Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua – FAREM Matagalpa

Monografía para optar al título de Ingeniero en Sistemas de Información.

Tema:

"Evaluación de la Infraestructura de la Red LAN, Empresa "CECOCAFEN", basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, Primer Semestre 2016".

Autoras:

Br. Sherly Antonia Blandón

Br. Sbetlana Galdámez Rocha

Tutor:

Lic. Erick Noel Lanzas Martínez

Asesores:

Lic. Pedro Gutiérrez

Lic. Anabell Pravia

Matagalpa, Junio 2016

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua – FAREM Matagalpa

Monografía para optar al título de Ingeniero en Sistemas de Información.

Tema:

"Evaluación de la Infraestructura de la Red LAN, Empresa "CECOCAFEN", basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, Primer Semestre 2016".

Autoras:

Br. Sherly Antonia Blandón

Br. Sbetlana Galdámez Rocha

Tutor:

Lic. Erick Noel Lanzas Martínez

Asesores:

Lic. Pedro Gutiérrez

Lic. Anabell Pravia

Matagalpa, Junio 2016

DEDICATORIA

A Dios:

Por ayudarme en el trayecto de la carrera, que a pesar de los obstáculos que se presentaron he logrado culminar mi carrera universitaria.

A mi familia:

Por apoyarme incondicionalmente para poder llegar a estas instancia de mis estudios, dándome lo mejor sin que nada me faltara, por bríndame su amor, consejos, motivación y deseo de superación. Gracias, porque su presencia ha ayudado a construirme y forjarme como la persona que ahora soy.

A los docentes:

Por transmitirme sus diversos conocimientos, paciencia y dedicación, en el trayecto de educación universitaria y que en la vida necesitamos más que saberes y experiencias.

SHERLY ANTONIA BLANDÓN

DEDICATORIA

A Dios, por ser mi fuente de fortaleza, mi mano derecha, y sustento, me ha dado la capacidad para que mis metas se cumplieran. Gracias porque en ti todo es posible.

A mi familia por su apoyo incondicional, por su esfuerzo y sacrificio que han hecho por mí. Me han dado lo que soy como persona, mis valores, principios y perseverancia para lograr mis objetivos.

A los docentes que han conformado parte de mi formación en todos estos años, me brindaron sus conocimientos y apoyo para seguir adelante.

SBETLANA DE LOS ÁNGELES GALDÁMEZ ROCHA

AGRADECIMIENTO

Primeramente a nuestro tutor Lic. Erick Lanzas, por la orientación, el seguimiento y la supervisión continúa para culminar esta investigación.

A todos aquellos docentes que estuvieron dispuestos a brindarnos su apoyo incondicionalmente y aquellos que sin esperar nada a cambio nos brindaron sus conocimientos en la elaboración de este trabajo.

En especial al profesor Pedro Gutiérrez que nos ayudó en la parte metodológica, la profesora Anabell Pravia por su asesoría en COBIT, profesora Guisselle Martínez y Cleidys Flores que nos aclararon dudas en el trayecto de la investigación.

Igualmente a la empresa CECOCAFEN que nos dieron la oportunidad de realizar dicha investigación y brindarnos toda la información necesaria.

CARTA AVAL DEL TUTOR

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

FACULTAD REGIONAL MULTIDISCIPLINARIA, MATAGALPA

UNAN – MANAGUA, FAREM – MATAGALPA

El suscrito tutor de Monografía para optar al título de Ingeniería en Sistemas de Información, de la Facultad Regional Multidisciplinaria de Matagalpa, de la Universidad Nacional Autónoma de Nicaragua, UNAN – Managua, por este medio extiende:

CARTA AVAL

A los bachilleres ***Sherly Antonia Blandón*** *(Carné 10066980)* y ***Sbetlana de los Ángeles Galdámez Rocha*** *(Carné 11062040)*, dado que el informe final titulado: "*Evaluación de la infraestructura de Red LAN en CECOCAFEN basado en el modelo de objetivo de control COBIT 4.1, Matagalpa I Semestre 2016*", cumple los requisitos establecidos para su defensa ante el tribunal examinador.

Dado en la ciudad de Matagalpa, a los veintiocho días del mes de abril del año dos mil dieciséis.

Lic. Erick Noel Lanzas Martínez

Tutor de Monografía

RESUMEN

La presente investigación tiene como objetivo la evaluación de la infraestructura de la red LAN, “Empresa CECOCAFEN”, Matagalpa, Periodo 2016.

El trabajo se estructuró basado en los objetivos específicos, de los cuales descienden las variables de estudio que han sido desarrolladas en el marco teórico y que apoyan la veracidad y cientificidad de la investigación. De igual manera se elaboró un diseño metodológico que guío la metodología de investigación aplicada, esta comprende el enfoque de investigación, población, muestra, las técnicas e instrumentos para la recolección de la investigación.

Para la recolección de información se elaboraron instrumentos, basados en el marco teórico, estos consistieron en una guía de entrevista al encargado de informática, encuesta a los usuarios que hacen uso de la red, guía de observación a elementos de interés.

Los resultados de la investigación demuestran que no existe una administración que garantice la seguridad física y lógica de los recursos de TI, el cual no tiene políticas de seguridad, plan preventivo y correctivos para acciones inesperadas, no existe un control de los dispositivos, no existe estándar para el cableado eléctrico y cableado estructurado, además no existe una documentación de la red tanto física como lógica. Para dar soluciones a esta problemática se propone una guía para mejorar la infraestructura de la red.

ÍNDICE

ÍNDICE DE ANEXOS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

Hoy en día la globalización y la necesidad de mejorar los procesos, han llevado a distintas organizaciones a automatizar sus principales actividades. Para ello una de las formas más comunes, es la implementación de redes informáticas, las cuales permiten el intercambio de datos, información o recursos, lo que viene optimizando los flujos de trabajo y comunicación.

Esto ha conllevado a que se implementen redes internas también llamadas LAN, las cuales requieren de parámetros de calidad que aseguren un buen funcionamiento y garanticen confiabilidad en las operaciones realizadas.

La empresa CECOCAFEN como una entidad industrializadora cuenta con distintas áreas que soportan los diversos procesos que se llevan a cabo para la toma de decisiones. Se tiene implementada una red LAN con el objetivo de crear canales más flexibles y óptimos de trabajo que apoyen dichos aspectos operativos.

Algunas de las dificultades destacables es la ausencia en la calidad de los servicios, red mal estructurada, entre otras, las cuales podría tener consecuencias negativas a corto plazo en las labores de la empresa.

Debido a esto el objetivo de estudio de esta investigación se centró en realizar una evaluación de la infraestructura de la red LAN en la “Empresa CECOCAFEN”, basado en el modelo de objetivo de control COBIT 4.1, en el primer semestre 2016, para conocer fortalezas y debilidades, y proponer posibles soluciones a los problemas existente, con el fin de ayudar a mejorar aspectos organizativos y tecnológicos dentro de la empresa.

Esta investigación se estructuro de los objetivos específicos planteados, los cuales dan origen a las variables de estudio que guían el marco teórico que fortalece la veracidad de la investigación. Además se definió un diseño metodológico que soporta la metodología de la investigación aplicada, el tipo y enfoque de investigación, universo de estudio, las técnicas de recopilación de datos, instrumentos y las variables que serán evaluadas.

II. ANTECEDENTES

Los presentes antecedentes son investigaciones realizadas a nivel internacional y local, que están relacionados con la temática de estudio en la presente investigación, la cual trata la evaluación de la infraestructura de una red LAN. A continuación se resumen los resultados de dichas investigaciones:

En Quito Ecuador:

Matutes & Quispe (2006), realizaron una auditoría de la gestión de la seguridad de red de datos del Swissotel, basada en COBIT, para analizar y diagnosticar la actual gestión de seguridad de la red, donde se concluyó que no existía una conciencia formal por parte de la gerencia de TI para asegurar la correcta gestión de la seguridad, proponiendo procesos que ayuden a identificar controles que garanticen la seguridad de la información.

Callay & Sánchez (2012), llevaron a cabo una auditoría informática a los servicios de red de Transelectric, con la finalidad de ayudar a mejorar aspectos organizativos y tecnológicos dentro de la empresa, donde se encontró que hubo un desempeño aceptable en los equipos, se recomendó tomar como referencia el trabajo realizado para evaluaciones próximas basado en los resultados obtenidos.

Cuesta & Cumanda (2010), se llevó a cabo una auditoría física y lógica a las redes de comunicaciones de computadores de la fábrica Pasamanería S.A, con el propósito de analizar el estado de la infraestructura de red, donde se identificó que en algunas de las áreas de la empresa se tuvieron deficiencias en cuanto al funcionamiento y estado de la red, se recomendó la herramienta ULTRAVNC la cual es de ayuda para el administrador de la red al momento de dar soporte a usuarios con problemas.

En la Universidad Católica “Santo Toribio de Magrovejo”, Perú, Santa María (2012), elaboró una tesis donde propone buenas prácticas para auditar redes inalámbricas, en base a metodologías COBIT 4.1, NTP-ISO-IEC 27001/27002, para el dominio de diseño, administración y seguridad a la vez brinda actividades o herramientas de apoyo para la eficiencia de red.

En la ciudad de México, Álvarez (2005), elaboró auditoría de seguridad en redes, aplicando definiciones en planeación, políticas, uso y responsabilidades en los centros de cómputo, y estándares internacionales, para evaluar el grado de efectividad de la estructura de red bajo el estándar de COBIT, donde concluyeron que le dan soporte a los recursos administrados en cuanto a la infraestructura de red.

En Matagalpa, Mendoza (2012), realizó tesis con el fin de evaluar la red de computadores de UNAN Managua, FAREM Matagalpa, donde describió la condición actual de la red, encontrando fortalezas y debilidades en la seguridad lógica y física de la infraestructura, de lo cual elaboró una propuesta técnica para reforzar y disminuir sus debilidades, así como aumentar la seguridad y protección.

III. JUSTIFICACIÓN

La investigación consiste en realizar una evaluación de la infraestructura de la Red LAN, en la empresa CECOCAFEN, lo cual servirá de ayuda para el análisis y orientación de recomendaciones para un mejor rendimiento de la red.

Las razones que conlleva la investigación es que actualmente la empresa no cuenta con una estructura de red adecuada, además la configuración de la misma no se encuentra de manera correcta, ya que no existe una documentación que sirva de guía para mejorarla.

La importancia de esta investigación se centra en la obtención de información sobre el desempeño de la red y su respectiva configuración, para determinar el grado de madurez y seguridad de la misma, así se podrá analizar la información recabada para implementar las mejoras pertinentes que optimicen los procesos que se ejecuten por medio de la red.

La evaluación de la red tendrá impacto en la empresa, ya que actualmente cuenta con deficiencia en el funcionamiento de la infraestructura de la red, además permitirá llevar un mejor control de la distribución de los equipos y la configuración de la misma para evitar posibles amenazas y vulnerabilidades.

En base a los resultados del trabajo se aportará una guía de apoyo, la cual beneficiará directamente a los involucrados que se encargan de la informática para el mejoramiento de la red e indirectamente a las áreas y a los procesos que se llevan a cabo en dicho lugar para que estos se puedan agilizar y generar confiabilidad.

IV. PLANTEAMIENTO DEL PROBLEMA

CECOCAFEN, cuenta con una Red LAN para apoyar a las distintas áreas en los procesos a los que se dedican, los cuales son: Base de datos contable, correo electrónico y toda la información de la empresa.

De forma exploratoria se puede notar que a la red no se le da un mantenimiento y administración óptima, lo cual a corto plazo podría tener consecuencias negativas sobre los procesos que se llevan a cabo, esto porque no hay un área de informática definida que asegure los soportes necesarios.

Por lo anterior descrito se plantea la siguiente problemática: ¿Cómo es la infraestructura de Red LAN, empresa CECOCAFEN, basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, primer semestre 2016?

V. OBJETIVOS

General:

Evaluar la infraestructura de la Red LAN, “Empresa CECOCAFEN”, basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, Primer Semestre 2016.

Específicos:

- Describir el funcionamiento de la infraestructura de la Red LAN.
- Identificar Problemáticas en la infraestructura de la red LAN, tomando en cuenta el modelo de objetivo de control COBIT 4.1.
- Valorar el grado de afectación de las problemáticas encontradas a la infraestructura de la red LAN, tomando en cuenta el modelo de objetivo de control COBIT 4.1.
- Proponer guía que corrija las problemáticas detectadas en la infraestructura de la Red LAN.

VI. MARCO TEÓRICO

6.1 El modelo objetivo de control COBIT 4.1

Según Isaca (2007), COBIT, es un marco de referencia y un juego de herramientas de soporte, permitiendo a la gerencia cerrar brecha con respecto a los requerimientos de control, temas técnicos, riesgos de negocio, y comunicar ese nivel de control a los Interesados.

El modelo de objetivo de control COBIT 4.1 cuenta con 4 dominios y 34 procesos como son:

- Planear y Organizar

PO1 Definir un Plan Estratégico de TI.
PO2 Definir la Arquitectura de la Información.
PO3 Determinar la Dirección Tecnológica.
PO4 Definir los Procesos, Organización y Relaciones de TI.
PO5 Administrar la Inversión en TI.
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia.
PO7 Administrar Recursos Humanos de TI.
PO8 Administrar la Calidad.
PO9 Evaluar y Administrar los Riesgos de TI.
PO10 Administrar Proyectos.

- Adquirir e Implementar.

AI1 Identificar soluciones automatizadas.
AI2 Adquirir y mantener software aplicativo.
AI3 Adquirir y mantener infraestructura tecnológica.
AI4 Facilitar la operación y el uso.
AI5 Adquirir recursos de TI.
AI6 Administrar cambios.
AI7 Instalar y acreditar soluciones y cambios.

- Entregar y Dar Soporte

DS1 Definir y administrar los niveles de servicio.

DS2 Administrar los servicios de terceros.

DS3 Administrar el desempeño y la capacidad.

DS4 Garantizar la continuidad del servicio.

DS5 Garantizar la seguridad de los sistemas.

DS6 Identificar y asignar costos.

DS7 Educar y entrenar a los usuarios.

DS8 Administrar la mesa de servicio y los incidentes.

DS9 Administrar la configuración.

DS10 Administrar los problemas.

DS11 Administrar los datos.

DS12 Administrar el ambiente físico.

DS13 Administrar las operaciones.

- Monitorear y Evaluar

ME1 Monitorear y Evaluar el Desempeño de TI.

ME2 Monitorear y Evaluar el Control Interno.

ME3 Garantizar el Cumplimiento Regulatorio.

ME4 Proporcionar Gobierno de TI.

De los cuales, éstos poseen una serie de objetivos de control, al analizar el documento se han seleccionado 2 dominios que van acorde al tema como son: adquirir e implementar **(AI)** y entrega y dar soporte **(DS)**. El primer dominio **AI** porque incluye aspectos de cambios y mantenimientos a los distintos recursos que componen la infraestructura de la red y **(DS),** porque se basa en **l**a prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

6.1.1 PO4 Definir los Procesos, Organizaciones y Relación de TI

Cubre las estrategias y tácticas, donde se debe implementar una estructura organizacional y una estructura tecnológica apropiada, que ayude a la empresa a tomar decisiones apropiadas en cuanto a los recursos de TI.

6.1.1.1 PO4.5 Estructura Organizacional

Según Isaca (2007), la estructura organizacional es establecer una estructura interna y externa que refleja las necesidades del negocio y el nivel de dependencia para satisfacer los objetivos de negocio esperado y las circunstancia cambiantes.

(Torres, 2008, p. 32), quien cita a (Daft, 2007, p. 17), explica que una “estructura organizacional es donde se proporcionan las etiquetas para describir las características internas de una organización. Crean una base para medir y comparar organizaciones”.

Los conceptos anteriores aseguran que una estructura organizacional es una jerarquía donde se define funciones, roles y responsabilidades dentro de la empresa, lo cual permite lograr las metas establecidas. Además existen muchos tipos de estructura que operan diferentes para adaptarse a las necesidades de cualquier negocio.

Hoy en día existen empresas que no tienen establecida una estructura organizacional, por lo que no permite tomar una buena decisión en cuanto a la optimización de los recursos de TI y a los diferentes problemas que se puedan presentar.

6.1.2 AI6 Administración de cambio

Todos los cambios, incluyendo el mantenimiento de emergencia y parches relacionados con la infraestructura de red deben ser administrados formalmente y controladamente, para garantizar la reducción de riesgo que puedan implicar algún tipo de afectación. El objetivo de control evaluado para este proceso es cambio de emergencia.

6.1.2.1 AI6.3 Cambio de emergencia

Para (Isaca, 2007, p. 94), el cambio de emergencia “es establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido”.

Este proceso consta de actividades planificadas para llevar a cabo cambios urgentes que se le realizan a los servicios de red y que deben ser documentado de manera física o electrónica.

La mayoría de las empresas no cuentan con un procedimiento de cambios de emergencia, ya que no lo consideran importante o porque no analizan que es imprescindible tener un plan para evitar consecuencias negativas.

6.1.3 DS3 Administrar el desempeño y capacidad

Es el proceso de revisar el desempeño actual y los procesos de los recursos de TI, basados en los requerimientos de carga de trabajo, almacenamiento y contingencias; brindando la seguridad de que los recursos de información estén disponibles. A continuación se detallan los procesos para este dominio.

6.1.3.1 DS3.2 Capacidad y desempeño actual

(Isaca, 2007, p. 110), expresa que la capacidad y desempeño actual es “revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicios acordados”.

Es un diagnóstico que se realiza de manera periódica a la red para analizar el estado de la misma, involucrando criterios como velocidad y calidad para transferir los datos, esto nos permite garantizar que si la capacidad acordada es suficiente para las necesidades requeridas.

Existen algunas ocasiones donde la administración informática de determinada empresa no da la suficiente importancia para monitorear los recursos y servicios

prestado, de manera que los empleados se quejan cuando no pueden transmitir la información a la persona destinada o porque el ancho de banda está demasiado bajo para navegar.

6.1.3.2 DS3.4 Disponibilidad de recursos de TI

(Isaca, 2007, p. 110), afirma que la disponibilidad de recursos de TI es “brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencia, requerimientos de almacenamiento y ciclos de vida de los recursos de TI”.

Pardo (2009), explica que la disponibilidad de los recursos de TI es desarrollar, medir y aprobar un plan de disponibilidad de los equipos informáticos y la continuidad de los servicios, para asegurar que puedan seguir trabajando bajo cualquier circunstancia.

Las citas anteriores aportan que el objetivo de este proceso es asegurar que los servicios prestados por la administración de TI garanticen en nivel máximo de disponibilidad en los recursos, para satisfacer los objetivos del negocio y para entregar la calidad de servicio que este demande, esto basado en planes de contingencia que minimicen cualquier riesgo posible.

A nivel local, empresas como la de acueductos y alcantarillados, cuenta con un plan de contingencia, ya que en caso de que ocurra una interrupción del suministro eléctrico, cuentan con una planta de emergencia para que los recursos informáticos existentes sigan funcionando y para que los empleados tengan siempre la máxima disponibilidad de los recursos.

6.1.3.3 DS3.5 Monitoreo y reporte

Se trata del monitoreo continuo del desempeño y la capacidad de los recursos de TI, lo cual sirve para mantener y poner a punto el desempeño actual de TI y para reportar la disponibilidad hacia el negocio del servicio prestado, Isaca (2007).

La importancia del monitoreo y reporte es prevenir problemas, ya sea por aumento de carga de trabajo o fallas de seguridad, además permite resolver problemas inminentes con avisos y alertas pertinentes, reforzar los puntos débiles de la infraestructura y sobre todo dar mejoras y optimizaciones en el uso de los recursos.

Algunas instituciones bancarias de Matagalpa, cuentan con un plan de actividades, lo cual vincula a un encargado de monitorear y reportar rendimiento, incidencias o anomalías en las operaciones de carácter informático.

6.1.4 DS4 Garantizar la continuidad de servicio

Es desarrollar, mantener y probar los planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad, con el fin de minimizar la probabilidad y el impacto de interrupciones mayores en los servicios de TI.

6.1.4.1 DS4.2 Planes de continuidad de TI

Según (Isaca, 2007, p. 114), los planes de continuidad de TI son “desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio”.

(Peña, 2005, p. 15), afirma que “el plan de continuidad de TI debe estar alineado con el plan general de continuidad del negocio, para asegurar consistencia”.

Los dos autores hacen ver la importancia de las estrategias o medidas de seguridad adecuadas que toda empresa debe de emprender para minimizar riesgos, ya sea para situaciones de emergencia, desastres naturales entre otros, a fin de evitar el paro total de las funciones de un negocio.

El plan de continuidad de TI que implementan algunos supermercados están basado en contingencias o experiencias que ayudan a evaluar los riesgo a los que

están expuesto, por esta razón ellos poseen planes fundamentados en procedimientos que orientan al personal a actuar para restaurar los servicios ante una interrupción inesperada.

6.1.4.2 DS4.3 Recursos críticos de TI

Isaca (2007), cita que la continuidad de los recursos críticos de TI se centra en la atención en los puntos determinados como lo más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.

Son todos aquellos recursos que la empresa considere activos o importantes y que cualquier falla que presente debe de contar con un plan que lo reemplace o lo recupere.

En la actualidad, hay pocos negocios que cuentan con la visibilidad necesaria para diseñar procesos y políticas claras que se centren en los recursos críticos para evitar la existencia de riesgos, esto debido a que no se tiene un buen gobierno y una buena administración de los activos de TI.

6.1.4.3 DS4.6 Entrenamiento del plan de continuidad

(Isaca, 2007, p. 114), define que el entrenamiento del plan de continuidad de TI es "asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre".

Se trata de la capacitación constante del personal pertinente en cuanto a las normativas y acciones que deben ejecutar según sus responsabilidades.

Las organizaciones además de tener un plan de continuidad, contingencias, entre otras medidas deberían preocuparse por entrenar al personal correspondiente sobre los procedimientos a seguir en caso de un incidente o desastre, además de las responsabilidades y roles a cumplir en este tipo de medidas, lo cual asegura

que las personas involucradas participen y se comprometan para que el plan sea un éxito.

6.1.4.4 DS4.8 Recuperación y reanudación de los servicios de TI

(Isaca, 2007. P. 114), especifica que la recuperación y reanudación de los servicios de TI son “planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios”.

Son un conjunto de actividades que ayudan a garantizar el correcto funcionamiento de los servicios después de un fallo, esto con el propósito de no arriesgar los recursos que proveen los servicios necesitados.

Con los Bancos cuentan con un conjunto de procedimientos y estrategias que aseguran la reanudación de los servicios informáticos críticos al momento de un incidente, lo cual les genera un impacto mínimo o nulo ante un evento no deseado.

6.1.4.5 DS4.9 Almacenamiento de respaldo fuera de las instalaciones

(Isaca, 2007, p. 114), argumenta que el almacenamiento de respaldo fuera de las instalaciones es “almacenar fuera de las instalaciones todos los medios de respaldos, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio”.

Hostalia (2012), asegura que si la información es importante o confidencial es necesario tener un backup alternativo en un lugar externo a salvo de robos o desastres naturales.

Los autores contribuyen con similares aportes que son de importancia en los respaldos fuera de las instalaciones para asegurar que la información mantenga un control máximo de seguridad y evitar consecuencias potencialmente graves de pérdida de datos o interrupción del servicio en caso de que ocurra un desastre dentro del local.

La mayorías de las fábricas realizan los respaldos en las nubes, para evitar consecuencias graves de pérdidas de datos o interrupción de servicios que se presente inesperadamente, además otra de las formas de respaldo es por medio de disco duro, de manera que los beneficia a la reducción de costo.

6.1.5 DS5 Garantizar la seguridad de los sistemas

Es el establecimiento y mantenimiento de roles y responsabilidad de seguridad, políticas, estándares y procedimientos sobre la infraestructura de la red, además permite realizar monitoreo de seguridad y pruebas periódicas así como la realización de acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

En este proceso se seleccionaron seis objetivos de control de acuerdo a la temática abordada, los que se describirán a continuación

6.1.5.1 DS5.2 Plan de seguridad de TI

(Isaca, 2007, p. 118), explica que un plan de seguridad de TI es “trasladar los requerimientos de negocio, riesgo y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad”.

Un plan de seguridad debe de incluir todos los procesos y servicios involucrados para ofrecer una mejor seguridad en las actividades del negocio, además para identificar amenazas y vulnerabilidades de la red.

Las organizaciones hoy en día deben de contar un plan de seguridad, lo cual se enfoque en las debilidades que presentan, identificación de amenazas y evaluar los riesgos para implementar políticas de seguridad, estándares y métodos. Un plan de seguridad ayuda a toda organización a analizar estudios de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

6.1.5.2 DS5.3 Administración de identidad

Para (Isaca, 2007, p. 118), la administración de identidad debe de “asegurar que todos los usuarios (internos, externos, y temporales) y su actividad en sistema de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificable de manera única”.

Montoya & Restrepo (2012), define la administración de identidades, como un conjunto de procesos que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales.

Los autores citados anteriormente explican que este proceso permite llevar un control al acceso de los sistemas informáticos y a las instalaciones dentro de la organización, además para administrar la autenticidad de usuarios, derechos, restricciones de acceso y que sus actividades sean identificadas de manera única, con el propósito de evitar malintencionado de los propios usuarios, espionaje y sabotaje de intrusos.

En algunas empresas como la de acueductos y alcantarillados, se cuentan con políticas de identidad de usuario, lo cual les facilita el control de acceso a los diferentes recursos, con el objetivo de mitigar riesgo y que el negocio evolucione de manera segura y flexible.

6.1.5.3 DS5.4 Administración de cuentas del usuario

Según (Isaca, 2007, p. 118), la administración de cuentas del usuario se trata de “garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuarios”.

La administración de la cuenta de usuario es parte esencial dentro de una organización, lo cual permite verificar la autenticidad e identidad de cada individuo y personalizar los recursos a utilizar, además se establecen mecanismo de solicitud, suspensión, modificación y cierre de cuentas de usuario.

En los beneficio llevan una administración de cuenta de usuario para establecer los privilegios que va a tener cada persona y así garantizar que la información del equipo sea privada y segura.

6.1.5.4 DS5.9 Prevención, detección y corrección de software malicioso

Isaca (2007), argumenta sobre poner en práctica medidas preventivas, detectivas y correctivas en toda la organización para proteger los sistemas de la información y a la tecnología contra malware.

Esta actividad establece medidas de prevención, detección y corrección, es decir contar con parches de seguridad y antivirus actualizados para proteger los sistemas de información y a la tecnología contra software malicioso, ya sea virus, gusanos, spyware, correo basura, entre otros. Esto incluye implementar políticas, estándares, procedimientos de TI y realizar monitoreo de seguridad y pruebas periódicas.

En algunas empresas, como la de acueductos y alcantarillados, poseen medidas para prevenir software malicioso como: la actualización de software, antivirus actualizados con licencias, restricción de acceso a internet, entre otros, para que no se propaguen programas no deseados y que la información y el equipo estén seguro.

6.1.5.5 DS5.10 Seguridad de la red

Según Isaca (2007), la seguridad de la red es el uso de técnicas de seguridad y procedimientos de administración para autorizar acceso y controlar los flujos de información desde y hacia la red.

Para (Carracedo, 2011, p. 24), la seguridad de la red es “un conjunto de técnicas que tratan de minimizar la vulnerabilidad de los sistemas o de la información en ellos contenida”.

Lo anterior descrito por los autores refleja que la seguridad es un factor importante para garantizar que el funcionamiento sea el óptimo en todas las máquinas de una red y que los usuarios posean los derechos que les han sido concedidos, para evitar pérdidas de datos, acceso no autorizado y posibles daños a la red.

En las empresas Bancarias la seguridad de la red es de un nivel alto, lo cual permite prevenir que los hackers no puedan borrar, modificar o robar información confidencial, estas empresas implementan mecanismos de seguridad que protegen la comunicación y todas las actividades que se realizan en el día frente a los distintos atacantes.

6.1.6 DS9 Administración de la configuración

Es establecer y mantener un repositorio de configuraciones completo y preciso, crea una efectiva administración de la configuración y facilita una mayor disponibilidad, minimiza los problemas y los resuelve más rápidos.

6.1.6.1 DS9.1 Repositorio y línea base de configuración

(Isaca, 2007, p. 134), afirma que el repositorio y línea base de configuración es "establecer una herramienta de soporte y un repositorio central que contenga toda la información relevante sobre los elementos de configuración, monitorear y grabar todos los activos y los cambios a los activos".

Se trata de mantener documentado todas las configuraciones funcionales correspondientes a los dispositivos, para evitar cualquier retraso en momento en que se requiera un cambio.

Otro de los aspectos importante que deberían considerar las organizaciones es llevar un control de los parámetros de configuración de ciertos recursos tales como, un routers, un switch, entre otros, con el objetivo de garantizar la continuidad de los servicios o recursos que requieren las empresas.

6.1.7 DS10 Administración de problemas

Identifica recomendaciones para la mejora, mantenimiento de registro de problemas y la revisión del estatus de las acciones correctivas, de tal manera que mejora los niveles de servicios, reduce costos y mejora la conveniencia y satisfacción del usuario.

6.1.7.1 DS10.1 Identificación y clasificación de problemas

(Isaca, 2007, p. 138), cita que la Identificación y clasificación de problemas es "implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes".

Añadiendo a lo citado por el autor se puede complementar que la administración de problemas, también debería incluir las acciones a tomar en cuenta para evitar o corregir un riesgo.

Hoy en día en algunas organizaciones los encargados en el área informática, no logran solventar los problemas en tiempo y forma que se presentan, por esta razón los empleados se quejan de los informáticos, por eso las empresas deben concebir un formato de gestión de riesgo.

6.1.8 DS11 Administración de datos

Establecer procedimientos efectivos para administrar librerías de medios, respaldos, configuración de datos y la eliminación apropiada de medios. Ayuda a garantizar la calidad, oportunidad y disponibilidad de la información.

6.1.8.1 DS11.5 Respaldo y restauración

Se trata de definir e implementar procedimiento de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad, Isaca (2007).

Es muy importante realizar respaldos periódicamente de los sistemas en uno o varios dispositivos, ya sea automático o en aplicaciones, para evitar pérdidas de datos, en caso de que sufra una avería electromecánica o un error en su estructura lógica, para continuar con las actividades rutinarias.

El respaldo para las organizaciones debe ser de vital importancia, ya que en caso de distintos eventos puede recuperarlo, esto permite que la información cuente con la integridad y disponibilidad en cualquier momento que la empresa lo requiera.

6.1.9 DS12 Administración del ambiente

Este proceso define requerimientos físicos del centro de datos como: la selección de instalaciones apropiadas, el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico.

6.1.9.1 DS12.2 Medidas de seguridad física

(Isaca, 2007, p. 146), indica que las medidas de seguridad físicas es “definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio”.

Esto implica implementar medidas de prevención contra las amenazas a los recursos y la información confidencial, de manera física como son: protección de hardware, acceso físico, electricidad, temperaturas extremas, entre otras.

Hoy en día existen instituciones que no cuentan con medidas de protección y salvaguarda, ya que no analizan las amenazas a las que pueden estar sometidas y la importancia de implementar medidas de protección como: tarjeta con alarma, llevar un control de las persona que tiene acceso a los cuartos de servidores, hardware, suministro ininterrumpido de corriente, polo tierra entre otros.

6.1.9.2 DS12.3 Acceso físico

(Isaca, 2007, p. 146), explica que el acceso físico es “definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias”.

Es garantizar la seguridad global de la red y los sistemas conectados a ella para prevenir riesgo y que no tengan acceso personas no autorizadas. Una de las medidas importantes es usar una clave basada en una tarjeta o cualquier otro dispositivo para acceder físicamente e identificar el usuario en la red.

Toda empresa debe implementar medidas de protección que impidan el acceso sin autorización, para evitar daños e interferencia a las instalaciones y a la información, de manera que regule y controle periódicamente el acceso de las distintas áreas, además contar con mecanismo de detección y protección contra intrusos.

6.1.9.3 DS12.4 Protección contra factores ambientales

Para (Isaca, 2007, p. 146), la protección contra factores ambientales es “diseñar e implementar medidas de protección contra factores ambientales”.

Son mecanismo de prevención para disminuir riesgo, por eso es importante tener un plan de contingencia para tener conocimiento en un dado caso que se presente una situación inesperada.

Otro de los aspectos importantes para la protección de los servicios o activos informáticos es la mitigación de los factores ambientales, de tal manera que en el plan de acción o la gestión de riesgos de las entidades debe incluir medidas que minimicen riesgos contra estos factores, algunas de estas medidas preventivas que deberían tomar en cuenta son extinguidores, alarmas contra incendios entre otros.

6.1.9.4 DS12.5 Administración de instalaciones físicas

Según (Isaca, 2007, p. 146), la administración de instalaciones físicas es "administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud".

Es controlar las entradas y salidas, no solo del propio laboratorio o centro de cómputo, sino de las instalaciones en donde se ubican, por lo que deben estar siempre debidamente controlados para evitar el acceso de personas no autorizadas, además asegura que los empleados, proveedores, personal de servicio y visitantes cumplan con los procedimientos de seguridad.

En la actualidad, son pocas las instituciones que cuentan con una buena administración de instalaciones física, de tal manera, que los equipos de cómputo y los data center están expuesto a riesgos y mayormente a desastre.

6.2 Infraestructura de la red LAN

La infraestructura de Red LAN o Local Área Network, consiste en la conexión tanto física (hardware) como también lógica (software) en un entorno cercano, cuya finalidad es la de compartir los recursos de un sistema determinado.

6.2.1 Funcionamiento de la estructura física

El funcionamiento de la estructura física de una Red LAN se basa en compartir los recursos y la información en la distancia, con la finalidad de asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir costos generales en estas acciones.

6.2.1.1 Cableado

(Simbaña, 2010, p. 45), indica que “el cable estructurado es un enfoque sistemático del cableado. Es un método para crear un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, los administradores de red y cualquier otro técnico que trabaje con cables”.

Según (Cohen & Asín, 2014), el cableado “son aquellos que pueden transmitir datos por medio de pulsos electricos o de luz”.

Los conceptos anteriores aseguran que al crear una red se está creando un sistema de conexión físico con el objetivo de implantar una o varias redes para que exista un medio de comunicación o transmisión de datos.

Hoy en día, la estructura de la red cableada es la más tradicional en todas las empresas, lo cual les permite un óptimo desempeño de manera fiable, flexible, una mejor seguridad de intercambio de información, de comunicación entre otras.

6.2.1.1.1 Cable de Par Trenzado sin Apantallamiento

Este tipo de cable cuenta sólo con el efecto de cancelación producido por los pares trenzados de hilos que limita la degradación de la señal que causa la interfaz electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). Los cables UTP tienen un alcance de 100 m (328 ft), Villareal (2010).

(Poó, 2010, p. 7), define que el cable UTP es un “cable de pares trenzado sin blindaje. Son los mas comunes y prácticamente solo se usan en categoria 5 mejorada”.

(Alfano, 2010, p. 149), afirma que el cable UTP “el material aislante recubre cada uno de los ocho cables individuales. Los pares están trenzados entre sí. Depende únicamente del efecto "cancelación". El número de trenzas por metro determina su tolerancia a emisiones electromagnéticas y de radio”.

Las citas anteriores aportan que el cable UTP es el más utilizado en redes, por su bajo costo, pero no tiene la capacidad de llevar la señal a larga distancia en la red, pero es accesible y fácilmente de cambiar en caso de que sufra fallo.

Este tipo de cable actualmente en las empresas se ha convertido en el estándar de las redes LAN, para la transmisión de datos y señales telefónicas, lo cual es utilizado para unir dispositivos, ya sea del módem a la computadora o de PC a PC, permitiendo cierta protección de interferencia electromagnéticas del ambiente y los demás cables, además por su costo, flexibilidad y fácil de instalar.

6.2.1.1.2 Cable de Par Trenzado Apantallado

Según Villareal (2010), cada par de hilos está envuelto en un papel metálico para aislar mejor los hilos del ruido. El cableado STP reduce el ruido eléctrico desde el interior del cable. Asimismo, reduce la EMI y la RFI desde el exterior del cable, tiene un alcance de 100 m, con una velocidad de transmisión de 100 Mbps.

(Poó, 2010, p. 7), especifica que el “cable de par trenzado apantallado, lleva una malla alrededor de cada par, dado la proteccion radioelectrica respecto del entorno como de unos pares sobre otros, usa conectores con un contacto adicional envolvente”.

Para Alfano (2010), en este tipo de cable, cada par va recubierto por una malla conductora que actúa de pantalla frente a interferencias y ruido eléctrico. Su impedancia es de 150 ohm, sin embargo es más costoso y requiere más instalación. La pantalla del STP, para que sea más eficaz, requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal). Suelen utilizarse conectores RJ-49.

Los tres autores hacer ver que en el cable STP su capa es de mayor protección y de alta calidad, es decir protege los datos de intermodulaciones exteriores, por lo que puede soportar máximas tasas de transmisiones a grandes distancias sin interrupciones en las señales.

Son pocas las organizaciones que cuentan con cable STP, por lo que es muy caro, robusto y de instalaciones difíciles, pero la importancia de este cable es que brinda mayor protección ante toda clase de interferencia.

6.2.1.1.3 Cable de Par Trenzado Apantallado

Según (Poó, 2010, p. 7), el cable FTP "es un cable de par trenzado apantallado en el que la pantalla es una lámina de alumino".

Alfano (2010), explica que en el cable FTP sus pares no están apantallados pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias externas. Su impedancia es de 120 ohms y sus propiedades de transmisión son más parecidas a las del UTP. Además, puede utilizar conectores RJ-45.

Los autores contribuyen con diferentes aportes que son de importancia, ya que su estructura es una cubierta global, para tener un nivel alto en cuanto a las interferencias externas. Permite transmisiones de datos y señales analógicas a altas velocidades con un rendimiento superior.

En algunas empresas como en los aeropuertos cuentan con cable FTP cat. 6, el cual garantiza que la información cuente con su alto desempeño a pesar de las condiciones de interferencia de alto nivel o comportamientos heterogéneos. Este tipo de cable por sus características es uno de los más demandados en el mercado.

6.2.1.1.4 Cable Coaxial

Villareal (2010), argumenta que el cable coaxial es un cable con núcleo de cobre envuelto en un blindaje grueso. Se utiliza para conectar computadoras en una red. Existen diversos tipos de cable coaxial como: 10BASE5: funciona a 10 Mbits/seg con una longitud máxima de 500 m y 10BASE2: funciona a 10 Mbits/seg, con una longitud máxima de 185 m.

El cable coaxial, se trata de un conductor cilíndrico exterior que rodea un solo conductor interior, ambos conductores están aislados entre sí. En el centro del cable hay un único hilo de cobre o alguna aleación conductiva, rodeado por un aislante flexible. Una pantalla de cobre trenzado actúa como segundo conductor. Finalmente una cubierta aislante recubre el conjunto, Alfano (2010).

Los autores citados anteriormente define que el cable coaxial es utilizado para transportar señales eléctricas a grandes velocidades, su apantallamiento protege los datos que se transmiten, absorbiendo el ruido, de forma que no pase por el cable y no exista distorsión de datos; la malla de hilos absorbe las señales electrónicas perdidas, de forma que no afecten a los datos que se envían a través del cable interno. Además es capaz de transportar de forma fiable los datos a grandes distancias.

El cable coaxial fue uno de los más utilizados en las redes locales debido a su alta capacidad y resistencia a las interferencias, su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos. Actualmente son utilizados en las redes de telefonías, para varias señales, incluyendo, voz, videos y datos.

6.2.1.1.5 Cable fibra óptica

Una fibra óptica es un conductor de cristal o plástico que transmite información mediante el uso de luz. Debido a que está hecho de cristal, no se ve afectado por la interferencia electromagnética ni por la interferencia de radiofrecuencia. Este cable puede alcanzar distancias de varias millas o kilómetros antes de que la señal deba regenerarse, Villareal (2010).

Para (Alfano, 2010, p. 148), “es un medio capaz de conducir transmisiones de luz modulada. Es diferente al resto de cables no usa pulsos eléctricos, sino de luz. El cable consta de dos fibras paralelas separadas, recubiertas de material protector”.

Lo anterior descrito por los autores refleja que el medio de transmisión de datos consiste en un hilo fino transparente por el que se envían pulsos de luz que son los datos a transmitir, también permite enviar gran cantidad de datos a una gran

distancia, se puede clasificar como un medio de transmisión por excelencia, al ser inmune a las interferencias electromagnéticas.

Son pocas las entidades que utilizan el cable de fibra óptica, por su alto costo, y el de estructurar un vidrio de alta calidad para su mejor desempeño, pero una de las ventajas de implementar este tipo de cable es que la pérdida de señal es mínima, cuenta con un óptimo ancho de banda, además con un peso y tamaño reducidos y se puede usar a largas distancias.

6.2.1.2 Servidores

(Sierra, 2014, p. 32), explica que “un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al servicio de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información”.

Son capaces de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Se puede ejecutar en cualquier tipo de computadora, incluso en computadoras conocidas como "servidor" y, en la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento.

La mayoría de las compañías poseen servidores para realizar múltiples tareas generales y la administración de carga de trabajo de gran importancia, reforzando la productividad, protegiendo los sistemas y datos, mejorando la velocidad y eficiencia de aplicaciones y transacciones de datos e incrementando el desempeño y seguridad.

6.2.1.2.1 Tipos de servidores

Hay muchos tipos de servidores caracterizados por el hecho de establecer el modelo cliente-servidor, pero también hay muchas diferencias entre ellos. A continuación, se explicarán los tipos de servidores más utilizados en una Red LAN.

- **Servidores web**

(Sánchez, 2010, p. 3), argumenta que el servidor web es un “programa diseñado para permitir la interacción entre ordenadores. Suele funcionar permaneciendo a la espera de peticiones. Cuando las recibe responde a ellas transfiriendo documentos de tipo hipertexto”.

Según Lara (2010), un servidor web recibe peticiones de clientes y responde con el envío de ficheros solicitados, texto plano o binarios. Escucha las peticiones en el puerto: 80: HTTP, 443: HTTPS el servidor busca el archivo solicitado, si lo encuentra, lo transmite; sino envía un mensaje de error.

“Son los encargados de recibir las peticiones referidas a páginas o elementos de la web y devolver el resultado de la petición. Si la petición fue válida, lo traduce de forma legible al usuario”, (Sánchez, 2012, p. 5).

Los conceptos anteriores definen que los servidores web procesan aplicaciones del lado del servidor, realiza conexiones bidireccionales y unidireccionales con el cliente, generando un tipo de respuesta en un lenguaje del lado del cliente; el código o respuesta recibido por el cliente es compilado y ejecutado por un navegador web. Para la transmisión de todos estos datos suele utilizarse protocolos, generalmente el utilizado es el protocolo HTTP para estas comunicaciones.

En la actualidad son pocas las organizaciones que cuentan con servidores web, por su elevado precio, pero es una herramienta indispensable, ya que permite respaldar la información, es rápido, seguro y confiable.

- **Servidor Protocolo de Transferencia de Archivos**

(Arias, 2015, p. 15), explica que un “servidor FTP es un programa especial que se ejecuta en un servidor conectado normalmente en Internet (aunque puede estar conectado en otros tipos de redes). La función del mismo es permitir el desplazamiento de datos entre diferentes servidores / ordenadores”

Su funcionamiento transcurre desde un equipo cliente que se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo. Es decir, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.

Toda empresa debe implementar servidores FTP, por lo que otorga una mayor eficiencia al transferir archivos de gran tamaño, cuenta con la reanudación automática de las descargas de archivos, lo cual es beneficioso para los usuarios con conexiones a Internet lentas o poco confiables, además cuenta con una serie de características de seguridad, de manera que solo los usuarios autorizados pueden tener acceso a los datos, sin la posibilidad de que alguien intercepte los datos descifrables.

- **Servidor Proxy**

Para (Sánchez, 2013, p. 20), el servidor proxy “es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino”.

(García , 2012, p. 10), define que “un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web. Funciona como cortafuegos y filtro de contenidos”.

(Brotons, 2013, p. 8), afirma que un servido proxy “es un servidor que hace de intermediario entre los PCs de la red y el routers de conexión a internet de forma que cuando un usuario quiere acceder a internet, su PC realiza la petición al servidor proxy”.

Las citas anteriores aportan que este tipo de servidores ayuda a mejorar el rendimiento en internet, ya que almacena las páginas más utilizadas en su cache, también permite mejorar la seguridad para evitar software malicioso o algún filtro.

En algunas empresas utilizan este tipo de servidores para denegar páginas que no considera relevante para el usuario, además para evitar filtraciones tanto interna como externa, ya que la información es valiosa y debe estar siempre segura.

6.2.1.3 Sala de servidores

Es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento eléctrico (servidores, sistema de almacenamiento de datos, entre otros), con objeto de tener acceso a la información necesaria para sus operaciones, Ferrer (2009).

Se trata de la ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Puede ser un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Las empresas deben tomar en cuenta siempre la seguridad de sus datos, es por eso que deben existir cuartos de servidores regidos con políticas y normas donde solo personas autorizadas tengan accesos, y así salvaguardar lo más vital, como lo es la información.

6.2.1.4 Estaciones de trabajo

Para Kons (2010), es la manera como se encuentran ubicados, teniendo en consideracion la factibilidad de uso de los medios, la velocidad de operación de las máquinas y la precisión del trabajo.

Al asignar unidades de trabajo a un usuario se le brinda una segmentación o ciertas cantidades de almacenamiento al momento en el que ingrese a la red, esto con el propósito de que el usuario tenga un acceso y almacenamiento limitado.

Toda empresa debe contar con estaciones de trabajo, ya que ofrecen fiabilidad, compatibilidad, escalabilidad, mayor rendimiento y arquitectura avanzada en entornos multiprocesos.

6.2.1.4.1 Perfiles de Usuarios

Para (Hernández, 2010, p. 18), el perfil de usuario “son aquellos conjuntos de datos que este necesita poseer para cubrir un objetivo determinado”.

Díaz (2012), explica que el perfil de usuario es el que permite crear permisos genericos para cada usuario que pertenezcan a una determinada categoria en el sistema o en la red.

Los autores hacen ver la importancia de la creación de un entorno personalizado específicamente para cada usuario, donde se configura el escritorio de la PC y los programas al que este tiene acceso. Esta configuración es hecha solo por personas autorizadas o en la mayoría de los casos un administrador.

Este método es muy utilizado en algunas empresas, como los bancos, ya que permite llevar un control interno de los usuarios que tienen acceso a la red, de esta manera ayuda llevar un registro de las actividades de cada usuario.

6.2.1.5 Dispositivos Intermediarios

Cuadros (2012), cita que los dispositivos intermediarios proporcionan conectividad y operan detrás de escena, asegurando que los datos fluyan a través de la red. Conectan hosts y varias redes individuales para formar una internetwork.

Argumenta (Peña, 2014, p. 32), que “los dispositivos intermediarios proporcionan conectividad entre redes y administran los flujos de datos por la red”.

Los autores contribuyen con similares aportes sobre el funcionamiento de los dispositivos intermediarios, ya que son los encargados de recibir y transmitir los datos a su destino, los cuales estos se clasifican como: dispositivos que dan

acceso a la red, puntos de accesos inalámbricos, dispositivos de interconexión y dispositivos de seguridad.

En la actualidad la mayoría de las empresas hacen uso de los dispositivos intermediarios para transferir datos de una área a otra, además estos permite que se pueda expandir la red según las necesidades.

6.2.2 Funcionamiento de la estructura lógica

El Funcionamiento de la estructura lógica de una Red LAN es la planeación y diseño de la implementación de la red; en sí, todos los protocolos que requiere la red para que funcione, también es la estructura en la que se forma una red.

6.2.2.1 Direcciones de protocolo de internet

(CISCO, 2014, p. 2), cita que "una dirección IP es un direccionamiento usado para identificar únicamente un dispositivo en una red del IP".

Es una etiqueta numérica, que identifica de manera lógica y jerárquica, a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol). La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP. Llamándose a esta forma de asignación de dirección IP como dirección IP dinámica.

Algunas empresas llevan un control de las IP, lo cual les facilita identificar las pc que están conectadas a la red y a su usuario, además permite encontrar la ubicación de la pc que está dando problema, este es un mecanismo de gran importancia para cualquier empresa.

6.2.2.2 Intranet

(Cohen & Asín, 2014, p. 216), afirma que la intranet es "básicamente, la utilización de la tecnología de hardware y software de internet con un enfoque hacia el

interior de la organización es lo que ahora se llama como intranet. Es una red privada que utiliza los protocolos TCP/IP de internet ”.

Para Delgado (2011), la intranet son redes corporativas a las que no se tiene acceso desde redes externas o solo parcialmente a algunos servicios, comúnmente correo corporativo y algunos otro fines como: informativo, comercio electrónico, etc.

Los autores citados anteriormente definen que la intranet se utiliza para compartir hardware sin necesidad de movilizarse hasta ellos como: una impresora, un fax, un escáner entre otros, además se utiliza para compartir y distribuir información a los equipos que están conectados.

La mayoría de las empresas como los bancos, utilizan intranets porque optimiza la comunicación, el flujo oportuno de los negocios, reduce costos operativos y ahorro de tiempo. También aumenta la eficiencia y productividad de las operaciones y mejora los tiempos de respuesta

6.2.2.3 Topología de Red

Según (García & Muñoz, 2014, p.13), la topologia de red “es la representación de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente denominados nodos)”.

Para (Cohen & Asín, 2014, p. 199), “es la forma en que se estructura, es decir, la distribución de los nodos (nodo denota cualquier computadora o dispositivo conectados a la red)”.

Lo anterior descrito por los autores explican que la topología de red es un diseño aplicado a la construcción de la red, sea en el plano físico o lógico. Es decir, arquitectura de nodos interconectados. Un nodo es el punto en el que una curva se intercepta a sí misma.

En la actualidad existen muchas topologías de red que se han implementado en diversos entornos empresariales, el cual cada una de estas topologías tienen sus

propios puntos fuertes, que permite que los dispositivos estén conectados para comunicarse entre sí.

6.2.2.3.1 Tipos de Topología

Es la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cuál topología es la más apropiada para una situación dada. Las topologías más comunes se describirán a continuación.

- **Topología Jerárquica**

(Castelán, 2011, p. 42), indica que “son fácil de agregar o quitar nuevos equipos de computos, pero suelen ocasionar cuellos de botellas”.

“Esta topologia también se conoce como estructura de árbol debido a que tiene una computadora raiz en el primer nivel, a la cual se enlaza el primer nivel de computadoras”, (Cohen & Asín, 2014, p. 201).

Los autores especifican que la topología jerárquica enlaza los hubs/switches de tal forma que, un nodo central quede en la parte superior y de ahí se desglosen todas las conexiones existentes, el sistema se enlaza con un computador que controla el tráfico de la topología.

Algunas empresas usan este tipo de topología, ya que son fácil para cubrir áreas extensas y establece fácilmente funciones de gestión de red para conocer lo que sucede con los nodos subordinados.

- **Topología Bus**

“Una topología de bus es multipunto. Un cable largo actúa como una red troncal que conecta todos los dispositivos en la red”, (García & Muñoz, 2014, p. 13).

Según (Martínez & Reyna, 2012, p. 12), la “topología de bus es la que todas las estaciones están conectadas a un único canal o segmento de comunicaciones por

medio de unidades interfaz y derivadores. Las estaciones utilizan este canal para comunicarse con el resto".

Para (Cohen & Asín, 2014, p. 200), "esta topología permite que todas las estaciones reciban la informacion que se transmite, una estacion transmite y todas las restantes escuchan. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de red".

Los tres autores hacen ver que si la red en este tipo de topología crece el desempeño va disminuyendo, además si un canal falla el resto queda incomunicado, porque están conectado a un único canal. El tipo de cableado que se usa puede ser coaxial, par trenzado o fibra óptica

Algunas empresas utilizan este tipo de red, ya que su trabajo de instalación es muy sencillo y sus elementos a emplear no son costosos, y en particular si una conexión se daña o se desconecta una computadora, su reparación es barata y fácil de arreglar.

- **Topología de Estrella**

(García & Muñoz, 2014, p. 14), argumenta que "en la topología en estrella cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central. Los dispositivos no están directamente enlazados entre sí".

Según (Ariganello, 2014, p. 69), la topologia de estrella "los sitios remotos estan conectado aun punto central que por lo general presta un servicio o una aplicación".

Consiste en conectar todas las estaciones a un nodo común, conocido con el nombre de concentrador (Hub, Switch, Router, Gateway). Este tipo de topología el concentrador se encarga de conmutar los datos entre las distintas estaciones, Bueno (2011).

La topología en estrella permite reducir la posibilidad de fallo en la red, conectando todos los nodos a un nodo central, este concentrador central reenvía todas las

transmisiones recibidas de cualquier nodo periférico. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanece intacto.

La ventaja de usar la topología de estrella en las empresas serían muchas, ya que si se desconecta una PC, solo esta queda fuera de la red, además posee un sistema que agrega fácilmente nuevos equipos, ya que es de reconfiguración rápida, costo económico, evita prevenir daños o conflictos, entre otros.

- **Topología de Anillo**

Según (Castelán, 2011, p. 42), la topologia de anillo es el que "utiliza un único canal con repetidores de señal en cada computadora. La información viaja en un sentido del anillo y tiene diferentes modos de conexión: escucha, transmite y cortocircuito".

Para García & Muñoz (2014), en una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa de dispositivo a dispositivo, hasta que alcanza su destino.

Para (Bueno, 2011, p. 3), la topologia de anillo "consiste en conectar las estaciones una en serie con la otra formando un anillo cerrado. La información debe pasar de una estación a otra hasta que llega al destinatario de la misma, generalmente la información es de tipo unidireccional".

Los autores citados anteriormente explican que las estaciones se conectan formando un anillo. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación. Pero unas de la desventaja es que si algún nodo de la red se cae, la comunicación en todo el anillo se pierde.

Este tipo de topología es el menos usado actualmente en las organizaciones por lo que interrumpe el proceso de todas las actividades de la empresa cuando se

produce un error en uno de los nodos, pero una de las ventajas es que su rendimiento no decae cuando muchos usuarios están utilizando la misma red.

- **Topología Malla**

(Castelán, 2011, p. 43), afirma que la topologia malla “utiliza diferentes caminos para enviar la información de una computadora a otra, es fiable, inmunidad a fallos y cuello de botella. Si un componente falla o esta ocupado se vuelve e encaminar el tráfico”.

“En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta”, (García & Muñoz, 2014, p. 14).

La topología en malla permite llevar los mensajes de un nodo a otro por diferentes caminos, ofreciendo total redundancia, fiabilidad y tolerancia a fallos superiores, por lo que cada dispositivo de la red tiene sus puertos de entrada y salida.

Algunas entidades utilizan este tipo de topología por que no requiere de un nodo central, además cuenta con una reducción de riesgos de fallos, es decir, que si se produce un error en un nodo, sea importante o no, no implica la caída de toda la red.

6.2.2.4 Antivirus

(Mosquera & Restrepo, 2011, p. 27), afirma que un antivirus “es un programa cuya finalidad es prevenir y evitar la infección de virus, impidiendo su propagación”.

“Un antivirus es un programa de seguridad que se instala en la computadora o dispositivo móvil para protegerlo de infecciones por malware. El término “malware” es cualquier tipo de software malintencionado, como virus, gusanos, troyanos o spyware”, (López, 2016, p. 17).

(Bongiovanni, 2008, p. 7), especifica que el antivirus “es cualquier metodología, programa o sistema para prevenir la activación de virus, su propagación y contagio de un sistema y su inmediata eliminación y la reconstrucción de archivos o de áreas afectadas por los virus informáticos”.

Por lo anterior descrito los antivirus son utilizados para proteger nuestra computadora y una de la funciones es monitorear cada una de las actividades que realiza el usuario en tiempo real, para detectar y anular los virus existentes.

Toda organización implementa antivirus para mantener siempre la información salvaguardada, que el sistema esté libre de intrusos, virus, y agresores malintencionados, además consume muy pocos recursos, es de fácil uso, fácil instalación, es muy ligero, rápido, eficaz y configurable.

6.2.3 Gestión de Seguridad

Se refiere a los mecanismos que dispone el administrador de una red para monitorear los recursos, los permisos de uso de estos recursos asignados a usuarios y el uso en sí que se le da a estos.

Para cumplir satisfactoriamente con la realización de estas tareas, es necesario tomar en consideración ciertas políticas de seguridad.

6.2.3.1 Políticas de Seguridad

(Benítez, 2013, p. 23), argumenta que las politicas de seguridad es “establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan con los servicios asociados a ellos”.

(Correa, 2011, p. 75), explica que las politicas de seguridad son “establecer medidas y patrones técnicos de administración y organización de las tecnologías

de Información y comunicaciones TIC´s de todo el personal comprometido en el uso de los servicios informáticos".

Al hacer un análisis de las posibles amenazas que puede sufrir un sistema de red, se debe diseñar políticas de seguridad, con el objetivo de establecer responsabilidades o reglas de estricto cumplimiento para tratar de minimizar riesgo.

Algunas empresas como los bancos implementan las políticas de seguridad, para asegurar de que todos sus miembros conozcan sus responsabilidades, mantener y salvaguardar la protección de sus recursos y sobre todo la información.

6.2.3.2.3 Análisis de Riesgo

(Mendoza, 2014, p. 51), afirma que el análisis de riesgo es una "metodologías que consisten en la identificación, análisis y evaluación sistemática de la probabilidad que ocurra daños asociados a los factores externos, fallas en los sistemas, la red, entre otros, con la finalidad de controlar o minimizar las consecuencias".

Para Ferrer (2007), el análisis de riesgos es identificar amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica, con el fin de generar un plan de control que garanticen un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Para salvaguardar la infraestructura de red y un activo importante como lo es la información, se deben realizar estudio de las posibles amenazas que permita evaluar, preparar planes y ejecutarlos para minimizar riesgos.

Las empresas actualmente implementan un análisis de riesgos, para identificar las fuentes de amenazas, para valorar cuales son los recursos importantes que se deben proteger para crear normas o políticas de seguridad.

VII. PREGUNTAS DIRECTRICES

1. ¿Cómo es el funcionamiento de la infraestructura de la red LAN?

2. ¿Cuáles son las problemáticas de la infraestructura de la red LAN, tomando en cuenta el modelo de objetivo de control COBIT 4.1?

3. ¿Cuál es el grado de afectación de las problemáticas encontradas a la infraestructura de la red LAN, tomando en cuenta el modelo de objetivo de control COBIT 4.1?

VIII. DISEÑO METODOLÓGICO

8.1 Enfoque de Investigación

Para (Hernández, Fernández, & Baptistas, 2010, p. 4), la investigación cuantitativa "usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías".

Según (Hernández, Fernández, & Baptistas, 2010, p. 7), la investigación cualitativa "Utiliza la recoleccion de datos sin medicion numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación".

El enfoque de la investigación es cuantitativo con elementos cualitativos, cuantitativo porque la problemática de estudio está apoyada en un marco teórico que da origen a la operacionalización de variables. Para la recolección de datos se hizo uso de técnicas cuantitativas tales como la encuesta (Ver Anexo 8). El enfoque cualitativo está basado en las entrevistas que se aplicaron (Ver Anexo 2, 3, 4, 5, 6, 7), las cuales no se analizaron de manera estadística y observaciones no participativas (Ver Anexo 9).

8.2 Alcance de la Investigación

(Hernández, Fernández, & Baptistas, 2010, p 80), explican que la investigación descriptiva "buscan especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencia de un grupo o población".

La investigación es del tipo descriptiva, ya que se especificaron las características y dificultades de un servicio funcional en una organización.

8.3 Por su Corte

(Hernández, Fernández, & Baptistas, 2010, p.151), explican que el corte transversal es el que "recolectan datos en un solo momento, en un tiempo único.

Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado".

Esta investigación es transversal, puesto que la recolección de datos se hizo en un periodo determinado, en este caso en el primer semestre del 2016.

8.4 Por su Diseño

(Hernández, Fernández, & Baptistas, 2010, p. 149), definen la investigación no experimental como un "estudio que se realizan sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para después analizarlos".

La investigación es del tipo no experimental, debido a que únicamente se realizó un análisis del fenómeno investigativo sin alterar la naturaleza del mismo.

8.5 Universo de Estudio

El universo de estudio está conformado por el encargado del área informática, y los 40 usuarios que hacen uso del servicio de red.

Según (Sequeria & Cruz, 2009, p. 50) el muestreo por conveniencia "es un tipo de muestreo probabilístico, donde el investigador define los criterios o condiciones que debe cumplir cualquier elemento para que sea parte de la muestra".

Es un muestreo por conveniencia porque solamente se encuestaron a 20 usuarios, ya que no todos permanecen en la empresa, considerando que el 50% es representativo.

8.6 Recolección y análisis de datos

La veracidad de la información está fundamentada en el método teórico y para la recolección de los datos se hizo uso de técnicas como:

- Entrevista al encargado de informática (Ver Anexo 2, 3, 4, 5, 6, 7).
- Encuesta a los usuarios (Ver Anexo 8).
- Observación no participativa a la infraestructura de la red (Ver Anexo 9).

Instrumentos:

- Guía de encuesta.
- Guía de entrevista.
- Guía de Observación.
- Tabla de las situaciones encontrada.
- Matriz de riesgos para las situaciones encontradas.

La información recabada se analizó mediante la triangulación para determinar los contrastes tanto en entrevistas, encuestas y la observación, de igual manera esto permitió graficar los resultados y elaborar el informe, para lo cual se utilizó software de aplicación en este caso Microsoft Excel 2013. Basado en el COBIT las distintas situaciones encontradas se analizaron generando al final un conjunto de recomendaciones pertinentes.

8.7 Variable de Estudio (Ver Anexo 1)

- El modelo de objetivo de control COBIT 4.1
- Infraestructura de la red LAN

ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Esta investigación tiene como propósito principal evaluar la Infraestructura de la Red LAN de la "Empresa CECOCAFEN", basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, Primer Semestre 2016. Para alcanzar dicho propósito se plantearon objetivos específicos, los cuales se enfocan en describir el actual funcionamiento de la red, para identificar problemáticas que afectan a la misma y así mismo valorar el grado de afectación que pueda tener a corto o largo plazo.

La información esencial recolectada se obtuvo mediante entrevistas al involucrado que se encargan de la informática en la empresa (Ver Anexo 2, 3, 4, 5, 6, 7), se realizó una encuesta a los usuarios que utilizan los servicios de la red (Ver Anexo 8) y finalmente se realizó una guía de observación (Ver Anexo 10).

Para el procesamiento de la información se construyó una matriz de resultados para las entrevistas realizadas (Ver Anexo 11), dicha investigación se complementó con el resultado de las encuestas aplicadas a los usuarios y la guía de observación.

Descripción de ámbito

La cooperativa central cafetalera del norte (CECOCAFEN) cuenta con 4 cooperativas como son: SOLCAFÉ, Agroindustria, CECOCAFEN y caja del norte. Actualmente su producto en el mercado es el café Sabor Nica, emplean más de 200 persona, pero 40 son las que utilizan computadoras.

Esta empresa cuenta con una infraestructura de red que no se le da un uso y mantenimiento adecuado debido a que no existe un área de TI definida, sino que se subcontrata a personal externo de la empresa en caso de que se presente algún problema grave, pero por lo general los usuarios buscan como resolver el problema sin tener conocimiento alguno.

La empresa tiene cuatro servidores marca Dell con capacidad de 250 gigabit de respaldo, se conectaban por Virtual Private Network (VPN) para gestionar la información, básicamente los usuarios iniciaban sesión y de ahí cargaban su perfil que iba a usar, se contaban con 5 disco duros uno de ellos manejaba el sistema y los otros hacían la función de que si un disco se caía se ponía el otro, era una rutina de respaldo. En estos servidores se llevaba las bases de datos contables, el correo electrónico y toda la información de la empresa, los cuales se dañaron por falta de medidas de protección y mantenimiento, actualmente llevan cuidadosamente la contabilidad, el resto de la información los usuarios las almacenan en memorias externas personales y en los mismos equipos.

El cableado estructurado que usan es el UTP categoría 5 pero presenta problemas en la comunicación de la diferentes áreas, ya que está dañado porque se encuentra desprotegido y en algunas áreas este se encuentra tirado sin algún orden en particular.

Las topologías de red que cuenta la empresa son: de estrella y estrella extendida. El inconveniente es que no existe conexión entre las cooperativas que conforman la empresa, el cual al compartir información lo hacen vía Skype y correo electrónico. El ancho de banda existente para las cooperativas es el siguiente:

- Cooperativa central (CECOCAFEN): 10 mbps
- SOLCAFÉ: 3 mbps
- Agroindustrias: 2 mbps
- Cooperativa de ahorro y crédito: 5 mbps

Estructura organizacional

Según el entrevistado, la empresa no dispone en la estructura organizacional de un área de TI (Ver Anexo 11), lo que se corroboró mediante observación en el organigrama de la empresa CECOCAFEN (Ver Anexo 12), esto viene a representar una debilidad, ya que al presentarse problemas en la red se tiene que

recurrir al llamado de la persona que brinda el servicio de informática temporal, ocasionando retrasos en los procesos y creando mayores inconvenientes.

Según Isaca (2007), la estructura organizacional es establecer una estructura interna y externa que refleja las necesidades del negocio y el nivel de dependencia para satisfacer los objetivos de negocio esperado y las circunstancia cambiantes.

Cambio de emergencia

El entrevistado argumentó que no existe un formato de control de cambio de emergencia (Ver Anexo 11), lo que implica que está para resolver un problema cuando lo requiera sin tener un plan a seguir.

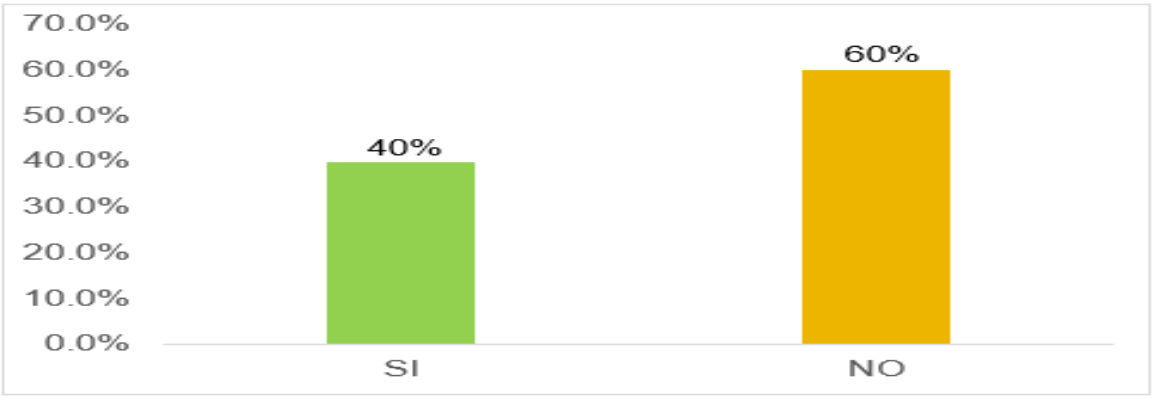


Gráfico 1. Disponibilidad de los recursos para dar soluciones inmediatas

Fuente: resultado de investigación, encuesta realizada a usuarios.

Se preguntó a los usuarios sobre si el personal de TI cuenta con los recursos necesarios para brindar soluciones inmediatas (Ver Anexo 8), obteniéndose en un 60% que no se cuenta con los recursos necesarios y un 40% dispone de dichos recursos.

Se observó que no hay un personal de TI permanente que brinde servicios informáticos a la empresa (Ver Anexo 10).

La empresa ante un problema que requiera solución rápida, no cuenta con el personal ni con el material para dar una solución inmediata a dichos problemas. La

causa es debido a la falta de conocimiento y experiencia por parte del gerente sobre los riesgos, la severidad de los mismos y el esfuerzo de examinar dicho problema, el cual puede generar un problema a grandes rasgos, poniendo vulnerable a la red y el flujo de trabajo que se realiza.

Es importante la elaboración de un plan de emergencia, ya que especifica procedimientos para manejo de situaciones súbitas inesperadas, el cual su objetivo es reducir las posibles consecuencias.

Para (Isaca, 2007, p. 94), el cambio de emergencia "es establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido".

Capacidad y desempeño actual

A través de entrevista (Ver Anexo 11) el encargado de informática explicó que los equipos no tienen la capacidad para suplir las necesidades tomando en cuenta que es muy básico para la escalabilidad de los servicios, por lo que hay equipos que están obsoletos y desactualizados.

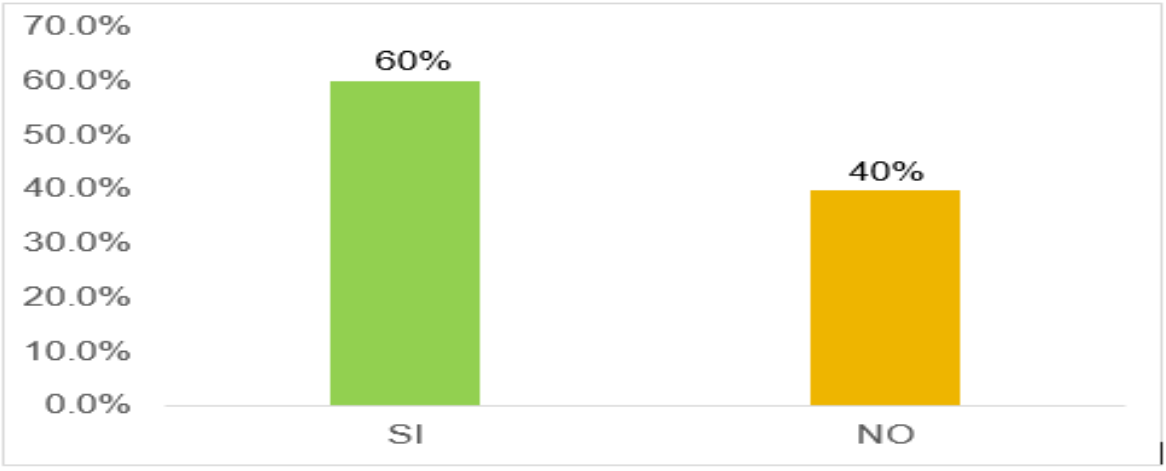
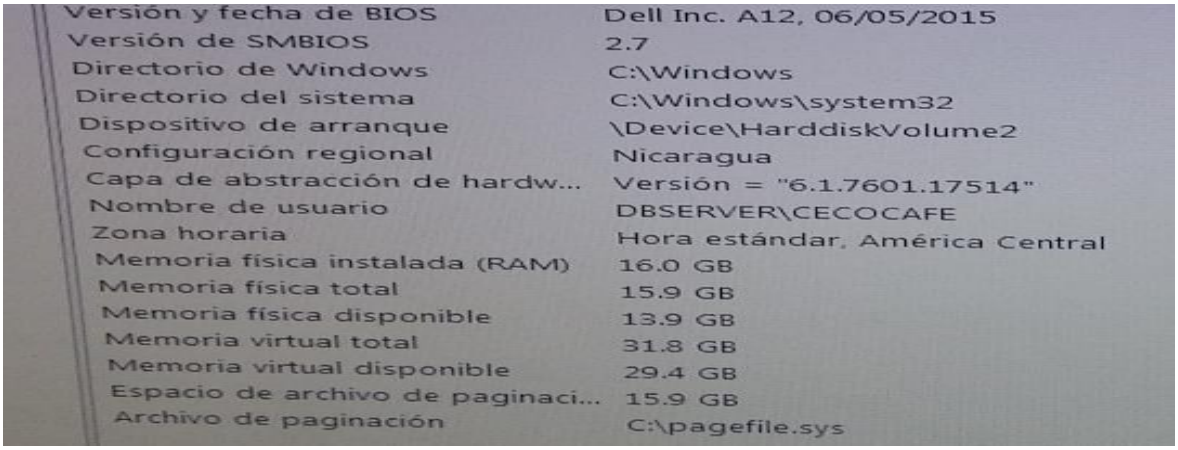


Gráfico 2. Capacidad de los equipos informáticos

Fuente: resultado de investigación, encuesta realizada a usuarios.

Se indagó con los usuarios sobre la capacidad de funcionamiento del equipo del cual hacen uso (Ver Anexo 8), resultando el 60% ve de manera positiva el funcionamiento de los equipos y el 40% niega que no hay capacidad.

La empresa cuenta con algunos equipos nuevos, el inconveniente es que según el rol que tiene los usuarios no tienen la capacidad para ejercer sus actividades eficientemente (Ver Anexo 10).



Versión y fecha de BIOS	Dell Inc. A12, 06/05/2015
Versión de SMBIOS	2.7
Directorio de Windows	C:\Windows
Directorio del sistema	C:\Windows\system32
Dispositivo de arranque	\Device\HarddiskVolume2
Configuración regional	Nicaragua
Capa de abstracción de hardw...	Versión = "6.1.7601.17514"
Nombre de usuario	DBSERVER\CECOCAFE
Zona horaria	Hora estándar, América Central
Memoria física instalada (RAM)	16.0 GB
Memoria física total	15.9 GB
Memoria física disponible	13.9 GB
Memoria virtual total	31.8 GB
Memoria virtual disponible	29.4 GB
Espacio de archivo de paginaci...	15.9 GB
Archivo de paginación	C:\pagefile.sys

Figura 1. **Capacidad de equipo**

Fuente: Propia a partir de observaciones realizada en CECOCAFEN.

Según los resultados obtenidos entre el encargado de TI y usuarios no coincide en sus opiniones, debido a que 32% de los usuarios cuentan con laptops y equipos de escritorio con buena capacidad que ayudan a realizar sus actividades de forma óptima, pero no están asignadas a los puestos donde más se requiere. Es importante que la empresa revise un plan de redistribución de los equipos según requerimientos y necesidades de cada puesto y en aquellos casos extremos reemplazar los equipos que ya dieron su vida útil.

(Isaca, 2007, p. 110), expresa que la capacidad y desempeño actual es “revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicios acordados”.

Al entrevistado se le preguntó sobre la capacidad del ancho de banda, el cual expresó que es el óptimo para lo que fue contratado que es para comunicación, correo o mensajería (Ver anexo 11), pero que presenta problemas al momento de querer bajar un archivo.

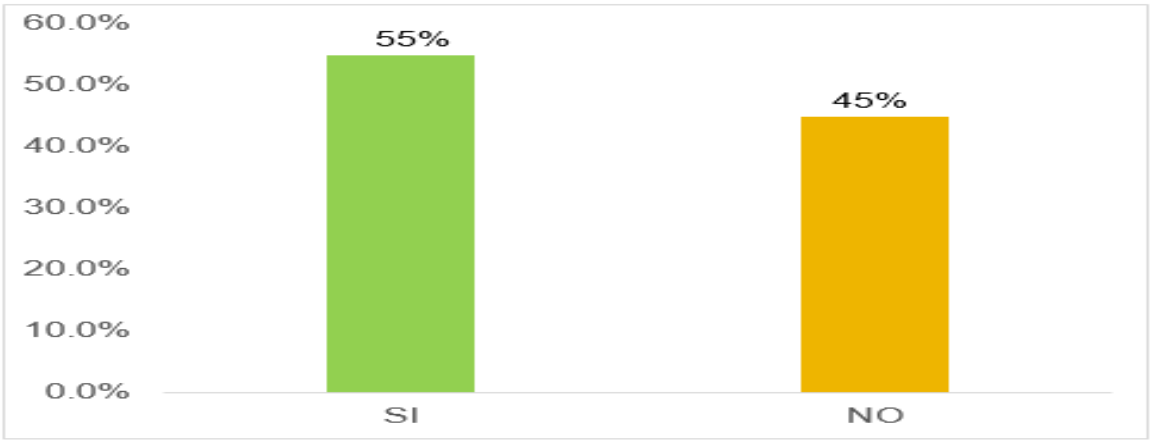


Gráfico 3. Capacidad del ancho de banda.

Fuente: resultado de investigación, encuesta realizada a usuarios.

Otro de los indicadores evaluados de la capacidad y desempeño actual fue, si el internet es el óptimo para las actividades que desempeña (Ver Anexo 8), y se obtuvo que un 55% respondió que sí y el restante dijo que no.

Se notó que los usuarios hacen uso inadecuado como: descargan música, video, conectarse de cualquier dispositivo que no son propios de la empresa y realizan otras actividades que consume todo el ancho de banda (Ver Anexo 10).

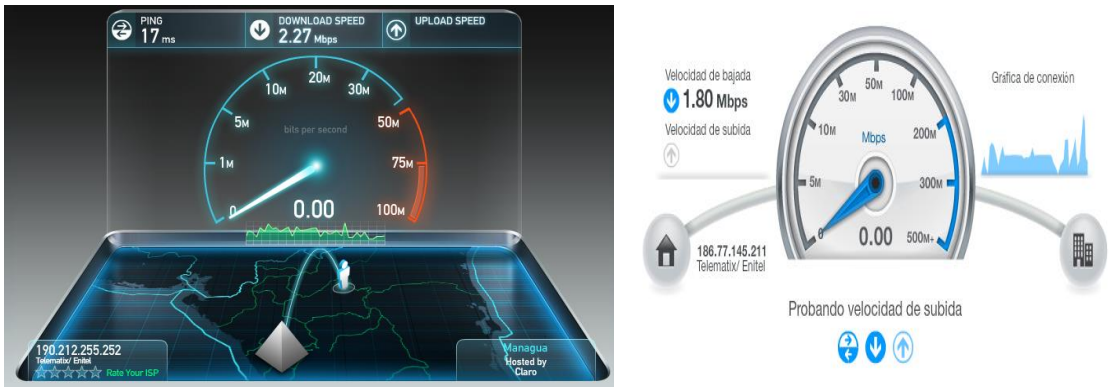


Figura 2. Capacidad de velocidad del internet

Fuente: Propia a partir de observaciones realizada en SOLCAFÉ y Agroindustria.

Se apreció que el ancho de banda existente es el óptimo para apoyar las actividades diarias según lo que mencionan usuarios y el encargado de TI, el inconveniente es que no hay políticas para administrar el ancho de banda. Esto provoca que los usuarios tengan libre acceso y den uso inadecuado, ya sea reproduciendo videos, realizando descargas, entre otras, que tomando en cuenta el número de usuarios hacen que el internet reduzca en capacidad.

Disponibilidad de los recursos de TI

Con el encargado de informática se indago sobre un plan de contingencia para la disponibilidad de los recursos de TI donde él explicó que no hay un plan de contingencia, pero en caso de que se vaya la luz no todos los equipos trabajan (Ver Anexo 11), lo único que pueden seguir trabajando son las laptops.

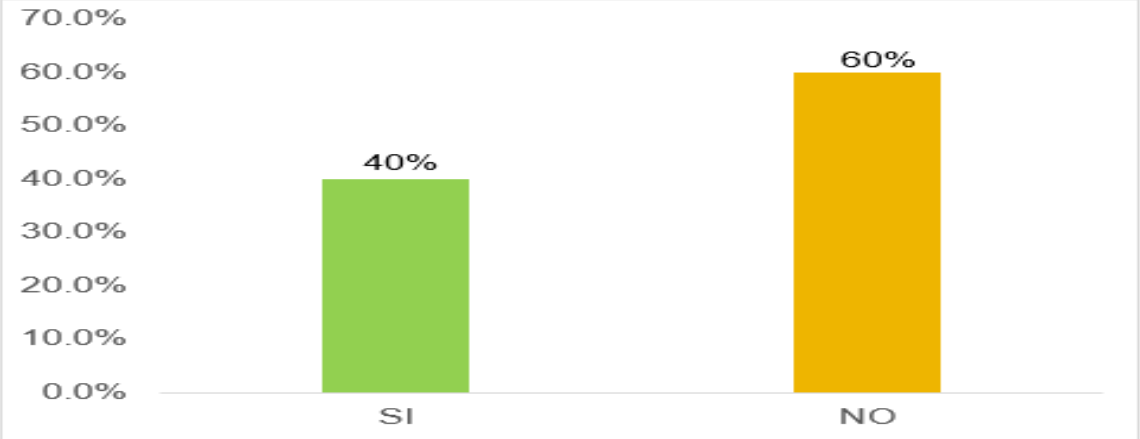


Gráfico 4. Disponibilidad de los equipos para funcionar en caso de emergencia

Fuente: resultado de investigación, encuesta realizada a usuarios.

De igual manera se le preguntó a los usuarios (Ver Anexo 8), donde se obtuvo que un 60% de los usuarios contesto que no.

Basado en los resultados obtenidos existe una concordancia entre usuarios y encargado de TI al explicar que no todos los equipos se mantienen funcionando en todas las circunstancias, de igual manera el encargado de TI explicó que la

gerencia considera irrelevante la disponibilidad de recursos de trabajo, ya que en caso de que haya altos y bajos de energía no poseen una planta eléctrica ni UPS (Sistema de alimentación ininterrumpida), y la mayoría de las computadoras no cuentan con batería, provocando pérdida de información, o daños a los equipos. Deberían minimizar los efectos negativos de la interrupción del servicio, mediante la identificación y análisis proactivo de la causa de los incidentes.

Pardo, (2009) explica que la disponibilidad de los recursos de TI es desarrollar, medir y aprobar un plan de disponibilidad de los equipos informáticos y la continuidad de los servicios, para asegurar que puedan seguir trabajando bajo cualquier circunstancia.

Sobre la disponibilidad del encargado de informática para responder a las necesidades de los usuarios, el entrevistado a expresado que no siempre, porque genera costo, además porque el gerente no quiere contratar a un informático permanente (Ver Anexo 11), porque hay semanas que no presentan ningún inconveniente, el cual no se le puede estar pagando por estar sentado, por esta razón él sugiere que solo se subcontraten en caso de emergencia.

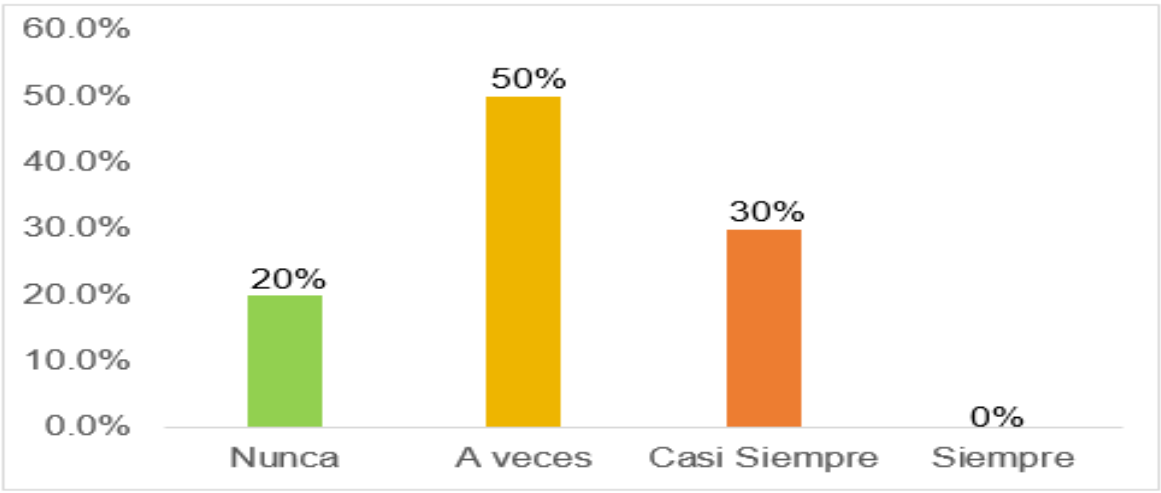


Gráfico 5. Disponibilidad del encargado de TI para responder a las necesidades de los usuarios

Fuente: resultado de investigación, encuesta realizada a usuarios.

Igualmente se interrogó con los usuarios (Ver Anexo 8), encontrándose que más de la mitad de los usuarios han tenido una experiencia aceptable cuando se trata de la disponibilidad del encargado de TI para la resolución de problemas, aclaración de inquietudes u otros aspectos de índole informático.

Según los resultados obtenidos entre el encargado de TI y los usuarios hay una concordancia, por lo que no siempre está disponible cuando el usuario lo necesita, ya que ejerce otras actividades en la empresa que requiere tiempo y es contratado por un determinado tiempo, además como los 3 lugares quedan separados al informático se le dificulta moverse.

La gerencia debería tener conocimiento sobre el papel que juega el informático en la gestión empresarial, ya que desempeña distintas funciones relacionadas con la utilización, mantenimiento, explotación de la red y demás recursos informáticos, además al contratar a una persona permanentemente garantiza la disponibilidad y continuidad de los recursos de TI.

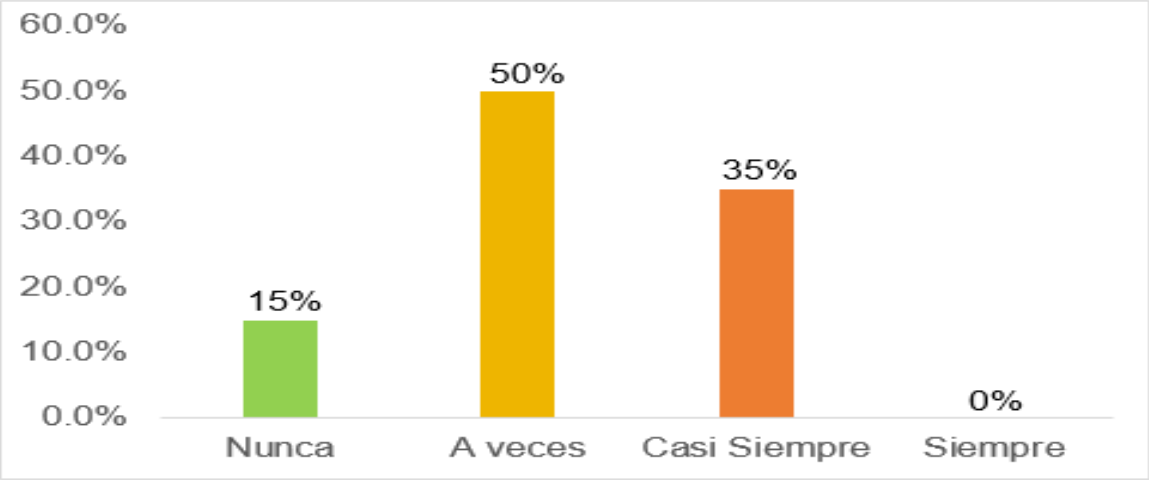


Gráfico 6 Frecuencia para dar soluciones en tiempo adecuado

Fuente: resultado de investigación, encuesta realizada a usuarios.

Sobre el indicador de disponibilidad de recurso de TI, se indagó si el servicio de TI soluciona las incidencias en un tiempo adecuado (Ver Anexo 8), esto reflejó como resultado que un 50% de los usuarios respondieron que a veces los problemas se le resuelven en un tiempo específico, siguiendo con un 35% casi siempre.

Con los resultados obtenidos se concluyó que el informático no soluciona los problemas en un tiempo adecuado, porque no es permanente, carece de información y le da prioridades a los problemas más importantes, provocando inconformidad en los usuarios, además porque no puede resolver todo en un mismo tiempo los problemas que se presentan tanto en la red como en los equipos informáticos. Por esta razón es que los usuarios para poder realizar las operaciones diarias, ellos buscan la manera de resolverlo conllevando a que las soluciones no sean las más adecuadas.

La gerencia debería analizar que al no tener un informático seguirá surgiendo problemas y cada vez más grave, ya que para poder resolverlo tienen que esperar que la persona que se subcontrata esté disponible, provocando ineficiencia en los equipos y en la red. Por eso es importante establecer un plan para que las operaciones sigan surgiendo sin ningún problema.

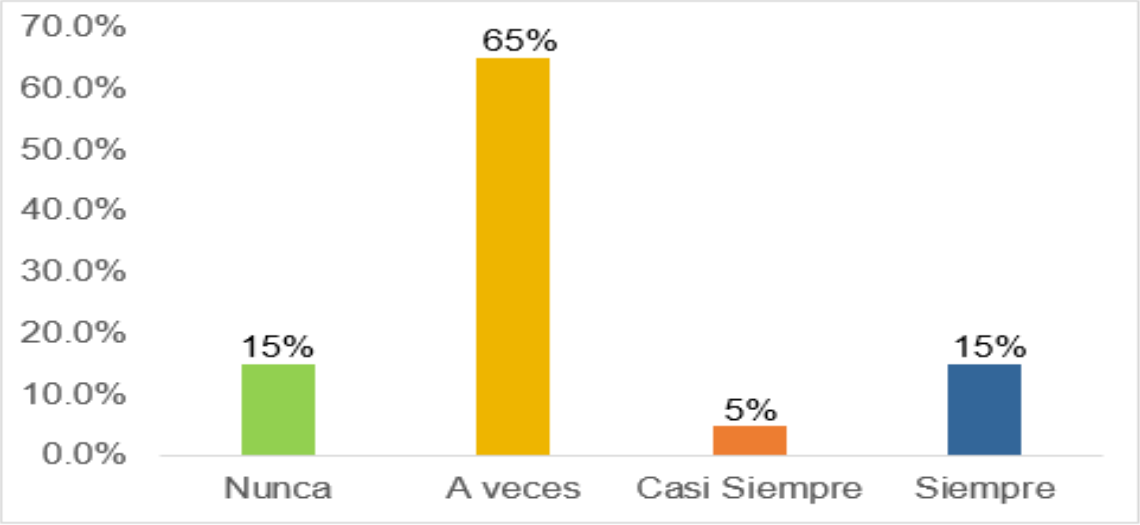


Gráfico 7. Frecuencia para informar los plazos de conclusión de los servicios

Fuente: resultado de investigación, encuesta realizada a usuarios.

Sobre el indicador disponibilidad de recurso de TI, se averiguó si el personal de TI le informa con precisión acerca de los plazos de conclusión del servicio que se está prestando (Ver Anexo 8), obteniéndose que la mayoría de los usuarios son informado con frecuencia.

Mediante la observación se ha podido apreciar que tenían problemas con el servicio del correo electrónico, ya que no habían pagado la mensualidad, problema del cual no se les informó a los usuarios (Ver Anexo 10).

Se determinó que en ocasiones no se les informa a los usuarios en tiempo y forma sobre el plazo de los servicios que se están prestando como es el caso que coincidió con el día de la visita a esta empresa donde se observó que habían inconvenientes al momento de comunicarse entre las áreas, es un problema que se debería evitar para que los usuarios estén preparados ante esta eventualidad, evitar molestia y desgaste innecesarios.

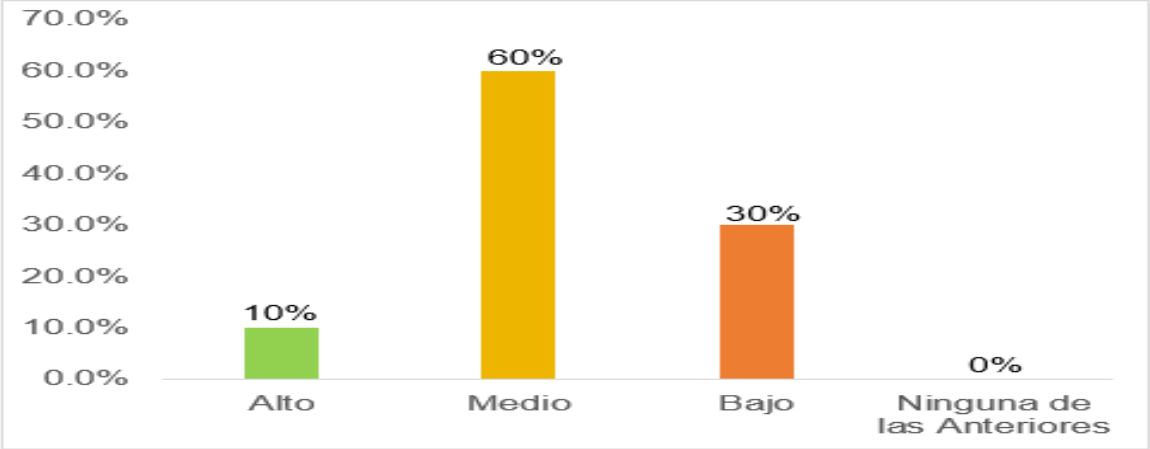


Gráfico 8. El nivel de satisfacción que brinda el servicio de TI

Fuente: resultado de investigación, encuesta realizada a usuarios.

También del indicador se investigó sobre el nivel de satisfacción que brinda el servicio de TI en cuanto a la resolución de problemas de los recursos de TI (Ver Anexo 8), se encontró que un 60% de los usuarios tiene un nivel medio de satisfacción acompañado de un nivel alto, el restante de los usuarios consideran una satisfacción baja.

Debido a que todos los informáticos que se han subcontratado no han jugado un papel eficiente que les resuelva un problema sin que siga manifestando, en algunos casos lo dejan a media y en otras no saben cómo resolverlo, esto ha provocado retraso en las labores diarias y que el usuario no se sienta satisfecho.

Se indagó mediante entrevista que no siempre cumple el plazo, porque el escenario es nuevo para el encargado de informática y que hay problemas que se le dificultan al momento de resolverlo (Ver Anexo 11).

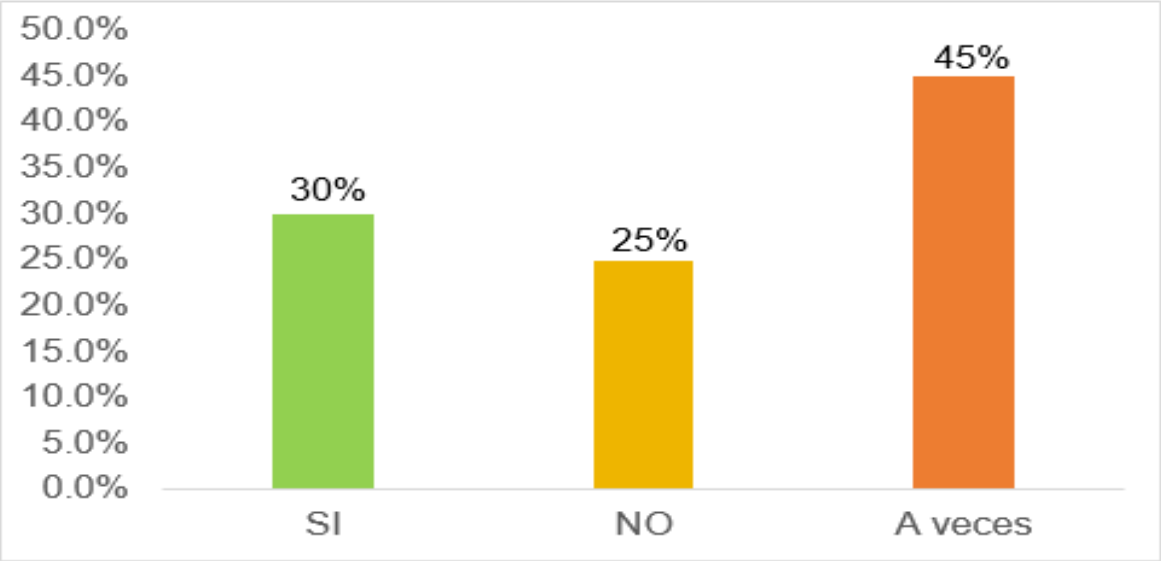


Gráfico 9. Cumplimientos de los plazos acordados

Fuente: resultado de investigación, encuesta realizada a usuarios.

Otro de los ítem evaluados del mismo indicador fue el cumplimiento del plazo que el informático se compromete al resolver un problema (Ver Anexo 8), obteniendo que el 45%, dijo que a veces lo hace, seguido a un 30% que si cumple en un determinado tiempo.

Basado en los resultados obtenido entre el encargado de TI y la mayoría de los usuarios hay una concordancia, por lo que él es un diseñador de la empresa, el cual no tiene los conocimientos necesarios para resolver problemas graves, debería tomar en cuenta que hay problemas que se requiere tiempo y saber el grado de dificultad para comprometerse en un tiempo determinado, por eso es importante que se disponga de una persona calificada para dar respuesta a las necesidades que demanda tanto los medios como los usuarios de este servicio.

Monitoreo y reporte

Se le preguntó al entrevistado del monitoreo y reporte, él manifestó que se le hace monitoreo las 24 horas a los equipos para saber el uso adecuado que le están dando los usuarios, pero que no se le realiza monitoreo a la red (Ver anexo 11).

La infraestructura de red requiere de un monitoreo permanente que permita la supervisión de todos sus componentes, ya que están expuesto a interrupciones de servicios, ataques a los dispositivos, tráficos anómalos o comportamientos dentro de la red, el cual deberían evitar colapsos o saturaciones que puedan poner en riesgo la continuidad de las operaciones. Al implementar un sistema, ayuda a llevar un control constante, donde refleja defectos, anomalías, y un reporte que corrija en tiempo y prevenir futuros inconvenientes que le puedan salir caro.

Se trata del monitoreo continuo del desempeño y la capacidad de los recursos de TI, lo cual sirve para mantener y poner a punto el desempeño actual de TI y para reportar la disponibilidad hacia el negocio del servicio prestado, Isaca (2007).

Plan de continuidad de TI

En cuanto al plan de continuidad de TI el entrevistado explicó que solamente se corrigen los problemas, pero no existe un plan correctivo ni preventivo, tampoco hay un plan de continuidad de los servicios ni un proveedor de internet alternativo (Ver Anexo 11).

Se apreció mediante la observación que no existe documentación del plan de continuidad de TI, tampoco un plan preventivo y correctivo para acciones inesperadas (Ver Anexo 10).

La empresa carece de un plan que les permita sistematizar las acciones ante un problema o prevenirlo antes de que surja, ya que todo lo hacen de forma reactiva, esto es una desventaja que pueden tener consecuencias graves.

Un plan global garantiza el buen funcionamiento y fiabilidad de los equipos informáticos y disminuye los posibles riesgos, el cual permite la rápida

recuperación de la operación y de la información en caso de presentarse algún evento como fallas de hardware o software, que afecte el flujo normal de las actividades.

Según (Isaca, 2007, p. 114), los planes de continuidad de TI son “desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio”.

Recurso critico de TI

Con el entrevistado se consultó sobre los recursos críticos de TI, explicó que no se tienen documentados los recursos críticos de TI (Ver Anexo 11), ni medidas de protección.

No existe una selección de los recursos más importante de la empresa para darle prioridad y protegerlos de cualquier circunstancia, el cual están expuesto a pérdida financiera y de información crítica del negocio. Los recursos críticos de TI son una parte fundamental en la empresa, el cual se debería dividir y distinguir la importancia de cada uno de ellos para dar la especial atención y poder garantizar la seguridad, ya que es un paso para lograr los objetivos de la empresa.

Isaca (2007), cita que la continuidad de los recursos críticos de TI se centra en la atención en los puntos determinados como lo más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.

Entrenamiento del plan de continuidad de TI

Al entrevistado se le preguntó del entrenamiento del plan de continuidad de TI, donde argumentó que los usuarios no reciben capacitación, porque no hay un plan de continuidad de TI (ver Anexo 11).

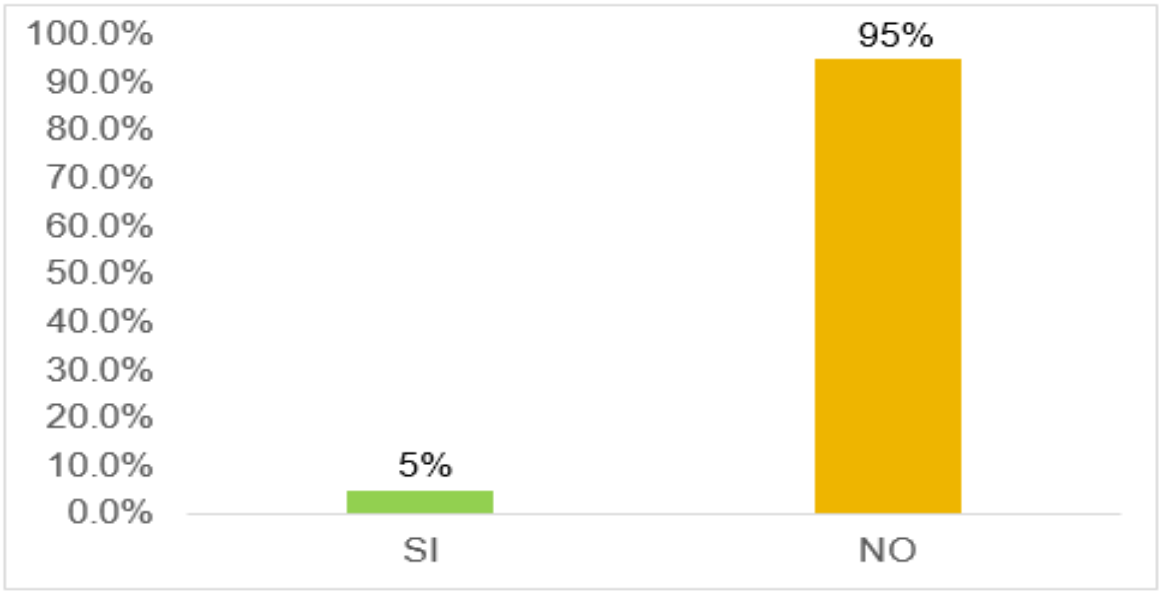


Gráfico 10. Capacitación constante a los usuarios

Fuente: resultado de investigación, encuesta realizada a usuarios.

Se indagó también con los usuarios (Ver Anexo 8), el cual 95% respondieron que no reciben capacitación para garantizar la continuidad de TI.

Según los resultados obtenidos entre el encargado de TI y los usuarios existe una concordancia, por lo que no existe un plan de continuidad de TI para capacitar al personal. El plan permite prevenir, atender y mitigar en caso de que surja un incidente.

Se deberían preocupar por capacitar al personal involucrado de acuerdo a un plan de acción con el propósito de preparar, saber el riesgo que los rodea, cómo enfrentarla y reducir sus efectos.

(Isaca, 2007, p. 114), define que el entrenamiento del plan de continuidad de TI es "asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre".

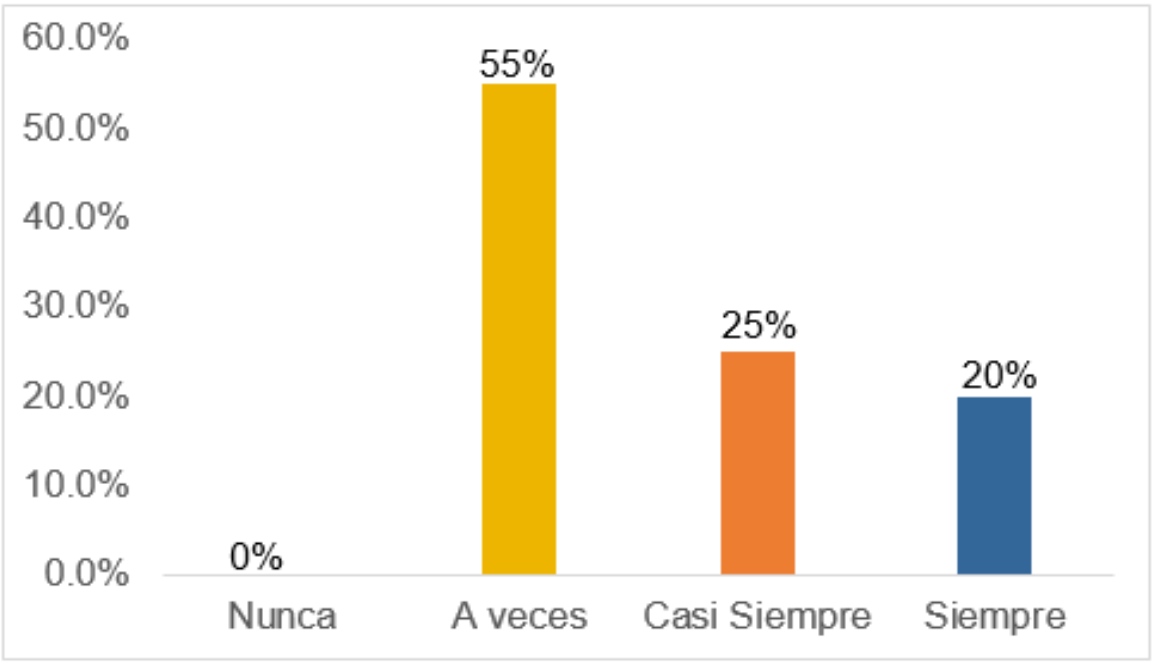


Gráfico 11. Conocimiento o habilidades del encargado de TI

Fuente: resultado de investigación, encuesta realizada a usuarios.

También se averiguó de los conocimientos o habilidades que demuestra el informático al momento de algún problema a los usuarios (Ver Anexo 8), el cual refleja que el 55% a veces cuenta con los conocimientos necesarios y el 25% asegura que casi siempre busca la manera de dar un servicio de calidad.

Se apreció mediante la entrevista que se le realizó al encargado de informática que cuenta con un conocimiento básico acerca de la temática (Ver Anexo 10).

La persona que está ejerciendo el papel de encargado de TI no cuenta con los conocimientos y habilidades suficiente, por esta razón es que ciertos problemas se le dificultan resolverlos en tiempo y forma, y en algunas ocasiones cuando un equipo ya no funciona él solicita al gerente que se debe comprar uno nuevo sin la revisión alguna. Esto implica gastos innecesarios, el cual se podría reparar o darle mantenimiento si lo requiere.

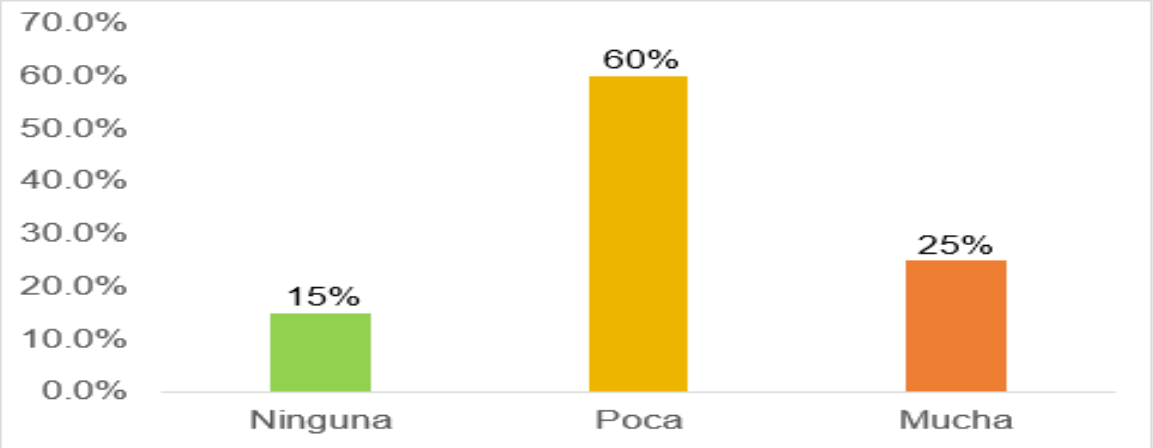


Gráfico 12. Confianza y seguridad para resolver problemas de la red

Fuente: resultado de investigación, encuesta realizada a usuarios.

Finalmente para el indicador se preguntó sobre la atención y capacitación del servicio de TI, se preguntó a los usuarios si les transmite confianza y seguridad (Ver Anexo 8), el 60% manifiesta que es poca la confianza, seguido de un 25% que brinda mucha confianza.

Debido a que es poco tiempo que está ejerciendo el papel de informático, es que no existe mucha confianza, además los usuarios han tenido malas experiencias con el personal que se han subcontratado anteriormente, el cual entre ambas parte no hay un esfuerzo por brindar confianza.

La confianza es un estado de seguridad y optimismo que debería manifestarse en ambas partes para crear un ambiente donde trabajen como equipo eficientemente.

Recuperación y reanudación de los servicios de TI

Se indago mediante entrevista sobre las prioridad de los servicios que deben ser reanudados en el periodo de recuperación de TI, el cual manifestó que no hay porque no se han presentados incidente de esta magnitud (Ver Anexo 11).

No cuentan con la clasificación de los servicios más importante para establecer prioridad, el cual no se preocupan por impedir que una imprevista y grave

interrupción de los servicios de TI de fuerza mayor tenga consecuencias catastróficas para el negocio, ya que no cuentan con el personal apto ni con material para reanudar los servicios lo más pronto posible. La gerencia debería tomar conciencia de la importancia de elaborar una documentación de los servicios más importantes para que estén preparados en caso de que surja un incidente imprevisto y que sean los primordiales para reanudarlos.

(Isaca, 2007, p. 114), especifica que la recuperación y reanudación de los servicios de TI son “planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios”.

Almacenamiento de respaldo fueras de las instalaciones

Siempre con el entrevistado se indagó del almacenamiento de respaldo fuera de las instalaciones, el cual explicó que existe respaldo en disco externos, pero que están dentro de la empresa sin protección alguna solo cuenta con usuario y contraseña para acceder a la información y solo una persona tiene guardado los dispositivos sin ningún contrato establecido (Ver Anexo 11).

Mediante la observación se notó que la persona encargada de llevar los medios de almacenamiento no se encontraba, el cual implica que en caso de un incidente la información no está disponible (Ver Anexo 10).

Según los resultados la empresa no analiza el riesgo que pueden enfrentar antes un incidente, ya que en caso de que ocurra la información puede perderse sin la recuperación alguna, además están expuesta al fracaso por lo que no se cuenta con las medidas de protección necesaria para evitar robos, modificación o daños a la misma.

Los respaldos fuera de las instalaciones son importantes para evitar consecuencias potencialmente graves, además al tener un personal adecuado que administre los respaldos permite que la información esté disponible cuando se requiera.

Hostalia (2012), asegura que si la información es importante o confidencial es necesario tener un backup alternativo en un lugar externo a salvo de robos o desastres naturales.

Plan de seguridad de TI

Se le preguntó al entrevistado del plan de seguridad de TI, el cual argumentó que no existe un plan de seguridad de TI (Ver Anexo 11).

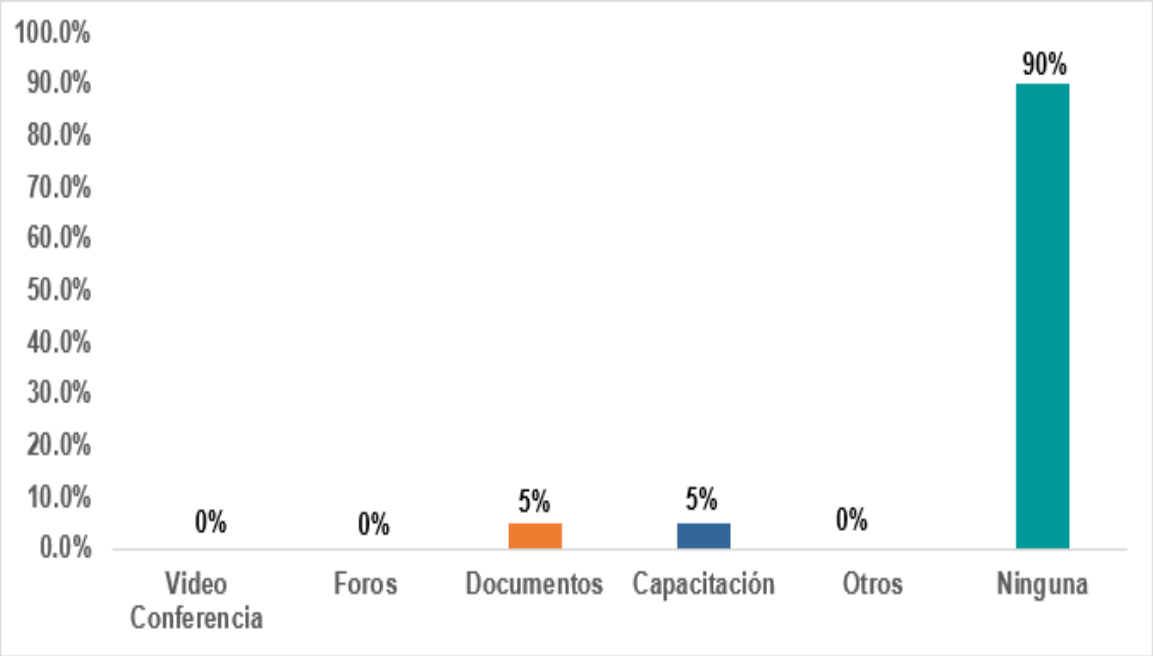


Gráfico 13. El plan de seguridad de TI

Fuente: resultado de investigación, encuesta realizada a usuarios.

Mediante una pregunta de selección múltiple se encuestó a los usuarios de qué manera se les da a conocer sobre el plan de seguridad de TI (Ver Anexo 8), el 90% dijo que no reciben ninguna capacitación acerca del plan y el 5% por medio de capacitación y documentos.

Se notó que tanto el encargado de informática como los usuarios pueden sacar los equipos fuera de la empresa sin control alguno (Ver Anexo 10).

No existe un conjunto de medios administrativos, técnicos y personal que garantice el nivel de seguridad apropiado de los bienes y servicios que presta la empresa, ni existe un análisis de riesgos, el cual están expuestos a amenazas. Por eso se deberán clasificar los recursos críticos más importante de la organización para elaborar un plan de seguridad donde refleje los procedimientos, las responsabilidades de las personas encargadas de cumplir las políticas para prevenir y detectar vulnerabilidades, amenazas y así mitigar que el riesgo no sea mayor.

(Isaca, 2007, p. 118), explica que un plan de seguridad de TI es “trasladar los requerimientos de negocio, riesgo y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad”.

Administración de identidades

Se apreció mediante entrevista que para la administración de identidades utilizan usuario, contraseña y par el correo tiene una llave maestra (Ver Anexo 11).

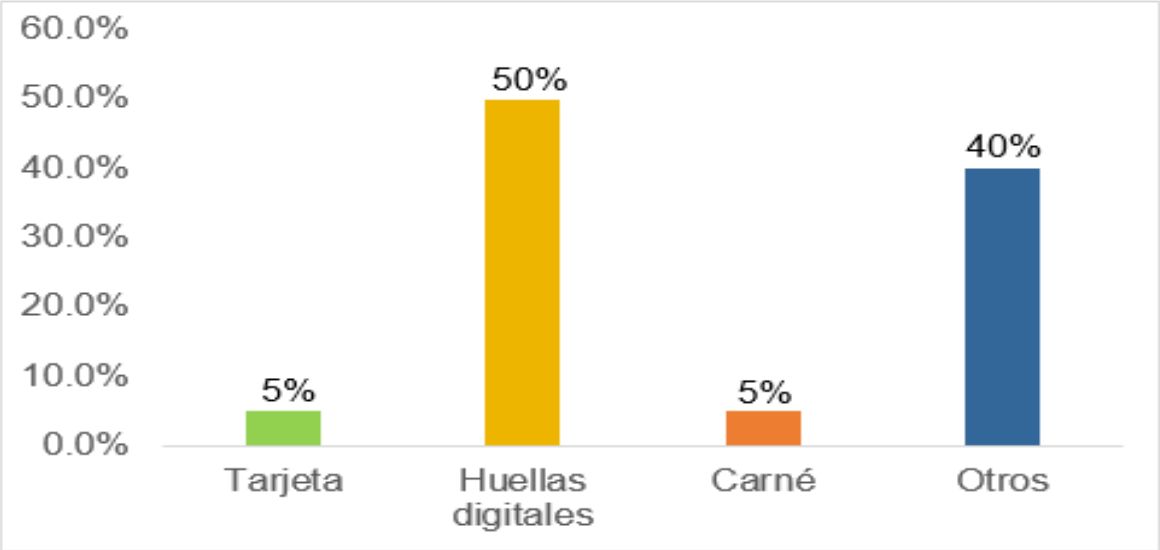


Gráfico 14. Administración de identidades

Fuente: resultado de investigación, encuesta realizada a usuarios.

Igualmente se interrogó a los usuarios (Ver Anexo 8), el cual el 50% dijo que era por medio de huella digitales, seguido a que el 40% dice que es por medio de usuario y contraseña.

Mediante observación se notó, que no hay un equipo donde los usuarios registren su huella digital para poder acceder a las instalaciones, tampoco carné que los identifique, ni mucho menos tarjeta, lo único es el usuario y la contraseña para los equipos (Ver Anexo 10).

En base a los resultados obtenidos la empresa no cuenta con mecanismo de identificación en las diferentes áreas, que minimice el riesgo que terceras personas manipulen o tengan accesos a lugares que no les corresponde.

La empresa debería de mejorar la administración de identidad de todos los usuarios internos y externos para llevar un control de las personas que entran y salen, también realizar monitoreo y generar reportes para que la organización sea segura.

Montoya & Restrepo (2012), define la administración de identidades, como un conjunto de procesos que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales.

Administración de cuentas de usuario

A través de entrevista (Ver Anexo 11) el encargado explicó que no hay un criterio a seguir para gestionar una cuenta de usuario, que en la mayoría de los casos se reasigna equipos con un nuevo usuarios y contraseña, tampoco existe privilegios ni documentación alguna.

Se pudo apreciar que los equipos no cuentan con un administrador, sino que nada más se realiza una cuenta para asignar el equipo (Ver Anexo 10).

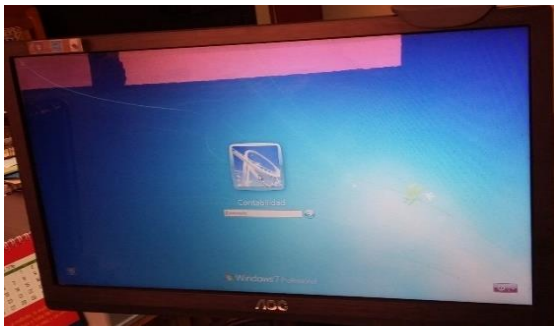


Figura 3. Cuenta de usuario

Fuente: Propia a partir de observaciones realizada en CECOCAFEN.

No se lleva un control para establecer privilegios de cada usuarios, ya que pueden instalar programas, modificar, entre otras actividades que deberían ser restringidas, además no existe un mecanismo que le de baja a un usuario en caso de que deja de ser parte de la empresa, por lo que están expuestos a daños a los equipos, manipulación e infiltración de información.

Según (Isaca, 2007, p. 118), la administración de cuentas del usuario se trata de "garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuarios".

Prevención y corrección de software malicioso

Con el encargado de informática se averiguo sobre los programas que poseen para la identificación y corrección de software malicioso (Ver Anexo 10), donde este manifestó que debido a la carencia de servidores esta actividad no se realiza de forma centralizada sino que se apoyan del antivirus que poseen en cada una de las máquinas, software el cual se mantiene actualizado.

Se notó que no cuentan con programas de calidad para prevenir y corregir software malicioso, el cual están expuesto a spam, virus, entre otros (Ver Anexo 10).

La información y los demás recursos informáticos utilizados en una empresa deberían ser prioridad cuando se trata de seguridad, es por ello que se debe estar atento a aquellos programas maliciosos de origen externo que puedan generar perjuicios. Debido a la inconciencia de la gerencia la red informática está muy vulnerable, lo que a corto o mediano plazo puede significar serios problemas en el desarrollo de las actividades diarias y el desempeño de los equipos, además no hay un interés por adoptar nuevas medidas que ayuden en el control del software malicioso.

Isaca (2007), argumenta sobre poner en práctica medidas preventivas, detectivas y correctivas en toda la organización para proteger los sistemas de la información y a la tecnología contra malware.

Seguridad en la red

El entrevistado expreso que no hay programa de detección ni prevención de intruso, no hay corta fuego, ni segmentada la red (Ver Anexo 10).

La gerencia debería de darle la atención y protección necesaria para garantizar la seguridad de la red, el cual están expuestos a amenazas tanto internas como externas al tener desprotegida la red.

Para (Carracedo, 2011, p. 24), la seguridad de la red es “un conjunto de técnicas que tratan de minimizar la vulnerabilidad de los sistemas o de la información en ellos contenida”.

Repositorio y línea base de configuración

Sobre la línea base de configuración el encargado de TI ha expresado de que de manera formal no existe un repositorio de configuración donde se tengan los datos de los dispositivos de la red, también mencionó que los antiguos encargados de TI se han llevado la información de los routers dejando a la empresa sin ningún tipo

de información sobre sus dispositivos lo que ha provocado reiniciar de fábrica algunos de estos borrando las configuraciones que se tenían (Ver Anexo 10).

Por lo antes expuesto, se considera necesario que el actual encargado de TI elabore un repositorio o documento con las configuraciones de los equipos y que este actué de manera ética sin ninguna mal intención de perjudicar nuevamente a la empresa. Además que, mientras él sea el encargado que se haga responsable de tener respaldo de dicho repositorio y darle seguimiento periódico a estas configuraciones.

(Isaca, 2007, p. 134), afirma que el repositorio y línea base de configuración es "establecer una herramienta de soporte y un repositorio central que contenga toda la información relevante sobre los elementos de configuración, monitorear y grabar todos los activos y los cambios a los activos".

Identificación y clasificación de los problemas

Siempre con el entrevistado se indagó sobre un plan de gestión de riesgos y criterios para su debida clasificación (Ver Anexo 10), donde éste descarto completamente la existencia del plan.

Un riesgo puede suponer una amenaza con distintos grados de afectación sobre cualquier persona o institución siempre y cuando este no se mantenga bajo control, la empresa CECOCAFEN se encuentra muy vulnerable ya que no se tiene un plan de gestión de riesgos que le ayude a clasificar y tomar medidas proactivas o correctivas que ayuden a mitigar la ocurrencia de una situación no deseada que implique afectaciones serias para las actividades y procesos que se realizan en la empresa.

(Isaca, 2007, p. 138), cita que la Identificación y clasificación de problemas es "implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes".

Respaldo y restauración

Siempre hablando de la administración de datos, con el entrevistado se consultó sobre la ejecución de respaldos y restauraciones, los recursos que se realizan respaldo y restauración, las frecuencias de estas tareas y un registro detallado de ellas en una bitácora (Ver Anexo 10), como se mencionó en el apartado anterior se llevan a cabo tareas de respaldo y también agrego que estas se hacen diariamente, las restauraciones las descartó y también menciono la ausencia de una bitácora para estas tareas.

Se observó que tuvieron que restaurar el correo electrónico para la comunicación entre las diferentes áreas (Ver Anexo 10).

Para que la empresa se mantenga a la vanguardia es necesario mantener los datos actualizados y así hacer frente a cualquier eventualidad. Es importante que los respaldos sean probados con cierta periodicidad lo que generara una buena restauración para que todos los procesos fluyan con normalidad, igualmente a estas actividades de respaldo y restauración se les debe dar seguimiento para poder determinar responsabilidades ante cualquier equivocación.

Se trata de definir e implementar procedimiento de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad, Isaca (2007).

Medidas de seguridad físicas

Se le preguntó al entrevistado sobre las medidas de seguridad físicas (Ver Anexo 10), donde manifestó que nada más tienen a un vigilante y cámaras de seguridad.

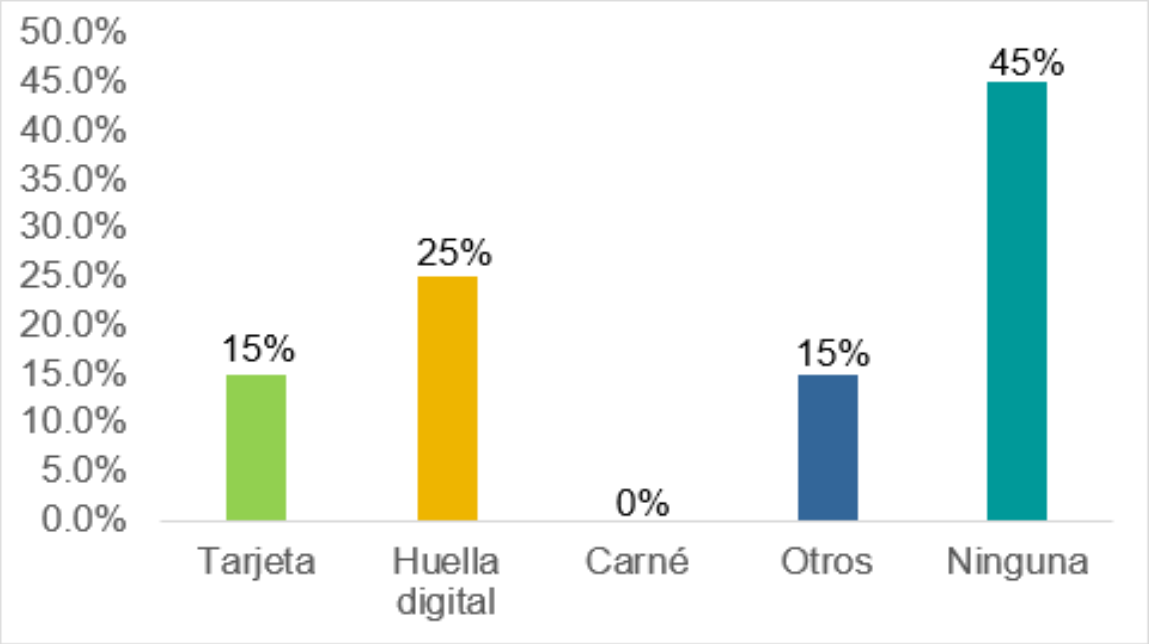


Gráfico 15. Seguridad física de los recursos de TI

Fuente: resultado de investigación, guía de observación.

De igual manera se preguntó sobre las medidas de la seguridad física de los recursos de TI (Ver Anexo 8), encontrándose que el 45% de los usuarios dicen que no existe ninguna medida de seguridad y el 25% lo hacen a través de huellas digitales.

Durante la observación se notó que no hay medidas de protección y salvaguarda que ayude a llevar un control de las personas que entran y salen en las áreas restringidas (Ver Anexo 10).

La empresa no cuenta con mecanismos de prevención ni detección para proteger físicamente los recursos del sistema, ya que están expuesto a riesgo que les puede traer consecuencias graves e incluso ponen en peligro la existencia de la propia organización, por eso deberían de protegerse de las amenazas tanto de la naturaleza, los propios medios como el hombre, es decir, garantizar la seguridad de la infraestructura, recursos y sistemas de TI.

(Isaca, 2007, p. 146), indica que las medidas de seguridad física es “definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio”.

Sobre la rotulación adecuada en las instalaciones, el entrevistado expresó que si existen.

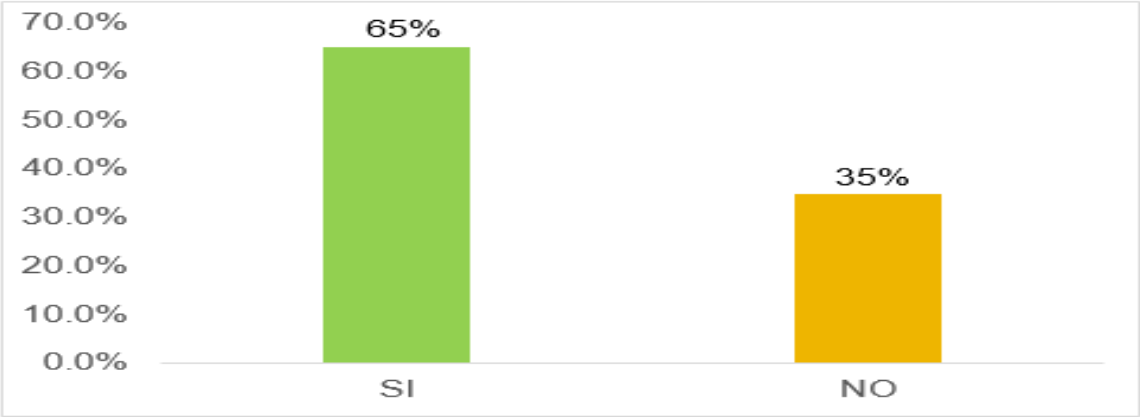


Gráfico 16. Rotulación adecuada en las instalaciones

Fuente: resultado de investigación, encuesta realizada a usuarios.

Se abarcó del indicador de la existencia de la rotulación adecuada en las instalaciones con los usuarios (Ver Anexo 8), el 65% reflejo que si existe.

Se apreció que no existen rotulaciones pertinentes en algunas áreas, de manera que el usuario puede moverse por las instalaciones sin ninguna restricción.

Figura 4. Rotulación

Fuente: Propia a partir de observaciones realizada en CECOCAFEN.

Según los resultados obtenidos entre encargados y usuarios existen una concordancia por lo que ellos creen que son para identificar cada área y las de incendios pero realmente no existen. Esto es un riesgo para la empresa porque debe de restringir el paso a terceras personas y a las que no lo amerita, ya que tiene que ser una medida de protección para evitar robos, peligros laborales entre otros.

Acceso físico

Con el entrevistado se averiguó sobre mecanismos para permitir el acceso físico al centro de datos y el monitoreo de dicha actividad (Ver Anexo 11), este mencionó que cuando los servidores funcionaban solo era una persona la que podía entrar al cuarto, además descartó la existencia de otro tipo de medidas para proteger recursos de TI.

Existen routers que se encuentran en las mismas oficinas donde hay trabajadores lo que puede provocar que estos sean manipulados sin saber el daño que pueden ocasionar.

Las empresas para poder avanzar y lograr desempeñarse dependen en gran medida de la información con la que cuentan y en principio de aquellos procesos y recursos que se encargan de procesarla, es por ello que estos recursos deberían ser considerados valiosos y se debería garantizar medidas de seguridad para protegerlos de cualquier situación y que solo quienes realmente estén autorizados puedan ejercer manipulación sobre ellos.

(Isaca, 2007, p. 146), indica que las medidas de seguridad física son “definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio”.

Protección contra factores ambientales

Con el entrevistado se indagó de la existencia sobre las medidas para controlar factores ambientales (Ver Anexo 11), sin embargo, expresó que no existen medidas, solo extintores en caso de que surja un incidente, el cual se corroboró mediante observación dicha existencia.

Es necesario crear conciencia de los riesgos potenciales que se corren al no ejecutar ningún tipo de medidas contra circunstancias ambientales, igualmente hay que destacar que están expuestos a riesgo no solo recursos materiales sino también humanos, la gerencia debería preocuparse por proteger a todos los recursos existentes y así gestionar medidas que contemple las acciones a realizar cuando ocurra un siniestro.

Para (Isaca, 2007, p. 146), la protección contra factores ambientales es “diseñar e implementar medidas de protección contra factores ambientales”.

Administración de las instalaciones físicas

Se preguntó al entrevistado sobre estándares que rijan la construcción de las instalaciones físicas existentes y estándar para el cableado eléctrico, el cual dijo que no existe ningún tipo de estándar tanto para las instalaciones físicas como estándar para el cableado porque se usa de todo tipo de cable (Ver Anexo 11).

El apoyo en estándares ayuda a evitar problemas de índole legal, igualmente permiten tener edificaciones o estructuras en base a las necesidades de la empresa, también los recursos no se ven expuestos o tan vulnerables a factores ambientales o aquellos que atenten a la salud de los empleados.

Figura 5. Cableado eléctrico

Fuente: Propia a partir de observaciones realizada en SOLCAFE.

Según (Isaca, 2007, p. 146), la administración de instalaciones físicas es "administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud".

Cableado

Con el encargado de informática se indagó sobre el cableado, el cual manifestó que cuentan con cableado estructurado categoría 5, pero los problemas que presentan es que este no puede estar a la intemperie, ya que es muy delicado y a larga distancia no funciona o la red se cae (Ver Anexo 11).

Mediante la observación también se ha podido apreciar que en algunas áreas este cableado está dañado y se encuentra tirado sin ningún tipo de protección lo que permite que este sea manipulado o dañado (Ver Anexo 10).

Figura 6. Cableado estructurado

Fuente: Propia a partir de observaciones realizada en SOLCAFÉ.

Debido a que el cableado de red es el medio de comunicación estándar en la empresa deberían de preocuparse por protegerlo contra factores ambientales, que pueden afectar la comunicación y transmisión de información entre las diferentes áreas, que podrían generar consecuencias negativas en las labores diarias de los usuarios.

(Simbaña, 2010, p. 45), indica que “el cable estructurado es un enfoque sistemático del cableado. Es un método para crear un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, los administradores de red y cualquier otro técnico que trabaje con cables”.

Servidores

Sobre los servidores el encargado de informática argumentó que actualmente no existen servidores porque se dañaron (Ver Anexo 11).

Se ha podido apreciar que la causa del daño fue por el altibajo de la luz eléctrica o falta de mantenimiento, lo cual dañó la tarjeta madre, estos se encuentran tirados, llenos de polvo. La información que se transmite no es confiable, por lo que cada usuario puede hacer modificación (Ver Anexo 10).

Figura 7. Servidores

Fuente: Propia a partir de observaciones realizada en SOLCAFÉ y CECOCAFEN.

Estos equipos son indispensables en la empresa, por lo que son un medio de almacenamiento y procesamiento de toda la información, mejor protección en los sistemas de información, control en los equipos que están conectados a la red, la creación de usuarios para una mejor gestión de carpetas compartidas y permisos, es por eso que deberían contar con servidores donde la información sea confiable, integra y esté disponible, además evitarán pérdida de tiempo al compartir programas y equipos.

(Sierra, 2014, p. 32), explica que “un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al “servicio” de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información”.

Sala de servidores

Se indagó mediante entrevista que actualmente no existe un cuarto de servidor (Ver Anexo 11).

Se pudo notar que no se hicieron estudios del lugar donde estaban los servidores, el cual estaban expuesto a exceso de humedad, al polvo, ruido, sin aire acondicionado y sin las medidas de seguridad adecuadas (Ver Anexo 10).

Figura 8. Sala de servidores

Fuente: Propia a partir de observaciones realizada en SOLCAFÉ.

Un servidor está compuesto de componentes electrónicos que necesitan de una temperatura adecuada y una sala que no tenga polvo que puede tener partículas metálicas que obstruya la ventilación del mismo, provocando problemas de funcionamiento, paradas inesperadas y componentes estropeados. La ubicación es un factor importante que deberían tomar en cuenta, ya que una mala ventilación pueden acortar la vida útil del equipo y un desgaste mucho mayor del que debería tener, además no tiene que estar expuesto a la vista y acceso de cualquier usuario, por lo que contienen datos sustanciales.

Es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento eléctrico (servidores, sistema de almacenamiento de datos, entre otros), con objeto de tener acceso a la información necesaria para sus operaciones, Ferrer (2009).

Estaciones de trabajo

Se le preguntó al entrevistado sobre la existencia de un inventario de los recursos lógicos y físicos de la red, el cual negó la existencia del mismo (Ver Anexo 11).

Se notó que al momento de solicitar el documento de control de los recursos no fue mostrado, por lo que no existe, tampoco existe un control de los privilegios de cada usuarios por lo que tienen acceso a todo (Ver Anexo 10).

Para una buena administración de los recursos de cómputo con los que cuenta la empresa debería ser necesaria la idea de crear un inventario de los equipos con los que se cuenta con el fin de identificar los usuarios correspondientes con cada equipo y las acciones que realiza. Igualmente la creación de cuentas de usuario con privilegios limitados evitara cualquier tipo de situación tal como: daños en el sistema, fuga de información entre otros.

Para (Kons, 2010), es la manera como se encuentran ubicados, teniendo en consideracion la factibilidad de uso de los medios, la velocidad de operación de las maquinas y la precision del trabajo.

Dispositivo intermediario

Siempre con el entrevistado se le preguntó sobre los dispositivos intermediarios, control de estos, funcionalidad y plan de mantenimiento para los mismos (Ver Anexo 11), argumentó que los switch conectan las aplicaciones o sistemas que permiten la señal de internet por cableado y los routers transmite la señal inalámbrica, igualmente no se tiene un control detallado de los mismos y también expresó que no existe ningún plan de mantenimiento para estos.

Mediante la observación se pudo notar que algunos de los dispositivos están a la intemperie, llenos de polvo, pinturas y a simple vista, pueden ser manipulado por cualquier usuario (Ver Anexo 10).

Figura 9. Dispositivos intermediarios

Fuente: Propia a partir de observaciones realizada en SOLCAFÉ, CECOCAFEN y Ahorro y crédito.

Estos dispositivos permiten la expansión de la red y la comunicación entre las diferentes áreas, el cual es importante implementar medidas para su protección y así evitar que sufran daños que puedan afectar las distintas operaciones de la empresa. Además al darle mantenimiento se garantiza la vida útil del equipo y reducir costos innecesarios.

Cuadros (2012), cita que los dispositivos intermediarios proporcionan conectividad y operan detrás de escena, asegurando que los datos fluyan a través de la red. Conectan hosts y varias redes individuales para formar una internetwork.

Direcciones IP

Al entrevistado se le preguntó sobre el control de la IP, utilización de IP dinámicas o estáticas y criterios de cada una de ellas (Ver Anexo 11), el cual manifestó que no existe control de la IP por lo que cualquier dispositivos se puede conectar, también existe IP estática nada más para la persona que lleva la contabilidad para garantizar la seguridad, el resto se conecta de manera dinámica.

Se observó que no existe una documentación de las IP (Ver Anexo 10).

La gestión de las direcciones IP permite que se tenga una visualización de la estructura de la red identificando que recursos utilizan direcciones de manera estáticas o dinámicas, también ayuda al momento de asignar direcciones a nuevos equipos e igualmente garantiza la detección de conflictos entre las mismas.

(CISCO, 2014, p. 2), cita que “una dirección IP es un direccionamiento usado para identificar únicamente un dispositivo en una red del IP”.

Intranet

Se le peguntó al entrevistado sobre la documentación de los usos u objetivos de la red, el cual argumentó que no existe (Ver Anexo 11).

Por falta de conocimiento del encargado de TI y la gerencia no existe una documentación sobre la importancia que juega la intranet en el desempeño de la empresa, lo que podrá ser una desventaja al momento de querer competir con organizaciones del mismo rubro, ya que no se conoce el potencial de esta herramienta o metodología de trabajo.

(Cohen & Asín, 2014, p. 216), afirma que la intranet es “la utilización de la tecnología de hardware y software de internet con un enfoque hacia el interior de la organización es lo que ahora se llama como intranet. Es una red privada que utiliza los protocolos TCP/IP de internet ”.

Topología de red

Sobre la topología de red el entrevistado expreso que no sabe cuál es la topología que cuenta la empresa (Ver Anexo 11).

Se observó que cada cooperativa tiene su propia topología, en Agroindustria, CECOCAFEN y Caja del Norte son de tipo estrella y SOLCAFÉ es estrella extendida, la cual se le debería hacer una documentación tanto de la topología física como lógica (Ver Anexo 10 y 13).

Este tipo de topología que posee la empresa cuenta con inconvenientes, ya que tiene una limitación por lo que no se puede pasar más de 100 mtrs., provocando que en las otras áreas no tengan conexión de internet, además porque requiere de

más cable y dispositivos intermediarios para establecer dicha conexión. Además al poseer una documentación se tiene conocimiento del funcionamiento de la red.

Según (García & Muñoz, 2014, p. 13), la topologia de red “es la representación de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente denominados nodos)”.

Antivirus

Con el entrevistado se indago sobre el tipo de antivirus, la licencia y que beneficios les trae (Ver Anexo 11), el cual manifestó que cuentan con Norton, que la licencia costo $80 dólares que cubre a todas las máquinas y que las maquinas no cuentan con virus porque se actualiza automática.

Se observó que la mayoría de las maquinas tenían virus, ya que se estaba creando una cuenta de usuario fantasma (Ver Anexo 10).

Según los resultados obtenidos la empresa está expuesta a que se modifique o se borre información, ocurran daños a los sistemas como a los equipos mismos, por lo que se debería adquirir un antivirus de calidad para que los equipos estén protegidos ante cualquier amenaza de virus o posibles ataques.

(Mosquera & Restrepo, 2011, p. 27), afirma que un antivirus “es un programa cuya finalidad es prevenir y evitar la infección de virus, impidiendo su propagación”.

Políticas de seguridad

En cuanto a las políticas de seguridad el entrevistado explicó que no hay políticas de seguridad (Ver Anexo 11), mediante observación se confirmó que no existen por lo que no se tiene una documentación que apruebe su existencia.

La entidad debería desarrollar un conjunto de principios y reglas para gestionar la protección de la información, tomando en cuenta todos aquellos aspectos que ponen en peligro la información como medidas técnicas, organizativa, recursos

humanos y seguridad físicas de las instalaciones para garantizar la confidencialidad, integridad y disponibilidad de la misma.

(Benítez, 2013, p. 23), argumenta que las politicas de seguridad es “establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan con los servicios asociados a ellos”.

Análisis de Riesgo

A través de entrevista (Ver Anexo 11) se reflejó que no se realizan auditoría en el área de informática.

Mediante observación en el organigrama está definida el área de auditoria pero el papel que ejercen es en la parte de contabilidad (Ver Anexo 10).

Es importante que la empresa realice un diagnóstico de forma sistemática para detectar el uso de los recursos y el flujo de información, con personal especializado, con el objetivo de salvaguardar el activo empresarial, la integridad de los datos, llevar a cabo eficazmente los fines de la organización y la utilización eficientemente de los recursos para realizar mejoras y logras las metas empresariales, ya que están expuesto a espionajes, perdida de información sin que la gerencia se den cuenta.

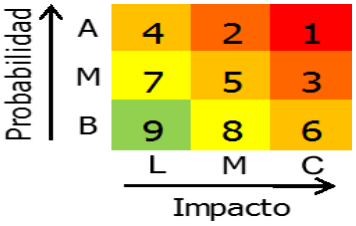
(Mendoza, 2014, p. 51), afirma que el análisis de riesgo es una “metodologías que consisten en la identificación, análisis y evaluación sistemática de la probabilidad que ocurra daños asociados a los factores externos, fallas en los sistemas, la red, entre otros, con la finalidad de controlar o minimizar las consecuencias”.

A continuación se presenta una tabla donde se manifiestan los principales riesgos a los cuales se encuentra vulnerable la empresa. Los riesgos proceden de cada una de las situaciones encontradas, igualmente se presentan los posibles resultados y los síntomas que pueden generar cada uno de los riesgos, cabe

destacar que en algunas situaciones el riesgo puede ser el posible resultado y que algunos riesgos no presentan síntoma alguno.

Para medir el grado de afectación la tabla posee dos campos, uno para definir la probabilidad de ocurrencia del riesgo y otro para definir el impacto del mismo, una vez que se identifiquen estos dos parámetros permitirá definir el nivel de prioridad para la mitigación del riesgo, el cual se asigna mediante una numeración en la escala del 1 al 9, donde menor sea el valor del digito asignado mayor será la atención para dicho riesgo, de igual manera también se asigna un color, todo esto se aprecia en el campo “prioridad” de la tabla.

Para establecer la prioridad de un riesgo, depende de los parámetros asignado de la probabilidad que pueden ser: alto, medio y bajo y los de impacto que son: leve, medio y catastrófico. Una vez definido el grado de probabilidad y el de impacto se tiene que identificar el dígito que coincida con la intersección de las dos opciones seleccionadas, por ejemplo: probabilidad media e impacto medio el valor resultante es 5.



A= Alto **M=** Medio **B=** Bajo

L= Leve **M=** Medio **C=** Catastrófico

Fuente: COBIT 4.1

TABLA DE RIESGOS

N°.	Riesgo	Posibles Resultados	Síntomas	Probabilidad			Impacto			Prioridad
				A	M	B	C	M	L	
1	Mala administración de los recursos y servicios de TI, vulnerabilidad en la infraestructura de la red y la información	Daños en la infraestructura de la red , equipos y manipulación indebida de la información	Quejas de los usurarios por servicios interrumpidos indefinidamente, equipos en mal estado	X			X			1
2	Interrupción en los servicios, suspensión en las labores de la empresa	-	Suspensión en las labores de la empresa	X			X			1
3	Ineficiencia en la realización de las labores en la empresa	Actividades ineficientes	Equipos de trabajos lentos		X			X		5
4	Los usuarios pueden desenfocarse de sus labores diarias	Trabajos ineficientes e ineficaces, ralentización en la comunicación entre las diferentes áreas e intercambio de información	Trafico de red lento	X			X			1
5	Interrupción en la actividades diarias	Quejas de los usuarios del mal funcionamiento de recursos o dispositivos de TI	No existe un sistema UPS, ni planta eléctrica	X			X			1

N°.	Riesgo	Posibles Resultados	Síntomas	Probabilidad			Impacto			Prioridad
				A	M	B	C	M	L	
6	Interrupción de las actividades diarias. Interrupción en los servicios de TI. Daños a los equipos e infraestructura de la red	**-**	Retardo para dar soluciones a problemas. Soluciones ineficaces.	**X**			**X**			**1**
7	Vulnerabilidad en la red	Filtración, espionaje, robo de información	Inestabilidad en los recursos de red	**X**			**X**			**1**
8	Daños a la infraestructura de red e información	Inestabilidad en los sistemas y equipos de trabajos. Pérdida de información.	Perdida o duplicación de archivos Equipos de trabajos lentos	**X**			**X**			**1**
9	Falta de atención para los recursos críticos y la prioridad para los mismos	**-**	Retrasos en los labores diarias, suspensión de los servicios y queja de los usuarios		**X**		**X**			**3**
10	Discontinuidad de los servicios	Retrasos en las labores		**X**			**X**			**1**
11	Pérdida de información critica	Fracaso de la empresa		**X**			**X**			**1**
12	Exposición a pérdida de información o restauración de información inválida	Fracaso de la empresa Toma de decisiones en base a información imprecisa	No se logran los objetivos de la empresa a corto plazo	**X**			**X**			**1**

N°.	Riesgo	Posibles Resultados	Síntomas	Probabilidad			Impacto			Prioridad
				A	M	B	C	M	L	
13	Pérdida de información, de equipos de trabajos y afectaciones al recurso humano	Personal y recursos de TI expuesto a riesgo	Los usuarios no saben cómo proceder ante una determinada situación		**X**		**X**			**3**
14	Daños en los recursos de TI, robo o alteración de información, actividades indebidas	Pérdida de recursos Pérdidas financieras	Uso incorrecto de los recursos, acciones sin autorización	**X**			**X**			**1**
15	Acceso sin autorización a áreas restringidas de la empresa	Daños a recursos e información	-		**X**			**X**		**5**
16	Operaciones indebidas en los sistemas críticos. Daños a los recursos de red	Pérdida en la competitividad del negocio	Información no confiable Carencia de comunicación entre las áreas	**X**			**X**			**1**
17	La red está expuesta a daños e infiltraciones interna y externa	Daños en los recursos lógicos y físicos de la red	Robo y alteración de información	**X**			**X**			**1**
18	Infiltraciones en los sistemas, estaciones de trabajo, servidores y dispositivos intermediarios de la red	Desconfiguración de la infraestructura de red, daño de equipos de red	Ralentización en los equipos, alteración de información	**X**			**X**			**1**
19	Pérdida de configuraciones importantes de la red	Daños e incomunicación indefinida en la infraestructura de la red	Discontinuidad de servicios (Internet)			**X**			**X**	**9**

N°.	Riesgo	Posibles Resultados	Síntomas	Probabilidad			Impacto			Prioridad
				A	M	B	C	M	L	
20	Exposición a incidentes o afectación a los recursos físicos, humanos, entre otros	No se podrían mitigar situaciones en un tiempo especifico	Retraso indefinido para solucionar problemas	**X**			**X**			**1**
21	Información desactualizada en los sistemas Toma de decisiones errónea	Metas y objetivos de la empresa afectados	-	**X**			**X**			**1**
22	Perdida de información	Metas y objetivos de la empresa afectados	**-**							
23	Equipos informáticos expuesto a daño o robo	**-**	No existe medidas físicas	**X**			**X**			**1**
24	Personal expuesto a riesgo contra factores ambientales	**-**	Falta de rotulación importante en algunas áreas o pasillos		**X**		**X**			**3**
25	Vulnerabilidad contra factores ambientales	Exposición a riesgo a los recursos de TI	No hay un estándar para las instalaciones físicas		**X**		**X**			**3**
26	Se puede afectar la comunicación entre las áreas y la suspensión del servicio de internet	-	Algunos equipos quedan incomunicados		**X**			**X**		**5**
27	Se puede afectar la comunicación entre las áreas y la suspensión del servicio de internet	Actividades suspendidas indefinidamente	-		**X**		**X**			**3**
28	Información no confiable, sin actualización, no hay control de los privilegios de los usuarios	Tomas de decisiones erróneas, daños en los equipos	Servidores vulnerables a fallas frecuentes	**X**			**X**			**1**

N°.	Riesgo	Posibles Resultados	Síntomas	Probabilidad			Impacto			Prioridad
				A	M	B	C	M	L	
29	Infraestructura de red expuesto a daños por factores ambientales	Pérdidas económicas e información	Humedad, exceso de ruido, polvo	**X**			**X**			**1**
30	Exposición a daños o manipulación a los servidores	Suspensión de servicios y daños a la infraestructura de red	Personas con acceso cercano al cuarto de servidores	**X**			**X**			**1**
31	Daños a los dispositivos intermediarios	Inversión económicas innecesarios	Fallas en la comunicación o en los servicios		**X**		**X**			**3**
32	Conflicto de acceso a los servicios por mala distribución de las direcciones IP Complejidad para identificar problemas de comunicación en la red	-	No hay acceso a los servicios de red		**X**			**X**		**5**
33	Afectación en las áreas por no identificar dispositivo con mal funcionamiento	No se podría dar solución inmediata a conflicto, ya que no se tiene documentación de la conexión de los dispositivos	Daños a los equipos u otros recursos de la red		**X**		**X**			**3**
34	Pérdidas económicas, daños a la infraestructura	-	Pérdidas de equipos e información, desconexión de equipos, daños en la infraestructura		**X**		**X**			**3**

N°.	Riesgo	Posibles Resultados	Síntomas	Probabilidad			Impacto			Prioridad
				A	M	B	C	M	L	
35	Exposición a sobre voltaje a los equipos	Daños a los equipos, suspensión de las actividades e incendios	Fluctuación en el voltaje de la corriente eléctrica	**X**			**X**			**1**
36	Robo de los recursos informáticos	Pérdidas económicas	-		**X**				**X**	**7**

En la siguiente tabla está definido el nivel de madurez de la empresa, lo cual se realizó mediante la evaluación de los procesos del COBIT. Se evaluaron los dominios: planear y organizar, adquirir e implementar y entrega y dar soporte, para cada uno de ellos se resaltan los respectivos procesos evaluados asignándoles un nivel de madurez en la escala del 0 al 5.

Cada dominio tiene definido el cien por ciento de cumplimiento, el porcentaje obtenido para cada dominio afectará el porcentaje de madurez total que también tiene definido el cien por ciento como máximo de cumplimiento. De igual manera los resultados se pueden apreciar gráficamente.

NIVEL DE MADUREZ

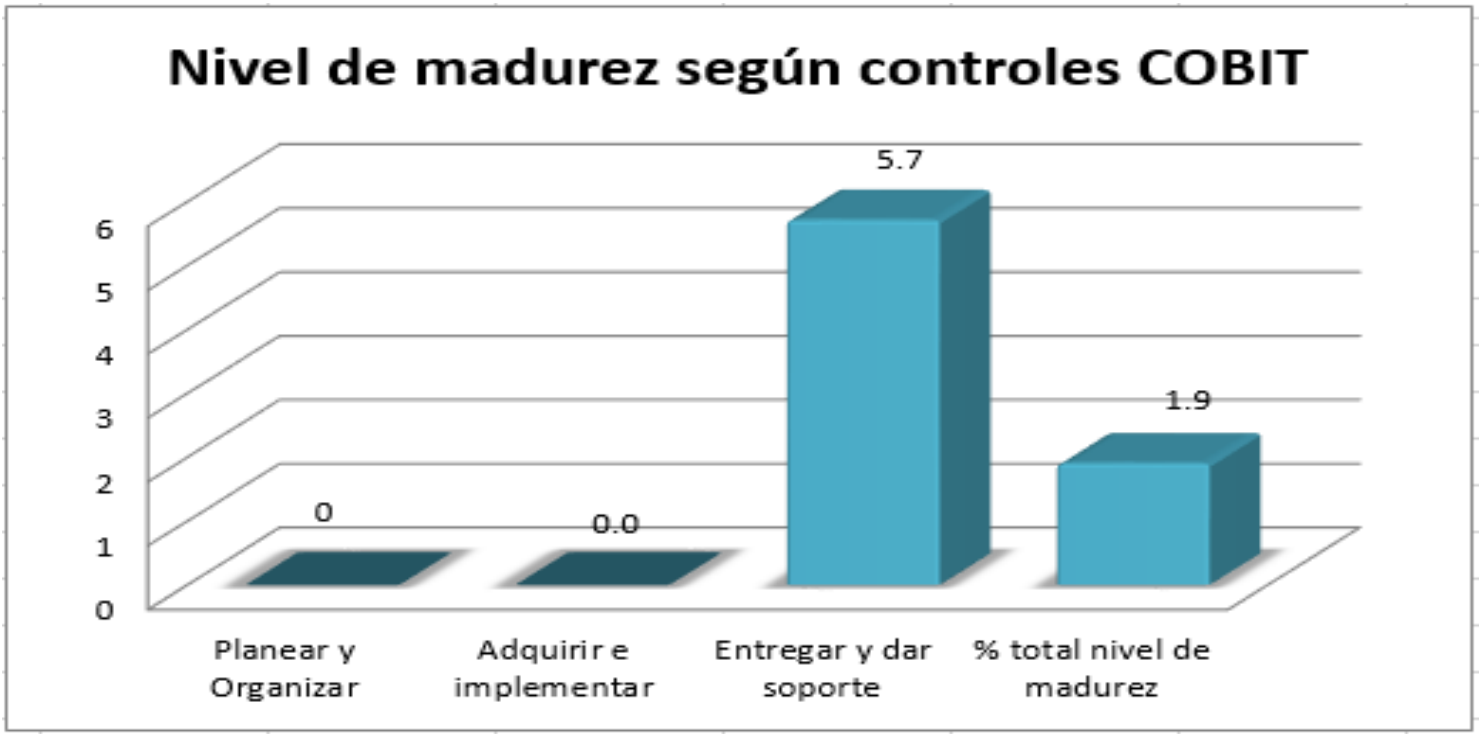
Nivel de madurez de la empresa según objetivos de control COBIT 4.1

Dominio	Procesos	Nivel de madurez	Modelo de madurez
Planear y organizar	PO1 - Definir un plan estratégico de TI.		
	PO2 - Definir la arquitectura de información.		
	PO3 - Determinar la dirección tecnológica.		
	PO4 - Definir los procesos, organización y relaciones de TI.	No existente	0
	PO5 - Administrar la inversión de TI.		
	PO6 - Comunicar las aspiraciones y la dirección de la gerencia.		
	PO7 - Administrar los recursos humanos de TI.		
	PO8 - Administrar la calidad.		
	PO9 - Evaluar y administrar los riesgos de TI.		
	PO10 - Administrar proyectos		
		Total % del dominio	**0.0**
Adquirir e implementar	AI1 - Identificar soluciones automatizadas.		
	AI2 - Adquirir y mantener software aplicativo.		
	AI3 - Adquirir y mantener infraestructura tecnológica.		
	AI4 - Facilitar la operación y el uso.		
	AI5 - Adquirir recursos de TI.		
	AI6 - Administrar cambios.	No existente	0
	AI7 - Instalar y acreditar soluciones y cambios.		
		Total % del dominio	**0.0**
Entregar y dar soporte	DS1 - Definir y administrar los niveles de servicio.		
	DS2 - Administrar los servicios de terceros.		
	DS3 - Administrar el desempeño y la capacidad.	Inicial/ Ad Hoc	1
	DS4 - Garantizar la continuidad del servicio.	No existente	0
	DS5 - Garantizar la seguridad de los sistemas.	No existente	0
	DS6 - Identificar y asignar costos.		
	DS7 - Educar y entrenar a los usuarios.		
	DS8 - Administrar la mesa de servicios y los incidentes.		
	DS9 - Administrar la configuración.	No existente	0
	DS10 - Administrar los problemas.	No existente	0
	DS11 - Administrar los datos.	No existente	0
	DS12 - Administrar el ambiente físico.	Inicial/ Ad Hoc	1
	DS13 - Administrar las operaciones.		
		Total % del dominio	**5.7**
Monitorear y evaluar	ME1 - Monitorear y evaluar el desempeño de TI.		
	ME2 - Monitorear y evaluar el control interno.		
	ME3 - Garantizar el cumplimiento regulatorio.		
	ME4 - Proporcionar gobierno de TI.		
		Total % del dominio	**0**
		% total nivel de madurez	1.9

Escala (0-5)	
No existente	0
Inicial / Ad Hoc	1
Repetible pero no intuitivo	2
Definido	3
Administrable y medible	4
optimizado	5

Resultados	
Planear y Organizar	**0**
Adquirir e implementar	**0.0**
Entregar y dar soporte	**5.7**
% total nivel de madurez	**1.9**

GRÁFICO DEL NIVEL DE MADUREZ



Propuesta para mejorar la infraestructura de la Red LAN, “Empresa CECOCAFEN”

Central de Cooperativas Cafetaleras del Norte

24 de Febrero 2016 - 28 de Abril 2016

Responsables:

Sherly Antonia Blandón

Sbetlana Galdámez Rocha

Lugar y fecha del dictamen: Matagalpa, 28 de abril 2016

24 de febrero del 2016

Ing. Byron Castillo

Encargado de TI de la empresa CECOCAFEN

Matagalpa, Nicaragua

Presentamos el resultado de la evaluación a la infraestructura de red, “Empresa CECOCAFEN” comprendida entre el 24 febrero hasta el 28 de Abril 2016. El reporte incluye conclusiones y opiniones respecto a la evaluación de infraestructura de red realizada. La evaluación fue elaborada de acuerdo al modelo de objetivos de control COBIT 4.1 expedido por ISACA. La evidencia obtenida provee una base razonable para conclusiones y hallazgos referentes a los objetivos de la evaluación.

X

Sherly Blandón
Encargada de la evaluación

TABLA DE CONTENIDO

ÍNDICE DE ANEXO

INTRODUCCIÓN

La presente guía consiste en mejorar la infraestructura de la red LAN de la empresa “CECOCAFEN”, basado en el modelo de objetivo de control COBIT 4.1, lo cual servirá de apoyo para realizar una buena administración a la misma.

La guía contempla las debilidades de acuerdo a los procesos establecidos, los cuales han guiado el dictamen para describir el estatus del ambiente de control interno y conocer el nivel de madurez que se encuentra la empresa. De igual manera se realizó una tabla de riesgo para identificar cuáles son los procesos necesarios de intervención y la tabla de situaciones relevantes para recomendación de forma óptima.

El objetivo de la guía es la resolución de los problemas encontrados que afecta el desempeño de la red, la reestructuración mediante estándar, la seguridad tanto física como lógica, su respectiva documentación y la existencia de una administración adecuada, con el fin de ayudar a mejorar aspectos organizativos y tecnológicos.

RESUMEN EJECUTIVO

Este trabajo consistió en la creación de una guía que sirva para mejorar la infraestructura de red LAN de la empresa “CECOCAFEN”, bajo el modelo de objetivo de control COBIT 4.1, periodo del 24 febrero hasta el 28 de Abril 2016, con el objetivo de evaluar el desempeño de la red.

La presente guía ha sido llevada a cabo acorde a los objetivos específicos propuestos, los cuales han guiado actividades sistemáticas para la obtención de los resultados plasmados. De igual forma se ha utilizado el modelo de objetivo de control COBIT 4.1 emitido por ISACA, el cual permitió encontrar los hallazgos conforme a los procesos establecidos en el modelo, para así valorar y determinar el nivel de madurez en cada uno de los procesos.

Se elaboraron instrumentos para la recolección de evidencia e información relevante y su posterior análisis, los cuales consistieron en entrevistas para el encargado del área de TI, encuesta a los usuarios y observaciones, formato de situaciones encontradas, matriz de riesgos, formato para determinar el porcentaje de nivel de madurez por cada proceso evaluado y a nivel general.

Basados en evidencia sólida y pertinente se remitió a concluir, que el desempeño de la infraestructura de red de la empresa se encuentra en punto donde la prioridad para un mejor rendimiento y desempeño es la administración de los cambios que se realizan, el seguimiento de los mismos y la acreditación de que estos no son los más adecuados frente a las necesidades, el nivel de madurez según los resultados es de **1.9%**, tal y como se muestra en la gráfica, lo que indica un valor bajo, que abre puertas para formar una conciencia en la gerencia y el encargado de TI para mejorar procesos y alinear la infraestructura con las estrategias del negocio.

ALCANCE DEL ESTUDIO REALIZADO

De acuerdo al contrato establecido por parte de la entidad evaluada, se presenta una guía de mejora de la infraestructura de red LAN en la empresa "CECOCAFEN", comprendida entre el 24 febrero al 28 de abril 2016. El alcance consistió en la evaluación de la infraestructura de red como también:

En evaluar:

- El área de TI en el organigrama.
- Cambio de emergencia.
- Seguridad en la red (Monitoreo a la red, programas de detección y protección de intrusos, segmentación de la red, programas cortafuegos, antivirus).
- Hardware los registros de cambio, responsables entre otros aspectos que puedan comprometer la seguridad de los mismos.
- Las instalaciones.
- Plan preventivo, correctivo antes acciones inesperadas.
- Plan de contingencia.
- Plan de continuidad de TI
- Topología física y lógica de la red.
- Estándar para la estructuración del actual cableado eléctrico, cableado estructurado y sala de servidores.
- Mecanismos de respaldos y restauración de información, bitácora.
- Políticas de seguridad.
- Mecanismos para la autorización de acceso físico.
- Gestión de riesgo.
- Factores ambientales.
- Servidores (características y capacidad).
- Rotulaciones pertinentes.
- Administración de identidades, cuentas de usuarios.
- Prevención, detección y corrección de software malicioso.
- Línea de configuración.

OBJETIVOS DE LA GUÍA

General:

Mejorar la infraestructura de la Red LAN, “Empresa CECOCAFEN”, basado en el Modelo de Objetivo de Control COBIT 4.1, periodo 2016.

Específicos:

- Elaborar dictamen del nivel de madurez de la empresa
- Recomendar actividades que mitiguen las problemáticas encontradas
- Mostrar tabla de situaciones relevantes

METODOLOGÍA DE LA GUÍA

Para mejorar la infraestructura de red se determinó el alcance y los objetivos de la guía, se realizó un pre evaluación, que incluyó la obtención y registro de una comprensión de la empresa “CECOCAFEN”, misión, las operaciones y tecnología de apoyo. Se describió las necesidades operacionales, legales, reglamentarias y la infraestructura de TI.

El plan de evaluación incluyo:

Políticas y procedimientos obtenidos y revisados.
Factores críticos de éxito identificados para las operaciones de TI.
Criterios de evaluación identificados así mismo el estado de los controles internos.

El proceso de la guía se realizó basado en COBIT 4.1, el cual es un marco de referencia que sirve para el control y supervisión de las tecnologías de la información.

El COBIT 4.1 consta de 4 dominios:

- Planear y Organizar
- Adquirir e Implementar.
- Entrega y Dar Soporte.
- Monitorear y Evaluar.

De estos 4 dominios solo se tomaron encuentra: **Planear y organizar, Adquirir e implementar y entrega y dar soporte,** el domino Monitorear y evaluar no se incluyó, ya que este engloba la parte de gobierno de TI, el cual es un proceso donde se requiere la participación activa de todas las áreas de la institución.

Según los dominios del COBIT, los procesos contemplados para mejorar fueron:

Planear y Organizar

- Estructura organizacional

Adquirir e Implementar

- Cambio de emergencia.

Entrega y Dar Soporte

- Capacidad y desempeño actual
- Disponibilidad de recursos de TI
- Monitoreo y reporte
- Planes de continuidad de TI

- Recursos críticos de TI
- Entrenamiento del plan de continuidad
- Recuperación y reanudación de los servicios
- Almacenamiento de respaldo fuera de las instalaciones
- Administración de la seguridad de TI
- Plan de seguridad de TI
- Administración de identidad
- Administración de cuentas de usuario
- Prevención, detección y corrección de software malicioso
- Seguridad de la red
- Repositorio y línea de la configuración
- Identificación y clasificación de problemas
- Acuerdos de almacenamientos y conservación
- Respaldo y restauración
- Medidas de seguridad física
- Acceso físico
- Protección contra factores ambientales
- Administración de instalaciones físicas

RESULTADOS Y HALLAZGOS

El propósito de esta sección es para proveer una explicación detallada de los hallazgos, nivel de madurez del proceso evaluado, recomendaciones y datos para las mismas. Estas situaciones se harán basadas en los objetivos de control COBIT 4.1 evaluados. Para definir el nivel de madurez está conformado por no existente: 0, inicial/ Ad Hoc: 1, repetible pero intuitivo: 2, definido: 3, Administrado y medible: 4, Optimizado: 5.

Dominio: Planear organizar
Proceso: PO4, Definir los procesos, Organización y relaciones de TI
Objetivos de control:

- PO4.5 Estructura Organizacional.

Dictamen:
PO4. 0 No existente: Existe un organigrama general de toda la empresa, pero no está definida el área de TI, el cual se subcontrata al personal que brinde servicios informáticos. Aunque es necesario mencionar que este tipo de decisión han puesto en riesgo la información valiosa.

El área de TI carece de independencia, autoridad y adecuada segregación de funciones ante las áreas a las que brinda servicios.

HALLAZGO	RECOMENDACIÓN
No existe un área de TI	Crear el área de TI y que esté bajo el dominio de la gerencia

Dominio: Adquirir e implementar.
Proceso: AI6 Cambio de emergencia.
Objetivos de control:

- AI6.3 Cambio de emergencia.

Dictamen:
AI6. 1 No existente: No existe un proceso formal para la administración de cambios en caso que se requiera, además no cuentan con la disponibilidad del personal ni el material, por lo que no hay conciencia del beneficio de la buena administración de cambios para evitar interrupciones en las operaciones de las diferentes áreas (Ver anexo 39- F=8).

HALLAZGO	RECOMENDACIÓN
No están preparados antes un cambio inesperado	Elaborar un formato de emergencia y establecer las actividades al momento

	de realizar dicha actividad
No cuenta con los equipos ni con el personal para brindar soluciones	Adquirir equipos informáticos en caso de brindar soluciones inmediatas

Dominio: Entrega y dar Soporte
Proceso: DS3 Administrar el desempeño y capacidad.
Objetivos de control:

- DS3.2 Capacidad y desempeño actual.
- DS3.4 Disponibilidad de recurso de TI.
- DS3.5 Monitoreo y reporte.

DS3. 1 Inicial /Ad Hoc: El proceso de planeación del desempeño y la capacidad es informal, por lo que las acciones antes un problema son de forma reactiva, a la larga el desempeño de los recursos TI no será óptimo para satisfacer las necesidades de la empresa, tampoco los equipos están disponible en caso de una interrupción provocando retrasos en los labores diarios, otros de los problemas es el internet, el cual al momento de mandar mensaje o compartir información es lenta o no llega a su destino, no se monitorea tanto la red como los recursos de TI para tener un buen funcionamiento (Ver Anexo 4, 5, 6, 7, 33, 34, 39-F=9).

HALLAZGO	RECOMENDACIÓN
Ralentización al abrir un programa o tener varios al mismo tiempo en algunas áreas	Redistribuir los equipos según el rol de cada usuario
Interrupción en la actividades diarias	Implementar el sistema UPS (Sistema de alimentación ininterrumpida) o una planta eléctrica
Desaprovechamiento del internet (Usuarios descargan música, videos, entre otros)	Redistribuir el ancho de banda según la necesidad de los usuarios.
	Implementar el sistema Ntop para llevar a cabo dicha tarea
Interrupción de las actividades diarias	Elaborar un plan de contingencia con su aprobación, actualización y que se ponga a prueba
Vulnerabilidad en la red	Implementar el sistema Ntop[1] para monitorear la red

[1]**Ntop:** Es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y para ayudar a detectar malas configuraciones de algún equipo. También ordena el tráfico de red de acuerdo con muchos criterios, incluyendo la dirección IP, puerto, protocolo, entre otros.
Para más información ver el link: http://www.ntop.org/products/traffic-analysis/ntop/

Dominio: Entrega y dar Soporte
Proceso: DS4 Garantizar la continuidad de servicio.
Objetivos de control:

- DS4.2 Planes de continuidad de TI.
- DS4.3 Recursos críticos de TI.
- DS4.6 Entrenamiento del plan de continuidad de TI.
- DS4.8 Recuperación y reanudación de los servicios de TI.
- DS4.9 Almacenamiento de respaldo fuera de las instalaciones.

DS4. 0 No existente: No hay conocimiento por la gerencia y el encargado de informática sobre los riesgos, la vulnerabilidad y amenazas en las operaciones de TI, ya que no hay un plan de continuidad que garantice los servicios de TI, tampoco poseen un plan preventivo y correctivo para las acciones inesperadas, un proveedor alterno para los servicios que brinda la empresa, no hay prioridad alguna de los recursos críticos, no tienen establecido las prioridades de los servicios que deben ser reanudados en caso que se requiera, no hay respaldo fuera de la empresa de igual manera no existe un plan de seguridad para los dispositivos de respaldo.

HALLAZGO	RECOMENDACIÓN
Exposición a virus, daños a los equipos e información	Elaborar un plan preventivo y correctivo para acciones inesperadas
Falta de atención para los recursos críticos, retrasos en los labores diarias, suspensión de los servicios y queja de los usuarios	Elaborar un plan de continuidad de TI, actualizarlo y ponerlo a prueba
Discontinuidad de los servicios	Estudiar la posibilidad de tener proveedores alternativos para los servicios brindados por la empresa
Pérdida de información critica	Elaborar un plan de almacenamiento externo de los respaldo
Exposición a pérdida de información o restauración de información invalida	Elaborar un plan de seguridad para los dispositivos de almacenamientos
Falta de conocimiento del personal sobre el plan de continuidad	Elaborar un plan de capacitación

Dominio: Entregar y dar soporte.
Proceso: DS5 garantizar la seguridad de los sistemas.
Objetivos de control:

- DS5.2 Plan de seguridad de TI.
- DS5.3 Administración de identidad.
- DS5.4 Administración de cuenta de usuario.
- DS5.9 Prevención, detección y corrección de software malicioso.
- DS5.10 Seguridad de la red.

DS5. 0 No existente: Hay una total falta de procesos reconocibles de administración de seguridad, el cual no existe un plan para la seguridad de TI ni una administración pertinente que garantice las responsabilidades, tampoco hay privilegio de los usuarios ni documentación, ya que pueden navegar y adquirir información que no les corresponde, además no hay programas de detección ni protección de intruso, no está segmentada la red tampoco existe cortafuego para la seguridad de la red (Ver anexo 8, 24, 25, anexo 43-F=17, anexo 44-F=18).

HALLAZGO	RECOMENDACIÓN
Daños en los recursos de TI, robo o alteración de información, actividades indebidas	Crear, aprobar y poner a prueba políticas de seguridad de TI
Acceso a las diferentes áreas sin identificación alguna	Crear y aplicar medidas de administración de identidad
Acceso indebido a los recursos de la red	Delimitar privilegio por cada usuario
La red está expuesta a daños e infiltraciones interna y externa	Adquirir antivirus de calidad (Kaspersky), Implementar el sistema IDS (Sistema detección de intruso), IPS (Sistema protección de intruso) y firewall
Acceso de información a persona no autorizada, espionaje, entre otras	Segmentar la red

Dominio: Entregar y dar soporte.
Proceso: DS9 Administración de la configuración.
Objetivos de control:

- DS9.1 Repositorio y línea base de configuración.

DS9 0 No existente: La gerencia no valora los beneficios de tener una documentación que sea capaz de administrar y reportar las configuraciones de los dispositivos, ya que en caso de que se quiera cambiar la contraseña de un routers se tiene que resetear, en donde el usuario también tiene el privilegio de configurarlo sin ningún problema.

HALLAZGO	RECOMENDACIÓN
Reinicio constante de los dispositivos (routers)	Elaborar la documentación correspondiente de las configuración de los dispositivos

Dominio: Entregar y dar soporte.
Proceso: DS10 Administración de problema.
Objetivos de control:

- **DS10.1** Identificación y clasificación de problema.

DS10. 0 No existente: No hay conciencia para identificar la causa de un problema, el cual no tienen un plan de gestión de riesgo para identificar las debilidades que le sirva para desarrollar estrategias que minimice o eviten estos riesgo (Ver anexo 44-F=19).

HALLAZGO	RECOMENDACIÓN
Exposición de incidente o desastre a los recursos físicos, humanos, entre otros	Crear, aprobar y poner a prueba un plan de gestión de riesgo

Dominio: Entregar y dar soporte.
Proceso: DS11 Administración de datos.
Objetivos de control:

- DS11.5 Respaldo y restauración.

DS11. **0 No existente:** La calidad y la seguridad de los datos es deficiente por lo que no existe los medios necesarios para respaldar la información, no hay una bitácora de los procesos de respaldo y restauración, ni medidas de protección.

HALLAZGO	RECOMENDACIÓN
Manipulación, modificación y perdida de información	Elaborar un plan de respaldo y restauración de información y realizar bitácora de los procesos que se llevan a cabo

Dominio: Entregar y dar soporte.
Proceso: DS12 Administración de ambiente.
Objetivos de control:

- DS12.2 Medidas de seguridad física.
- DS12.3 Acceso físico.
- DS12.4 Protección contra factores ambientales.
- DS12.5 Administración de instalaciones físicas.

DS12. 1 Inicial / Ad Hoc: No hay conciencia sobre la necesidad de proteger las instalaciones, ya que el personal se puede mover por la misma sin restricción alguna, por lo que no existe un monitoreo de los controles ambientales en las instalaciones o el movimiento del personal, además no cuentan con un estándar para las instalaciones físicas. Pero hay que destacar que cuentan con protección contra fuego (extintores), pero no se protege del polvo, tierra, exceso de calor y humedad (Ver Anexo 9, 10, anexo 45-F=20).

HALLAZGO	RECOMENDACIÓN
Equipos informáticos expuesto a daño	Crear medidas para la seguridad física y mecanismos de autorización al centro de datos
Personal expuesto a riesgo contra factores ambientales	Implementar las rotulación que hacen falta
Vulnerabilidad contra factores ambientales	Estudiar la actual estructura de las edificaciones existente
Equipos con mal funcionamiento o daños, incendios, cortes eléctricos y sobre voltaje (Ver anexo 45-F=21)	Implementar el estándar para el cableado eléctrico IEC 60364-1[2]

Otras situaciones

HALLAZGO	RECOMENDACIÓN
Daños en el cableado de red	Implementar el estándar TIA/IEA 568 B.1[3]
Se desconoce la funcionalidad del cableado de red en la conexión de los equipos	Implementar el estándar TIA/IEA 606 [4]para el etiquetado para el cableado de la red
Información no confiable, sin actualización	Reparar los servidores dañados o gestionar la adquisición para nuevos. Utilizar el sistema CentOs[5] para configurar servidores web y Proxy Squid para que la red sea más segura.
Equipos expuesto a daños por factores ambientales	Realizar estudio para determinar la mejor estructuración del cuarto de servidores y aplicar el estándar TIA/IEA 569 A[6]
Expuesto a daños o manipulación a los servidores	Elaborar, aprobar y poner a pruebas políticas de seguridad a la sala de

[2] IEC (Comisión eléctrica internacional), es una norma para diseñar, desarrollar, inspeccionar o mantener instaciones eléctricas para garantizar la seguridad. Esta norma permite implementar las técnicas y los reglamentos para una instalación correcta.
Para ver más información ver link: http://www.schneider-electric.com.co/documents/News/automation-control/Guia_de_%20diseno_de_instalaciones_electricas_2010.pdf

[3] Estándar para definir los tipos de cables, distancias, conectores, arquitecturas, terminaciones de cables, características de rendimiento, requisitos de instalación de cable y métodos de pruebas de los cables instalados.

[4] Identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios.

[5] CentOS: Es una distribución de LINUX gratuita que está basada en la distribución Red Hat Enterprise Linux (RHEL) y proxy Squid: es un servidor que hace de intermediario entre los PCs de la red y el router de conexión a Internet, puede denegar a web, ftp, email, messenger, entre otras. Para más información ver link: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html

[6] Estándar para que la sala de servidores quede exitosamente diseñada, construida y equipado.
Para ver más información ver link: http://www.revista.unam.mx/vol.5/num5/art28/art28-1c.htm

	servidores
Exposición a daños a los dispositivos intermediarios	Realizar mantenimiento a los dispositivos intermediarios y realizar una bitácora de los mismos.
Crecimiento desmesurado de la red	Elaborar un documento para el control de IP
No existe una visibilidad del funcionamiento y comunicación de la red	Elaborar una documentación de la topología física y lógica de la red
Exposición a robo, manipulación, modificación y daños de información y recursos de red	Crear, aprobar y poner a prueba las políticas de seguridad
Exposición a riesgo de los recursos de TI	Realizar una auditoria informática y asignar a persona apropiadas para dicha realización
Robo de equipos informáticos, no existe control de los activos informáticos	Elaborar un inventario de los recursos
Información no confiable	Realizar una red privada virtual VPN para que diferentes cooperativas estén conectadas y utilizar pfSense [7]para su debida configuración

[7] PFSense: Es una distribución personalizada FreeBSD adaptado para su uso como firewall y routers Verlink : https://alexalvarez0310.wordpress.com/category/portal-cautivo-con-pfsense/instalacion-de-pfsense/

SITUACIONES RELEVANTES

Detalle de las situaciones encontradas

Empresa "CECOCAFEN"
Área de Informática

Situación	Causa	Solución
No existe una área de TI	Falta de conocimiento por parte de la gerencia sobre el área de TI	Crear el área de TI y que este bajo el dominio de la gerencia
No están preparados antes un cambio inesperado	➢ No existe un formato de emergencia ➢ No cuentan con los equipos para brindar soluciones, ni con el personal	➢ Elaborar, aprobación y poner a prueba un formato de emergencia ➢ Adquirir equipos informáticos en caso de brindar soluciones inmediatas
Ralentización al abrir un programa o tener varios al mismo tiempo en algunas áreas	Capacidad limitada en los equipos	Redistribuir los equipos según el rol de cada usuario
Desaprovechamiento del internet (Usuarios descargan música, videos, entre otras)	No existe una administración adecuada del ancho de banda de la empresa	➢ Redistribuir el ancho de banda, según la necesidad de los usuarios ➢ Implementar la herramienta Ntop para llevar a cabo dicha tarea
Interrupción de las actividades diarias	No existe un plan de contingencia ante eventos inesperados	Elaborar un plan de contingencia, con su aprobación, actualización y que se ponga a prueba
Vulnerabilidad en la red	No existe monitoreo en la red	Implementar un sistema como Ntop para monitorear la red, ya que es libre
Exposición a virus, daños a los equipos e información	No existe un plan preventivo y correctivo para acciones inesperadas	Elaborar un plan preventivo y correctivo
Interrupción en la actividades diarias	No existe un sistema UPS o una planta eléctrica	Implementar el sistema UPS (Sistema de

		alimentación ininterrumpida) o una planta eléctrica
Falta de atención para los recursos críticos, retrasos en los labores diarias, suspensión de los servicios y queja de los usuarios	No existe un plan de continuidad de TI	Elaborar un plan de continuidad de TI, actualizarlo y ponerlo a prueba
Discontinuidad de los servicios	No existe proveedores alternativos para los servicios brindados	Estudiar la posibilidad de tener proveedores alternativos para los servicios brindados por la empresa
Pérdida de información critica	No existen copias de los respaldo fuera de la empresa	Elaborar un plan de almacenamiento externo de los respaldo
Exposición a pérdida de información o restauración de información invalida	No existe un plan de seguridad para los dispositivos de almacenamientos	Elaborar un plan de seguridad para los dispositivos de almacenamientos
Falta de conocimiento del personal sobre el plan de continuidad de TI, contingencia, factores ambientales y políticas de seguridad.	No existe un plan de capacitación para el personal	Elaborar un plan de capacitación
Daños en los recursos de TI, robo o alteración de información, actividades indebidas	No existen políticas o normas para garantizar la seguridad de TI	Crear, aprobar y poner a prueba políticas de seguridad de TI
Acceso a las diferentes áreas sin identificación alguna	No cuentan con métodos para administración de identidad	Crear y aplicar medidas de administración de identidad
Acceso indebido a los recursos de la red	No llevan control de los privilegios por cada usuario	Delimitar privilegio por cada usuario
La red está expuesta a daños e infiltraciones interna y externa	No cuentan con programa de identificación y corrección de software malicioso	Adquirir antivirus de calidad (Kaspersky), Implementar el sistema IDS (Sistema detección de intruso), IPS (Sistema protección de intruso) y firewall
Acceso de información a persona no autorizada, espionaje, entre otras	No esta segmentada la red	Segmentar la red, realizar (VLAN)
Reinicio constante de los	No existe documentación de	Elaborar la documentación

dispositivos (routers)	las configuración de los dispositivos	correspondiente de las configuración de los dispositivos
Exposición de incidente o desastre a los recursos físicos, humanos, entre otros	No existe un plan de gestión de riesgo	Crear, aprobar y poner a prueba un plan de gestión de riesgo
Manipulación, modificación y perdida de información	No existe un plan de respaldo y restauración de información de información, ni bitácora de los procesos que se llevan acabo	Elaborar un plan de respaldo y restauración de información y realizar bitácora
Equipos informáticos expuesto a daño	No hay medidas para la seguridad física, ni mecanismos para autorización de acceso físico al centro de datos	Crear medidas para la seguridad física y mecanismos de autorización al centro de datos
Personal expuesto a riesgo contra factores ambientales	No existen rotulación pertinentes en algunas áreas	Implementar las rotulación que hacen falta
Vulnerabilidad contra factores ambientales	No existe un estándar para las instalaciones físicas	Estudiar la actual estructura de las edificaciones existente
Daños en el cableado de red	No existe estándar o norma estructurar el cableado de red	Implementar el estándar TIA/IEA 568 B.1, apartado 4 y 5
Se desconoce la funcionalidad del cableado de red en la conexión de los equipos	No existe estándar para el etiquetado de los cableados de la red	Implementar el estándar TIA/IEA 606
Información no confiable, sin actualización	No existen servidores	Reparar los servidores dañados o gestionar la Adquisición para nuevos. Utilizar el sistema CentOs para configurar servidores web y proxy squid para que la red sea más segura.
Equipos expuesto a daños por factores ambientales	No se realizó estudio sobre la ubicación actual del cuarto de servidores	Realizar estudio para determinar la mejor estructuración del cuarto de servidores y aplicar el estándar TIA/IEA 569 A
Expuesto a daños o manipulación a los servidores	No existe políticas de seguridad para el cuarto de servidores	Elaborar, aprobar y poner a pruebas políticas de seguridad a la sala de servidores
Exposición a daños a los	No se le da mantenimiento a	Realizar mantenimiento a

dispositivos intermediarios	los dispositivos intermediarios, ni bitácoras de los procesos que se llevan a cabo	los dispositivos intermediarios y realizar una bitácora de los mismos.
Crecimiento desmesurado de la red	No se llevan una documentación para el control de las IP	Elaborar un documento para el control de IP
No existe una visibilidad del funcionamiento y comunicación de la red	No existe documentación de la topología física y lógica de la red	Elaborar una documentación de la topología física y lógica de la red e implementar el estándar TIA/IEA 606
Exposición a robo, manipulación, modificación y daños de información y recursos de red	No existen políticas de seguridad	Crear, aprobar y poner a prueba las políticas de seguridad
Equipos con mal funcionamiento o daños, incendios, cortes eléctricos y sobre voltaje	No existe estándar para el cableado eléctrico	Implementar el estándar para el cableado eléctrico IEC 60364-1
Robo de equipos informáticos, no existe control de los activos informáticos	No existe un inventario de los recursos físicos y lógicos	Elaborar un inventario de los recursos

Elaborado por (Nombre y Firma)

Aprobado por (Nombre y Firma)

CONCLUSIONES

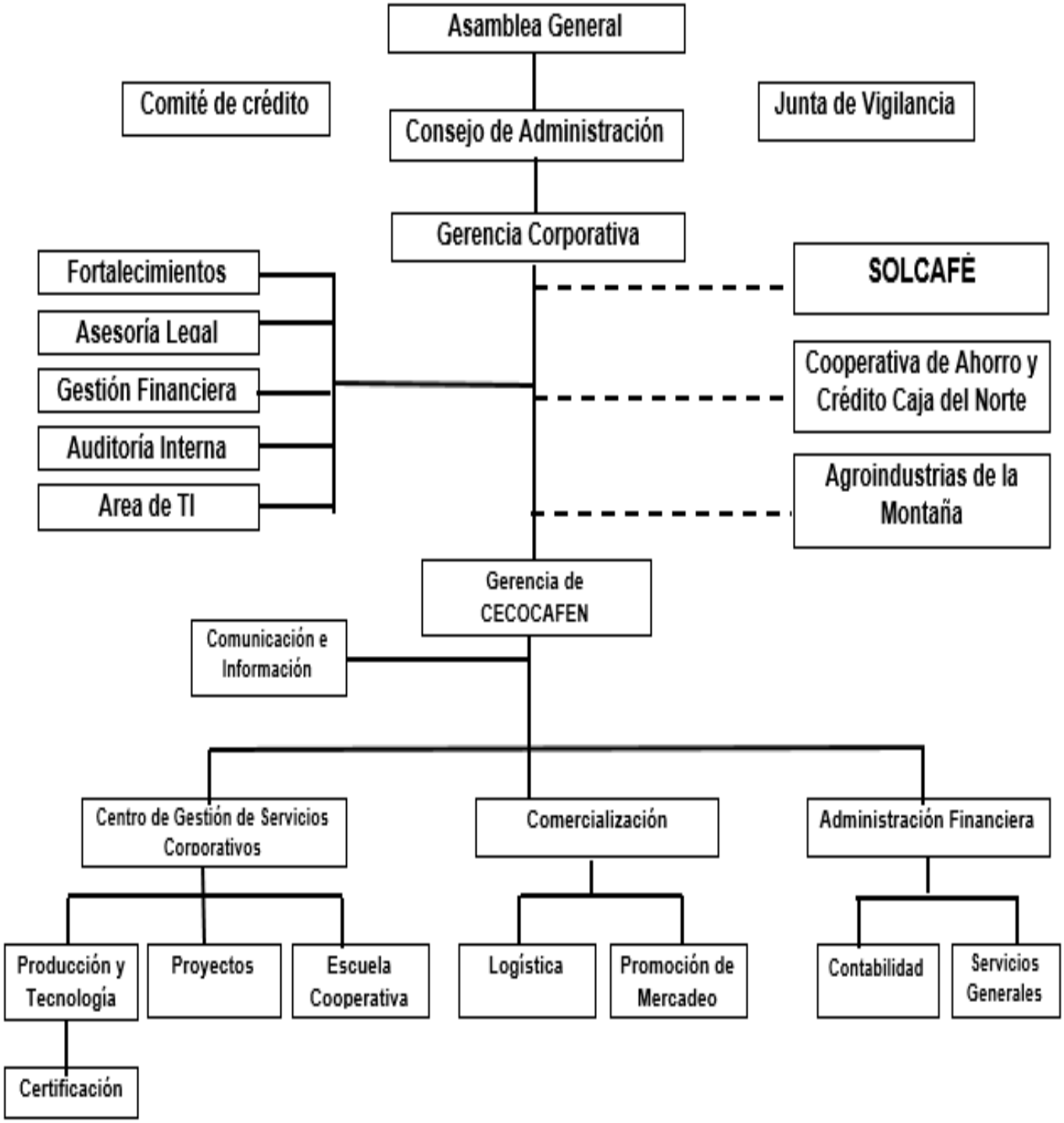
COBIT 4.1 (Objetivo de control para tecnología de información y tecnología relacionada), es un modelo de evaluación y monitoreo que enfatiza el control de la empresa y la seguridad de la misma, además provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

El dictamen permitió conocer el nivel de madurez donde se obtuvo el 1.9% del nivel de los procesos, lo cual indica que la empresa está expuesta a riesgos que a mediano plazo afectara las operaciones de la empresa y a los recursos de TI. Se realizó una tabla de riesgo donde los resultados reflejaron que la mayoría de los problemas que presentan requieren de atención inmediata, para garantizar la optimización de los procesos y los recursos de TI.

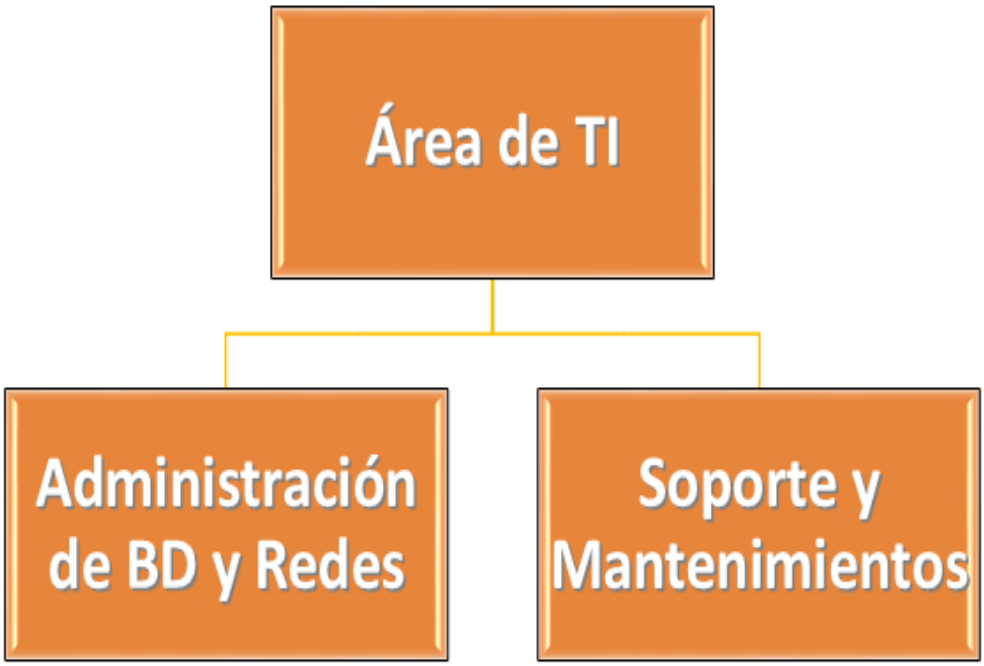
Además se realizó una tabla de situaciones relevantes para dar a conocer los principales problemas para priorizarlos al momento de aplicar mejoras y así ayude a lograr los objetivos y metas de la empresa. El beneficio de esta guía es para orientar a la gerencia de unas series de recomendaciones para cada uno de los problemas que presenta la red y así controlar y gestionar de una manera factible los recursos de TI.

Anexos

Anexo N° 1 Organigrama propuesto

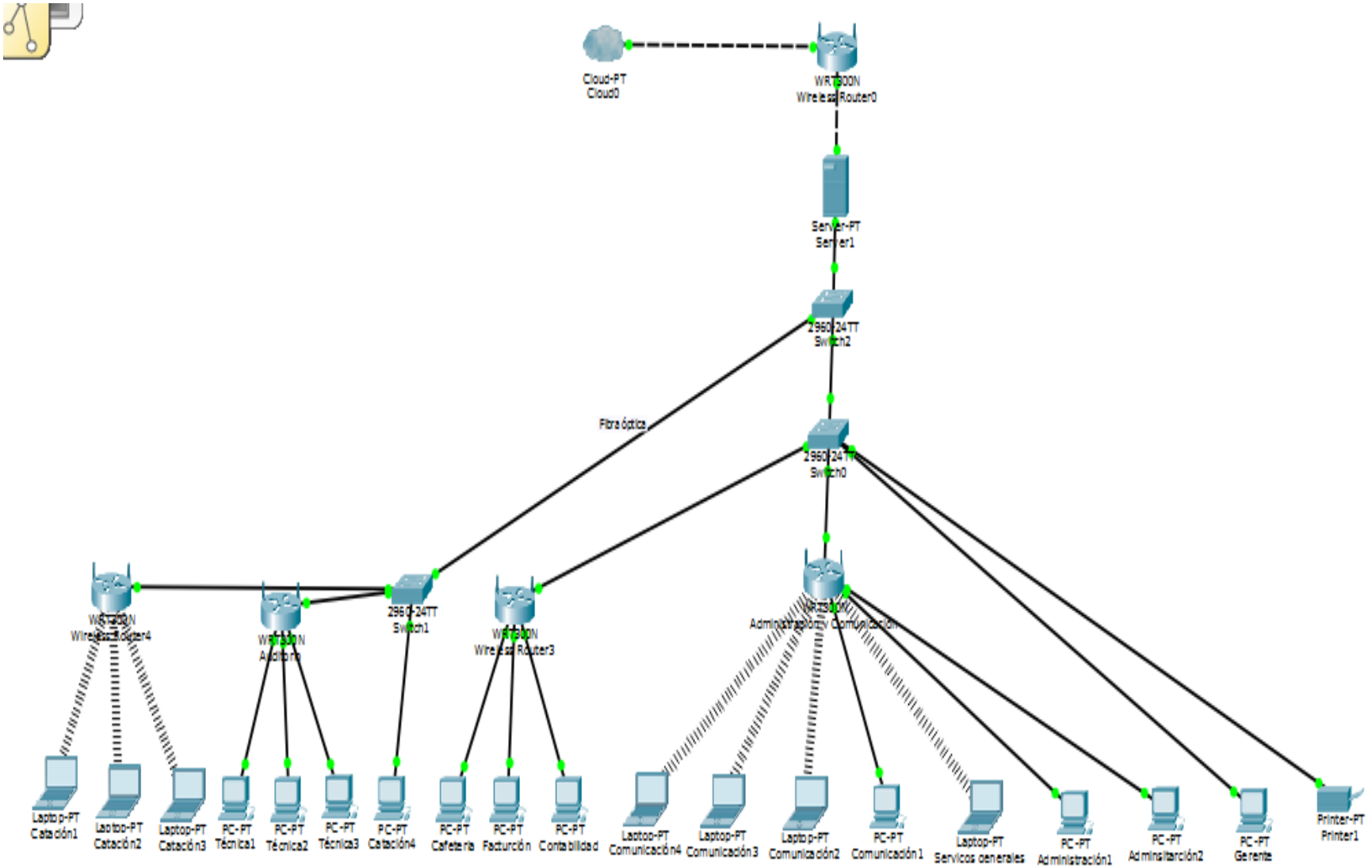


Anexo N° 2 Estructura propuesta del área de TI

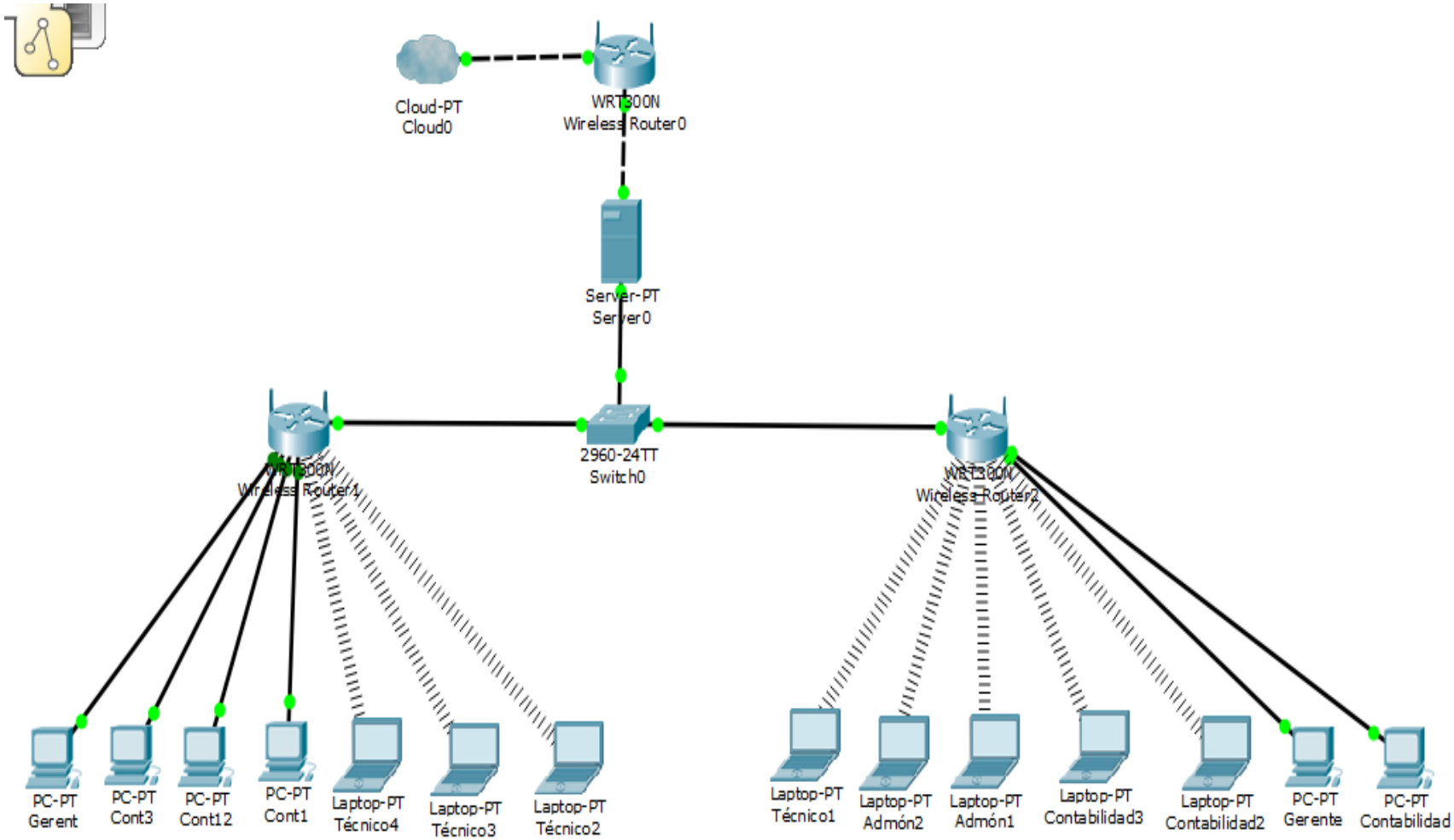


Cargo	Perfil
Administrador de BD y Redes	Ingeniero en Sistemas o Ingeniero en Informática
Soporte y Mantenimientos	Técnico en Mantenimiento

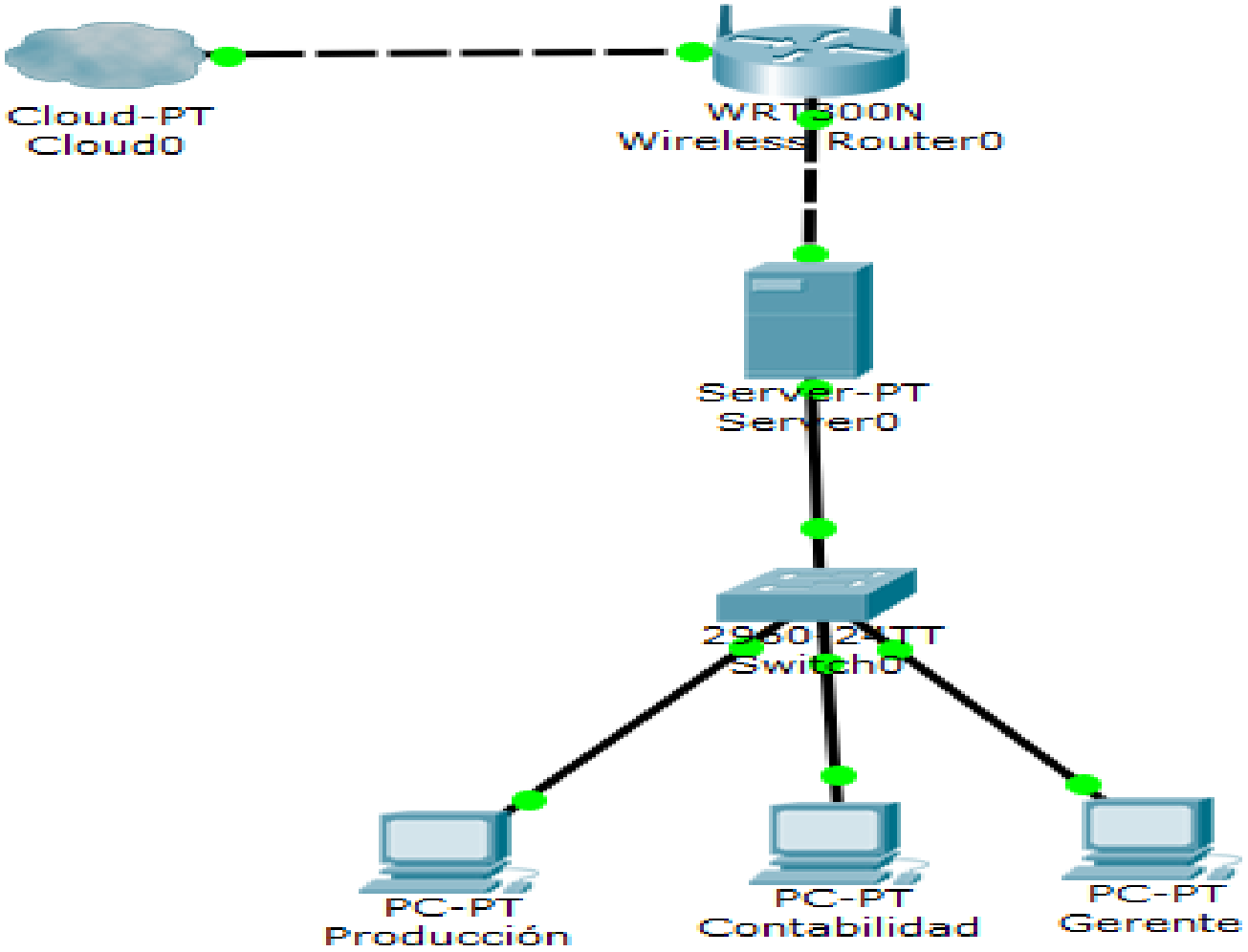
Anexo N° 3 Topología lógica propuesta SOLCAFÉ



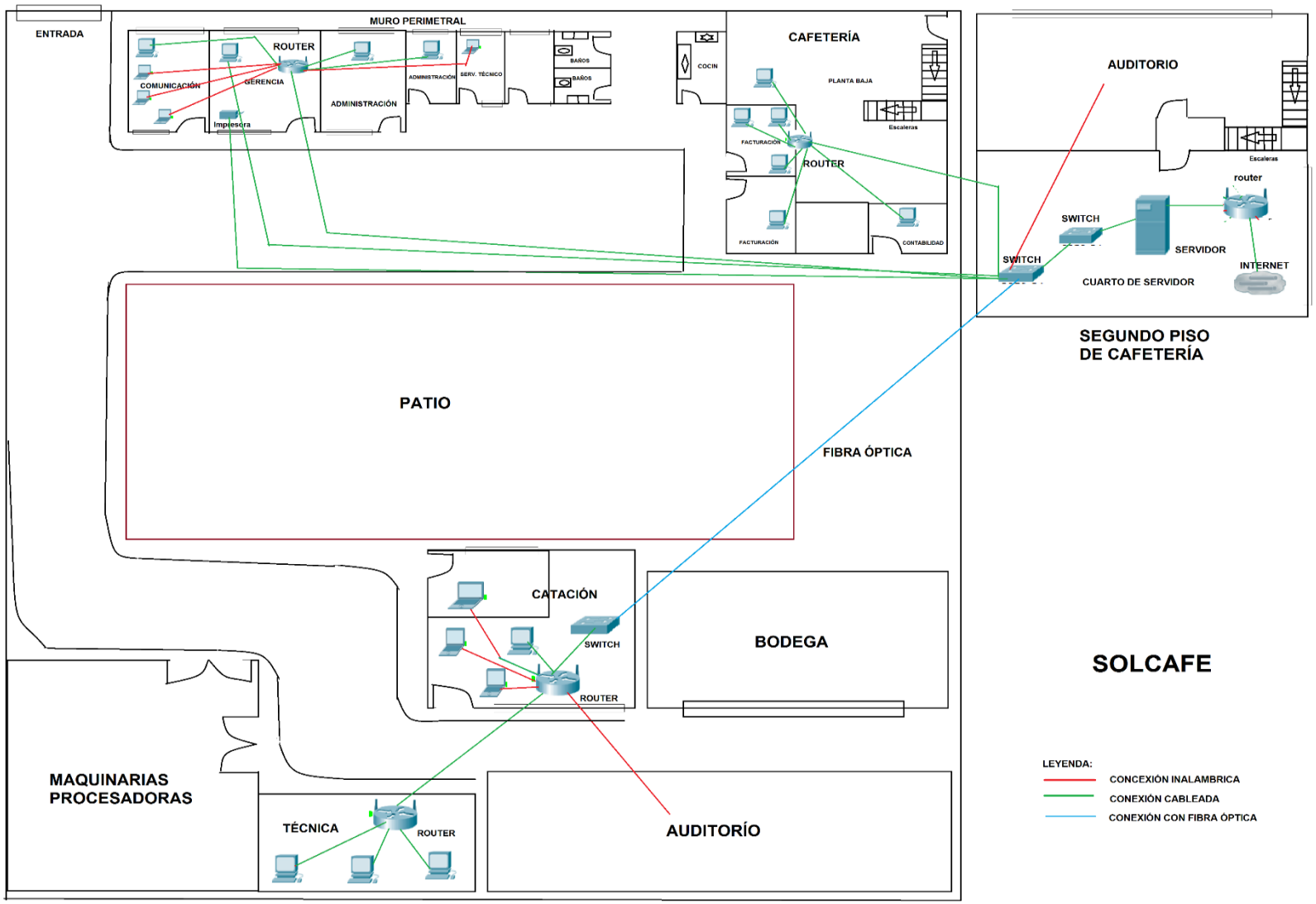
Anexo N° 4 Topología lógica propuesta CECOCAFEN y Ahorro y crédito



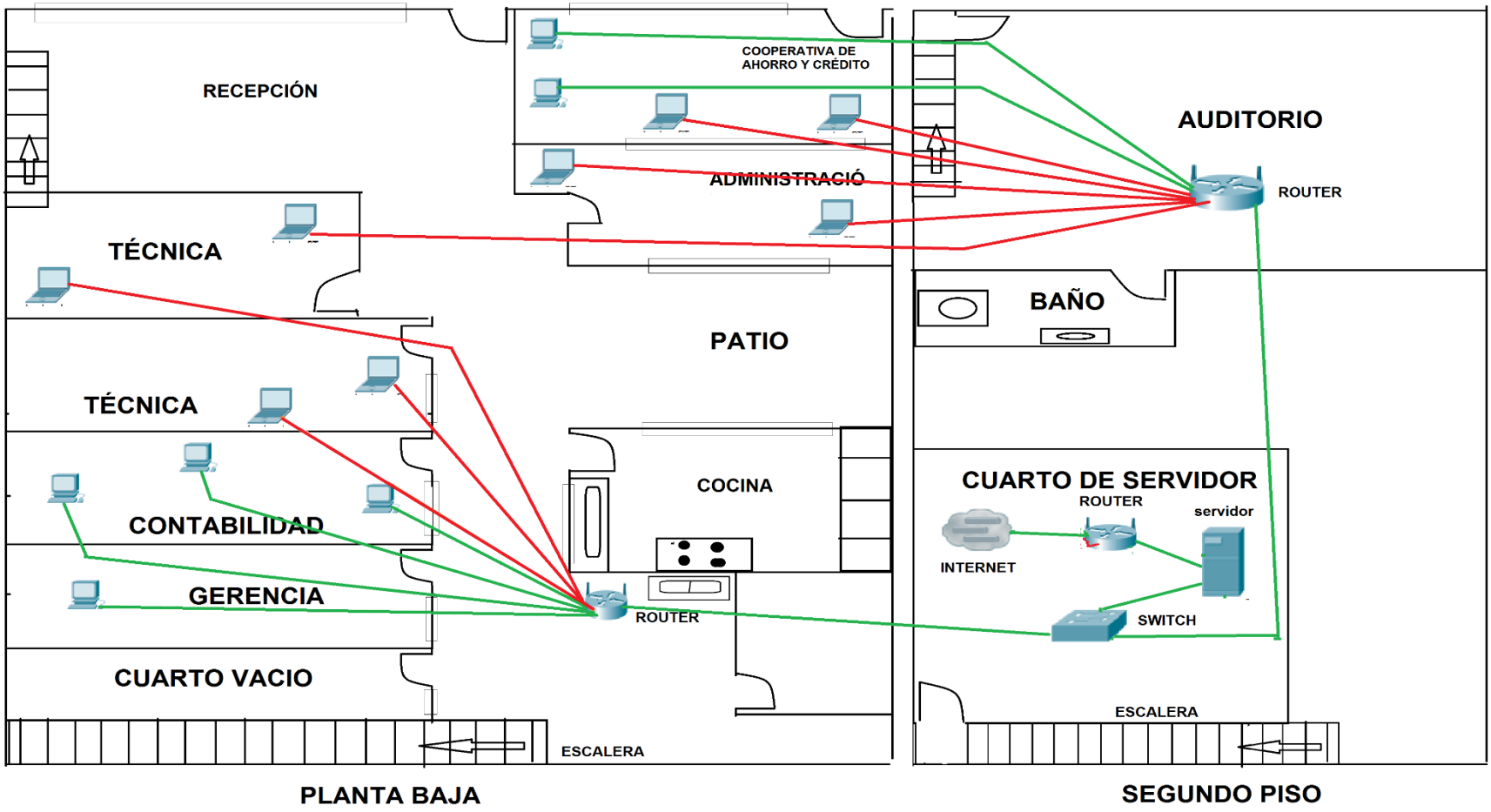
Anexo N° 5 Topología lógica propuesta Agroindustria



Anexo N° 6 Topología física propuesta SOLCAFÉ



Anexo N° 7 Topología Física propuesta CECOCAFEN y Ahorro y crédito



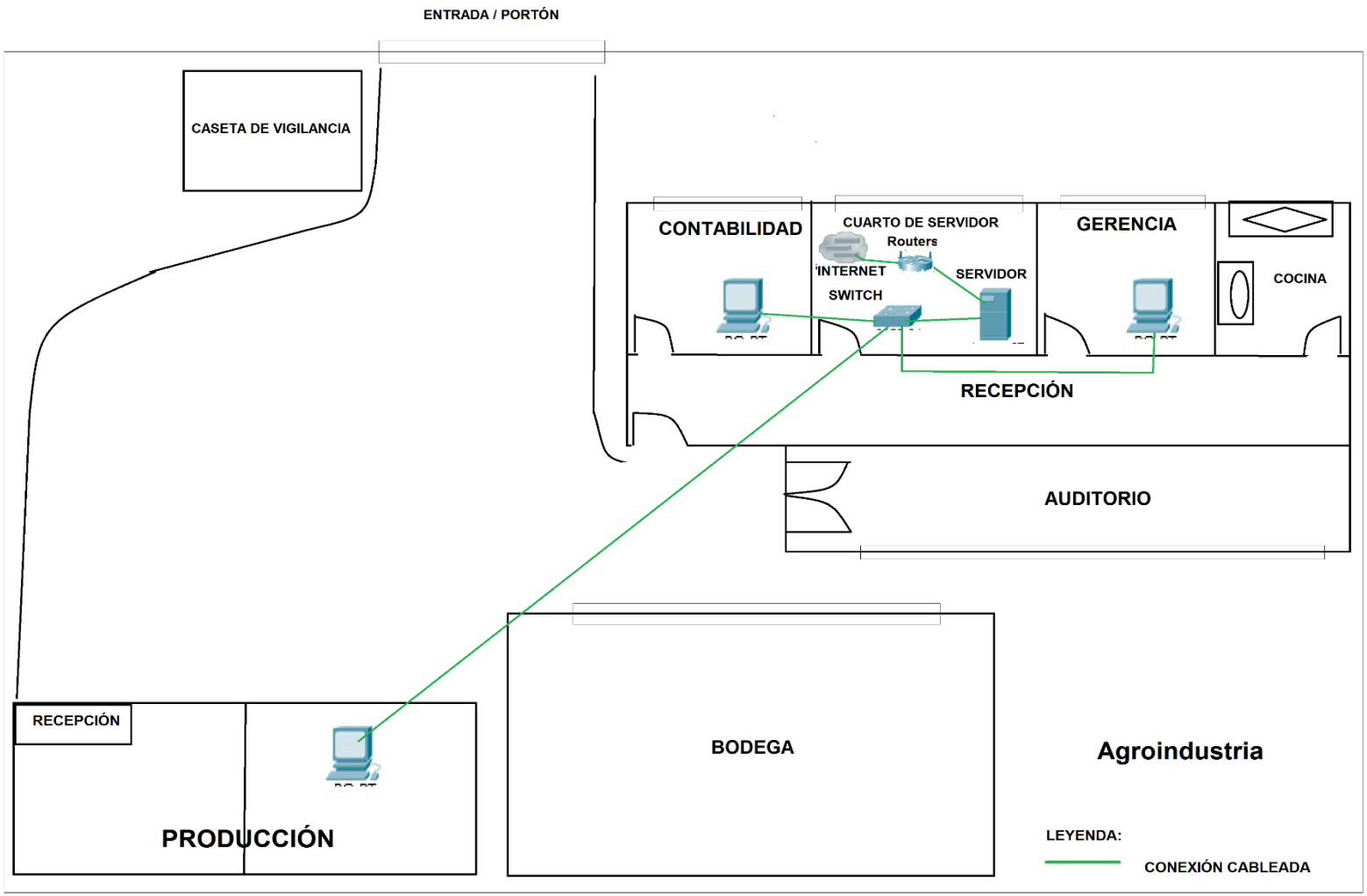
CECOCAFEN

LEYENDA:

CONCEXIÓN INALAMBRICA

CONEXIÓN CABLEADA

Anexo N° 8 Topología Física propuesta Agroindustria



IX. CONCLUSIONES

Según los resultados de la evaluación de la Infraestructura de la Red LAN en la empresa “CECOCAFEN”, basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, periodo 2016 se concluyó lo siguiente:

- Los procesos que se llevan actual en la red son: la gestión de la base de datos contable de la empresa, comunicación vía correo electrónico mediante un dominio de la empresa, gestión de información de las actividades y el servicio de página web. También no existe una administración que garantice la seguridad en los recursos internos y la red informática.
- Basados en los procesos del modelo COBIT se identificaron problemáticas como: la ausencia de un área de informática, la carencia de evaluación de la capacidad de los recursos de TI, la ausencia de un plan de continuidad de los servicios, la posible pérdida o ineficacia de la información, exposición y vulnerabilidad, ya que no se cuentan con un plan de gestión de riesgos, políticas de seguridad y otro tipos de afectaciones como las medidas de protección ambiental.
- Se determinó el grado de afectación de las problemáticas, mediante la evaluación de los procesos COBIT, el cual arrojó que la empresa posee el 1.9% de nivel de madurez en sus procesos, lo que explica las situaciones que se han descrito y que a mediano o largo plazo afectaran los recursos de TI y las operaciones de la empresa.
- A partir de los resultados obtenidos se elaboró una propuesta en la cual están reflejadas todas las situaciones basadas en los procesos del COBIT y que son consideradas riesgosas para la empresa, así mismo se plasman las recomendaciones pertinentes. De igual forma se plantean ideas alternativas en cuanto a la reestructuración orgánica de la empresa pensando en el aporte fundamental de un área de TI para la empresa.

También se propone un nuevo esquema de la estructuración de la red LAN tanto física como lógica.

X. RECOMENDACIONES

Para mejorar el rendimiento de la red, el grado de madurez y la seguridad de la empresa CECOCAFEN se recomienda:

A la gerencia:

- Utilizar como referencia la guía propuesta, con el fin de conocer el grado de madurez de la empresa en el ámbito informático.
- A partir de las incidencias reflejadas en la guía pueda implementar las mejoras pertinentes que optimicen los procesos de la red, llevar un mejor control de distribución de los equipos y mitigar lo más que se pueda amenazas y vulnerabilidades que afecten la integridad y funcionalidad de la red.
- Tenga conocimiento sobre la importancia de un área informática con el fin de controlar y garantizar la eficiencia y eficacia en los procesos críticos que se apoyan en la tecnología de la empresa.
- Implementar estándares para la estructuración de la red y documentación de la misma.

XI. BIBLIOGRAFÍA

Alfano, C. (2010). *Estructura, características y uso cableado de par trenzado.* Argentina.

Álvarez, L. (2005). *Seguridad Informática (Seguridad en Redes).* México.

Arias, P. (2015). *Qué es un servidor FTP.*

Ariganello, E. (2014). *Redes Cisco, Guía de estudio para la certificación.* España: RA-MA.

Benítez, M. (2013). *Gestión integral.*

Bongiovanni, A. (2008). *Virus y Antivirus.* Argentina.

Brotons, E. (2013). *Servidor Proxy.*

Bueno, A. (2011). *Redes Informáticas.*

Callay, D., & Sánchez, L. (2012). *Auditoría informática a los servicios de red de Transelectric.* Ecuador.

Carracedo, J. (2011). *Introducción a la seguridad .* España.

Castelán, E. (2011). *Topologías de red.* México.

Cisco. (25 de Diciembre de 2014). *Direccionamiento de IP y conexión en subredes para los usuarios nuevos.* Obtenido de Cisco: http://www.cisco.com/cisco/web/support/LA/102/1025/1025418_3.pdf

Cohen, D., & Asín, E. (2014). *Tecnologías de la información. Estrategias y transformación en los negocios.* México: MC Graw Hill.

Correa, J. (2011). *Manual de políticas y estándares en seguridad informática.* Colombia.

Cuadros, M. (2012). *Tecnología en gestión de redes de datos.* México.

Cuesta, A., Cumanda, N., Japa, T., & Fernando, A. (2010). *Auditoría física y lógica a las redes de comunicaciones de computadores de la fábrica Pasamanería S.A.* Ecuador.

Delgado, A. (2011). La intranet en la organización, evaluación del conocimiento. *Revista Avanzada Científica*, 11.

Díaz, G. (2007). *Redes de Computadoras Introducción Arquitectura de Redes.* Venezuela.

Díaz, Y. (2012). *Usuarios y perfiles.*

Ferrer, J. (2009). *Centro de procesos de datos: el cerebro de nuestra sociedad.*

Ferrer, R. (2007). *Metodología de análisis de riesgo.* Colombia.

García, J. (2012). *UT-04 Instalaciones y Configuraciones de Servidores Proxy.*

García, J., & Muñoz, M. (2014). *Propuesta de implementación de comunicación unificadas con la integración de telefonía IP en la empresa TECPROTEL.* México.

Hernández, P. (2010). *Perfil de usuario.*

Hernández, R., Fernández, C., & Baptistas, M. (2010). *Metodología de investigación.* México: McGRAW - WHILL.

Hostalia. (18 de Septiembre de 2012). *Decálogo de buenas prácticas a la hora de realizar un backup.* Obtenido de Hostalia: http://pressroom.hostalia.com/wp-content/themes/hostalia_pressroom/images/whitepaper-Hostalia-backup2.pdf

Isaca. (2007). *Knowledge Center/COBIT 4.1 .* Obtenido de ISACA: http://www.isaca.org/knowledge-center/cobit/pages/downloads.aspx

Kons, S. (2010). *Diseño físico de las estación de trabajo.*

Lara, E. (2010). *Protocolo HTTP y servidores web.*

López, J. (2016). *¿Qué es un antivirus?* México.

Martínez, A., & Reyna, F. (2012). *Arquitecturas de red.*

Matutes, M., & Quispe, T. (2006). *Auditoría de la gestión de seguridad en la red de datos del Swissotel basado en Cobit.* Ecuador.

Mendoza, K. (2014). *Análisis de riesgos.* México.

Mendoza, L. (2012). *Evaluación de la red de computadores de UNAN Managua, FAREM Matagalpa.* Matagalpa.

Montoya, J., & Restrepo, Z. (2012). Gestión de identidades y control de acceso desde una perspectiva organizacional. *Ing. USBMed*, 23-34.

Mosquera, A., & Restrepo, A. (2011). *Los antivirus y sus tendencias futuras.* Colombia.

Pardo, V. (2009). *Sistema de gestión en servicios de TI.* Uruguay-América del sur.

Peña, J. (2005). *Cobit aplicado para asegurar la continuidad de las operaciones.*

Peña, J. (2014). *Comunicación a través de la red, dispositivos finales, dispositivos intermediarios, elementos de una red.*

Poó, J. (2010). *Cableado de Red de datos y telefonía.* España.

Sánchez, A. (2010). *Servidores web.*

Sánchez, J. (2012). *Sevidores de aplicaciones web.* Colombia.

Sánchez, V. (2013). *Servidores proxy.* España.

Santa Maria, F. (2012). *Buenas prácticas para auditar redes inálambricas aplicadas a las empresas del rubro hotelero de la ciudad de chiclayo.* Chiclayo.

Sequeria, V., & Cruz, A. (2009). *Investigación es fácil I manual de investigación .* Managua, Nicaragua: Grisell Remigio Hernández.

Sierra, M. (2014). *¿Qué es un servidor y cuales son los principales tipos de servidores? (Proxy, DNS, WEB, FTP, SMTP, ETC.).*

Simbaña, P. (Noviembre de 2010). *Análisis, diseño del cableado estructurado y propuesta de implementacion en la ilustre municipalidad del cantón sucúa.* Cuenca.

Torres, M. (2008). *Desarrollo de la Estructura Organizacional de un Área Académica de ciencias de la Comunicación.* México.

Villareal, M. (2010). *Cables de red.* México.

Anexos

Anexo N° 1.

Operacionalización de variable

	Variables	Concepto	Sub-variables	Indicadores	preguntas	Informantes	Técnicas
Evaluación de la Infraestructura de la Red LAN, Empresa "CECOCAFEN", basado en el Modelo de Objetivo de Control COBIT 4.1, Matagalpa, Primer Semestre 2016	**El modelo objetivo de control COBIT 4.1**	Es una guía que nos permite llevar un control y supervisión de la tecnología de la información	**PO Planear y Organizar**	**PO4.5** Estructura Organizacional	¿Por qué no existe un área de TI en el organigrama?	Encargado de informática	Entrevista y observación
			AI6 Administración de cambio	**AI6.3** Cambio de emergencia	¿Existe un formato de control de cambio de emergencia? ¿Cuáles son las actividades o pasos que se siguen al momento de realizar un cambio de emergencia? ¿Se pone a prueba el proceso de cambio de emergencia?	Encargado de informática	Entrevista y observación
					¿Cuentan con los recursos necesarios para brindar soluciones inmediatas?	Encargado de informática y usuarios	Entrevista y encuesta
			DS3 Administrar el desempeño y capacidad	**DS3.2** Capacidad y desempeño actual	¿Los equipos tienen la capacidad de apoyar procesos tomando en cuenta la escalabilidad de los servicios? ¿Cuál es el ancho de banda con el que cuenta la empresa?	Encargado de informática	Entrevista

					¿Cree que los equipos actuales poseen capacidad suficiente para apoyar los procesos de la empresa? ¿Cree usted que el ancho de banda es el óptimo para el desempeño de los procesos?	Encargado de informática y usuarios	Entrevista, encuesta y observación
				DS3.4 Disponibilidad de los recursos TI	¿Qué tipos de acciones se llevan a cabo cuándo el desempeño de TI no es el óptimo?	Encargado de informática	Entrevista y observación
					¿El plan de contingencia implica que los equipos deben estar disponibles en caso de emergencia? ¿Está disponible para responder a las necesidades de los usuarios?	Encargado de informática y usuarios	Entrevista y encuesta

					¿El servicio TI soluciona sus incidencia en un tiempo adecuado? ¿El personal del servicio TI le informa con precisión acerca de los plazos de conclusión del servicio que se está prestando? ¿Cuál es el nivel de satisfacción que le brinda el servicio de TI en cuanto a la resolución de problemas de los recursos de TI? ¿El servicio de TI cumple los plazos cuando se compromete a hacer algo en un tiempo determinado?	Usuarios	Encuesta
				DS3.5. Monitoreo y reporte	¿Se realiza monitoreo a los recursos de TI o servicios de la red? ¿Qué herramientas utilizan para el monitoreo de los recursos de TI o la red? ¿Con que frecuencia monitorean los recursos de TI o servicios de la red? ¿Se realiza reportes del monitoreo? ¿En caso de anomalía que se refleje en los reportes, que acciones se realizan?	Encargado de informática	Entrevista
			DS4 Garantizar la continuidad de servicio	**DS4.2** planes de continuidad de TI	¿Existe un plan preventivo y correctivo para acciones inesperadas? ¿Cuáles son los objetivos	Encargado de informática	Entrevista y observación

					perseguidos con el plan de continuidad de los recursos de TI? ¿Quiénes son los encargados de elaborar el plan de continuidad de TI? ¿Cada cuánto se le realiza pruebas al plan de continuidad de TI? ¿Se realizan mejoras al plan de continuidad de TI de acuerdo a los resultados de las pruebas? ¿Cuentan con proveedor alternativo para el servicio de internet?		
				DS4.3 Recursos críticos de TI	¿Se tienen documentado los recursos críticos de TI? ¿Se tienen definidas las prioridades de atención a los recursos críticos de TI? ¿Se tienen definidas las medidas de protección para los recursos críticos de	Encargado de informática	Entrevista y observación
				DS4.6 Entrenamiento del plan de continuidad de TI	¿Las personas involucradas reciben capacitaciones constantes respecto a los procedimientos, responsabilidades y roles para garantizar la continuidad de TI?	Encargado de informática y Usuarios	Entrevista y Encuesta
					¿El personal del servicio TI demuestra conocimiento o habilidades suficientes para resolver a los problemas de la red?	Usuario	Encuesta

					¿La atención y capacidad técnica del personal de servicio TI le transmite confianza y seguridad?		
				DS4.8 Recuperación y reanudación de los servicios de TI	¿Se tiene establecida la prioridad de los servicios que deben ser reanudados en el periodo de recuperación de TI? ¿El personal asignado es apto para realizar este tipo de acciones?	Encargado de informática	Entrevista y observación
				DS4.9 Almacenamiento de respaldos fueras de las instalaciones	¿La empresa posee algún tipo de política que implique el almacenamiento de los respaldos en sitios externos a la empresa? ¿Existe algún tipo de contrato con el agente externo que brinda este servicio? ¿Qué tipo de aspectos contempla el contrato?	Encargado de informática	Entrevista y observación
			DS5 Garantizar la seguridad de los sistemas	**DS5.2** Plan de seguridad de TI	¿Cuentan con un plan de seguridad de TI? ¿Se actualiza este plan? ¿Con que frecuencia actualizan el plan de seguridad de TI?	Encargado de informática	Entrevista y observación
					¿De qué manera se les da a conocer al personal involucrado sobre el plan de seguridad de TI?	Encargado de informática y usuario	Entrevista y encuesta

				DS5.3 Administración de identidad	¿Qué métodos utilizan para la administración de identidades de los usuarios que operan los recursos de TI de la empresa?	Encargado de informática y usuarios	Entrevista, encuesta y observación
					¿Se tienen identificados y documentados los permisos de los usuarios sobre los sistemas o aplicaciones?	Encargado de informática	Entrevista y observación
				DS5.4 Administración de cuentas del usuario	¿Qué tipo de criterios se evalúan para la gestión de cuentas de usuarios en las aplicaciones de la empresa? ¿Llevan un control de los privilegios que tiene cada usuario? ¿De qué forma se lleva control de los privilegios?	Encargado de informática	Entrevista y observación
				DS5.9 Prevención, corrección y detección de software maliciosos	¿Qué programas poseen para la identificación y corrección de software malicioso? ¿Mantienen actualizado estos tipos de programas? ¿Qué otras medidas alternas utilizan?	Encargado de informática	Entrevista y observación
				DS5.10 Seguridad de la red	¿Cuentan con programas de detección de intruso? ¿Cuentan con programas de protección de intruso? ¿Cuentan con programas cortafuego? ¿Esta segmentada la red? ¿Qué otras tecnologías o	Encargado de informática	Entrevista y observación

					técnicas utilizan para dar seguridad a la red?		
			DS9 Administración de la configuración	**DS9.1** Repositorio y línea base de configuración	¿Cuentan con una documentación funcional correspondiente de las configuraciones de los dispositivos? ¿Tienen un plan de actualización para la documentación?	Encargado de informática	Entrevista y observación
			DS10 Administración de problemas	**DS10.1** Identificación y clasificación de problemas	¿Cuáles son los criterios de clasificación de los problemas? ¿Existe priorización para la mitigación de riesgos? y ¿En que se basa? ¿Cuentan con medidas preventivas y correctivas para los riesgos detectados?	Encargado de informática	Entrevista y observación
			DS11 Administración de datos	**DS11.5** Respaldo y Restauración	¿Realiza mecanismo de respaldo y restauración? ¿A qué recursos se le realizan las acciones de respaldo y restauración? ¿Con que frecuencia se hace? ¿Se realiza una bitácora de los procesos de respaldo y restauración?	Encargado de informática	Entrevista y observación
			DS12 Administración del ambiente Físico	**DS12.2** Medidas de seguridad física	¿Qué medidas utilizan para la seguridad física? ¿Existe rotulación adecuada en las instalaciones?	Encargado de informática y usuario	Entrevista, encuesta y observación

				DS12.3 Acceso físico	¿Qué mecanismo utilizan para la autorización de acceso físico al centro de datos? ¿Se monitorea el acceso al centro de datos?	Encargado de informática	Entrevista y observación
				DS12.4 protección contra factores ambientales	¿Qué medidas utilizan para controlar factores ambientales?	El encargado de informática	Entrevista y observación
				DS12.5 Administración de instalaciones físicas	¿Cuentan con estándares o normas para las instalaciones físicas existentes? ¿Existen estándares para el cableado eléctrico?	El encargado de informática	Entrevista y observación
	Infraestructura de la Red LAN	Es una red local que puede alcanzar hasta 10 Mbps	**Funcionamiento de la estructura física**	Cableado	¿Existe Cableado Estructurado? ¿Qué tipo de cableado utilizan? y ¿porque? ¿Qué problemas se le han presentado al utilizar ese tipo de cableado? ¿Cuentan con algún estándar para el cableado estructurado? ¿Existe estándar para el etiquetado de los cableados de la red?	El encargado de informática	Entrevista y observación
				Servidores	¿Qué tipo de servidor cuenta la empresa? ¿Cuál es su capacidad de almacenamientos? ¿Con cuántos servidores cuenta la empresa? ¿Cómo están distribuido?		Entrevista y observación

				Sala de servidores	¿Dónde se encuentra ubicada la sala de servidores? ¿Qué procesos se llevaban a cabo en los servidores? ¿Hace cuánto se dañaron los servidores? Y ¿Cuáles son las causas? ¿Realizaron estudios para la selección de la ubicación? ¿Cuentan con políticas de acceso a la sala, mencione algunas? ¿Cuáles son las políticas de seguridad? ¿Se cuenta con un estándar que soporte la ubicación actual de la sala de servidores?		Entrevista y observación
				Estaciones de trabajo	¿Cuentan con inventarios de los recursos lógicos y físicos?		Entrevista y observación
				Dispositivos intermediarios	¿Con que tipos de dispositivos intermediarios cuenta la empresa? ¿Cuál es la función de cada uno de ellos? ¿Se les da mantenimientos a los dispositivos intermediarios? ¿Con que frecuencia se da el mantenimiento? ¿Existe una bitácora de los mantenimientos realizados a los dispositivos?		Entrevista y observación

					¿Existe inventario de los dispositivos intermediarios?		
			Funcionamiento de la estructura lógica	Direcciones IP	¿Cuentan con un control de IP? ¿Cómo es el control que llevan de las IP? ¿Utilizan direccionamiento estático o dinámico? ¿Qué criterios se toman en cuenta al momento de asignar la dirección IP a un dispositivo?		Entrevista y observación
				Intranets	¿Se encuentran documentados y aprobados los usos actuales de la red?		Entrevista y observación
				Topología de red	¿Qué tipo de topología cuentan? ¿Por qué utilizan este tipo de topología? ¿Existe documentación de la topología física y lógica de la red?		Entrevista y observación
				Antivirus	¿Qué tipo de antivirus utiliza? ¿Cuenta con licencia? ¿Qué beneficios le trae este tipo de antivirus?		Entrevista y observación
			Gestión de seguridad	Políticas de seguridad	¿Se encuentra documentada y aprobada las políticas de seguridad? ¿Se capacita al personal involucrado de acuerdo a sus rolles y responsabilidades en las políticas de seguridad? ¿Con que frecuencia se		Entrevista y observación

					actualizan las políticas de seguridad?		
				Análisis de riesgo	¿Cuentan con una auditoria interna o externa para el análisis de riesgo? ¿Qué perfil tienen los auditores?		Entrevista y observación

Anexo N° 2.

Entrevista 1

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de entrevista realizada al encargado del área de TI

Con el objetivo de conocer el nivel de madurez del área de TI en la empresa "CECOCAFEN", se realiza la presente entrevista agradeciendo de antemano su valiosa colaboración.

Entrevistado: _____ Firma: _____

Fecha: _____ Duración: 30 a 45 minutos

Interrogantes.

PO4.5 ¿Por qué no existe un área de TI en el organigrama?

AI6.3 ¿Existe un formato de control de cambio de emergencia?

AI6.3 ¿Cuáles son las actividades o pasos que se siguen al momento de realizar un cambio de emergencia?

AI6.3 ¿Se pone a prueba el proceso de cambio de emergencia?

AI6.3 ¿Cuentan con los recursos necesarios para brindar soluciones inmediatas?

DS3.2 ¿Cree que los equipos actuales poseen capacidad suficiente para apoyar los procesos de la empresa?

DS3.2 ¿Los equipos tienen la capacidad de apoyar procesos tomando en cuenta la escalabilidad de los servicios?

DS3.2 ¿Cuál es el ancho de banda con el que cuenta la empresa?

DS3.2 ¿Cree usted que el ancho de banda es el óptimo para el desempeño de los procesos?

DS3.4 ¿Qué tipos de acciones se llevan a cabo cuándo el desempeño de TI no es el óptimo?

DS3.4 ¿El plan de contingencia implica que los equipos deben estar disponibles en caso de emergencia?

DS3.4 ¿Está disponible para responder a las necesidades de los usuarios?

DS3.4 ¿Cumple los plazos cuando se compromete a hacer algo en un tiempo determinado?

DS3.5 ¿Se realiza monitoreo a los recursos de TI o servicios de la red?

DS3.5 ¿Qué herramientas utilizan para el monitoreo de los recursos de TI o la red?

DS3.5 ¿Con que frecuencia monitorean los recursos de TI o servicios de la red?

DS3.5 ¿Se realiza reportes del monitoreo?

DS3.5 ¿En caso de anomalía que se refleje en los reportes, que acciones se realizan?

Anexo N° 3.

Entrevista 2

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de entrevista realizada al encargado del área de TI

Con el objetivo de conocer el nivel de madurez del área de TI a la empresa "CECOCAFEN", se realiza la presente entrevista agradeciendo de antemano su valiosa colaboración.

Entrevistado: _____ Firma: _____

Fecha: _____ Duración: 30 a 45 minutos

Interrogantes.

DS4.2 ¿Existe un plan preventivo y correctivo para acciones inesperadas?

DS4.2 ¿Cuáles son los objetivos perseguidos con el plan de continuidad de los recursos de TI?

DS4.2 ¿Quiénes son los encargados de elaborar el plan de continuidad de TI?

DS4.2 ¿Cada cuánto se le realiza pruebas al plan de continuidad de TI?

DS4.2 ¿Se realizan mejoras al plan de continuidad de TI de acuerdo a los resultados de las pruebas?

DS4.2 ¿Cuentan con proveedor alternativo para el servicio de internet?

DS4.3 ¿Se tienen documentado los recursos críticos de TI?

DS4.3 ¿Se tienen definidas las prioridades de atención a los recursos críticos de TI?

DS4.3 ¿Se tienen definidas las medidas de protección para los recursos críticos de TI?

DS4.6 ¿Las personas involucradas reciben capacitaciones constantes respecto a los procedimientos, responsabilidades y roles para garantizar la continuidad de TI?

DS4.8 ¿Se tiene establecida la prioridad de los servicios que deben ser reanudados en el periodo de recuperación de TI?

DS4.8 ¿El personal asignado es apto para realizar este tipo de acciones?

DS4.9 ¿La empresa posee algún tipo de política que implique el almacenamiento de los respaldos en sitios externos a la empresa?

DS4.9 ¿Existe algún tipo de contrato con el agente externo que brinda este servicio?

DS4.9 ¿Qué tipo de aspectos contempla el contrato?

DS5.2 ¿Cuentan con un plan de seguridad de TI?

DS5.2 ¿Se actualiza este plan?

DS5.2 ¿Con que frecuencia actualizan el plan de seguridad de TI?

DS5.2 ¿De qué manera se les da a conocer al personal involucrado sobre el plan de seguridad de TI?

Anexo N° 4.

Entrevista 3

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de entrevista realizada al encargado del área de TI

Con el objetivo de conocer el nivel de madurez del área de TI a la empresa "CECOCAFEN", se realiza la presente entrevista agradeciendo de antemano su valiosa colaboración.

Entrevistado: _____ Firma: _____

Fecha: _____ Duración: 30 a 45 minutos

Interrogantes.

DS5.3 ¿Qué métodos utilizan para la administración de identidades de los usuarios que operan los recursos de TI de la empresa?

DS5.3 ¿se tienen identificados y documentados los permisos de los usuarios sobre los sistemas o aplicaciones?

DS5.4 ¿Qué tipo de criterios se evalúan para la gestión de cuentas de usuarios en las aplicaciones de la empresa?

DS5.4 ¿Llevan un control de los privilegios que tiene cada usuario?

DS5.4 ¿De qué forma se lleva control de los privilegios?

DS5.9 ¿Qué programas poseen para la identificación y corrección de software malicioso?

DS5.9 ¿Mantienen actualizado estos tipos de programas?

DS5.9 ¿Qué otras medidas alternas utilizan?

DS5.10 ¿Cuentan con programas de detección de intruso?

DS5.10 ¿Cuentan con programas de protección de intruso?

DS5.10 ¿Cuentan con programas cortafuego?

DS5.10 ¿Esta segmentada la red?

DS5.10 ¿Qué otras tecnologías o técnicas utilizan para dar seguridad a la red?

DS9.1 ¿Cuentan con una documentación funcional correspondiente de las configuraciones de los dispositivos?

DS9.1 ¿Tienen un plan de actualización para la documentación?

DS10.1 ¿Existe un plan de gestión de riesgos?

DS10.1 ¿Cuáles son los criterios de clasificación de los problemas?

DS10.1 ¿Existe priorización para la mitigación de riesgos? y ¿En que se basa?

DS10.1 ¿Cuentan con medidas preventivas y correctivas para los riesgos detectados?

Anexo N° 5.

Entrevista 4

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de entrevista realizada al encargado del área de TI

Con el objetivo de conocer el nivel de madurez del área de TI a la empresa "CECOCAFEN", se realiza la presente entrevista agradeciendo de antemano su valiosa colaboración.

Entrevistado: _____ Firma: _____

Fecha: _____ Duración: 30 a 45 minutos

Interrogantes.

DS11.5 ¿Realiza mecanismo de respaldo y restauración?

DS11.5 ¿A qué recursos se le realizan las acciones de respaldo y restauración?

DS11.5 ¿Con que frecuencia se hace?

DS11.5 ¿Se realiza una bitácora de los procesos de respaldo y restauración?

DS12.2 ¿Qué medidas utilizan para la seguridad física?

DS12.2 ¿Existe rotulación adecuada en las instalaciones?

DS12.3 ¿Qué mecanismo utilizan para la autorización de acceso físico al centro de datos?

DS12.3 ¿Se monitorea el acceso al centro de datos?

DS12.4 ¿Qué medidas utilizan para controlar factores ambientales?

DS12.5 ¿Cuentan con estándares o normas para las instalaciones físicas existentes?

DS12.5 ¿Existen estándares para el cableado eléctrico?

Anexo N° 6

Entrevista 5

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de entrevista realizada al encargado del área de TI

Con el objetivo de conocer el nivel de madurez del área de TI a la empresa "CECOCAFEN", se realiza la presente entrevista agradeciendo de antemano su valiosa colaboración.

Entrevistado: _____ Firma: _____

Fecha: _____ Duración: 30 a 45 minutos

Interrogantes.

1. ¿Existe Cableado Estructurado?
2. ¿Qué tipo de cableado utilizan? y ¿porque?
3. ¿Qué problemas se le han presentado al utilizar ese tipo de cableado?
4. ¿Cuentan con algún estándar para el cableado estructurado?
5. ¿Existe estándar para el etiquetado del cableado de la red?
6. ¿Qué tipo de servidor cuenta la empresa?
7. ¿Cuál es su capacidad de almacenamiento?
8. ¿Con cuántos servidores cuenta la empresa?
9. ¿Cómo están distribuidos?
10. ¿Dónde se encuentra ubicada la sala de servidores?

11. ¿Qué procesos se llevaban a cabo en los servidores?
12. ¿Hace cuánto se dañaron los servidores? Y ¿Cuáles son las causas?
13. ¿Realizaron estudios para la selección de la ubicación?
14. ¿Cuentan con políticas de acceso a la sala, mencione algunas?
15. ¿Cuáles son las políticas de seguridad?
16. ¿Se cuenta con un estándar que soporte la ubicación actual de la sala de servidores?
17. ¿Cuentan con inventarios de los recursos lógicos y físicos?
18. ¿Con que tipos de dispositivos intermediarios cuenta la empresa?
19. ¿Cuál es la función de cada uno de ellos?
20. ¿Se les da mantenimientos a los dispositivos intermediarios?
21. ¿Con que frecuencia se da el mantenimiento?
22. ¿Existe una bitácora de los mantenimientos realizados a los dispositivos?
23. ¿Existe inventario de los dispositivos intermediarios?

Anexo N° 7.

Entrevista 6

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de entrevista realizada al encargado del área de TI

Con el objetivo de conocer el nivel de madurez del área de TI a la empresa "CECOCAFEN", se realiza la presente entrevista agradeciendo de antemano su valiosa colaboración.

Entrevistado: _____ Firma: _____

Fecha: _____ Duración: 30 a 45 minutos

Interrogantes.

1. ¿Cuentan con un control de IP?
2. ¿Cómo es el control que llevan de las IP?
3. ¿Utilizan direccionamiento estático o dinámico?
4. ¿Qué criterios se toman en cuenta al momento de asignar la dirección IP a un dispositivo?
5. ¿Se encuentran documentados y aprobados los usos actuales de la red?
6. ¿Qué tipo de topología cuentan?
7. ¿Por qué utilizan este tipo de topología?
8. ¿Existe documentación de la topología física y lógica de la red?
9. ¿Qué tipo de antivirus utilizan?

10. ¿Cuentan con licencia?
11. ¿Qué beneficios les trae este tipo de antivirus?
12. ¿Se encuentra documentada y aprobada las políticas de seguridad?
13. ¿Se capacita al personal involucrado de acuerdo a sus roles y responsabilidades en las políticas de seguridad?
14. ¿Con que frecuencia se actualizan las políticas de seguridad?
15. ¿Cuentan con una auditoria interna o externa para el análisis de riesgo?
16. ¿Qué perfil tienen los auditores?

Anexo N° 8.

Encuesta

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de encuesta al Usuario

El objetivo de la encuesta es para conocer el grado de satisfacción de los/las usuarios en base al funcionamiento de los servicios informáticos que brinda en la empresa "CECOCAFEN", se le agradece de antemano su colaboración.

Marque con un X según corresponda

1. ¿Considera usted que el personal de TI cuenta con los recursos necesarios para brindar soluciones inmediatas?

   S I_____ NO _____

2. Basado en la calidad de trabajo que se le demanda ¿cree que el equipo del cual hace uso tiene la capacidad adecuada de funcionamiento?

   S I_____ NO _____

3. ¿Cree usted que el internet es el óptimo para las actividades que desempeña?

   S I_____ NO _____

4. ¿En caso de emergencia los equipos pueden seguir trabajando?

   S I_____ NO _____

5. ¿El servicio TI soluciona sus incidencia en un tiempo adecuado?

   Nunca_____ A veces_____

   Casi siempre_____ Siempre_____

6. ¿El personal del servicio TI le informa con precisión acerca de los plazos de conclusión del servicio que se está prestando?

Nunca_____ A veces_____

Casi siempre_____ Siempre_____

7. ¿Cuál es el nivel de satisfacción que le brinda el servicio de TI en cuanto a la resolución de problemas de los recursos de TI?

Alto_____ Medio_____

Bajo_____ Ninguna de las Anteriores_____

8. ¿El servicio de TI cumple los plazos cuando se compromete a hacer algo en un tiempo determinado?

Sí _____ No _____ A veces_____

9. ¿El personal del servicio de TI está disponible para responder a sus necesidades?

Nunca_____ A veces_____

Casi siempre_____ Siempre_____

10. ¿Ha recibido algún tipo de capacitación para garantizar la continuidad de TI ante acciones inesperadas?

Sí _____ No _____

11. ¿El personal del servicio TI demuestra conocimiento o habilidades suficientes para resolver a los problemas de la red?

Nunca_____ A veces_____

Casi siempre_____ Siempre _____

12. ¿La atención y capacidad técnica del personal de servicio TI le transmite confianza y seguridad?

Ninguna _____ Poca _____

Mucha _____

13. ¿De qué manera se les da a conocer al personal involucrado sobre el plan de seguridad de TI?

Video conferencia _____ Foros _____ Documento _____

Capacitación _____ otros _____ ninguna_____

14. ¿Qué métodos utilizan para la administración de identidades?

Tarjeta _____ huellas digitales _____ Carné _____

Otros (especifique) _____

15. ¿Qué medidas utilizan para la seguridad física de los recursos de TI?

Tarjeta _____ huellas digitales _____ Carnet _____

Otros (especifique) _____

16. ¿Existe rotulación adecuada en las instalaciones?

Sí _____ No _____

Anexo N° 9.

Observación

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de observación Beneficio **"CECOCAFEN"**

Ítem	Existe	No Existe	Observación
Organigrama de la empresa.			
Capacidad y desempeño de los equipos			
Capacidad del ancho de banda			
Formato de control de cambio			
Disponibilidad de los equipos en caso de emergencia			
Frecuencia para informar los plazos de conclusión de los servicios			
Monitoreo y reporte de la red y recursos de TI			
Documentación del plan de continuidad de TI			
Documentación del plan preventivo y correctivo para acciones inesperadas			
Documento de los recursos críticos de TI			
Documentación de la			

Políticas de protección y seguridad			
Documento del plan de capacitación a los usuarios del plan de contingencia, continuidad, factores ambientales y políticas de seguridad			
Documento contra factores ambientales			
Documento para la recuperación y reanudación de los servicios			
Almacenamiento de respaldo fuera de las instalaciones			
Documentación del plan de seguridad de TI			
Administración de identidades			
Documentación de administración de cuentas de usuarios y privilegios			
Prevención y corrección de software maliciosos			
Sistema de detección y protección de intruso			
Documentación del plan de gestión de riesgos			

Protección contra factores ambientales			
Seguridad física de los recursos de TI			
Rotulación adecuada			
Cableado			
Servidores			
Sala de servidores			
Estaciones de trabajo			
Estándar para el cableado eléctrico			
Polo tierra			
Firewall			
Documentación de los recursos físicos y lógicos			
Dispositivos intermediarios			
Documentación del control de las IP			
Documentación de los usos y objetivos de la red			
Antivirus			
Documentación física y lógica de la topología de red			
Documentación de las políticas de seguridad			

Anexo N° 10.

Observación

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria

UNAN Managua - FAREM Matagalpa

Guía de observación Beneficio **"CECOCAFEN"**

Ítem	Existe	No Existe	Observación
Organigrama de la empresa.	X		No está definida una área de TI en el organigrama
Capacidad y desempeño de los equipos	X		Mala distribución de los equipos y en algunos casos están obsoletos
Capacidad del ancho de banda	X		Descargan música, videos, entre otros. Cualquier dispositivo no propio de la empresa se puede conectar sin control alguno
Formato de control de cambio		X	No hay
Disponibilidad de los equipos en caso de emergencia		X	No hay planta eléctrica, ni UPS. La mayoría de las computadoras no tienen baterías estabilizadoras
Frecuencia para informar los plazos de conclusión de los servicios		X	Problemas con el servicio de correo electrónico, el cual no se les informó a los usuarios
Monitoreo y reporte de la red y recursos de TI		X	Ataque a los dispositivos. Tráfico anómalo, interrupción de servicios.
Documentación del plan de continuidad de TI		X	No hay un plan de continuidad de TI. No hay proveedor alternativo de internet
Documentación del plan preventivo y correctivo para acciones inesperadas		X	No hay
Documento de los recursos		X	No hay

críticos de TI			
Documentación de la Políticas de protección y seguridad		X	No hay
Documento del plan de capacitación a los usuarios del plan de contingencia, continuidad, factores ambientales y políticas de seguridad		X	No se presentó un plan de capacitación que ayude a los usuarios a prepararse ante una eventualidad
Documento contra factores ambientales		X	
Documento para la recuperación y reanudación de los servicios		X	No se cuenta tanto con el personal como el material adecuado
Almacenamiento de respaldo fuera de las instalaciones		X	No se pudo observar donde tenían los respaldos, ya que la persona encargada, en ese momento no se encontraba
Documentación del plan de seguridad de TI		X	Tanto el encargado como los usuarios pueden sacar los equipos fuera de la empresa, sin control alguno
Administración de identidades	X		No existe registro de huellas digitales, carné o tarjetas, solamente usuario y contraseña
Documentación de administración de cuentas de usuarios y privilegios		X	No cuentan con un administrador, nada más se realiza una cuenta para asignar los equipos. No cuentan con mecanismos para dar de baja a un usuario en caso que ya no trabaje en la empresa

Prevención y corrección de software maliciosos		X	No cuenta con programas de calidad para corregir y prevenir software malicioso
Sistema de detección y protección de intruso		X	
Documentación del plan de gestión de riesgos		X	
Protección contra factores ambientales	X		Solo cuentan con extintores contra fuegos
Seguridad física de los recursos de TI		X	No existen medidas de seguridad y salvaguardas, ni control de las personas que entran y salen en las áreas restringidas
Rotulación adecuada	X		Hacen falta rotulaciones como empresa. Las personas pueden moverse por las instalaciones sin restricción alguna
Cableado	X		Cableado dañado porque está a la intemperie. Cableado tirado en algunas áreas
Servidores		X	Están tirados, llenos de polvo, están dañados por altibajos de energía y falta de mantenimiento
Sala de servidores		X	Sin aire acondicionado, expuesto a exceso de humedad, polvo y ruido
Estaciones de trabajo	X		
Estándar para el cableado eléctrico		X	
Polo tierra	X		
Firewall		X	
Documentación de los recursos físicos y lógicos		X	

Dispositivos intermediarios	X		Algunos están a la intemperie, llenos de polvo, pintura y a simple vista
Documentación del control de las IP		X	No hay un documento del control de las IP
Documentación de los usos y objetivos de la red		X	
Antivirus	X		Compraron licencia de antivirus a U$ 80 para todas las máquinas
Documentación física y lógica de la topología de red		X	No saben qué tipo de topología hay
Documentación de las políticas de seguridad		X	

Anexo N° 11.

Matriz de resultados de entrevista aplicada al encargado del área de TI

Indicadores	Entrevistado
¿Por qué no hay un área de TI en el organigrama?	Porque no existe, el gerente no quiere contratar a un ingeniero porque gana $600 dólares por estar sentado, por lo que hay semanas que no presenta ningún inconveniente, por eso el prefiere hacer subcontratación cuando haya un problema grave.
¿Existe un formato de control de cambio de emergencia?	No hay
¿Cuáles son las actividades o pasos que se siguen al momento de realizar un cambio de emergencia?	No hay
¿Se pone a prueba el proceso de cambio de emergencia?	No hay
¿Cuentan con los recursos necesarios para brindar soluciones inmediatas?	Si
¿Cree que los equipos actuales poseen capacidad suficiente para apoyar los procesos de la empresa?	En número sí, pero no en capacidad de equipos
¿Los equipos tienen la capacidad de apoyar procesos tomando en cuenta la escalabilidad de los servicios?	Sí, pero muy básico porque hay equipos que están un poco obsoletos, desactualizados, entre otras cosa
¿Cuál es el ancho de banda con el que cuenta la empresa?	Varios porque son 4 ubicaciones diferentes, en la oficina central hay 10 mbps, SOLCAFÉ 3 mbps, en la Agroindustria 2 mbps y en la Cooperativa de ahorro y crédito 5 mbps
¿Cree usted que el ancho de banda es el óptimo para el desempeño de los procesos?	Tenemos internet exclusivamente para comunicación básica (mensajería y correo electrónico). El cual presenta problemas de comunicación de correo o mensajerías en todas las cooperativas menos en SOLCAFÉ a pesar que es poco nunca hay

	problema. Además para querer bajar un archivo es dilatado, pero para lo que fue contratado está muy bien que es para comunicación.
¿Qué tipos de acciones se llevan a cabo cuándo el desempeño de TI no es el óptimo?	Lo que hay al día de hoy es gestionar con el gerente la posibilidad de comprar dos servidores (1 SOLCAFÉ, 1 CECOCAFEN) para una base de datos importante que está en un equipo de uso doméstico. Ambas oficinas están utilizando equipos convencionales, no son de marca. Es una solución a corto plazo para descargar todo el peso de la gestión de la información en un servidor y para los quipos no hay una gestión, porque no hay capital para realizar cambios
¿El plan de contingencia implica que los equipos deben estar disponibles en caso de emergencia?	No hay plan de contingencia, pero en caso de que se vaya la luz no todos los equipos trabajan, las laptops sí, pero los equipos de escritorio no
¿Está disponible para responder a las necesidades de los usuarios?	No siempre porque genera costo, además como anterior le había explicado el gerente no quiere contratar a un informático permanente
¿Cumple los plazos cuando se compromete a hacer algo en un tiempo determinado?	No siempre, porque el escenario es nuevo y hay problemas que se dificultan al momento de resolverlo
¿Se realiza monitoreo a los recursos de TI o servicios de la red?	Actualmente sí, hay un sistema para monitorear el uso de los equipos para saber del uso adecuado del recurso internet y el tiempo horario de los

	trabajadores, se está monitoreando que se está haciendo con los equipos, pero no se monitorea la red.
¿Qué herramientas utilizan para el monitoreo de los recursos de TI o servicios de la red?	No hay para el monitoreo de la red pero para los recursos no te puedo decir
¿Con que frecuencia monitorean los recursos de TI o servicios de la red?	24 horas al día, es un servicio en la nube que nos está vigilando el uso de datos de los usuarios, hacía donde se están comunicando, si se está filtrando información, todo lo que se está haciendo. Queda guardado en un servidor y se puede monitorear cada cierto tiempo.
¿Se realiza reportes del monitoreo?	Si, diario.
¿En caso de anomalía que se refleje en los reportes, que acciones se realizan?	Se va a restringir más adelante el acceso al internet, no se podrá usar redes sociales, no páginas de descarga de archivos, películas, músicas, posiblemente se deje de usar internet de la empresa en los celulares. Todo lo que haga más lento el servicio se va a quitar. Solo para comunicación, pero por los momentos no se hace nada
¿Existe un plan preventivo y correctivo para acciones inesperadas?	No hay un plan preventivo ni correctivo solamente se corrige el problema cuando surge.
¿Cuáles son los objetivos perseguidos con el plan de continuidad de los recursos de TI?	No. hay
¿Quiénes son los encargados de elaborar el plan de continuidad de TI?	No hay
¿Cada cuánto se le realiza pruebas al plan	No hay

de continuidad de TI?	
¿Se realizan mejoras al plan de continuidad de TI de acuerdo a los resultados de las pruebas?	No hay
¿Cuentan con proveedor alternativo para el servicio de internet?	No hay, en caso extremo la gente se conecta de su móvil
¿Se tienen documentado los recursos críticos de TI?	No
¿Se tienen definidas las prioridades de atención a los recursos críticos de TI?	No
¿Qué medidas de protección se utilizan para los recursos críticos de TI?	No
¿Se tienen definidas las medidas de protección para los recursos críticos de TI?	No
¿Las personas involucradas reciben capacitaciones constantes respecto a los procedimientos, responsabilidades y roles para garantizar la continuidad de TI?	No, porque no hay un plan de continuidad
¿Se tiene establecida la prioridad de los servicios que deben ser reanudados en el periodo de recuperación de TI?	No, porque no ha surgido un caso así de esa magnitud
¿El personal asignado es apto para realizar este tipo de acciones?	No hay
¿La empresa posee algún tipo de política que implique el almacenamiento de los respaldos en sitios externos a la empresa?	No hay fuera de la empresa. Existe copia de la información de todas las oficinas en la oficina central CECOCAFEN
¿Existe algún tipo de contrato con el agente externo que brinda este servicio?	No, solo se eligió a una persona por mayoría de votos
¿Qué tipo de aspectos contempla el contrato?	Ninguno
¿Cuentan con un plan de seguridad para los dispositivos de almacenamientos?	No hay. Básicamente el disco externo tiene una contraseña y usuarios para accesar. Si se lo roban no podrán entrar a la información
¿Cuentan con un plan de seguridad de TI?	No hay
¿Se actualiza este plan?	No hay
¿Con que frecuencia actualizan el plan de seguridad de TI?	No hay

¿De qué manera se les da a conocer al personal involucrado sobre el plan de seguridad de TI?	No hay
¿Qué métodos utilizan para la administración de identidades de los usuarios que operan los recursos de TI de la empresa?	Los usuarios tiene su equipo con usuario y contraseña, los correos tienen clave maestra.
¿Se tienen identificados y documentados los permisos de los usuarios sobre los sistemas o aplicaciones?	No
¿Qué tipo de criterios se evalúan para la gestión de cuentas de usuarios en las aplicaciones de la empresa?	En términos de equipos no hay criterios a seguir, en la mayoría de los casos se reasigna equipo con un nuevo usuario para usarlo.
¿Llevan un control de los privilegios que tiene cada usuario?	No. Como no hay servidor no se asignan roles, todos tienen los mismos privilegios.
¿De qué forma se lleva control de los privilegios?	No hay
¿Qué programas poseen para la identificación y corrección de software malicioso?	Como no hay servidor todo se enfoca en el equipo que tiene el usuario. Básicamente el usuario tiene licencia del antivirus NORTON
¿Mantienen actualizado estos tipos de programas?	Si
¿Qué otras medidas alternas utilizan?	No hay
¿Cuentan con programas de detección de intruso?	No
¿Cuentan con programas de protección de intruso?	No
¿Cuentan con programas cortafuego?	No
¿Esta segmentada la red?	No
¿Qué otras tecnologías o técnicas utilizan para dar seguridad a la red?	Un filtro, un servicio externo que identifica la IP y filtra el acceso a una serie de páginas inadecuadas para el tipo de trabajo, por ejemplo las redes sociales

¿Cuentan con una documentación funcional correspondiente de las configuraciones de los dispositivos?	No, porque los informáticos que se han contratado se lo han llevado
¿Tienen un plan de actualización para la documentación?	No
¿Existe un plan de gestión de riesgos?	No
¿Cuáles son los criterios de clasificación de los problemas?	No
¿Existe priorización para la mitigación de riesgos? y ¿En que se basa?	No hay
¿Cuentan con medidas preventivas y correctivas para los riesgos detectados?	No
¿Realiza mecanismo de respaldo y restauración?	Casi nunca se ha dado el caso de restauración, solo se realizan respaldo para un eventual problema que se hace en las computadoras convencionales, memorias externas y disco duro
¿A qué recursos se le realizan las acciones de respaldo y restauración?	A la información como a las bases contables
¿Con que frecuencia se hace?	Diario
¿Se realiza una bitácora de los procesos de respaldo y restauración?	No
¿Qué medidas utilizan para la seguridad física?	Cámaras de vigilancia y el vigilante
¿Existe rotulación adecuada en las instalaciones?	Si
¿Qué mecanismo utilizan para la autorización de acceso físico al centro de datos?	No ha habido políticas de acceso
¿Se monitorea el acceso al centro de datos?	No
¿Qué medidas utilizan para controlar factores ambientales?	No hay solo existe extintor en caso de surja un incendio
¿Cuentan con estándares o normas para las instalaciones físicas existentes?	No
¿Existen estándares para el cableado eléctrico?	No, se usa de todo tipo de cable
¿Existe Cableado Estructurado?	Si
¿Qué tipo de cableado utilizan? y ¿porque?	Siempre se ha utilizado el cable categoría 5

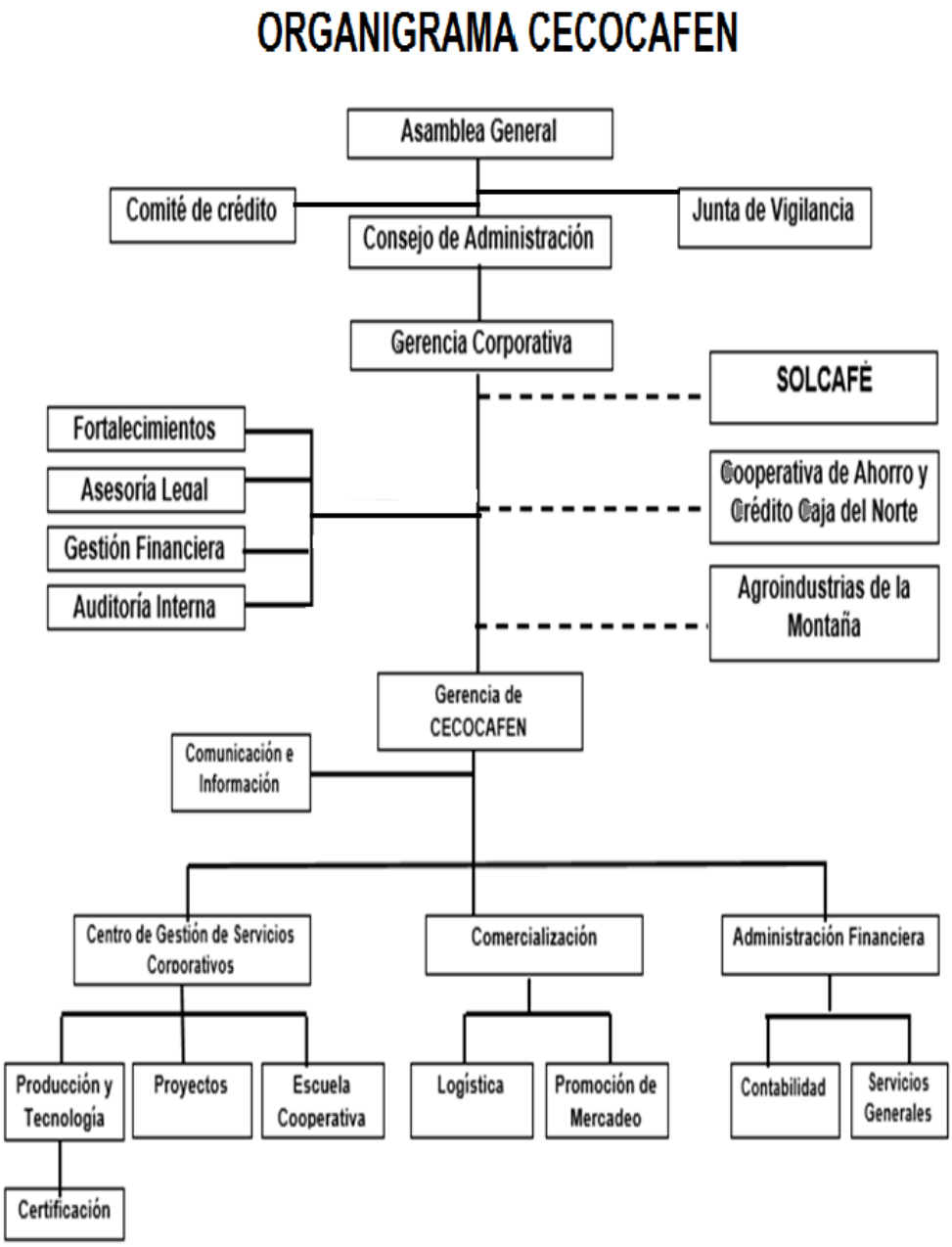
¿Qué problemas se le han presentado al utilizar ese tipo de cableado?	Es un cable que no puede estar a la intemperie, y es muy delicado, también a cierta distancia no funciona o la red se cae
¿Cuentan con algún estándar para el cableado estructurado?	No
¿Existe estándar para el etiquetado del cableado de la red?	No
¿Qué tipo de servidor cuenta la empresa?	No hay, porque se dañaron
¿Cuál es su capacidad de almacenamiento?	No hay
¿Con cuántos servidores cuenta la empresa?	Habían 4 pero todos se dañaron
¿Cómo están distribuidos?	Una por cada cooperativa
¿Dónde se encuentra ubicada la sala de servidores?	No hay
¿Qué procesos se llevan a cabo en los servidores?	Bases de datos contables, correo electrónico y toda la información de la empresa
¿Hace cuánto se dañaron los servidores? Y ¿Cuáles son las causas?	Hace 8 meses y las causas no lo se
¿Realizaron estudios para la selección de la ubicación?	No hay
¿Cuentan con políticas de acceso a la sala, mencione algunas?	No hay
¿Cuáles son las políticas de seguridad?	En general si, cámaras de vigilancia, vigilantes permanente las 24 horas.

¿Se cuenta con un estándar que soporte la ubicación actual de la sala de servidores?	No hay
¿Cuentan con inventarios de los recursos lógicos y físicos?	Si
¿Con que tipos de dispositivos intermediarios cuenta la empresa?	Routers, Switch, modem.
¿Cuál es la función de cada uno de ellos?	Los Switch conectan la aplicación o sistema con una serie de usuarios, y poder distribuir a través de cables la señal de internet y el sistema de impresión. Los Routers son para la conexión inalámbrica de las laptops.
¿Se les da mantenimientos a los dispositivos intermediarios?	No, solo limpieza.
¿Con que frecuencia se da el mantenimiento?	No hay
¿Existe una bitácora de los mantenimientos realizados a los dispositivos?	No
¿Existe inventario de los dispositivos intermediarios?	No
¿Cuentan con un control de IP?	No
¿Cómo es el control que llevan de las IP?	No hay
¿Utilizan direcciones estáticas o dinámicas?	Las 2
¿Qué criterios se toman en cuenta al momento de asignar la dirección IP a un	Solo se asigna de manera estática la

dispositivo?	muchacha de contabilidad para darle seguridad, el resto es dinámica.
¿Se encuentran documentados y aprobados los usos actuales de la red?	No
¿Qué tipo de topología cuentan?	No saben
¿Por qué utilizan este tipo de topología?	No saben
¿Existe documentación de la topología física y lógica de red?	No
¿Qué tipo de antivirus utiliza?	Norton
¿Cuenta con licencia?	Si la licencia costo $80 para todas las computadoras
¿Qué beneficios les trae este tipo de antivirus?	No hay problemas de virus en las computadoras, ya que se actualiza automáticamente
¿Se encuentra documentada y aprobada las políticas de seguridad?	No hay
¿Se capacita al personal involucrado de acuerdo a sus roles y responsabilidades en las políticas de seguridad?	Si
¿Con que frecuencia se actualizan las políticas de seguridad?	No
¿Cuentan con una auditoria interna o externa para el análisis de riesgo?	Sí, pero no en el área de informática.
¿Qué perfil tienen los auditores?	No se sabe

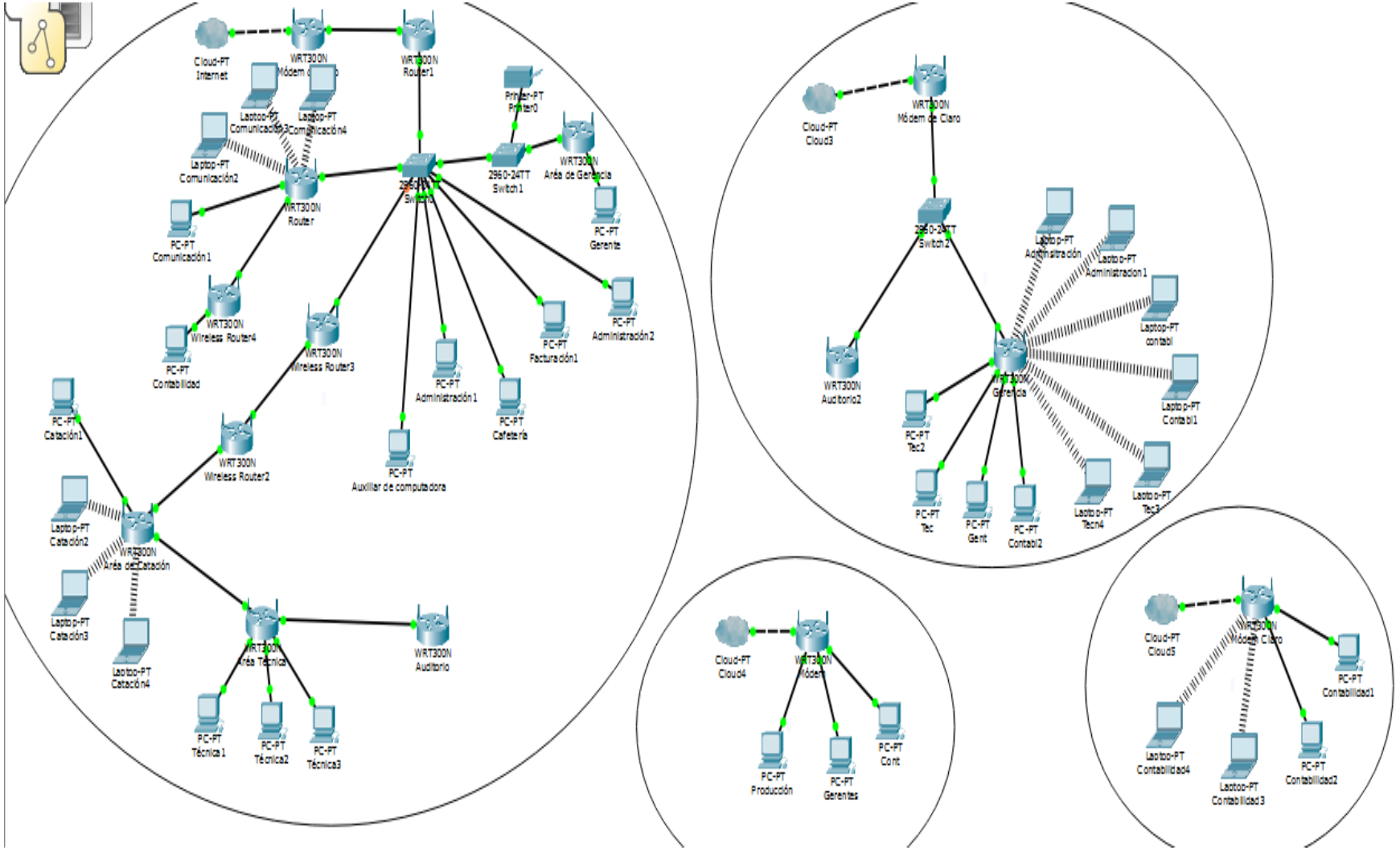
Anexo N° 12.

Organigrama Actual de la empresa



Anexo N° 13.

Topología lógica actual de la red CECOCAFEN



Anexo N° 14.

Ficha de visita

Ficha de visita

Nombre: _____

Cargo: _____

Fecha: _____ **Hora:** _____

Observación:

Firma: _____