto se ha podido analizar la información recopilada, la cual será expuesta al administrador de la empresa Rosas del Corazón.

Área: Seguridad lógica

Tabla 6.37. Hallazgos componente 1

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-001	
Hallazgos de la Auditoría	
Componente:	Acceso de los usuarios a sistemas, sistemas operativos y bases de datos
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de seguridad
Práctica:	DSS05.4: Gestionar la identidad del Usuario y el Acceso Lógico
Evidencia:	La entrevista, el cuestionario, la observación directa
Condición	
No existe el listado de definiciones de los roles y responsabilidades relacionadas con TI	
Criterio	
(410-02 Segregación de funciones) La empresa debe definir las funciones y responsabilidades de los usuarios que serán claramente definidas y formalmente comunicadas para que se ejerzan con suficiente autoridad y respaldo. Esto garantiza una adecuada segregación, evitando funciones incompletas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.	
Causa	
La falta de un departamento informático, y la falta de administración del área de TI	
Efecto	
Al no tener definidos los roles y responsabilidades de cada usuario, no se puede gestionar las soluciones en medio de un fallo en el sistema	
Conclusión	
La aplicación correcta de los controles de acceso a los sistemas informáticos es muy importante, esto sirve para aumentar la seguridad e integridad de la información.	
Recomendación	
Se recomienda a largo plazo incluir a una persona a tiempo completo para el control y gestión del área de TI en la empresa Rosas del Corazón. También crear un documento donde se especifique los roles y responsabilidades para los usuarios y sean formalmente comunicados al personal.	

Fuente: Diego Quillupangui

Tabla 6.38. Hallazgos Componente 2

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-002	
Hallazgos de la Auditoría	
Componente:	Acceso de los usuarios a programas o archivos
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de seguridad
Práctica:	DSS05.6: Gestionar Documentos sensibles y dispositivos de Salida
Evidencia:	La observación directa, la entrevista
Condición	
No existe un control de acceso a la información privada de la empresa Algunos computadores son usados por más de un usuario	
Criterio	
(500-01 Controles sobre sistemas de información) Los sistemas de información contarán con controles adecuados que garanticen razonablemente la protección de la información según su grado de sensibilidad, confidencialidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles.	
Causa	
Inexistencia de controles adecuados sobre la administración de TI	
Efecto	
Aumenta el riesgo de fraude o alteración de la información. Aumenta la inseguridad en cuanto al manejo de la información.	
Conclusión	
Establecer controles adecuados es de gran importancia para llevar un control y mantener de manera más segura la información de la empresa y la confidencialidad de cada usuario.	
Recomendación	
Se recomienda la establecer controles generales de aplicación y operación que garanticen la protección de la información según su grado de sensibilidad y confidencialidad. Es recomendable cifrar la información importante de la empresa para evitar el uso mal intencionado de la información.	

Fuente: Diego Quillupangui

Tabla 6.39. Hallazgos Componente 3

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-003	
Hallazgos de la Auditoría	
Componente:	Disposición de sistemas alternos en caso de fallos
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS02: Gestionar los servicios de Seguridad
Práctica:	DSS02.5: Resolver y recuperarse ante incidentes
Evidencia:	La entrevista, la observación directa
Condición	
No existen control de fallos ocasionados en el área de TI No existe un servidor alterno No existen un plan de continuidad de las operaciones	
Criterio	
(410-11 Plan de Contingencias) Incorporar controles, sistemas de aseguramiento de la calidad y gestión de riesgos, al igual que directrices y estándares tecnológicos. Un plan de respuesta a los riesgos que incluye la definición y asignación de roles críticos para administrar los riesgos de TI.	
Causa	
La falta de un plan de recuperación ante desastres en el área de TI	
Efecto	
No se puede identificar las posibles causas de daños provocados o daños imprevistos en las TI. Se podría detener parcial o totalmente las actividades de la empresa. Se podría perder información, y podría generar pérdidas cuantiosas para la empresa.	
Conclusión	
Es muy importante un plan de contingencia que describa las acciones a tomar en caso de emergencias.	
Recomendación	
Se recomienda establecer un plan de continuidad que describa las acciones a tomar en caso de una emergencia o suspensión del procesamiento de la información por fallos o problemas en las TI.	

Fuente: Diego Quillupangui

Tabla 6.40. Hallazgos Componente 4

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-004	
Hallazgos de la Auditoría	
Componente:	Existencia de software de protección (antivirus, firewall)
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de Seguridad
Práctica:	DSS05.1: Proteger contra software malicioso (malware)
Evidencia:	La observación directa, la entrevista
Condición	
Falta de actualización de parches de seguridad del Sistema Operativo Filtros de correo no deseado están desactivados.	
Criterio	
(410-10 Seguridad de tecnología de información) Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidad o incidentes de seguridad identificados.	
Causa	
Las TI en la empresa son un tema parcialmente desatendido por la gerencia administrativa	
Efecto	
La falta de actualización del Sistema Operativo crea vulnerabilidades en la seguridades del SO. El correo no deseado puede sobrecargar la red LAN, obstruir los servidores de correo y llenar los buzones de mensajes no deseados.	
Conclusión	
Mantener los equipos actualizados, aumenta la seguridad, elimina la vulnerabilidad e inestabilidad de la computadora.	
Recomendación	
Se recomienda implementar y administrar las seguridades a nivel del Sistema Operativo Crear una lista de contactos de correo deseado y listas de remitentes seguros.	

Fuente: Diego Quillupangui

Tabla 6.41. Hallazgos Componente 5

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-005	
Hallazgos de la Auditoría	
Componente:	Control de acceso de los usuarios a los servicios de internet
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de Seguridad
Práctica:	DSS05.2: Gestionar la seguridad de la red y las conexiones
Evidencia:	La entrevista, la observación directa
Condición	
No existe un reglamento de control de acceso para el uso del servicio de internet WIFI	
Criterio	
(410-14 Sitio web, servicios de internet e intranet) Elaborar normas, procedimiento e instructivos de instalación, configuración y utilización de los servicios de internet, intranet y correo electrónico, a base de las disposiciones, normativas y requerimientos de los usuarios externo e internos.	
Causa	
Los objetivos del área informática no están alineados con los objetivos empresariales de la empresa Rosas del Corazón	
Efecto	
El no tener un control de acceso y normativas de uso al servicio de internet, hace que algunos usuarios accedan y puedan ocasionar un conflicto en la red o saturar la red informática de la empresa.	
Conclusión	
Un estricto control de uso de TI y utilizar medidas de seguridad y procedimiento permite una mejor gestión para proteger la información, los servicios y recursos informáticos que se usan en la empresa.	
Recomendación	
Se recomienda elaborar normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, a base los requerimientos de los usuarios externos e internos.	

Fuente: Diego Quillupangui

Tabla 6.42. Hallazgos Componente 6

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-006	
Hallazgos de la Auditoría	
Componente:	Control de acceso de los usuarios a los equipos
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de Seguridad
Práctica:	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Evidencia:	Cuestionario, la entrevista, la observación directa
Condición	
No existe un control de acceso del personal que accede a los equipos servidores No existen políticas de seguridad informática	
Criterio	
(410-12 Administración de Soporte de Tecnología de Información) Definición y manejo de niveles de servicio y de operaciones para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacitaciones tecnológicas.	
Causa	
No existe un interés real de la gestión administrativa del área de TI para que existan políticas de seguridad informática en la empresa.	
Efecto	
Podría provocar accidentes o acciones malintencionadas por personas que no pertenecen al área de TI, limita las garantías de disponibilidad e integridad de la información.	
Conclusión	
Mantener una gestión clara sobre el manejo de TI es de vital importancia para garantizar la confiabilidad y disponibilidad de la información en una entidad.	
Recomendación	
Se recomienda a corto plazo definir por escrito el manejo de niveles de servicio y de operación de usuarios de acuerdo a las necesidades de la empresa.	

Fuente: Diego Quillupangui

Tabla 6.43. Hallazgos Componente 7

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-007	
Hallazgos de la Auditoría	
Componente:	Informes de acceso y visitas a las instalaciones
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de Seguridad
Práctica:	DSS05.5: Gestionar el acceso físico a los activos de TI
Evidencia:	La observación directa, la entrevista
Condición	
No existe un departamento de operaciones – Departamento de Sistemas No hay un registro de actividades de soporte técnico de personal externo de la empresa	
Criterio	
(410-12 Administración de Soporte de Tecnología de Información) Seguridad de los sistemas bajo otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.	
Causa	
No tomar en cuenta el área de TI como parte importante en la toma de decisiones de la empresa. Desinterés parcial del control de acceso de personal externo a los activos de TI	
Efecto	
Al no tener el control de acceso del personal que ingresa al área de TI, no se puede garantizar la seguridad de los activos de TI, al mismo tiempo no garantiza la integridad y disponibilidad de la información.	
Conclusión	
Es importante que todas las personas que tenga acceso a la infraestructura de TI la empresa estén identificados.	
Recomendación	
Se recomienda otorgar una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información. Crear un registro de actividades de visitantes.	

Fuente: Diego Quillupangui

Tabla 6.44. Hallazgos Componente 8

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-008	
Hallazgos de la Auditoría	
Componente:	Inventario de equipos y Software
Dominio:	Construir, Adquirir e Implementar (BAI)
Proceso:	BAI09: Gestionar los Activos
Práctica:	BAI09.1: Identificar y registrar activos actuales
Evidencia:	La entrevista, la observación directa
Condición	
No cuenta con un almacén o bodega de TI	
Criterio	
Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento, que están justificados y protegidos físicamente. Es importante tener un inventario de hardware y software actualizado, así como también el lugar donde se almacene el equipamiento informático	
Causa	
El área administrativa no ha gestionado de manera correcta el uso de una bodega exclusiva para el equipamiento de TI	
Efecto	
El no contar con un inventario de lo que se tiene en operaciones y en bodega, hace que el área de TI este vulnerable por falta de equipamiento de repuestos o piezas del equipo informático.	
Conclusión	
Llevar un control de operaciones y un control de activos, genera confianza en el área de TI, permite una mejor gestión administrativa de recursos.	
Recomendación	
Se recomienda a largo plazo crear un almacén o bodega de equipamiento informático con partes y piezas. Se recomienda actualizar los activos de TI de la empresa.	

Fuente: Diego Quillupangui

Tabla 6.45. Hallazgos Componente 9

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-009	
Hallazgos de la Auditoría	
Componente:	Revisión de la red (factor ambiental, físico y humano)
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de Seguridad
Práctica:	DSS05.2: Gestionar la seguridad de la red y las conexiones
Evidencia:	La observación directa, la encuesta
Condición	
La empresa no cuenta con un cuarto de comunicaciones propio	
Criterio	
El cuarto de telecomunicaciones es el espacio utilizado exclusivamente para alojar equipos de comunicaciones.	
Causa	
La empresa ha ido incrementando el equipamiento informático sin ninguna planificación previa	
Efecto	
Los equipos se encuentran en riesgo ante desastres naturales (inundaciones), ingreso de personal no autorizado, robos.	
Conclusión	
Mantener un equipamiento tecnológico correctamente conlleva a aplicar normas de seguridad que resguarden el acceso a la información y uso de los sistemas informáticos y los mantengan siempre operativos.	
Recomendación	
Se recomienda a largo plazo el diseño e implementación de un cuarto de telecomunicaciones considerando la disponibilidad del espacio, escalabilidad aplicando las medidas de seguridad tanto físicas como lógicas, debe contar con los servicios de electricidad, canalización y distribución del cableado de datos.	

Fuente: Diego Quillupangui

Tabla 6.46. Hallazgos Componente 10

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-010	
Hallazgos de la Auditoría	
Componente:	Controles para la instalación y uso de dispositivos externos
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS05: Gestionar los servicios de Seguridad
Práctica:	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Evidencia:	La entrevista, la observación directa
Condición	
No existe una política en cuanto a la instalación y uso de dispositivos externos	
Criterio	
(410-04 Políticas y procedimientos) Definir y difundir políticas y procedimientos que regulen las actividades relacionadas con tecnología de información en la empresa, estos de actualizaran permanentemente.	
Causa	
No existe un control de acceso a la información importante que administra cada área de la empresa	
Efecto	
Fácil accesibilidad a la información delicada de la empresa. Permite realizar copias de archivos sin restricciones de uso. Podría generar fraude informático. Copiar y socializar información privada de la empresa	
Conclusión	
Considerar muy seriamente el control de uso de dispositivos externos en los computadores de la empresa.	
Recomendación	
Se recomienda a corto plazo definir, documentar y difundir las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnologías de información.	

Fuente: Diego Quillupangui

Tabla 6.47. Hallazgos Complemento 11

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-011	
Hallazgos de la Auditoría	
Componente:	Respaldo de información crítica
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS04: Gestionar la continuidad
Práctica:	DSS04.7: Gestionar acuerdos de respaldo
Evidencia:	La entrevista, la observación directa
Condición	
No existe una planificación para el respaldo de la información	
Criterio	
(410-10 Seguridad de tecnología de información) Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado. Almacenamiento de respaldos con información crítica o sensible en lugares externos a la empresa.	
Causa	
No existe una planificación que ayude a la gestión de respaldos de la información.	
Efecto	
Perdida de información valiosa para la empresa. En caso de un siniestro, no tendría respaldos actualizados que permitan reestablecer la información importante.	
Conclusión	
Cada área es importante, y muchos más el área de seguridad informática, ya que se almacena información vital para buen funcionamiento de la empresa	
Recomendación	
Se recomienda a corto plazo definir los procedimientos para la obtención y gestión de respaldos de la información sensible de la empresa.	

Fuente: Diego Quillupangui

Tabla 6.48. Hallazgos Complemento 12

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-012	
Hallazgos de la Auditoria	
Componente:	Plan de continuidad
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS04: Gestionar la continuidad
Práctica:	DSS04.1: Definir la política de continuidad del negocio, objetivos y alcance
Evidencia:	La entrevista, la observación directa
Condición	
No existe un plan de continuidad ante un desastre natural o provocado	
Criterio	
(410-11 Plan de Contingencias) El plan de continuidad de las operaciones que contemplará la puesta en marcha de un servidor alterno, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.	
Causa	
El personal de TI no ha tomado las medidas específicas en caso de accidentes provocados o no para restaurar el sistema informático.	
Efecto	
Riesgo de pérdida de la información y pérdida de sistemas, pérdidas económicas representativas para la empresa	
Conclusión	
Los planes de continuidad son importantes dentro de un área, en especial del área informática, ya que lleva información de vital importancia para el correcto funcionamiento de la empresa.	
Recomendación	
Se recomienda a corto plazo definir e implementar un plan de continuidad acorde a las necesidades de la empresa, alineadas a los objetivos de TI, con el fin de resguardar la información.	

Fuente: Diego Quillupangui

Tabla 6.49. Hallazgos Componente 13

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-013	
Hallazgos de la Auditoría	
Componente:	Plan de Contingencia
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS02: Gestionar las peticiones y los Incidentes de Servicio
Práctica:	DSS02.5: Resolver y recuperarse de incidentes
Evidencia:	La entrevista, la observación directa
Condición	
La empresa no cuenta con un plan de contingencia	
Criterio	
(410-11 Plan de Contingencias) Definir e implementar un plan de contingencia que describa las acciones a tomar en caso de una emergencia. Este plan será difundido entre las personas responsables de su ejecución y deberá ser sometido a pruebas.	
Causa	
Falta de implementación de un plan de contingencia por parte del encargado del área de TI	
Efecto	
La empresa puede tener pérdidas de información muy graves que representen pérdidas significativas para la empresa.	
Conclusión	
La aplicación de planes de contingencia asegura la información de la entidad, salvaguardando los recursos técnicos y humanos de la empresa.	
Recomendación	
Se recomienda a corto plazo definir e implementar un plan de contingencia, la aplicación del plan de contingencia permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.	

Fuente: Diego Quillupangui

Tabla 6.50. Hallazgos Componente 14

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-014	
Hallazgos de la Auditoría	
Componente:	Plan de mantenimiento de Hardware y Software
Dominio:	Entregar, dar Servicio y Soporte (DSS)
Proceso:	DSS01: Gestionar las Operaciones
Práctica:	DSS01.3: Supervisar la infraestructura de TI
Evidencia:	La entrevista, la observación directa
Condición	
Los usuarios no están al tanto de los mantenimientos de TI	
Criterio	
(410-12 Administración de soporte de tecnología de Información) Definir, aprobar y difundir procedimientos de operaciones que faciliten una adecuada administración del soporte tecnológico y garantice la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos.	
Causa	
La falta de comunicación de los planes de mantenimiento y los trabajos a realizar por parte del encargado del área de TI.	
Efecto	
Al no realizar un mantenimiento preventivo planificado a los equipos informáticos, se asume el riesgo de daños graves en cuanto al sistema operativo o daños graves en cuanto a las partes o piezas internas del computador que podrían llevar a paralizar las actividades sin previo aviso.	
Conclusión	
Es importante tener un plan de mantenimiento, al mismo tiempo es importante socializar con antelación las acciones a llevar por parte del área de TI	
Recomendación	
Se recomienda a corto plazo definir y difundir los procedimientos de operaciones que faciliten una adecuada administración del soporte tecnológico que garantice la seguridad, integridad y confiabilidad de los recursos y datos de TI.	

Fuente: Diego Quillupangui

Tabla 6.51. Hallazgos Componente 15

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-015	
Hallazgos de la Auditoría	
Componente:	Existe licenciamiento de los aplicativos instalados en el equipo informático
Dominio:	Construir, adquirir e Implementar (BAI)
Proceso:	BAI09: Gestionar los Activos
Práctica:	BAI09.5: Administrar licencias
Evidencia:	La entrevista, la observación directa
Condición	
No existen licenciamiento de software original – legal	
Criterio	
La instalación de software con licenciamiento legal garantiza el funcionamiento correcto del producto adquirido.	
Causa	
Uso de parches de software no legal	
Efecto	
Los programas que no utilizan una licencia legal no aceptan actualizaciones, y esto hace que corran el riesgo de ataques, errores en el sistema, el no contar con soportes del software ocasiona una debilidad en cuanto a la operatividad del programa.	
Conclusión	
Es muy importante mantener el licenciamiento del software para obtener actualizaciones y mantenimiento por parte del desarrollador del producto y tener programas estables para el usuario.	
Recomendación	
Se recomienda a corto o largo plazo adquirir licencias legales para el sistema operativo y las aplicaciones de oficina, para evitar inconvenientes del software en cuanto al uso de licencias ilegales.	

Fuente: Diego Quillupangui

Tabla 6.52. Hallazgos Componente 16

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-016	
Hallazgos de la Auditoría	
Componente:	Existencia de documentos de adquisición de equipos y software, contrato legar del proveedor de internet (ISP)
Dominio:	Alinear, Planificar y Organizar (APO)
Proceso:	APO10: Gestionar los Proveedores
Práctica:	APO10.3: Gestionar contratos y relaciones con proveedores
Evidencia:	La observación directa, la entrevista
Condición	
La empresa tiene contratos verbales con proveedores de equipos	
Criterio	
(410-08 Adquisiciones de infraestructura tecnológica) Las adquisiciones de nuevas tecnologías están alineadas a los objetivos de la organización, principios de calidad de servicio, portafolio de proyectos y servicios, y constarán en el la anual de contrataciones aprobado por la institución. Un contrato escrito garantiza seguridad y confianza de las dos partes.	
Causa	
La falta de compromiso de parte de los proveedores, ha generado una inseguridad al momento de realizar la compra de un nuevo producto.	
Efecto	
La falta de coordinación de tiempos, la inestabilidad formal, en cualquier momento cualquiera de las dos partes puede faltar a su palabra y evidenciar malas prácticas mercantiles.	
Conclusión	
Ante cualquier compromiso es necesario tener un contrato que avale por escrito el compromiso expresado entre las dos partes.	
Recomendación	
Se recomienda a largo plazo crear un portafolio de proveedores que contarán en un plan anual de contrataciones, aplicando cláusulas que beneficien a las dos partes y garanticen una mejor relación mercantil.	

Fuente: Diego Quillupangui

Tabla 6.53. Hallazgos Componente 17

EMPRESA ROSAS DEL CORAZÓN	
AUD-FOR-TIC-017	
Hallazgos de la Auditoría	
Componente:	Documentación de los sistemas utilizados para los servicios de la empresa
Dominio:	Construir, Adquirir e Implementar
Proceso:	BAI04: Gestionar la Disponibilidad y Capacidad
Práctica:	BAI04.4: Supervisar y revisar la Disponibilidad y la Capacidad
Evidencia:	La entrevista, la observación directa, la encuesta
Condición	
No posee documentación de los programas que se usan en la empresa	
Criterio	
(410-07 Desarrollo y adquisición de software aplicativo) Regular los procesos de desarrollo y adquisición de software aplicativos con lineamientos, metodologías y procedimientos. Deben considerarse estándares de desarrollo, de documentación y de calidad.	
Causa	
No ser propietario de los derechos de código de los programas	
Efecto	
Ocasionalmente el sistema informático puede fallar, pero al no tener el código del software, puede generar pérdida de recurso, mientras se espera una actualización o soporte por terceros.	
Conclusión	
Generar un propio software, que permita gestionar de manera eficiente los procesos de la entidad	
Recomendación	
Se recomienda a largo plazo diseñar e implementar un sistema informático propio para que pueda acoplarlo según las necesidades de la Empresa Rosas del Corazón y permita tener un soporte propio en cualquier momento.	

Fuente: Diego Quillupangui

6.18. Conclusiones y recomendaciones de la auditoria

Conclusiones:

- La aplicación de una auditoria informática, permite gestionar de mejor manera los procesos de tecnologías de información en la empresa, ajustándose a las necesidades de negocio, permitiendo a los administradores de la empresa ayudar en la toma de decisiones para mejorar los servicios de TI.
- Cada uno de los puntos analizados en la auditoria son de vital importancia para el buen desempeño de las tecnologías de la información, las gran parte de requerimientos, muchas ocasiones no son analizados por los administradores de la empresa, pero son necesarios para cumplir con los objetivos de la empresa y salvaguardar siempre las información y los sistemas informáticos.
- Los procesos aplicados en la auditoria informática ayudan al administrador de TI en la buena administración y una buena práctica de los procesos, permitiendo solucionar a corto o mediano plazo problemas que han sido causados por las debilidades señaladas en los resultados de la auditoria informática.

Recomendaciones:

- Luego de la revisión pertinente de las instalaciones se debe considerar cuáles son las medidas precautelares a aplicarse, y realizar cambios y actualizaciones según las recomendaciones a corto o largo plazo, ya que así se estaría cumpliendo con los objetivos de TI, que es administrar la información y los recursos de TI de la empresa.
- Realizar una evaluación constante de los procesos de TI, permitirá gestionar la seguridad de TI, esto afianzara y asegura de la información y la relación entre el área de TI con los usuarios de la empresa.
- La parte administrativa debe considerar involucrarse con los cambios tecnológicos y actualizaciones pertinentes, y el área de TI debe ser considerar como una parte esencial en la toma de decisiones de la empresa, ya que esto puede dar un giro radical en el uso de la tecnología para los objetivos de negocio.

7. PRESUPUESTO Y ANÁLISIS DE IMPACTOS

7.1. Presupuesto

Los gastos de este proyecto son la aplicación por prestación de servicios de auditoria informática, como se muestra a continuación:

- El valor hora de una auditoria radica en la prestación de servicios del personal profesional que aplica la auditoria, para lo cual se consideran solamente 5 días laborables de la semana (20 días al mes).

$ 5.00 la hora de auditoria: 4 horas diarias = $ 20.00 c/d

5 días a la semana = $ 20.00 * 5 = $ 100.00 dólares a la semana

- Se considera el viaje cada día a la empresa.

$ 0.50 centavos: pasaje diario (ida y vuelta)

0.50 * 5 = $ 2.50 a la semana

2.50 * 4 = 10.00 al mes

Tabla 7.54. Gastos servicios auditoria

SERVICIOS			
Cantidad	**Detalle**	**Valor Unitario**	**Valor Total**
4	Meses de Transporte	10.00	40.00
16	Semanas Servicios de Auditoria	100	1600.00
		Total	1640.00

Fuente: Diego Quillupangui

Tabla 7.55. Otros gastos

OTROS GASTOS		
Ítem	**Nombre**	**Valor Total**
1	Gastos de viajes fuera de auditoria	150.00
2	Alimentación	400.00
3	Anillado, Proyector, teléfono	25.00
	Total	575.00

Fuente: Diego Quillupangui

Tabla 7.56. Materiales de oficina

Materiales de oficina			
Detalle	**Cantidad**	**V. unitario (USD)**	**Valor Total (USD)**
Resmas de papel bond	3	3.50	10.50
Tinta de impresión	4	7.00	28.00
Esferos	8	0.30	2.40
Carpetas	5	0.30	1.50
CD	2	0.40	0.80
Internet /mes	4	25.00	100.00
Cuadernos	2	1.00	2.00
		Total	145.20

Fuente: Diego Quillupangui

Luego de analizar todo el presupuesto utilizado en la ejecución de este proyecto, se redacta un total de todo el costo de la auditoria, como se muestra en la siguiente tabla:

Tabla 7.57. Gastos Totales

Gastos Totales	
Detalles	**Valor total**
Servicios	1640.00
Otros Gastos	575.00
Materiales de oficina	145.20
Total	2360.20

Fuente: Diego Quillupangui

7.2. Análisis de Impactos

Impacto práctico:

El desarrollo de la auditoria informática impulsa a los administradores de TI a ejercer correctamente el uso de la tecnología en la empresa.

Impacto ambiental:

Permite administrar de mejor manera los efectos que producen los equipos informáticos dados de baja, evitando que contaminen el medio ambiente y la vida animal.

Impacto tecnológico:

Esta práctica disminuye el riesgo de ataques informáticos y aumenta la buena práctica, gestión y control de los recursos de TI en la empresa.

8. CONCLUSIONES Y RECOMENDACIONES

8.1. Conclusiones

- Es de mucha importancia recopilar la información utilizando técnicas de recolección de datos, ya que así se puede identificar de una manera muy clara la veracidad de la información que respalda la ejecución de la auditoria informática.
- El marco de referencia COBIT sirve de guía para la aplicación de metodologías ordenadas que ayudan a ejecutar una auditoria orientada a la seguridad, lo que permite garantizar la gestión y control de las TI.
- La aplicación de la auditoria al área informática de la empresa Rosas del Corazón, permite garantizar la seguridad física de los equipos, de la información y de la infraestructura tecnológica, al mismo tiempo fortalecerá el buen uso y optimización de recursos tecnológicos de la empresa.
- El informe de auditoría informática permite identificar las principales debilidades del área de TI, ya que emite recomendaciones que ayudan a tomar decisiones que fortalezcan la gestión y control del área informática y ayudan a aumentar la seguridad de las TI.

8.2. Recomendaciones

- Tener presente todo tipo de recursos tecnológicos que pueda ayudar a recopilar información, ya que el trabajo de campo depende mucho de los recursos utilizados eficientemente para respaldar la veracidad de la información.
- Conocer ampliamente la nueva metodología que ofrece el marco de referencia COBIT, la cual se ajusta a todo tipo de normas o reglamentos internacionales aplicables durante el proceso de auditoría.
- La aplicación de la metodología COBIT es muy útil, puesto que garantiza el control y gestión de las tecnologías de información de pequeñas y grandes empresas, se desenvuelve a lo largo de toda la empresa y se ajusta con facilidad a los requerimientos de la entidad a auditar.
- Al ejecutar la auditoria es necesario considerar las recomendaciones emitidas en el informe final de la auditoria, es necesario que la administración de la empresa tenga conocimiento de la evaluación y tome muy en cuenta los hallazgos de la auditoria, ya que la aplicación de las recomendaciones garantizan la seguridad, integridad, confiabilidad y disponibilidad de los recursos de TI y la información de la empresa.

9. REFERENCIAS

[1] F. Valencia, J. Tamayo, «JISTEM - Journal of Information Systems and Technology Management,» *Scielo,* vol. 14, nº 3, p. 19, 2017.

[2] Velásquez Pérez, T., Puentes Velásquez, A. M., & Pérez, Y. M., «Un enfoque de buenas prácticas,» *Revista Tecnura,* vol. 1, p. 11, 2015.

[3] I. M. A. Rodríguez, «Intranets: las tecnologías de información y comunicación en función de la organización,» *scielo,* vol. 4, p. 16, 2007.

[4] A. V. Melo, «EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27001,» *Revista de Derecho,* nº 29, p. 36, 2008.

[5] j. Voutssas, «Preservación documental digital y seguridad informática.,» *scielo,* Vols. %1 de %2http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X201000010, pp. 127-155, 2010.

[6] J. Barcelo, J. Inigo, R. Escale, E. Olive, X. Tornil, Redes de Computadoras, Barcelona, 2004.

[7] T. Saydam y T. Magedanz, «Redes, gestión de redes y servicio de administración,» vol. 4, nº 4, 1996.

[8] A. Barba, Gestion de Red, 1999, UPC.

[9] P. Aguilera, Seguridad Informática, 2010, EDITEX.

[10] L. Molero, «Planificación y Gestión de Red,» vol. 1, p. 49, 2010.

[11] R. Castello, Auditoria de Sistemas y Tecnologías de Información, 2008, Córdoba, Argentina.

[12] D. Arcentales, X. Caycedo, «Auditoría informática: un enfoque efectivo,» *Dominios de la Ciencias,* vol. 3, pp. 157-173, 2017.

[13] Piattini & Peso, «Auditoria Informática: un Enfoque practico,» 2003.

[14] G. Rivas, Auditoria Informática, 1988, España.

[15] J. Mckeever, Sistemas de Información para la Gerencia, 1984: Editorial Mc Graw Hill, Mexico.

[16] E. Angeles, Métodos y Técnicas de Investigación para Administración e Ingeniería, 2000, Madrid.

[17] F. Arias, El Proyecto de Investigación, 2010.

[18] L. &. C. González, El proceso de investigación Científica, 2011.

[19] D. Behar, Metodología de la Investigación, 2008.

[20] R. Meadows, «ISACA,» ISACA, 2018. [En línea]. Available: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-tiene-ya-disponible-la-version-en-espanol-de-COBIT-5.aspx. [Último acceso: 2018].

[21] E. Estébanes & J. Cano , «Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0,» *Ecorfan Journal,* vol. vol. 2, nº 5, pp. 109-131, 2011.

[22] I. Framework, «Un Marco de Negocio para el Gobierno y la Gestio de las TI de la Empresa,» 2012. [En línea]. Available: www.isaca.org/COBITuse..

[23] C. Escalada, «GUÍA DE AUDITORÍA PARA LA EVALUCION DEL CONTROL INTERNO DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE COBIT 5: CASO UCACUE,» *UPSE,* vol. Vol. III, nº 3, pp. 113-121, 2016.

[24] C. Martha, Inteligencia Artificial, 20015: CARAS, Toronto.

[25] L. Collantes, PROTECCION 3D, 2016: SDFR, California.

[26] R. Wolcott, Inteligencia Artificial, 2014: RERS, Florida.

[27] G. F. B. MARCILLO, Artist, *AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO "ALIANZA DEL VALLE" LTDA. APLICANDO COBIT 4.0.* [Art]. ESPE - Sangolqui.

[28] L. Barber, Inteligencia Artificial, 2013: CEP, New York.

[29] M. Mathy, Hologramas y Software, 2013: Española, Barcelona.

[30] J. McCarthy, Maquinas Inteligentes, 2014: MADDS, Madrid.

[31] M. Crift, Software y Hardware, 2013: CEXS, Londres.

[32] E. Norvig, Sistemas Inteligentes, 2013: BOOKNEWS, California.

[33] A. Perez, Robotica, 2014: FRESC, Buenos Aires.

[34] R. Puyol, Inteligencia Artificial, 2015: Española, Madrid.

[35] Q. Florest, Inteligencia Artificial, 2015: RESFE, Canada.

[36] C. Rents, Software inteligente, 2014: NEWS, New York.

[37] I. Silva, Inteligencia Artificial, 2013: RESTREPOS, California.

[38] D. Suarez, Sistemas de Desarrollo Inteligente, 2014: SEIJI, Madrid.

[39] M. Suarez, Software y la Inteligencia, 2014: ESTESCO, Barcelona.

[40] T. Floid, Inteligencia Artificial, 2015: LISE, Londres.

[41] L. Torra, Software y Hologramas, 2014: GRESDS, Santiango.

[42] T. Hernest, Software Inteligente, 2014: HWAR, California.

[43] C. Valecia, Robotica, 2014: COLMS, Medellin.

[44] Custons, Inteligencia Artificial, 2014: CEERP, Londres.

[45] R. Croffst, Memoria Inteligente, 2013, Toronto.

[46] C. Frort, Hologramas, 2014, California.

[47] Gutierrez, Holografia, 2011, Cali.

[48] M. Frind, Holograma, 2016: PERSE, Barcelona.

[49] R. Serra, Inteligencia Artificial, 2011: CHARRO, Mexico D.F..

[50] D. Arcentales, X. Caycedo, «Auditoría informática: un enfoque efectivo,» *Dominio de las Ciencias*, vol. 3, pp. 157-173, 2017.

ANEXOS

ANEXO 1

ENTREVISTA

Entrevista aplicada al gerente de la empresa Rosas del Corazón para recolectar información importante durante el proceso de auditoria

1. ¿Se ha realizado algún tipo de auditoria en la empresa en el área informática?
2. ¿El área Informática cuenta con una planificación estratégica?
3. ¿Existen políticas informáticas internas que conozca y se estén aplicando?
4. ¿Estas políticas son importantes?
5. ¿Quiénes están autorizados a acceder a los archivos y programas de la empresa?
6. ¿Todos los usuarios tienen usuario y contraseña para acceder a sus equipos de trabajo?
7. ¿Qué medidas de seguridad existen en la empresa?
8. ¿Es importante implementar un plan de contingencia?
9. ¿El personal está preparado para un ataque informático?
10. ¿El lugar de los servidores cuenta con todas las seguridades físicas?
11. ¿Hay alguna planificación en cuanto a la inversión anual para el área de TI?
12. ¿Cuán importante son las TI para Rosas del Corazón?
13. ¿Actualmente cómo se controlan las tecnologías de la información en la empresa?
14. ¿Existe un plan para restablecer operaciones en caso de un fallo en la TI?
15. ¿La empresa usa software libre?
16. ¿Se dispone a las contraseñas administrables para los servidores de la empresa?
17. ¿Quiénes tiene acceso a la red WIFI y bajo que parámetros?
18. ¿Alguna vez han tratado de hackear su red o el equipo informático y cuál fue su primera acción?
19. ¿Existen un plan de acción en caso de un fallo en la red?
20. ¿Quién toma decisiones en cuanto a los cambios de red?
21. ¿Cada que tiempo se realiza las actualizaciones de seguridades del sistema operativo?
22. ¿Poseen los usuarios restricciones de uso de su computador? En cuanto a uso a programas.
23. ¿Tienen una bodega para los equipos informáticos nuevos o descompuestos, partes y piezas?
24. ¿Existe un plan para tratar los equipos dañados?
25. ¿Existen acuerdos con proveedores de equipos informáticos?

26. ¿Cuál es el proveedor de internet?
27. ¿Los usuarios tiene acceso a internet libremente?
28. ¿Tienen un presupuesto asignado a mantenimiento?
29. ¿La empresa está preparado para un ataque cibernético?
30. ¿Desde su punto de vista es importante desarrollar políticas de seguridad informática y socializarlas con el personal?

Anexo 2

CUESTIONARIO

CONTROL INTERNO

El presente cuestionario está dirigido al personal que desempeña sus labores diarias en un equipo informático en los distintos departamentos de la empresa

1. ¿La empresa cuenta con un Departamento Informático?

Si ☐ No ☐

2. ¿Se efectúan respaldos planificados de la información de la empresa?

Si ☐ No ☐

3. ¿Se ejerce control del sistema informático?

Si ☐ No ☐

4. Utiliza usuario y contraseña para acceder a su equipo

Si ☐ No ☐

5. ¿El sistema cuenta con claves de seguridad?

Si ☐ No ☐

6. El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes.

Si ☐ No ☐

7. Existe un instructivo en el uso del software informático.

Si ☐ No ☐

8. Existen políticas para la seguridad del sistema informático.

Si ☐ No ☐

9. ¿Los equipos servidores están en un área segura?

Si ☐ No ☐

10. Cree que el computador tiene las seguridades necesarias

Si ☐ No ☐

Anexo 3

Tabla III.1. Formato hallazgos de la auditoria

EMPRESA ROSAS DEL CORAZÓN AUD-FOR-TIC-001	
Hallazgos de la Auditoría	
Dominio:	
Proceso:	
Práctica:	
Evidencia:	
Condición	
Criterio	
Causa	
Efecto	
Conclusión	
Recomendación	

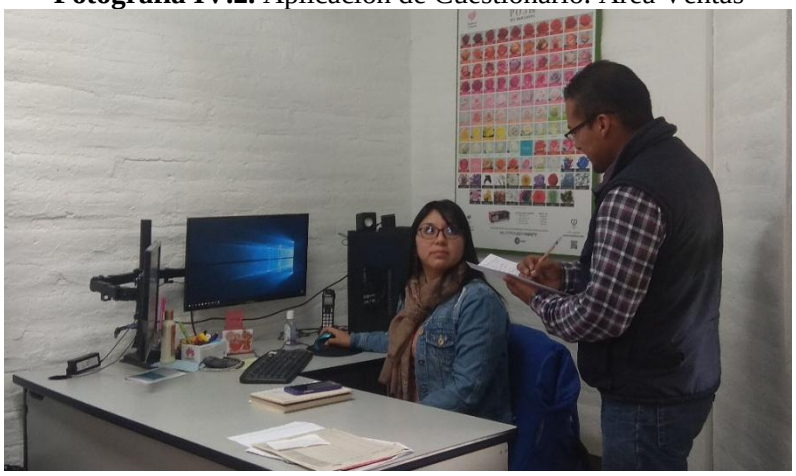
Fuente: [23]

Anexo 4

Fotografía IV.1. Entrevista con el administrador de la Empresa

Fuente: Diego Quillupangui

Fotografía IV.2. Aplicación de Cuestionario. Área Ventas

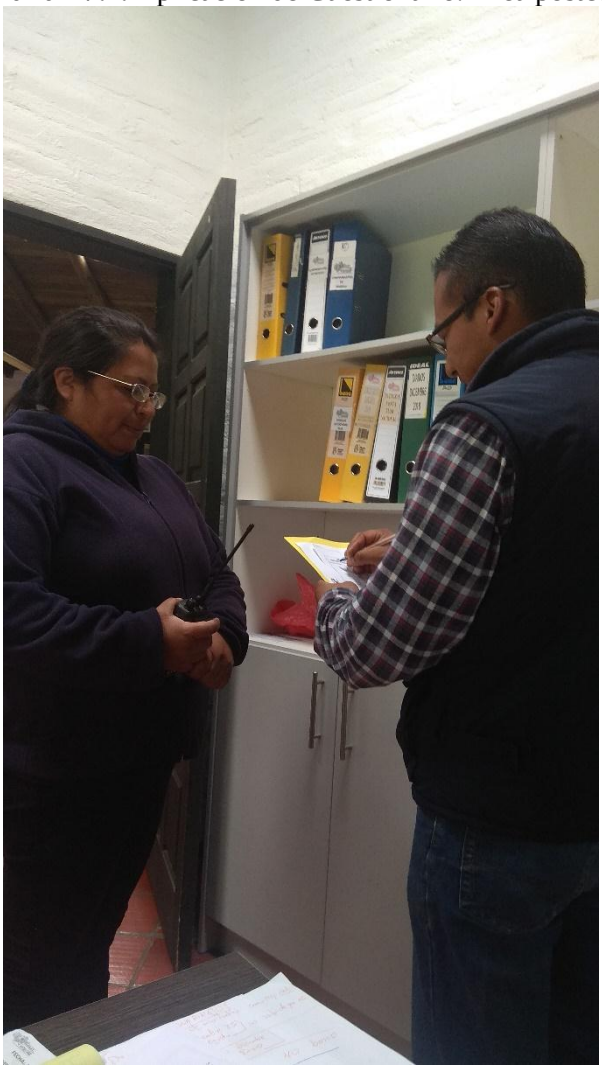


Fuente: Diego Quillupangui

Fotografía IV.3. Aplicación del Cuestionario. Área Contabilidad

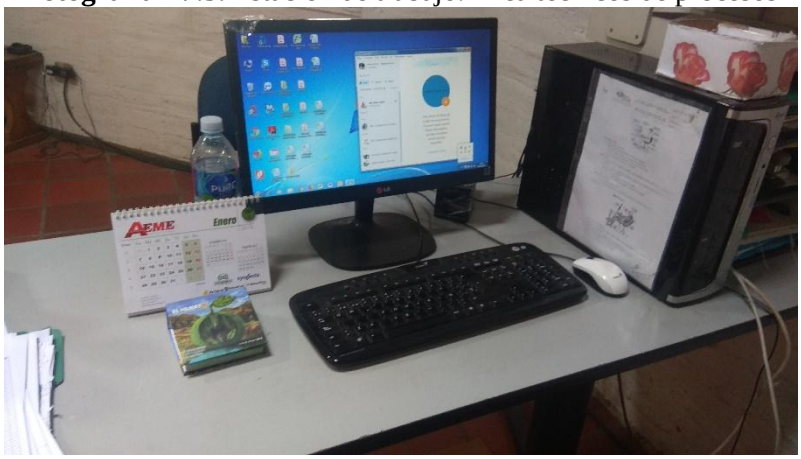
Fuente: Diego Quillupangui

Fotografía IV.4. Aplicación de Cuestionario. Área postcosecha



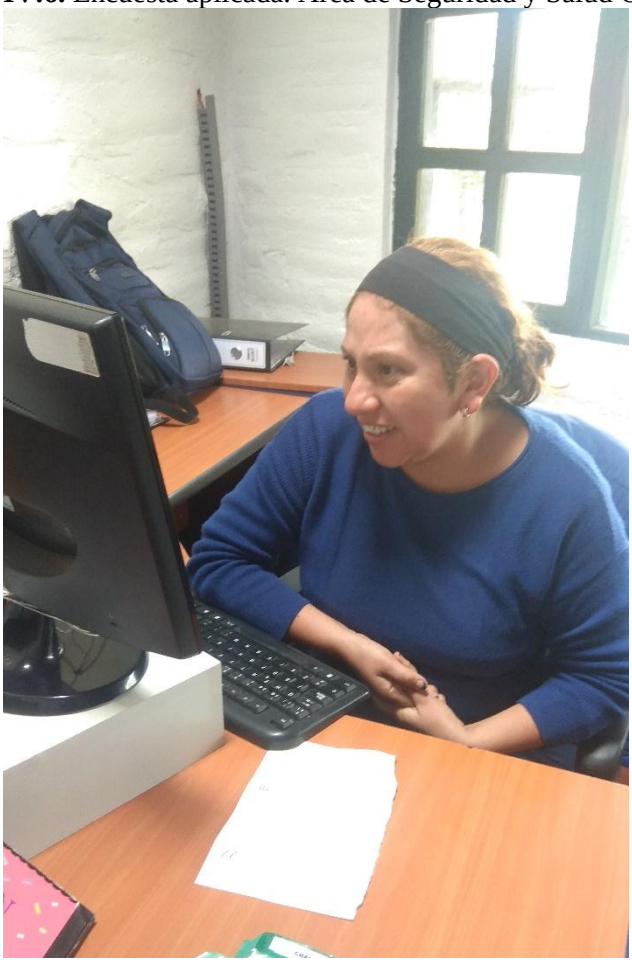
Fuente: Diego Quillupangui

Fotografía IV.5. Estación de trabajo. Área técnicos de procesos



Fuente: Diego Quillupangui

Fotografía IV.6. Encuesta aplicada. Área de Seguridad y Salud Ocupacional



Fuente: Diego Quillupangui

Fotografía IV.7. Área de empaque - Cuarto frio

Fuente: Diego Quillupangui

Anexo 5

EMPRESA ROSAS DEL CORAZÓN

AUDITORIA INFORMÁTICA DE LA EMPRESA

METODOLOGIA DE TRABAJO

COBIT 5.0

REALIZADO POR:

DIEGO QUILLUPANGUI

PERIODO

OCTUBRE 2018 – ENERO 2019

Introducción

La presente auditoria fue realizada en la empresa privada Rosas del Corazón, una empresa que nació en el año de 1993, con la finalidad de satisfacer a los clientes más exigentes como son: Rusia, Ucrania, Europa, Asia y EEUU.

La empresa Rosas del Corazón trabaja acorde a la naturaleza, ya que tiene el privilegio de tener mayor número de horas en el día, además de la altitud ideal para el cultivo de rosas. La calidad es un tema importante para la empresa así constantemente innova los controles de calidad y servicio al cliente.

Para la aplicación de la auditoria se toma como base los lineamientos del Marco de referencia de COBIT 5.0, para el efecto se cumplieron visitas a las instalaciones, se aplicaron encuestas y entrevistas al personal.

En los años cuarenta se empezaban a dar resultados relevantes en el campo de la computación, con sistemas de apoyos para estrategias militares, mientras seguía transcurriendo el tiempo, durante este tiempo la seguridad y el control se limitaba a dar custodia física a los equipos, y el uso de estos equipos era solamente realizado por personal altamente calificado.

Con el paso del tiempo, en la actualidad observamos un cambio general, que ha hecho que la tecnología forme parte esencial del trabajo en toda la entidad, empresa pública o privada, y la protección no sea solamente física.

Objetivo

- Realizar una Auditoria a la Seguridad Informática de la empresa Rosas del Corazón, mediante la revisión del ambiente de control, utilizando COBIT 5.0, con el fin de identificar debilidades y emitir recomendaciones que permitan minimizar los riesgos.

Alcance

Se evaluará la gestión administrativa de las Tecnologías de Información (TI) de la empresa Rosas del Corazón como la seguridad física, seguridad lógica, respaldos y plan de contingencia, Documentación de Software y Hardware.

Metodología del trabajo de auditoria

Para la presente auditoria se aplicó la metodología COBIT 5.0, la cual es un marco de negocio para el gobierno y la gestión de las TI de la Empresa.

COBIT ofrece métodos y métricas pero no impone procedimientos detallados, no es radical sino tolerante e incluso recomienda otras normas o marcos.

¿Cómo se aplica?

COBIT habilita el desarrollo de políticas claras y buenas prácticas para el control de TI a lo largo de las organizaciones.

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad

Descripción general del proceso

Estructura de la auditoria basada en COBIT

1) Situación actual de la empresa
2) Selección de recursos de TI
3) Análisis de Riesgos
4) Plan de Auditoria
5) Puesta en marcha de la auditoria
6) Resultado de la aplicación de la auditoria
7) Informe final de auditoria

INFORME LA AUDITORIA

SEGURIDAD LÓGICA

Tabla 58 Acceso usuarios

Nombre del Componente: Acceso de los usuarios a sistemas, sistemas operativos y BDD	
Hallazgo	No existe una evidencia que indique los roles y responsabilidades que cumple cada usuario. Cada usuario mantiene su información en un orden relacionado con su trabajo.
Recomendación	Se recomienda tener un documento donde se especifique los roles que cumple cada usuario en cuanto al uso de computador.

Conclusión del proceso:

Es muy importante tener un orden, ya que así el usuario podría realizar su trabajo más efectivo optimizando los recursos que tiene a su cargo.

Tabla 59 Disposición de sistemas alternos en caso de fallos

Nombre del Componente: Disposición de sistemas alternos en caso de fallos	
Hallazgo	La empresa no cuenta con un servidor que sustituya al servidor primario en caso de fallos o en caso de mantenimiento preventivo.
Recomendación	Se recomienda disponer de un servidor alterno para ser utilizado en caso de fallos en los sistemas informáticos aparte de tener respaldos de la información actualizada.

Conclusión del proceso:

Aplicar metodologías de seguridad en cuanto a los equipos informáticos, beneficia en gran manera a toda el área informática, ya que ante un fallo en los equipos, se podría restablecer los servicios más rápidamente.

Tabla 60 Existencia de software de protección (antivirus, firewall)

Nombre del Componente: Existencia de software de protección (antivirus, firewall)	
Hallazgo	Se pudo apreciar que existe un antivirus licenciado y actualizando, también se encontró que los parches de actualización del sistema operativo no están activados
Recomendación	Tener un control más estricto en cuanto a las actualizaciones del sistema operativo y programas, para prevenir riesgos de ataques maliciosos

Conclusión del proceso:

Tener un sistema operativo actualizado beneficia en gran manera, ya que es el modo de evitar problemas de vulnerabilidad y de funcionamiento del sistema operativo, tener un buen funcionamiento de las aplicaciones y los programas del equipo informático.

Tabla 61 Control de acceso de los usuarios a los servicios de internet Wifi

Nombre del Componente: Control de acceso de los usuarios a los servicios de internet Wifi	
Hallazgo	No existe un control de acceso de usuarios que permita regular quienes pueden utilizar el servicio de internet WIFI, y bajo que parámetros
Recomendación	Crear políticas de uso de los principales servicios que tiene el área de TI, que permita gestionar le manera más ágil, las conexiones de cada dispositivo inalámbrico.

Conclusión del proceso:

Tener políticas de acceso en cuanto a los servicios que pueden acceder los usuarios es muy útil, ya que permite tener un control más detallado de los usuarios/dispositivos que pueden acceder a la red WIFI.

SEGURIDAD FÍSICA

Tabla 62 Control de acceso de los usuarios a los equipos

Nombre del Componente: Control de acceso de los usuarios a los equipos	
Hallazgo	No se halló un registro de control de acceso y registro de acciones realizadas en los equipos servidores.
Recomendación	Se recomienda tener un registro de acceso de las personas a los equipos de los principales departamentos (servidores - pcs), lo cual permite llevar un control, de las acciones realizadas (mantenimiento preventivo/correctivo).

Conclusión del proceso:

Tener un registro de ingreso de personal es de mucho valor, ya que permite tener mayor control de seguridad en cuanto a los equipos servidores y mayor seguridad y confidencialidad de la información de la empresa.

Tabla 63 Inventario de equipos y software

Nombre del Componente: Inventario de equipos y software	
Hallazgo	No se cuenta con un control de software instalado en cada equipo
Recomendación	Se recomienda tener un manual de los programas a instalar en cada computador, según los requerimientos de cada área

Conclusión del proceso:

Tener un control del software instalado, ayuda a optimizar el uso de cada computador, y agilizar el trabajo del mismo.

Tabla 64 Revisión de la red (factor ambiental, físico, humano)

Nombre del Componente: Revisión de la red (factor ambiental, físico, humano)	
Hallazgo	La red se encuentra en buen estado, pero no se encontró un plan de mantenimiento de la red en cuando a los equipos activos de red (Switch, Router)
Recomendación	Crear un plan de mantenimiento de la red física

Conclusión del proceso:

Una planificación es importante en el área de TI, ya que ayuda al personal a realizar las gestiones de mantenimiento necesarias, gestión y uso de políticas de seguridad, prevención de riesgos en cuanto a fallos y adquisición y uso de nuevas tecnologías.

RESPALDOS Y PLANES DE CONTINGENCIA

Tabla 65 Respaldo de información Critica

Nombre del Componente: Respaldo de información Critica	
Hallazgo	No se halló un documento que especifique el plan de respaldo de la información.
Recomendación	Se recomienda tener un documento que permita el registro de los respaldos por escrito, un control más estricto de los respaldos

Conclusión del proceso:

Registrar las operaciones realizadas por el personal de TI, ayuda a evaluar el control de operaciones del personas de TI.

Tabla 66 Plan de continuidad

Nombre del Componente: Plan de continuidad	
Hallazgo	No existe una plan de continuidad en caso de una falla o ataque informático
Recomendación	Se recomienda tener un plan de continuidad para que el personal de TI ejecute acciones necesarias para restablecer el sistema

Conclusión del proceso:

Un plan de continuidad ayuda a que el personal de TI tenga una mejor gestión y control de los procedimientos a tomar en caso de un ataque o un fallo en el sistema.

Tabla 67 Plan de contingencia

Nombre del Componente: Plan de contingencia	
Hallazgo	No se halló un plan de contenga para el área de TI
Recomendación	Se recomienda diseñar e implementar un plan de contingencia en caso de un fallo grave en el área de TI.

Conclusión del proceso:

Tener un plan de acción en cuanto a fallos, ayuda a gestionar de manera más rápida y eficiente al personal de TI, ayudando a tomar decisiones rápidas para soluciones fallos en TI.

Tabla 68 Plan de mantenimiento de hardware y software

Nombre del Componente: Plan de mantenimiento de hardware y software	
Hallazgo	No existe un plan de mantenimiento
Recomendación	Crear un plan de mantenimiento de TI, y socializarlo con cada área para que el equipo de mantenimiento de TI cumpla su propósito

Conclusión del proceso:

Socializar el plan de mantenimiento ayuda a que los usuarios estén preparados, ayude en su planificación laboral y ayuda a cumplir los objetivos de TI de la empresa.

Conclusión de la auditoria

- La aplicación de una auditoria informática, permite gestionar de mejor manera los procesos de tecnologías de información en la empresa, ajustándose a las necesidades de negocio, permitiendo a los administradores de la empresa ayudar en la toma de decisiones para mejorar los servicios de TI.
- Cada uno de los puntos analizados en la auditoria son de vital importancia para el buen desempeño de las tecnologías de la información, las gran parte de requerimientos, muchas ocasiones no son analizados por los administradores de la empresa, pero son necesarios para cumplir con los objetivos de la empresa y salvaguardar siempre las información y los sistemas informáticos.
- Los procesos aplicados en la auditoria informática ayudan al administrador de TI en la buena administración y una buena práctica de los procesos, permitiendo solucionar a corto o mediano plazo problemas que han sido causados por las debilidades señaladas en los resultados de la auditoria informática.

Recomendaciones:

- Luego de la revisión pertinente de las instalaciones se debe considerar cuáles son las medidas precautelares a aplicarse, y realizar cambios y actualizaciones según las recomendaciones a corto o largo plazo, ya que así se estaría cumpliendo con los objetivos de TI, que es administrar la información y los recursos de TI de la empresa.
- Realizar una evaluación constante de los procesos de TI, permitirá gestionar la seguridad de TI, esto afianzara y asegura de la información y la relación entre el área de TI con los usuarios de la empresa.
- La parte administrativa debe considerar involucrarse con los cambios tecnológicos y actualizaciones pertinentes, y el área de TI debe ser considerar como una parte esencial en la toma de decisiones de la empresa, ya que esto puede dar un giro radical en el uso de la tecnología para los objetivos de negocio.