RESUMEN – TRABAJO DE GRADO

AUTORES	VICTOR MANUEL PÉREZ CONTRERAS
FACULTAD	INGENIERÍAS
PLAN DE ESTUDIOS	INGENIERÍA DE SISTEMAS
DIRECTOR	EDUAR BAYONA IBAÑEZ
TÍTULO DE LA TESIS	PLAN ESTRATÉGICO PARA LA GESTIÓN DEL SISTEMA DE INFORMACIÓN DE GEOLOCALIZACIÓN INKO DE LA EMPRESA COOTRANSHACARITAMA OCAÑA, BASADO EN LA NORMA ISO/IEC 27001/2013

RESUMEN
(70 PALABRAS APROXIMADAMENTE)

EL PLAN ESTRATÉGICO ES UN DOCUMENTO EN EL QUE LOS RESPONSABLES DE UNA ORGANIZACIÓN REFLEJAN CUAL SERÁ LA ESTRATEGIA A SEGUIR POR SU COMPAÑÍA EN EL MEDIO PLAZO. AUNQUE EN MUCHOS CONTEXTOS SE SUELEN UTILIZAR INDISTINTAMENTE LOS CONCEPTOS DE PLAN DIRECTOR Y PLAN ESTRATÉGICO, LA DEFINICIÓN **ESTRICTA** DE PLAN ESTRATÉGICO INDICA QUE ÉSTE DEBE MARCAR LAS DIRECTRICES Y EL COMPORTAMIENTO PARA QUE UNA ORGANIZACIÓN ALCANCE LAS ASPIRACIONES QUE HA PLASMADO EN SU PLAN DIRECTOR.

CARACTERÍSTICAS

PÁGINAS: 104	PLANOS: 0	ILUSTRACIONES: 18	CD-ROM: 1

PLAN ESTRATÉGICO PARA LA GESTIÓN DEL SISTEMA DE INFORMACIÓN DE GEOLOCALIZACIÓN INKO DE LA EMPRESA COOTRANSHACARITAMA OCAÑA, BASADO EN LA NORMA ISO/IEC 27001/2013

AUTOR:

VICTOR MANUEL PÉREZ CONTRERAS

Proyecto de Grado para Optar el Título de Ingeniero de Sistemas

Director:

EDUAR BAYONA IBÁÑEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

INGENIERÍA DE SISTEMAS

Ocaña, Colombia Agosto de 2016

Índice

Lista de tablas

Pág.

Lista de gráficas

Pág.

Lista de figuras

Lista de apéndices

Resumen

Un sistema de información es un conjunto de elementos que interactúan entre sí con un fin común; que permite que la información esté disponible para satisfacer las necesidades en una organización, un sistema de información no siempre requiere contar con recuso computacional aunque la disposición del mismo facilita el manejo e interpretación de la información por los usuarios. Los elementos que interactúan entre sí son: el equipo computacional (cuando esté disponible), el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

Entrada de información: proceso en el cual el sistema toma los datos que requiere.

Almacenamiento de información: pude hacerse por computadora o archivos físicos para conservar la información.

Procesamiento de la información: permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones

Salida de información: es la capacidad del sistema para producir la información procesada o sacar los datos de entrada al exterior.

Los usuarios de los sistemas de información tienen diferente grado de participación dentro de un sistema y son el elemento principal que lo integra, así se puede definir usuarios primarios quienes alimentan el sistema, usuarios indirectos que se benefician de los resultados pero que no interactúan con el sistema, usuarios gerenciales y directivos quienes tienen responsabilidad administrativa y de toma de decisiones con base a la información que produce el sistema

Introducción

El plan estratégico es un documento en el que los responsables de una organización reflejan cual será la estrategia a seguir por su compañía en el medio plazo. Aunque en muchos contextos se suelen utilizar indistintamente los conceptos de plan director y plan estratégico, la definición estricta de plan estratégico indica que éste debe marcar las directrices y el comportamiento para que una organización alcance las aspiraciones que ha plasmado en su plan director. De otra parte se forja como un documento sostenible en el tiempo, aunque debe estar atento a los cambios y supeditado a un proceso de acción, evaluación y reajustes. Es, en este sentido, un compromiso de gestión, compartido por las empresas que poseen el sistema, convirtiéndose este en una política institucional que trasciende las personas, en la medida que provee de los elementos indispensables para construir y consolidar una mejor información

El siguiente trabajo contiene un marco referencial, de la misma forma se puede encontrar el diseño metodológico, el cual se basó la investigación descriptiva; se elaboraron diferentes matrices que ayudaron a determinar una serie de estrategias que contribuirán al mejorar la calidad del servicio. El segundo apartado refiere a la descripción de los elementos que conforman su contexto de inserción en el marco de los nuevos lineamientos de la política.

Se detallan cuestiones referidas a su inserción local, provincial y regional para luego describir su Misión, Visión y Objetivos Institucionales, áreas estratégicas de intervención y objetivos de cada una de ellas así como un diagnóstico institucional mediante una matriz de fortalezas, oportunidades, debilidades y amenazas (FODA).

Capítulo 1: Plan estratégico para la gestión del sistema de información de geolocalización Inko de la empresa Cootranshacaritama Ocaña, basado en la norma ISO/IEC 27001/2013

1.1 Planteamiento del Problema

El sistema de Localización por Satélite (GPS: Global Position System) es el resultado de la experiencia recogida del satélite espacial estadounidense Vanguard (exclusivamente de uso militar), mismo que puso de manifiesto que la transmisión de señales de radio desde el espacio podría servir para orientarnos y situarnos en la superficie terrestre. Los equipos GPS en la actualidad se han convertido en una herramienta de trabajo, ya que pueden ser utilizados en aeronaves, para guiarse en el espacio, por los geólogos para la medición de movimientos telúricos, por ingenieros y guardia civil para monitoreo de monumentos o estructuras como puentes colgantes, para seguimiento vehicular unitario o de flota y evidentemente por la fuerza militar. La gran prueba de fuego del sistema GPS desde el punto de vista práctico como instrumento de ayuda a la navegación, se la realizó en Norteamérica con el trasbordador espacial Discovery en el mismo año en que se puso en funcionamiento el sistema, es decir, en 1993. Actualmente los satélites GPS pertenecen a una segunda generación denominada Block II. (García Alvares, 2016)

El giro tecnológico que ha tenido la industria nacional, los diferentes desarrollos de programas aplicaciones en el mercado, el cambio de la legislación colombiana en materia de protección de derechos de autor exige a las organizaciones una relación fuerte entre la auditoría y

los sistemas informáticos y por parte de las empresas considerar un proceso permanente de implementación del sistema de control interno con énfasis en ambientes de procesamiento electrónico de datos, refiere Solano (2011, pág.8). Esto ha hecho que la información cree un espacio bastante importante en todas las organizaciones, corriendo el riesgo de dejar de funcionar si no es tenida en cuenta, principalmente si se habla de empresas altamente automatizadas, siendo su seguridad un punto estratégico, basta con mirar sus actividades para conocer que la seguridad es el factor más determinante por el cual fracasan las organizaciones. (Carreón, 2015)

La empresa COOTRANSHACARITAMA Ocaña, maneja con el sistema de información de geolocalización INKCO, un monitoreo de los vehículos que se encuentran afiliados a la empresa, buscando con ello llevar un mejor control y brindar un excelente servicio a sus usuarios, mediante un sistema de información, sin embargo no cuenta con un Plan Estratégico que le permita manejar de forma segura dicho sistema lo que ocasiona riesgos que atentan contra la seguridad de la información.

Por lo tanto se plantea el proyecto “Plan estratégico para la gestión del sistema de información de geolocalización INKCO de la empresa COOTRANSHACARITAMA Ocaña, basado en la norma ISO/IEC 27001:2013, para verificar y recomendar las políticas de control que debe asumir la empresa.

1.2 Formulación del Problema.

¿Traerá beneficios para la empresa COOTRANSHACARITAMA de Ocaña, el diseño de un plan estratégico para el sistema de información de geolocalización INKCO?

1.3 Objetivos

1.3.1 General. Diseñar un plan estratégico para la gestión segura del sistema de información de geolocalización INKCO, de la empresa Cootranshacaritama, basado en la norma ISO/IEC 270012013.

1.3.2 Específicos. Realizar una auditoría al sistema INKCO que maneja la empresa Contrashacaritama Ocaña con el propósito de identificar las fortalezas, oportunidades, amenazas, debilidades y riesgos de la empresa.

Determinar los posibles controles que sean necesarios para mantener segura la información que se maneja a través del sistema de información de geolocalización INKCO.

Estructurar el documento del Plan estratégico.

Socializar a la directiva de la empresa Cootranshacaritama, sobre los resultados de la auditoría y el diseño del plan estratégico.

1.4 Justificación.

Actualmente, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas informáticas disponibles, buscando proteger los datos, de la aparición de nuevas amenazas en los sistemas informáticos. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías. Por ello, la integridad de la información, es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla en la integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema. (Educación, 2010)

Ahora bien, en el caso del área de tecnologías de información, que actualmente juega un papel protagónico, es necesario clarificar de qué manera contribuye al logro de los objetivos de la organización, para lo cual se establece el proceso de planeación estratégica de Tecnologías de Información (TI). Es reconocido que las TI son esenciales para manejar las transacciones, la información y el conocimiento necesario para ejecutar y sostener actividades económicas y sociales. Estas actividades cada vez son más globalizadas y requieren de la colaboración entre distintas entidades para ser satisfactorias, es por ello que la metodología de Gobernabilidad TI propende por gestionar tópicos como el alineamiento estratégico, la medición de los activos informáticos, la gestión de riesgo, la generación de valor y la administración de los recursos y activos de TI. (Gonzales, 2012)

Debido a lo anterior, COOTRANSHACARITAMA ha decidido incursionar en el mundo de gobernabilidad TI, para controlar su posicionamiento en la ciudad, trabajando con geoprocedimientos, mediante el programa de información INKCO, buscando controles de seguridad para proteger la información y permitan a la empresa desarrollarse eficientemente, a la vez de cumplir con las actividades sin tener inconvenientes que lleven a la paralización de las mismas. Para ello se plantea con el proyecto, la aplicación de la norma ISO/IEC 27001:2013, para verificar y recomendar las políticas de control que debe asumir la empresa.

1.5 Delimitaciones.

1.5.1 Conceptual. El presente diagnóstico se fundamentará en conceptos tales como: seguridad de la información, riesgos, políticas de seguridad de la información, controles, Norma ISO 27001:2013.

1.5.2 Operativa. El incumplimiento de los objetivos del presente trabajo, puede darse por factores ajenos al autor; sin embargo, en caso de presentarse inconvenientes, se buscará la asesoría a través del director del trabajo de grado.

1.5.3 Temporal. Se determina que el proyecto para su realización tendrá una duración de doce (12) semanas, de acuerdo con el cronograma de actividades que se incorpora al estudio.

1.5.4 Geográfica. Este proyecto se desarrollará en las instalaciones de la empresa COOTRANSHACARITAMA, en la ciudad de Ocaña, Norte de Santander.

Capítulo 2: Marco Referencial

2.1 Marco Histórico.

2.1.1 Antecedentes a nivel internacional.

No se encontraron antecedentes a nivel internacional, referentes al tema.

2.1.2 Antecedentes a nivel nacional.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior **– ICETEX**

2014

El Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior – ICETEX identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que el instituto establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada. Este documento describe las políticas y normas de seguridad de la información definidas por el ICETEX. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, el capítulo décimo segundo del título primero de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013. (exterior, 2015)

Los riesgos actuales aportan al modelo de gestión de seguridad de la información sugerido por el Ministerio de las Tecnologías de la Información ESTRATEGIA DE GOBIERNO EN LINEA el cual permite a la entidad identificar y minimizar los riesgos a que está expuesta la información y los procesos y elementos asociados a ella. Dado el gran esfuerzo y recursos que demanda el SGSI, la entidad ha venido adoptando transicionalmente una serie de políticas y medidas que le permitan ir avanzando hasta alcanzar el nivel de madurez necesario. Por lo anterior, la política y el desarrollo del SGSI serán revisadas con regularidad como parte del proceso de revisión gerencial, o en la medida que se sugieran cambios en el desarrollo del negocio, estructura, objetivos o estrategias que involucren aspectos afines. (social, 2013)

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el

Departamento Administrativo de la Presidencia de la República - DAPRE, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección General. Para ello, se presentó en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer y cumplir todos los directivos, funcionarios contratistas y terceros que presten sus servicios o tengan algún

tipo de relación con el Departamento Administrativo de la Presidencia de la República. (Republica, 2014)

2.1.3 Antecedentes a nivel regional. El diseño de las políticas de seguridad de la información basada en la ISO 27002, para la Alcaldía Municipal de La Playa de Belén, se plantean, teniendo en cuenta que la seguridad de la información y el estudio de amenazas de riesgos de la información proporcionan ventajas para implantar procedimientos, métodos y controles con el objeto de administrar, proteger y salvaguardar uno de los activos más importantes, como es la información. También repercute en el uso de recursos de hardware y el acceso controlado a las necesidades del usuario para cumplir eficientemente con sus actividades. Una política de seguridad de la información es una forma de comunicarse con los usuarios, pues las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la Institución. (Vergel Trigos & Sepulveda Arenas, 2015)

En vista de la importancia que tiene la seguridad en las tecnologías de la información, no es suficiente estudiar buenas prácticas y consejos sabios de personas que llevan una gran trayectoria en el área de la informática, sino que más aún, Normas Internacionales, son un beneficio de grandes magnitudes para cualquier organización con necesidades relacionadas con la seguridad de las tecnologías de la información, mediante la implementación de acciones y procedimientos necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información. Es por esto que se establecen las políticas de seguridad de la información para la alcaldía municipal de Río de Oro (Cesar), con el objetivo de proteger la información y demás activos importantes para esta, mediante la implementación de esta guía, que incluye las medidas

de seguridad necesarias que contribuirán a mantener la integridad, confidencialidad y disponibilidad de los datos, a través de la realización de sus labores diarias. (Sanchez, 2012)

2.1.4 Antecedentes a nivel local. Con esta guía se creó una herramienta que brinde apoyo para poder proteger nuestra información de la mejor manera y de acuerdo a la situación actual; y que oriente en ese camino, dando recomendaciones acerca de cómo mejorar los procesos para proteger la información. Conveniente a la necesidad que presenta el Hospital Emiro Quintero Cañizares correspondiente a la implementación de un nuevo sistema de información y teniendo en cuenta la gran utilidad que este representa para la institución, del cual recibirán beneficios el personal encargado de manipular dicho sistema, como los usuarios de la institución, debido a la agilidad y veracidad a la hora de trasmitir comunicación interna o externa, debido a la actividad que desempeña la institución y con la nueva implementación se fortalecería la estructura organizacional brindando así cualidades con las cuales la empresa, las utilizaría de forma adecuada para enfocar, dirigir, controlar las labores diarias y programas de expansión de sus servicios, además de incrementar su valor patrimonial. (Vergel Sanchez & Martinez Portillo, 2015)

La norma ISO 27001, cubre a todo tipo de organizaciones, este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS, La información actualmente es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se

encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros.

BSI historia. 1901 Nacimiento del BSI

1910 Creación del primer estándar

1926 Inicio del proceso de certificación de productos

1946 Creación de la ISO por parte de miembros del BSI

1979 Primer estándar para sistemas de gerencia (Bs 5750)

1992 Primer estándar sobre el medio ambiente

1999 Elaboración del estándar sobre seguridad de la información (BS 7799)

BSI historia 2. Desarrollo del estandar BS 7799

1993Reuniones de un grupo multi- sectorial

Primer borrador de codigo de practicas

1995 Publicacion Oficial BS 7799:1 codigo de buenas practicas

1998 Publicacon oficial BS 7799:2 especificaciones SGSI

1999 Publicidad oficial BS 7799:1999 parte 1 y 2

2002 Publicidad de nueva version BS 7799: 2

ISO/IEC 27002: historia.

2000 ISO/IEC 17799:2000 código de buenas practicas

2002 UNE ISO/IEC 17799 código de buenas prácticas

2004 UNE 71502 especificaciones SGSI

2005 ISO 17799:2005 código de buenas practicas

2005 ISO/IEC 27001 especificaciones SGSI

2007 ISO/IEC 17799 – ISO/IEC 27002

2013 ISO/IEC 27001:2013 borrador final 07/2013, norma a fines de 2013, esta versión tendrá 114 controles en 14 dominios (en la actual versión son 133 controles en 11 dominios)

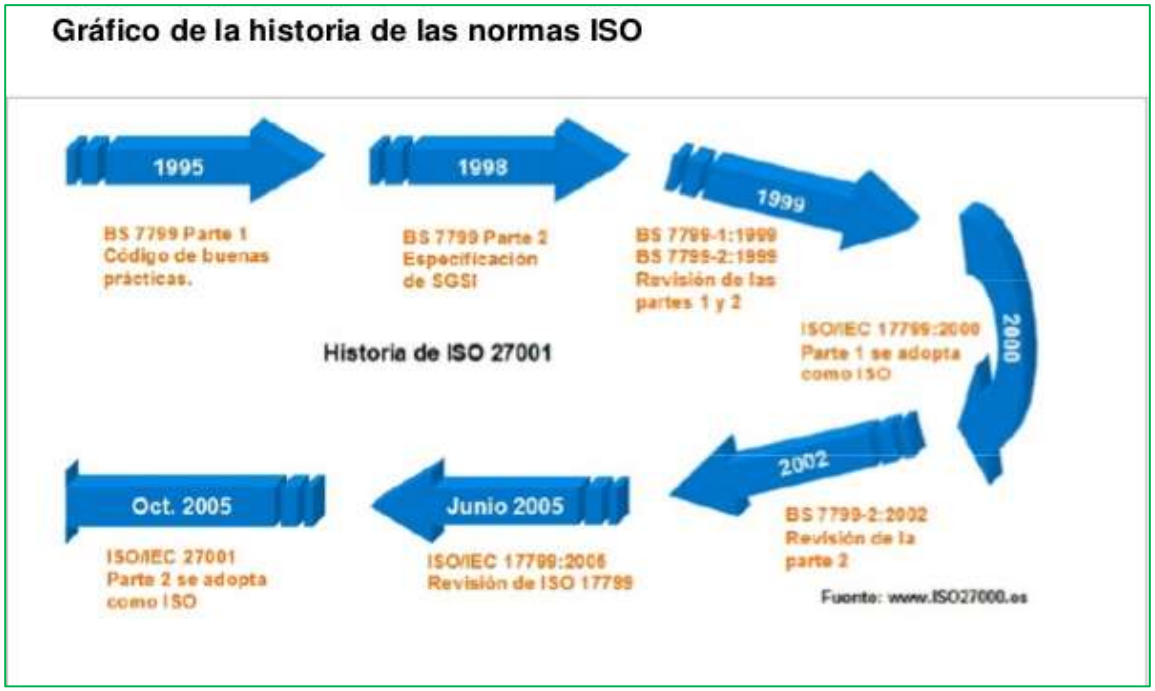


Figura 1. Historia de las normas ISO

2.2 Marco Conceptual.

2.2.1 Seguridad Informática. La definición de seguridad informática proviene entonces de los dos términos antes definidos. La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos y la información de daños accidentales o intencionados. (Villalon Huerta, 2004)

Objetivo de la seguridad informática. La seguridad informática tiene como principal objetivo proteger el activo más importante que tiene la empresa que es su información de los riesgos a los que está expuesta. Para que la información sea considerada confiable para la organización ya que sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación de la misma, esta deberá cubrir los tres fundamentos básicos de seguridad para la información que son:

Confidencialidad. Se define como la capacidad de proporcionar acceso a usuarios autorizados, y negarlo a no autorizados.

Integridad. Se define como la capacidad de garantizar que una información o mensaje no han sido manipulados.

Disponibilidad. Se define como la capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial. (Villalon Huerta, 2004)

2.2.2 Riesgos. Los riesgos se pueden definir como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y según la Organización Internacional por la Normalización (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños". A raíz de esta definición podemos concluir que cualquier problema que afecte al total funcionamiento de la empresa es considerado un riesgo o amenaza para la entidad. (Hernandez Pinto, 2006)

Tipos de amenazas a la seguridad. Ninguna empresa está exenta de sufrir amenazas a su seguridad, estas amenazas a las que son vulnerables las organizaciones son expuestas en la siguiente figura.

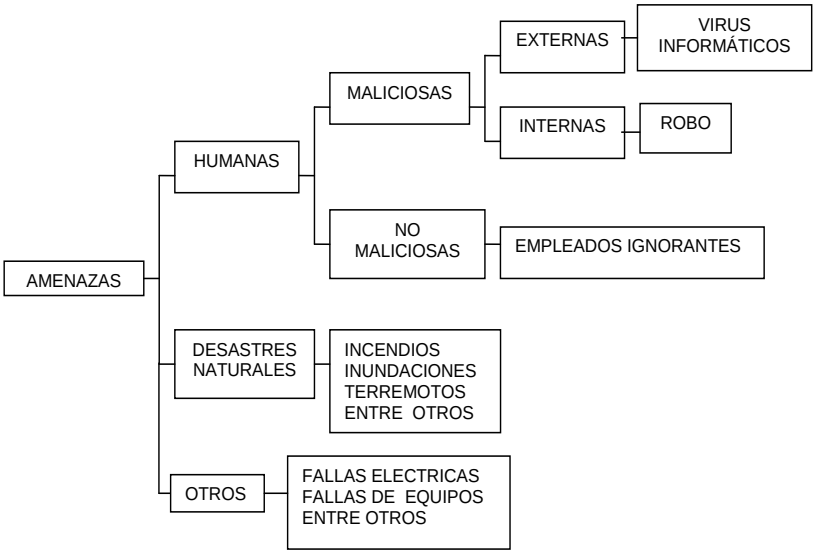


Figura 2. Tipos de Amenazas

Amenazas humanas. "Las amenazas humanas como su nombre lo indica son aquellas acciones provocadas por el hombre y pueden ser de dos tipos maliciosas y no maliciosas. (Lucena López, 1999)

Maliciosas. Las amenazas maliciosas son aquellas que se llevan a efecto con el propósito de causar daño a la organización.

Las amenazas externas que pueden afectar al desarrollo y buen funcionamiento de las actividades de las empresas son frecuentemente originadas por el acceso a internet, ya que en esta red existen una serie de peligros como son los virus, hackers, entre otros que infiltrándose en la red interna de la organización provocando daños como mal funcionamiento de los sistemas y pérdida de información.

Las amenazas internas más frecuentes son las originadas por los propios funcionarios y ex - funcionarios de la organización motivados por la falta de dinero o represalia por algún tipo de enfrentamiento que hayan tenido con un superior.

No maliciosas. Este tipo de amenazas son producidas en la mayoría de los casos por errores ocasionados por empleados que no cuentan con el conocimiento o adecuada capacitación en el manejo de equipos y sistemas".

Amenazas por desastres naturales. Estas amenazas originadas por la naturaleza son las menos frecuentes en las organizaciones pero aun así no podemos dejar de considerarlas.

Otras amenazas son aquellas referentes a las que están fuera del alcance del hombre como son las interrupciones eléctricas, fallas de equipos originadas por los cortes de energía o no mantenerlos en el ambiente adecuado aunque esta es una responsabilidad más bien de carácter humano; entre otros.

¿Cómo enfrentar los riesgos? Para (Lucena López, 1999), los problemas de seguridad se multiplican con gran facilidad, por lo que las empresas deben perfeccionar los sistemas y los procesos para evitar amenazas o abordarlas cuando se produzcan. Para garantizar que la información de nuestra organización posea las características de seguridad ya mencionadas como son la confidencialidad, integridad y disponibilidad se debe poner en práctica un plan de seguridad informática.

2.2.3 Plan estratégico de seguridad informática. Un plan estratégico de seguridad informática está basado en un conjunto de políticas de seguridad elaboradas previo a una evaluación de los riesgos que indicará el nivel de seguridad en el que se encuentre la empresa. Estas políticas deben ser elaboradas considerando las características del negocio, la organización, su ubicación, sus activos y tecnología que posee la empresa.

2.2.4 Evaluación de los riesgos. La evaluación de los riesgos es el proceso por el cual se identifican las vulnerabilidades de la seguridad.

Por tanto el objetivo general de evaluar los riesgos será identificar las causas de los riesgos potenciales, en toda la organización, a parte de ella o a los sistemas de información individuales, a componentes específicos de sistemas o servicios donde sea factible y cuantificarlos para que la Gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos, en los diferentes puntos de análisis. (Aguirre, 2006)

Los pasos para realizar una valoración de riesgos se detallan a continuación:

Identificar los riesgos

Análisis de los riesgos

Identificar riesgos. En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático, existen formas de identificarlos como:

Cuestionarios de análisis de riesgos. La herramienta clave en la identificación de riesgos son los cuestionarios los mismos que están diseñados para guiar al administrador de riesgos para descubrir amenazas a través de una serie de preguntas y en algunas instancias, este instrumento está diseñado para incluir riesgos asegurables e in-asegurables. El cuestionario de análisis de riesgos está diseñado para servir como un repositorio de la información acumulada de documentos, entrevistas e inspecciones. Su propósito es guiar a la persona que intenta identificar exposiciones a riesgo a través del proceso de la identificación en un modelo lógico y consistente.

Listas de chequeo de exposiciones a riesgo. Una segunda ayuda importante en la identificación de riesgos y una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo, las cuales son simplemente unas listas de exposiciones a riesgo.

Listas de chequeo de políticas de seguridad. Esta herramienta incluye un catálogo de varias políticas de seguridad que un negocio dado puede necesitar. El administrador de riesgos consulta las políticas recolectadas y aplicadas a la firma. (Echenique Garcia J. A., 2007)

Sistemas expertos. Un sistema experto usado en la administración de riesgos incorpora los aspectos de las herramientas descritas anteriormente en una sola herramienta. La naturaleza integrada del programa permite al usuario generar propósitos escritos y prospectos.

Análisis de riesgos. Una vez se hayan identificado los riesgos, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

Ponderación de los Factores de riesgo. Ponderar el factor de riesgo es darle un valor de importancia en términos porcentuales al mismo bajo los criterios de especialistas en el área informática que pueden identificar su impacto en la organización, teniendo en cuenta las posibilidades de que se puedan convertir en realidad.

Valoración del riesgo. La valoración del riesgo envuelve la medición del potencial de las pérdidas y la probabilidad de la pérdida categorizando el orden de las prioridades. (Aguirre, 2006)

Cuadrante	Valoración del riesgo
Impacto significante y probabilidad Alta	Alto
Impacto significante y probabilidad Baja	Medio-alto
Impacto insignificante y probabilidad Alta	Medio-bajo
Impacto insignificante y probabilidad Baja	Bajo

Una explicación más clara de la valoración es la siguiente:

Riesgo alto: Todos las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota.

Riesgo medio: Son exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.

Riesgo bajo: Exposiciones a pérdidas que no causan un gran impacto financiero.

2.2.5 Políticas de seguridad. Una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Si bien existen algunos modelos o estructuras para su diseño, estás tienen que ser elaboradas de forma personalizada para cada empresa para así recoger las características propias que tiene la organización.

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

Seguridad Física

Seguridad Lógica

Seguridad en redes

Seguridad en los recursos humanos

Seguridad en el Outsourcing

Planes de Contingencia

Elementos de una política de seguridad. Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

Objetivos de la política y descripción clara de los elementos involucrados en su definición.

Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.

Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.

Definición de violaciones y sanciones por no cumplir con las políticas.

Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer:

Explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. (Monterroso, 2006)

Deberán establecer las expectativas de la organización, tales expectativas deben tener relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Las políticas deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc. (Monterroso, 2006)

2.2.6 Seguridad Física. La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir el procesamiento de la información.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de cómputo.
Las principales amenazas que se prevén en la seguridad física son:

Desastres naturales, incendios accidentales tormentas e inundaciones.

Amenazas ocasionadas por el hombre.

Disturbios, sabotajes internos y externos deliberados.

Otras amenazas como las fallas de energía eléctrica o las fallas de los equipos.

Los recursos que se deben proteger físicamente van desde un simple teclado hasta un respaldo de toda la información que hay en el sistema, pasando por la propia máquina, igualmente se deben tener medidas de protección contra las condiciones climáticas y suministros de energía que pueden afectar la disponibilidad de los sistemas de información e interrumpir los procesos de la organización. (Monterroso, 2006)

Seguridad de acceso físico. Se refiere a las medidas de seguridad para evitar el acceso de personas no autorizadas a los dispositivos de hardware y cualquier medio de salida de información como fax, copiadoras entre otros, ubicados tanto en el área de sistemas como en las áreas usuarias. (Monterroso, 2006)

Organización. Para llevar un buen control de los accesos a la organización no sólo se requiere la capacidad de identificación, sino también negar asociarla a la apertura o cerramiento de puertas, permitir o negar accesos basados en restricciones de tiempo, área o sector de la empresa.

Existen varios métodos de control entre ellos están:

Guardias de seguridad

Detectores de Metales

Sistemas Biométricos

Seguridad con Animales

Protección Electrónica

Guardias de seguridad. *La utilización de guardias de seguridad será con el fin de controlar* el acceso de personas ajenas a la organización y del mismo personal que ahí trabaje; la guardianía debe ser durante las 24 horas del día y deben estar armados para lo cual el personal de seguridad debe poseer un permiso para el manejo de armas otorgado por la autoridad pertinente.

Algunas medidas de seguridad podrían ser:

Credenciales de identificación*:* Cualquier persona que ingrese a la organización deberá llevar una credencial.

Estás credenciales pueden clasificarse de la siguiente manera:

Normal o definitiva: para el personal permanente de planta.

Temporaria: para personal recién ingresado.

Contratistas: personas ajena a la empresa, que por razones de servicio deben ingresar a la misma.

Visitas.

Bitácora de registro de accesos: Las personas ajenas a la organización deberán llenar este formulario que deberá contener el motivo de la visita, hora de ingreso, etc.

Control de Vehículos*:* Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

La utilización de guardias de seguridad también tiene su desventaja que es el soborno del guardia por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o salir de la empresa con equipos que no ha sido autorizado su salida. (Monterroso, 2006)

Área de sistemas. El área de sistemas es considerada como la más sensible a las amenazas debido a que en ella están ubicados los equipos que contienen toda la información que es procesada en las áreas usuarias y se le debe brindar un control adecuado y exclusivo.

Dentro de la organización lo más óptimo para mantener la seguridad y evitar accesos no permitidos al área de sistemas es implementar como medio de protección los siguientes recursos:

Puerta con cerradura

Puerta de combinación

Puerta electrónica

Puertas sensoriales

Registros de entrada

Videocámaras

Escolta controladora para el acceso de visitantes

Puertas dobles

Alarmas

Seguridad en la ubicación y Dimensión del área de sistemas. Se refiere a las precauciones que se deben tomar en cuenta para la instalación física del área que servirá como eje central del procesamiento de la información de la empresa evitando de esta manera los accesos no permitidos, otras interrupciones y la falta de espacio físico para la adecuada operación del área.

Seguridad del equipamiento. La información vital de la organización es procesada en los equipos de computación los cuales deben recibir cuidados especiales para prevenir posibles fallas ocasionadas por la electricidad, temperatura o falta de mantenimiento del equipo que puedan provocar interrupciones mientras se estén procesando los datos. (Monterroso, 2006)

2.3 Marco Teórico

Hablar de evolución de seguridad es complejo, desde el inicio de la vida en comunidad, existían acciones para evitar amenazas, proteger la vida y las posesiones, allí se usaban métodos defensivos y se manejaban conceptos de alertar, evitar, detectar, alarmar y reaccionar a los diferentes hechos que podían suceder.

La familia, posteriormente diseñó esquemas de protección y se crearon lugares para resguardarse.

Algunos descubrimientos arqueológicos denotan con evidencias la importancia de la seguridad para los antiguas generaciones, entre estos tenemos las pirámides egipcias, el palacio de Sargon, el Dios egipcio Anubis, los Sumaricos, el Código de Hammurabi, entre otros.

Hasta se dice que Julio César utilizaba esquemas de seguridad en época de guerra y en el gobierno.

La seguridad moderna se originó con la revolución industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero de la administración Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice: "salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y traiciones por parte del personal, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio." (Hernandez Pinto, 2006)

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese los equipos, ni siquiera el empleado. Con la aparición de las computadoras, esta mentalidad se mantuvo, porque ¿Quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera.

Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

La ISO/IEC 27001:2013, es un estándar internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

En función del tamaño y necesidades se implementa un SGSI con medidas de seguridad más o menos estrictas, que en cualquier caso pueden variar a lo largo del tiempo.

El COBIT es un framework (también llamado marco de trabajo) de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de TI que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

Describe como los procesos de TI entregan la información que el negocio necesita para lograr sus objetivos. Para controlar la entrega, COBIT provee tres componentes claves, cada uno formando una dimensión del cubo COBIT.

Como un framework de gobierno y control de TI, COBIT se enfoca en dos áreas claves:

Proveer la información requerida para soportar los objetivos y requerimientos del negocio.

Tratamiento de información como resultado de la aplicación combinada de recursos de TI que necesita ser administrada por los procesos de TI.

2.4 Marco Legal.

2.4.1 Constitución Política de 1991. En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: “La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley” y en el 269, se soporta el diseño del sistema: “En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas”. (Congreso de la República , 2012)

2.4.2 Leyes informáticas colombianas. Ley estatutaria 1266 del 31 de diciembre de 2008: Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Congreso de la Republica , 2012)

2.4.3 Ley 1273 del 5 de enero de 2009. Delitos informáticos: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Congreso de Colombia, 2014)

2.4.4 Ley 1341 del 30 de julio de 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. (Congreso de la República, 2011)

2.4.5 Ley estatutaria 1581 de 2012: Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

4. Crea una especial protección a los datos de menores de edad.

5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

8. Crea el Registro Nacional de Bases de Datos.

9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos. (Congreso de Colombia, 2014)

2.4.3 Ley 603 de 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. (Congreso de la República, 2015)

2.4.4 El derecho de autor Constitución Política de 1991: En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

Ley 44 de 1993 (febrero 15), modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. (Congreso de la República , 2012)

2.4.5 Decreto 1360 de 1989 (junio 23). "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor". (Congreso de Colombia, 2010)

2.4.6 Decreto 1474 de 2002 (Julio 15). "Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)". (Congreso de la República, 2010)

2.4.7 Ley 734 de 2002, Numeral 21 y 22 del Art. 34: son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización" (Congreso de Colombia, 2010)

2.4.8 Decreto 1377 de 2013: Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. (Congreso de Colombia, 2015)

Capítulo 3: Diseño Metodológico

3.1 Tipo de Investigación.

Para llevar a cabo el presente proyecto se utilizará el tipo de estudio descriptivo, ya que los estudios descriptivos utilizan el método de análisis para lograr caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades, combinada con ciertos criterios de clasificación, sirve para ordenar, agrupar o sistematizar los objetos propuestos. Además, con la investigación descriptiva y el método cuantitativo, se buscará determinar hechos y características del problema en estudio mediante la pregunta, descripción y observación de situaciones concretas, facilitando así el análisis de las ventajas y los beneficios que traerá el plan estratégico para la gestión del sistema de información de geolocalización INKCO, de la empresa Cootranshacaritama Ltda, de la ciudad de Ocaña

3.2 Población y Muestra.

3.2.1 Población. La población está conformada por los empleados de la Cooperativa Cootranshacaritama Ltda., los cuales son en total 14 personas, distribuidos en las diferentes áreas de la empresa.

3.2.2 Muestra. Teniendo en cuenta la cantidad mínima de personas encontrada en la población, se tomará como muestra toda la población involucrada en el proceso.

3.3 Fuentes de Información.

Las fuentes de información son todos aquellos medios de los cuales procede la información, que satisfacen las necesidades de conocimiento de una situación o problema presentado y posteriormente será utilizado para lograr los objetivos esperados (p.29). De acuerdo a su origen se clasifican en:

Fuentes primarias. Contienen información original, que ha sido publicada por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más. Son producto de una investigación o de una actividad eminentemente creativa. Componen la colección básica de una biblioteca, y pueden encontrarse en formato tradicional impreso como los libros y las publicaciones seriadas; o en formatos especiales como las microformas, las videocasetes y los discos compactos.

Fuentes secundarias. Contienen información primaria, sintetizada y reorganizada. Están especialmente diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Componen la colección de referencia de la biblioteca y facilitan el control y el acceso a las fuentes primarias.

La fuente secundaria que se consultará está la Biblioteca Argemiro Bayona, de la Universidad Francisco de Paula Santander, asesores, especialistas y conocedores del tema.

Capítulo 4: Presentación de Resultados

4.1 Auditoría al Sistema INKCO que Maneja la Empresa Cootranshacaritama Ocaña con el Propósito de Identificar las Fortalezas, Oportunidades, Amenazas, Debilidades y Riesgos de la Empresa

La auditoría de sistemas tiene como objetivo evaluar sistemas informáticos en forma integral, los procedimientos y seguridad de los equipos electrónicos o hardware de los programas o software que posea la empresa sean propios o de modalidad de servicios.

La empresa Cootranshacaritama Ltda., se encuentra estructurada de la siguiente manera:

Misión. Somos una cooperativa afiliadora de vehículos de servicio público, que cuenta con un personal capacitado, dispuesto a implementar continuamente sistemas apropiados en busca de la excelencia, para brindar a sus asociados mejor calidad de vida y a sus usuarios comodidad, seguridad y un óptimo servicio, promoviendo los valores cooperativos de autoayuda, responsabilidad, solidaridad, equidad y compromiso.

Visión. Ser una empresa con responsabilidad social preocupada por la conservación del medio ambiente, económicamente sólida, moderna y tecnificada que a partir de la administración de vehículos promueva el mejoramiento de la calidad de vida del asociado mediante la prestación del servicio de transporte público con altos niveles de satisfacción de las necesidades de los usuarios generando un desarrollo socioeconómico para Ocaña y la región.

Objetivos. Facilitar a los asociados el suministro de todos los artículos que sean necesarios para el normal desarrollo y funcionamiento de la industria del transporte en forma solidaria.

Propiciar la educación cooperativa. Parágrafo: para el cumplimiento de sus objetivos la cooperativa podrá

Prestar los servicios que a continuación se detallan:

Atender los requerimientos sobre el mantenimiento al parque automotor y el consumo industrial, de acuerdo al registro de propiedad o tendencia de los vehículos vinculados a la cooperativa.

Administrar y coordinar la organización de los sistemas de transporte terrestre automotor de servicio público para pasajeros y carga, dentro de las rutas y horarios que les sean asignados, conforme a la legislación pertinente; así como también, encomiendas y envíos.

Administrar y prestar a sus asociados los servicios relacionados con la industria del transporte terrestre automotor de uso público para pasajeros; el de carga de pasajeros mixtos, y el de encomienda y giros. Los servicios de transporte de pasajeros se prestaran de acuerdo a la ruta y horarios fijados por las entidades competentes para zonas urbanas, suburbanas, metropolitanas, intermunicipales, interdepartamentales, nacionales e internacionales, mediante el Uso de buses, busetas, microbuses, camiones, camionetas, camperos y automóviles, así como de vehículos de

carga y pasajeros o mixtos y de acuerdo a la homologación establecida por la entidad competente.

Estructura organizacional. Contamos con una real estructura administrativa y operativa, lo cual le da la solidez, dinamismo y eficiencia para la prestación de sus servicios.

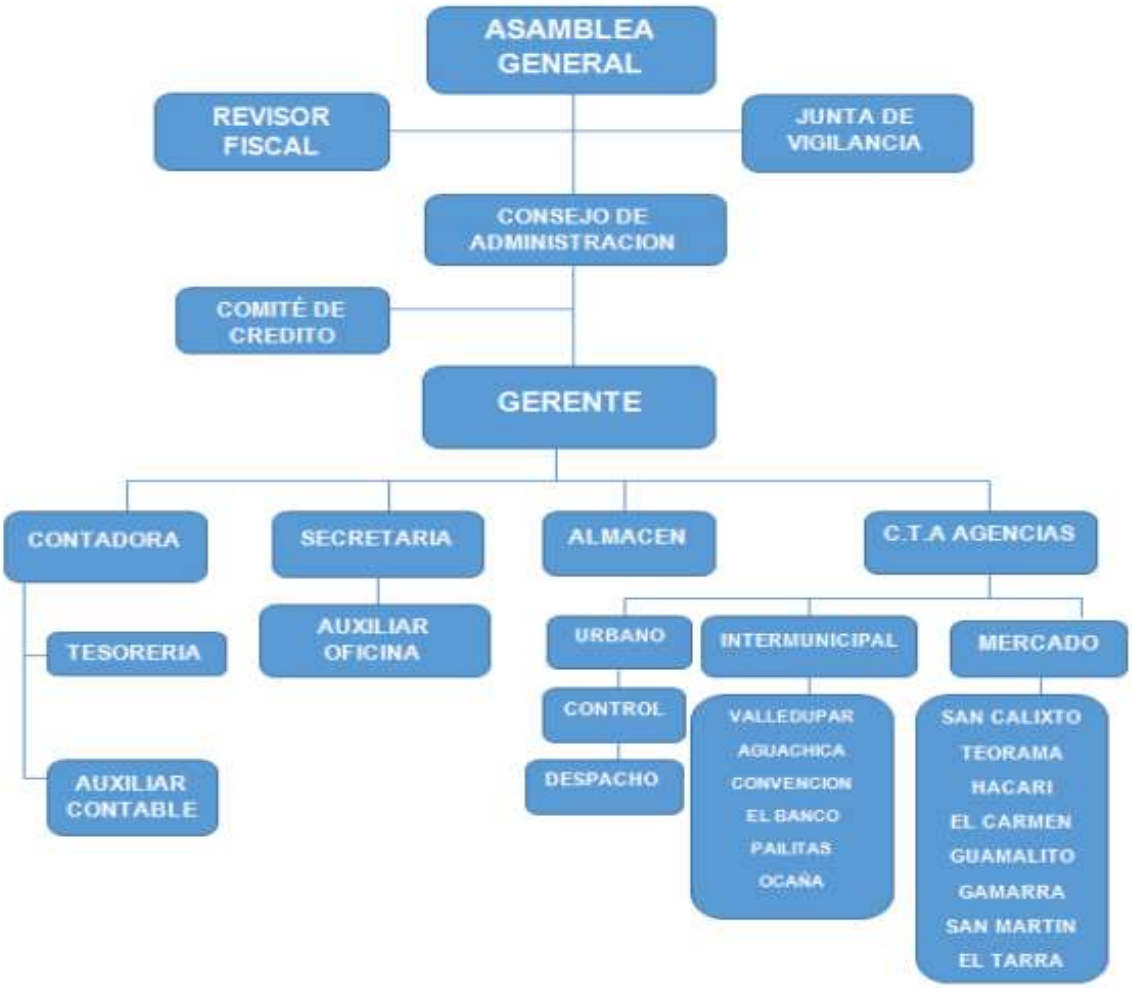


Figura 3. Estructura organizacional

Fuente: Cooperativa Cootranshacaritama, 2015.

Con el fin de realizar la auditoría al sistema INKCO, se realiza una lista de chequeo (apéndice B), para de esta manera obtener el resultado de la misma y así poder identificar las fortalezas, oportunidades, amenazas, debilidades y riesgos de la empresa, las cuales fueron llevadas a una matriz DOFA (tabla 4).

Cootranshacaritama implementa desde ya el sistema GPS para los vehículos que están adscritos a esta empresa. La tecnología permitirá brindar un mejor servicio tanto a los usuarios como a los transportadores.

La Cooperativa Cootranshacaritama, contrata empleados a los cuales se les solicita algunos requisitos para su contratación, como lo es referencias personales y su correspondiente licencia de conducción, soat, tarjeta de propiedad del vehículo. Igualmente, al ser contratados, se ingresan al sistema de acuerdo al procedimiento establecido. En la empresa no se realiza inventario de los recursos informáticos de la misma, no existiendo un informe que muestre la existencia de éstos en la cooperativa. Además, no se cuenta con un sistema de alarmas. En cuanto al antivirus cuenta con una versión actualizada.

En cuanto al área de sistemas, se mantiene un control en el ingreso de visitantes, al igual que de los socios en los horarios no hábiles.

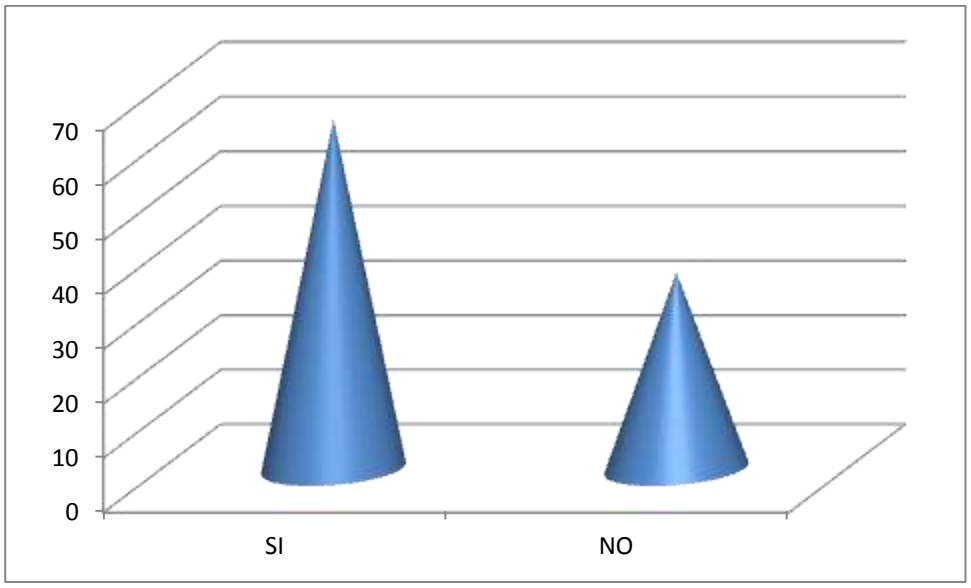
De otra se aplicó una encuesta a los empleados de la cooperativa Cootranshacarima ltda, con el objetivo de Diseñar un plan estratégico para la gestión segura del sistema de información de geolocalización INKCO, de la empresa, basado en la norma ISO/IEC 270012013.

Tabla 1.

La ubicación del centro de cómputo está libre de inundaciones, robos o cualquier situación que pueda poner en peligro los equipos.

Ítem	**Frecuencia**	**Porcentaje**
SI	9	64
NO	5	36
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 1. La ubicación del centro de cómputo está libre de inundaciones, robos o cualquier situación que pueda poner en peligro los equipos.

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

Según la afirmación de los empleados encuestados, el 64% dicen que el centro de cómputo está libre de inundaciones, robos, o cualquier otra situación que pueda llegar a afectar el

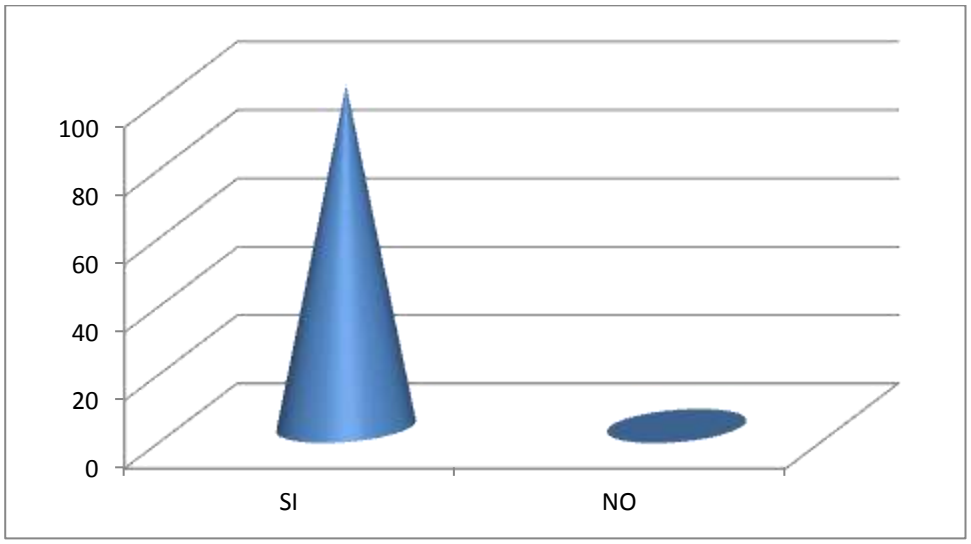
normal proceso del centro, lo que se constituye en una ventaja ya que dichos equipos no deben ser afectados por los factores antes mencionados, aunque no se puede desconocer que el 36% dicen que la seguridad no es la ideal y si están expuestos a peligros.

Tabla 2.

Lugar suficiente para los equipos

Ítem	**Frecuencia**	**Porcentaje**
SI	14	100
NO	0	0
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 2. Lugar suficiente para los equipos.

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

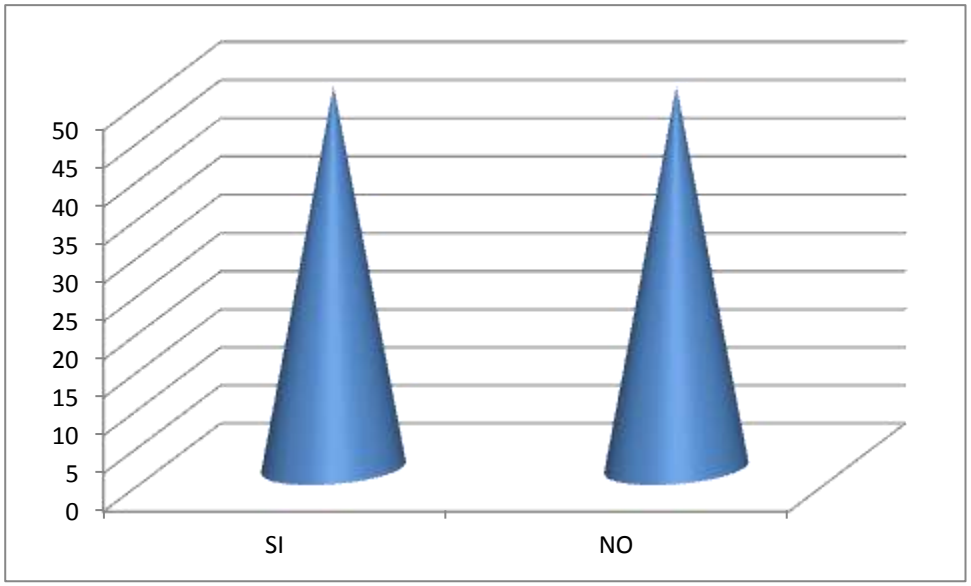
El 100% de los empleados encuestados afirman, que se cuenta con el espacio suficiente para la ubicación de los equipos existentes en la cooperativa, encontrándose en lugares amplios.

Tabla 3.

Adecuada iluminación

Ítem	Frecuencia	Porcentaje
SI	7	50
NO	7	50
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 3. Adecuada iluminación

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

La iluminación es la acción o efecto de iluminar. En la técnica se refiere al conjunto de dispositivos que se instalan para producir ciertos efectos luminosos, tanto prácticos como decorativos. Con la iluminación se pretende, en primer lugar, conseguir un nivel de iluminación - interior o exterior - , o iluminancia, adecuado al uso que se quiere dar al espacio iluminado, nivel que dependerá de la tarea que los usuarios hayan de realizar.

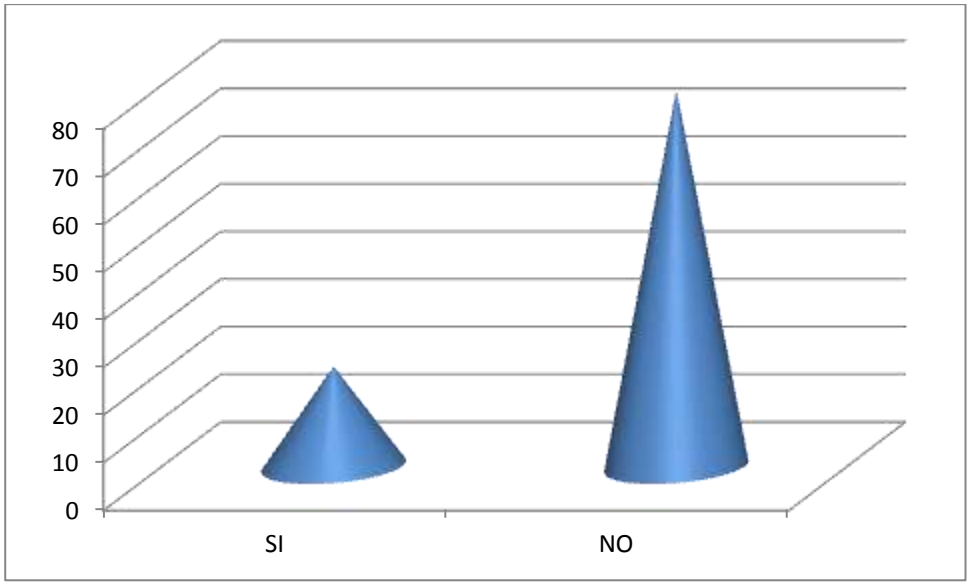
De acuerdo a lo anterior se debe decir que la iluminación del centro de cómputo es adecuada, y necesaria para la actividad que se realiza en la empresa, aunque no se puede desconocer que las opiniones en este concepto están divididas ya que el 50% dicen que adecuada y el 50% no adecuada.

Tabla 4.

Ductos del aire acondicionado limpios

Ítem	**Frecuencia**	**Porcentaje**
SI	3	21
NO	11	79
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 4. Ductos del aire acondicionado limpios

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

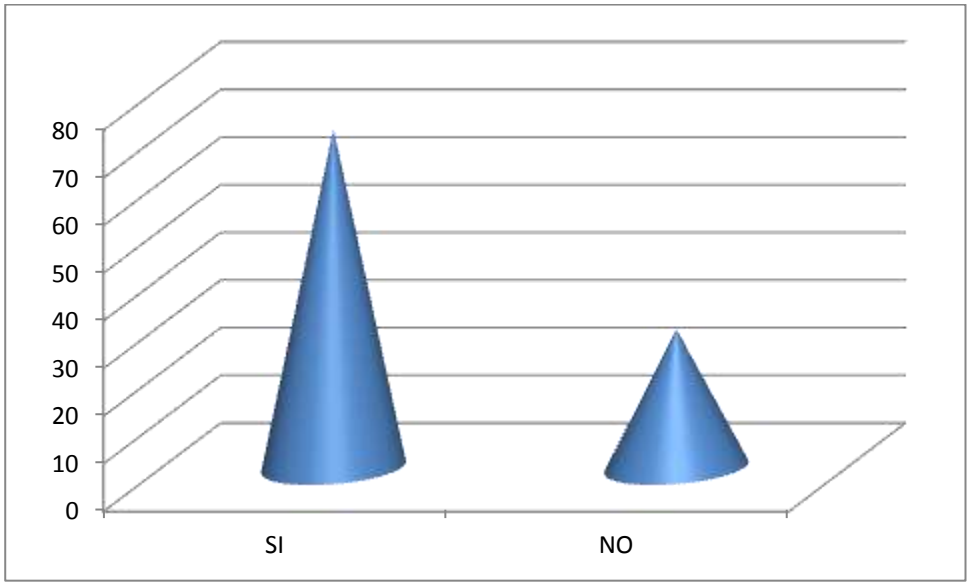
En cuanto a la limpieza de los ductos el 79% afirman que no se les hace el aseo necesario y correspondiente para tener un a adecuado funcionamiento de los mismos, por lo que en muchas ocasiones se calienta mucho el ambiente y esto puede llegar a dañar los equipos del centro, de otra parte tan solo el 21% dice que si se le realiza el mantenimiento adecuado.

Tabla 5.

Cableado correctamente instalado

Ítem	**Frecuencia**	**Porcentaje**
SI	10	71
NO	4	29
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 5. Cableado correctamente instalado

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

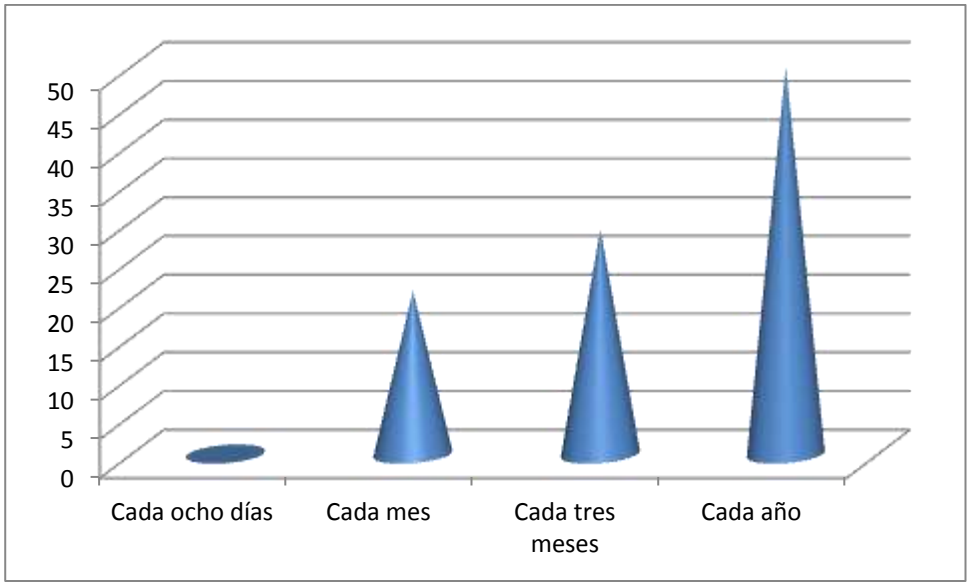
El 71% de los empleados encuestados afirman que el cableados está colocado de forma correcta, mientras que el 29% dicen que no ya que se encuentran cables que están sin asegurar, y pelados lo que puede ocasionar un corto y daño a los equipos.

Tabla 6.

Periodo se hace mantenimiento a los equipo

Ítem	Frecuencia	Porcentaje
Cada ocho días	0	0
Cada mes	3	21
Cada tres meses	4	29
Cada año	7	50
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 6. Periodo se hace mantenimiento a los equipo

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

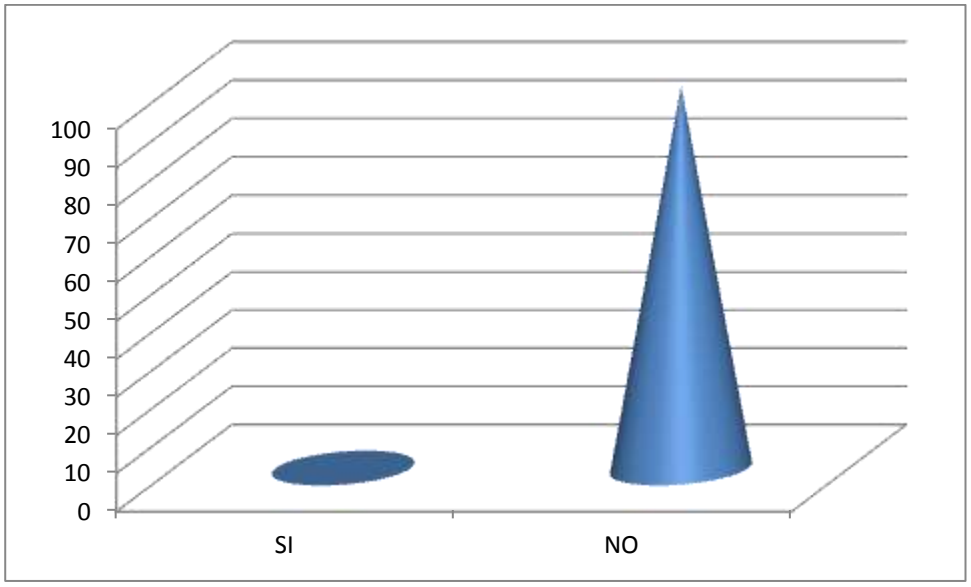
En cuanto al periodo de mantenimiento de los equipos se puede afirmar que la mayoría de los encuestados dicen que se hace cada año, siendo un periodo muy largo para dicha actividad, otro porcentaje alto dice que se realiza cada dos o tres meses, lo que demuestra que no se le da el cuidado adecuado a dichos equipos de cómputo, siendo estos fundamentales para la actividad desarrollada.

Tabla 7.

Manuales para cada programa y equipo

Ítem	**Frecuencia**	**Porcentaje**
SI	0	0
NO	14	100
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 7. Manuales para cada programa y equipo

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

Se denomina manual a toda guía de instrucciones que sirve para el uso de un dispositivo, la corrección de problemas o el establecimiento de procedimientos de trabajo. Los manuales son de enorme relevancia a la hora de transmitir información que sirva a las personas a desenvolverse en una situación determinada. En general los manuales son frecuentes acompañando a un determinado producto que se ofrece al mercado, como una forma de soporte al cliente que lo adquiere.

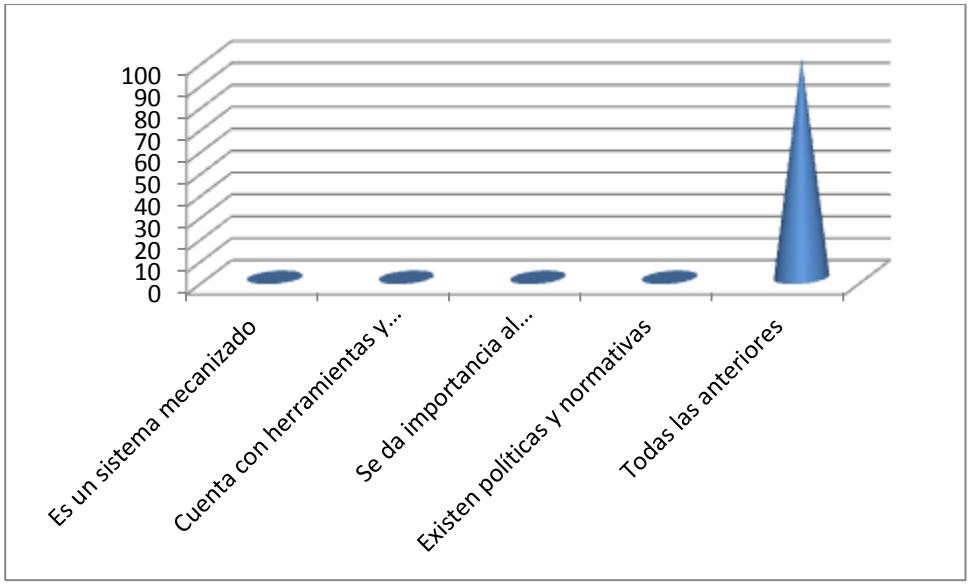
De acuerdo a lo que es un manual se debe decir que la totalidad de los encuestados afirman que en la empresa no ~~se~~ cuenta con manual para los programas y equipos

Tabla 8.

Fortalezas

Ítem	**Frecuencia**	**Porcentaje**
Es un sistema mecanizado	0	0
Cuenta con herramientas y procesos bien definidos	0	0
Se da importancia al adecuado manejo de información	0	0
Existen políticas y normativas	0	0
Todas las anteriores	14	100
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 8. Fortalezas

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

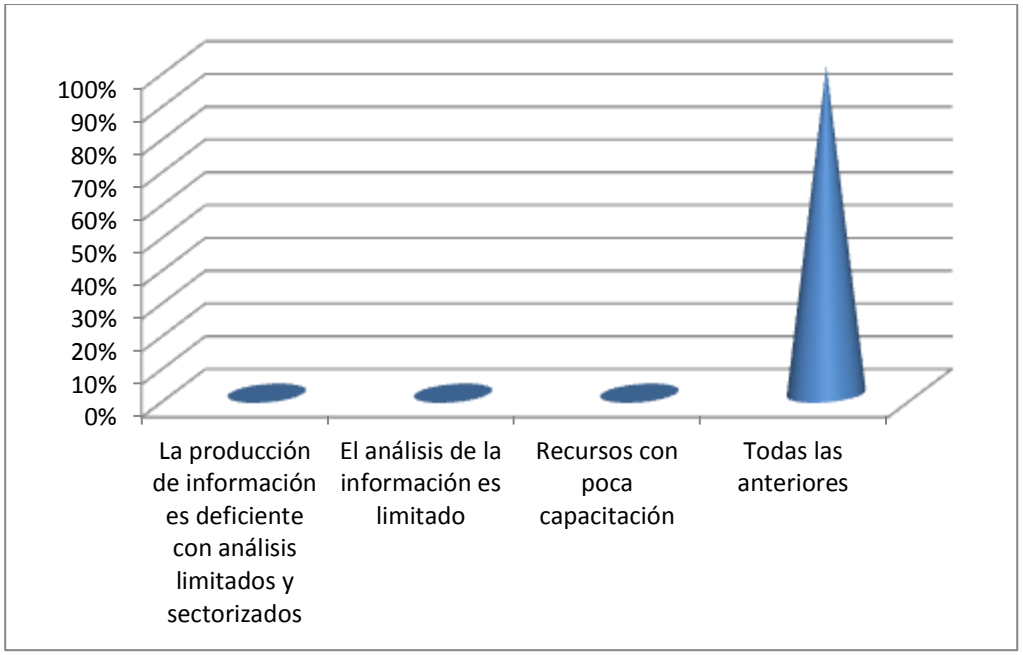
Según la totalidad de los encuestados el sistema de información cuenta con grandes fortalezas como es un sistema mecanizado, cuenta con herramientas y procesos bien definidos, se da importancia al adecuado manejo de información y existen políticas y normativas

Tabla 9.

Debilidades

Ítem	**Frecuencia**	**Porcentaje**
La producción de información es deficiente con análisis limitados y sectorizados	0	0
El análisis de la información es limitado	0	0
Recursos con poca capacitación	0	0
Todas las anteriores	14	100
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 9. Debilidades

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

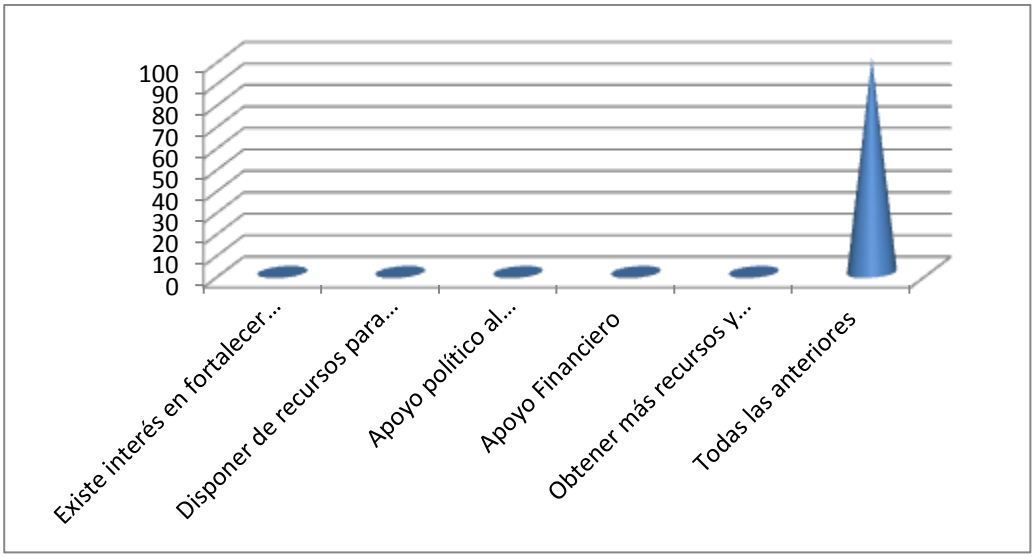
En cuanto a las debilidades no se puede desconocer que al igual que todas las empresas cuentan con debilidades como son la producción de información es deficiente con análisis limitados y sectorizados, el análisis de la información es limitado, recursos con poca capacitación y no se tiene un proceso científicamente valido de generación o procesamiento de información.

Tabla 10.

Oportunidades

Ítem	Frecuencia	Porcentaje
Existe interés en fortalecer el sistema de información	0	0
Disponer de recursos para realizar planificación estratégica	0	0
Apoyo político al desarrollo del diagnóstico	0	0
Apoyo Financiero	0	0
Obtener más recursos y tecnificados	0	0
Todas las anteriores	14	100
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 10. Oportunidades

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

El 100% de las personas encuestadas dicen que este tipo de sistema de información cuenta con grandes oportunidades como son la de fortalecer el sistema de información, disponer

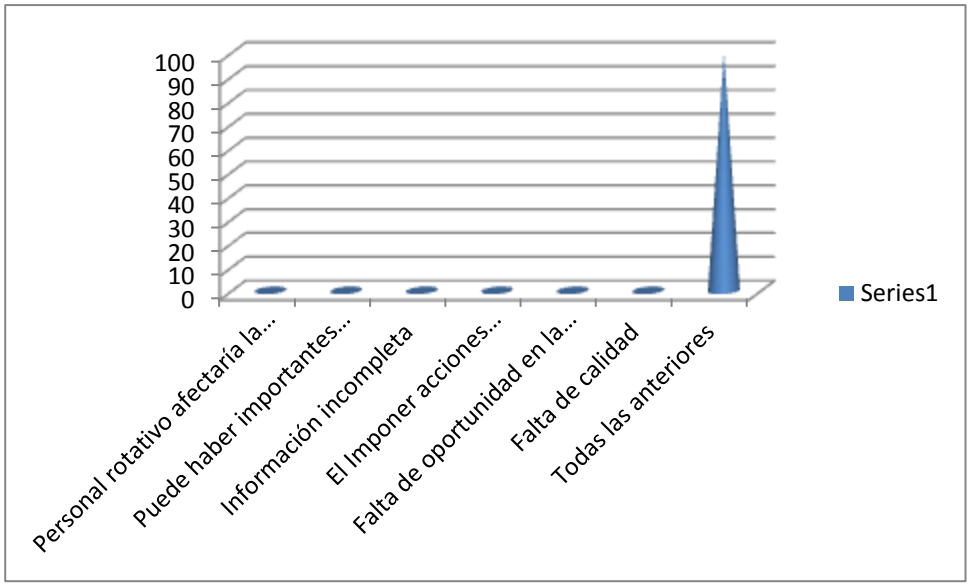
de recursos para realizar planificación estratégica, apoyo político al desarrollo del diagnóstico, apoyo Financiero, existe una oferta de apoyo técnico y financiero internacional para la implantación del sistema, obtener más recursos y tecnificados

Tabla 11.

Amenazas

Ítem	Frecuencia	Porcentaje
Personal rotativo afectaría la continuidad	0	0
Puede haber importantes rezagos en la información	0	0
Información incompleta	0	0
El Imponer acciones particulares	0	0
Falta de oportunidad en la información	0	0
Falta de calidad	0	0
Todas las anteriores	14	100
TOTAL	**14**	**100**

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda



Gráfica 11. Amenazas

Fuente. Encuesta aplicada a los empleados de la Cooperativa Cootranshacaritama Ltda

Por último no se puede desconocer que existen muchas amenazas al sistema de información, notándose entre otras, que el personal rotativo afectaría la continuidad del sistema, puede haber importantes rezagos en la información, información incompleta, el Imponer acciones particulares, falta de oportunidad en la información y falta de calidad, lo que en determinado caso puede llegar a afectar el sistema.

4.2 Posibles Controles que sean Necesarios para Mantener Segura la Información que se Maneja a través del Sistema de Información de Geolocalización INKCO

Teniendo en cuenta la auditoría realizada, en la cual se obtuvieron resultados en cuanto a los riesgos que se tienen en la seguridad de la información, se han analizado los mismos con el fin de dar a conocer una serie de controles que servirán de ayuda. Igualmente, el acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y éstos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Con el fin de mostrar a la cooperativa Cootranshacaritama los posibles controles que debe tener en cuenta, además de ser necesarios, para mantener segura la información que se maneja a través del sistema INKCO, se proponen los siguientes, tomado de (Alcaldía de Albania Santander, 2012)

4.2.1 Manejo apropiado de contraseña. Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.

Las contraseñas se deben mantener confidenciales en todo momento.

No compartir las contraseñas, con otros usuarios.

Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.

Selecciona contraseñas que no sean fáciles de adivinar.

Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre-definido.

Cambia tus contraseñas regularmente.

No utilizar la opción de almacenar contraseñas en Internet.

No utilizar contraseña con números telefónicos, nombre de familia etc.

No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

Crear una contraseña:

Contraseñas fuertes contienen números y letras.

Utilizar contraseña que tengan por lo menos 8 caracteres

4.2.2 Manejo apropiado de control de Virus. La Cooperativa deberá definir un producto estándar licenciado en entorno de sus estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computo.

El sistema de actualizaciones y detección diaria deberá estar automatizado a nivel central.

Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus, al área de soporte.

Los usuarios no podrán desinstalar o cambiar el producto de antivirus existente en su equipo.

Los dispositivos extraíbles, antes de ser usados deben ser escaneados con el antivirus.

4.2.3 Manejo de cuentas de sistemas. Toda cuenta de acceso que se requiera modificar deberá ser solicitada a través de los administradores de los sistemas o en la opción de cambio de contraseña.

El procedimiento de creación de cuentas, debe ser canalizado a través de los formularios correspondientes.

Cuenta de red: Esta cuenta corresponde a la que utilizará cada usuario para conectarse a su equipo PC. Esta se solicitará al área encargada.

Cuenta de Correo: Solicitarla formal al área encargada.

4.2.4 Manejo de acceso a internet. El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio. Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

No navegar por sitios no confiables.

Se prohíbe el uso de sitios de radios online.

Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet.

Se prohíbe el uso de sitios de chat (Messenger, chat, etc.).

Se prohíbe el uso de internet para actividades ilícitas.

Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.

Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo)

No permitir que el navegador de internet recuerde la contraseña automáticamente.

Evitar participar en juegos de entretenimiento en línea.

Si no está navegando por internet, cierre todas las ventanas abiertas.

Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.

Si requiere navegar en algún sitio bloqueado se deberá solicitar al área encargada.

4.2.5 Manejo de correo electrónico. La Cooperativa en lo posible deberá contar con filtros para identificar y bloquear correos no deseados (Spam o Virus)

El Correo electrónico institucional es de uso exclusivo para actividades relacionadas con la Cooperativa y queda restringido el uso para otros fines.

Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.

La contraseña de correo debe ser cambiada periódicamente.

No abrir link sospechosos llegados por correos electrónicos (bancos, tiendas, etc.).

No completar datos personales en correos electrónicos sospechosos.

Eliminar periódicamente los correos no deseados (spam o sospechoso).

4.2.6 Manejo de redes sociales. En lo posible la cooperativa deberá bloquear todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ellos, deberá enviar la solicitud formal al área correspondiente.

Cabe destacar que cualquier foto subida o comentario en Facebook, twitter o en alguna red social es responsabilidad exclusiva del que la emite.

4.2.7 Manejo de software. Se prohíbe la instalación que no cumpla con la las instrucciones del Área de Soporte y Operaciones.

Los usuarios no deben instalar aplicaciones ni descargar aplicaciones que podrían provocar alguna vulnerabilidad o inestabilidad en los servicios.

Toda solicitud debe ser canalizada por medio del área encargada de los sistemas de la cooperativa.

4.2.8 Manejo de dispositivos móviles. Para garantizar la seguridad y estabilidad de la red y los dispositivos móviles, se describen algunos concejos y manejo adecuado, de los mismos:

La instalación, configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área asignada para tal fin.

Las actualizaciones de sistemas operativos de los dispositivos móviles, debe ser coordinado con el área encargada, que es la responsable de realizar las actualizaciones.

Se debe mantener desactivada la red Wifi, Bluetooth, Infrarrojos, etc, en caso de que no esté siendo utilizada.

No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

No acceder a los enlaces solicitados a través de SMS/MMS/Email podría ser código malicioso.

4.2.9 Manejo computadores portátiles. Para garantizar la seguridad y estabilidad de la red de la Entidad se describen algunos consejos y manejo adecuado.

Todo computador portátil debe ser incorporado al dominio de la red de la Cooperativa, para esto sólo el área encargada.

Los computadores portátiles de la Cooperativa se han adquirido específicamente para facilitar el desarrollo de actividades laborales. Su uso debe estar relacionado con las actividades del área a la cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales

Los equipos portátiles deben permanecer en las instalaciones, durante los días y horarios hábiles de trabajo, pueden salir de las instalaciones, solo en el caso de utilizarlo en labores de la Cooperativa.

La instalación, configuración, modificación o eliminación de software sobre los equipos portátiles es responsabilidad exclusiva del área encargada.

El área encargada tiene la potestad para remover, sin notificar al funcionario, cualquier software que no esté autorizado por la División Informática.

La configuración, eliminación, modificación o cambio de sistema operativo es de responsabilidad del área encargada.

La configuración e instalación de hardware de los equipos portátiles, es responsabilidad de área asignada para tal fin, según corresponda.

Se debe mantener desactivada la red inalámbrica en caso de que no esté siendo utilizada.

No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

4.3 Estructurar el documento del plan estratégico.

La estructura del documento del plan estratégico, se encuentra en el capítulo 5.

4.4 Socializar a la Directiva de la Empresa Cootranshacaritama, sobre los Resultados de la Auditoría y el Diseño del Plan Estratégico

Una socialización es toda actividad realizada en una organización, respondiendo a sus necesidades, que busca mejorar la actitud, conocimiento, habilidades o conductas de su personal. Concretamente, la capacitación:

Busca perfeccionar al colaborador en su puesto de trabajo, en función de las necesidades de la empresa y en un proceso estructurado con metas bien definidas.

La necesidad de capacitación surge cuando hay diferencia entre lo que una persona debería saber para desempeñar una tarea, y lo que sabe realmente. Estas diferencias suelen ser descubiertas al hacer evaluaciones de desempeño, o descripciones de perfil de puesto.

Dados los cambios continuos en la actividad de las organizaciones, prácticamente ya no existen puestos de trabajo estáticos. Cada persona debe estar preparado para ocupar las funciones que requiera la empresa. El cambio influye sobre lo que cada persona debe saber, y también

sobre la forma de llevar a cabo las tareas. Una de las principales responsabilidades de la supervisión es adelantarse a los cambios previendo demandas futuras de capacitación, y hacerlo según las aptitudes y el potencial de cada persona.

En la socialización realizada a los directivos se les explicó los resultados arrojados de la auditoria y las propuestas hechas para mejorar la situación de la empresa.

SOCIALIZACIÓN No 1.

TEMA: Resultados de la auditoria y plan estratégico

OBJETIVO GENERAL

Capacitar a los directivos de la Cooperativa Cootranshacaritama.

CONTENIDO:

¿Qué es una auditoria?

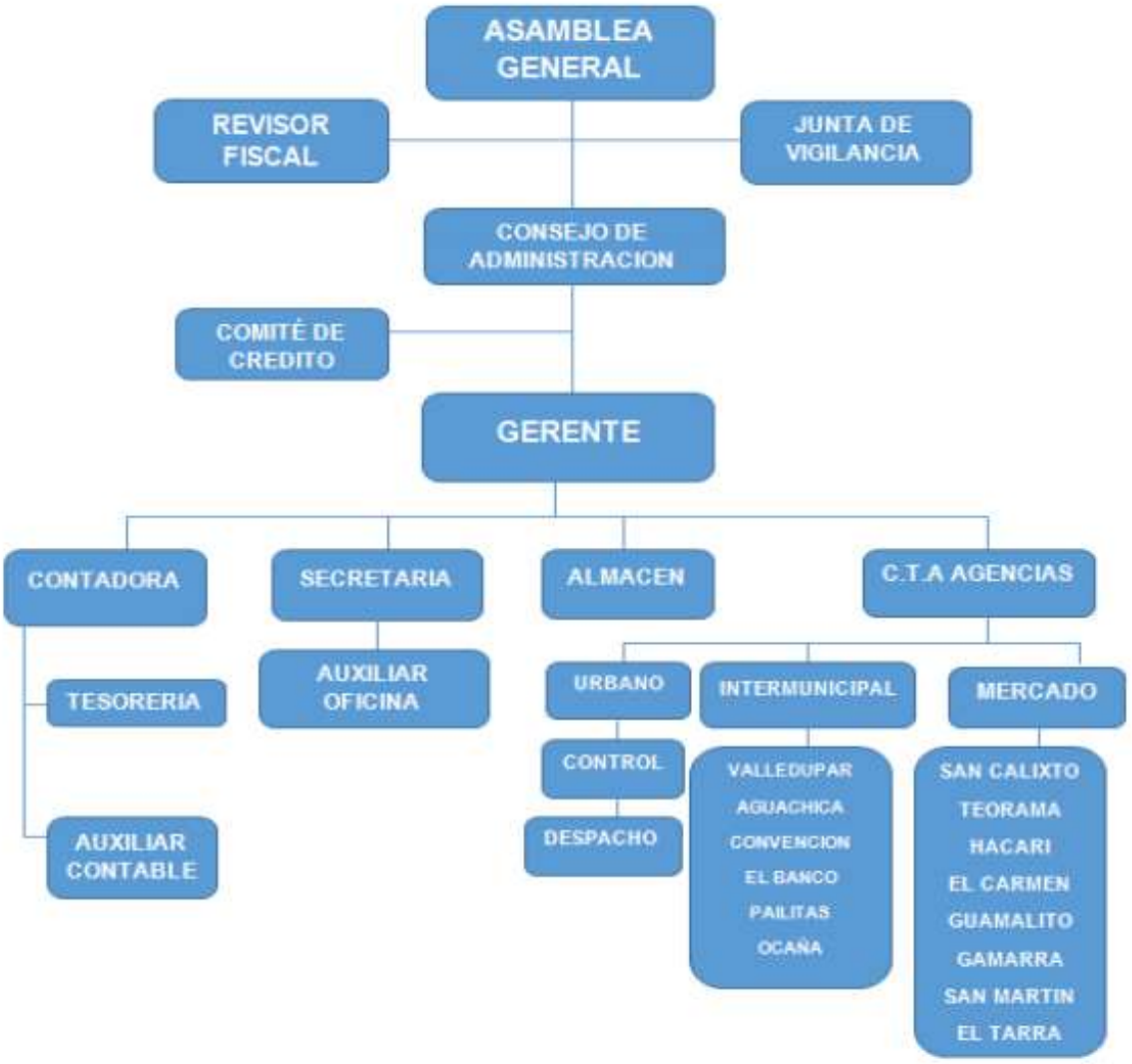
La auditoría de sistemas tiene como objetivo evaluar sistemas informáticos en forma integral, los procedimientos y seguridad de los equipos electrónicos o hardware de los programas o software que posea la empresa sean propios o de modalidad de servicios.

Herramientas administrativas encontradas en la empresa.

Misión. Somos una cooperativa afiliadora de vehículos de servicio público, que cuenta con un personal capacitado, dispuesto a implementar continuamente sistemas apropiados en busca de la excelencia, para brindar a sus asociados mejor calidad de vida y a sus usuarios comodidad, seguridad y un óptimo servicio, promoviendo los valores cooperativos de autoayuda, responsabilidad, solidaridad, equidad y compromiso.

Visión. Ser una empresa con responsabilidad social preocupada por la conservación del medio ambiente, económicamente sólida, moderna y tecnificada que a partir de la administración de vehículos promueva el mejoramiento de la calidad de vida del asociado mediante la prestación del servicio de transporte público con altos niveles de satisfacción de las necesidades de los usuarios generando un desarrollo socioeconómico para Ocaña y la región.

Estructura organizacional. Contamos con una real estructura administrativa y operativa, lo cual le da la solidez, dinamismo y eficiencia para la prestación de sus servicios.



Con el fin de realizar la auditoría al sistema INKCO, se realiza una lista de chequeo para de esta manera obtener el resultado de la misma y así poder identificar las fortalezas, oportunidades, amenazas, debilidades y riesgos de la empresa, lo que arrojo que la empresa y el sistema de información cuenta con grandes ventajas y oportunidades para el adecuado desarrollo de la empresa como también no se puede desconocer que se tienen muchas debilidades y amenazas que se deben convertir un estrategias contribuyendo a mejorar la situación interna de la cooperativa. De acuerdo a la lista de chequeo, se obtiene los siguientes resultados:

Cootrashacaritama implementa desde ya el sistema GPS para los vehículos que están adscritos a esta empresa. La tecnología permitirá brindar un mejor servicio tanto a los usuarios como a los transportadores. Por lo anterior se diseñó un manual de GPS, siendo un valor agregado al desarrollo de la investigación.

Cootranshacaritama implementa desde ya el sistema GPS para los vehículos que están adscritos a esta empresa. La tecnología permitirá brindar un mejor servicio tanto a los usuarios como a los transportadores.

La Cooperativa Cootranshacaritama, contrata empleados a los cuales se les solicita algunos requisitos para su contratación, como lo es referencias personales y su correspondiente licencia de conducción, soat, tarjeta de propiedad del vehículo. Igualmente, al ser contratados, se ingresan al sistema de acuerdo al procedimiento establecido.

En la empresa no se realiza inventario de los recursos informáticos de la misma, no existiendo un informe que muestre la existencia de éstos en la cooperativa. Además, no se cuenta con un sistema de alarmas. En cuanto al antivirus cuenta con una versión actualizada.

En cuanto al área de sistemas, se mantiene un control en el ingreso de visitantes, al igual que de los socios en los horarios no hábiles.

De otra parte se presenta un plan estratégico que permite evidenciar las falencias y fortalezas, como también plantear estrategias que ayuden a mejorar la situación actual.

¿Qué es un plan estratégico?

El plan estratégico es un programa de actuación que consiste en aclarar lo que pretendemos conseguir y cómo nos proponemos conseguirlo. Esta programación se plasma en un documento de consenso donde concretamos las grandes decisiones que van a orientar nuestra marcha hacia la gestión excelente.

5. Plan Estratégico

El plan estratégico es un programa de actuación que consiste en aclarar lo que pretendemos conseguir y cómo nos proponemos conseguirlo. Esta programación se plasma en un documento de consenso donde concretamos las grandes decisiones que van a orientar nuestra marcha hacia la gestión excelente. (Guía de la Calidad, 2016)

El objetivo del plan estratégico, es trazar un mapa de la organización, que nos señale los pasos para alcanzar nuestra visión, convertir los proyectos en acciones (tendencias, metas, objetivos, reglas, verificación y resultados). (Guía de la Calidad, 2016)

De otra parte el plan estratégico, se debe realizar para fomentar la vinculación entre los "órganos de decisión" (E.D.) y los distintos grupos de trabajo, buscando el compromiso de todos, para descubrir lo mejor de la organización: El objetivo es hacer participar a las personas en la valoración de las cosas que hacemos mejor, ayudándonos a identificar los problemas y oportunidades.

5.1 Modelo de negocio

Misión. Somos una cooperativa afiliadora de vehículos de servicio público, que cuenta con un personal capacitado, dispuesto a implementar continuamente sistemas apropiados en busca de la excelencia, para brindar a sus asociados mejor calidad de vida y a sus usuarios comodidad, seguridad y un óptimo servicio, promoviendo los valores cooperativos de autoayuda, responsabilidad, solidaridad, equidad y compromiso.

Visión. Ser una empresa con responsabilidad social preocupada por la conservación del medio ambiente, económicamente sólida, moderna y tecnificada que a partir de la administración de vehículos promueva el mejoramiento de la calidad de vida del asociado mediante la prestación del servicio de transporte público con altos niveles de satisfacción de las necesidades de los usuarios generando un desarrollo socioeconómico para Ocaña y la región.

Objetivos. Facilitar a los asociados el suministro de todos los artículos que sean necesarios para el normal desarrollo y funcionamiento de la industria del transporte en forma solidaria.

Propiciar la educación cooperativa. Parágrafo: para el cumplimiento de sus objetivos la cooperativa podrá prestar los servicios que a continuación se detallan:

Atender los requerimientos sobre el mantenimiento al parque automotor y el consumo industrial, de acuerdo al registro de propiedad o tendencia de los vehículos vinculados a la cooperativa.

Administrar y coordinar la organización de los sistemas de transporte terrestre automotor de servicio público para pasajeros y carga, dentro de las rutas y horarios que les sean asignados, conforme a la legislación pertinente; así como también, encomiendas y envíos.

Administrar y prestar a sus asociados los servicios relacionados con la industria del transporte terrestre automotor de uso público para pasajeros; el de carga de pasajeros mixtos, y el

de encomienda y giros. Los servicios de transporte de pasajeros se prestaran de acuerdo a la ruta y horarios fijados por las entidades competentes para zonas urbanas, suburbanas, metropolitanas, intermunicipales, interdepartamentales, nacionales e internacionales, mediante el Uso de buses, busetas, microbuses, camiones, camionetas, camperos y automóviles, así como de vehículos de carga y pasajeros o mixtos y de acuerdo a la homologación establecida por la entidad competente. Seguidamente, se procedió a identificar los riesgos del sistema de información, el cual arrojó los siguientes resultados:

Tabla 12.

Valor del riesgo

DESCRIPCION DEL RIESGO	VALORACIÓN			
	Impacto	probabilidad	ponderación del riesgo	Riesgo
1. Pérdida de información, por daño de equipo, porque no se cuenta con las instalaciones de seguridad necesarias para la protección de los equipos en caso de una situación inesperada.	3 (alto)	3 (alta)	3*3= 9	9 (alto)
2. Perdida de información, infraestructura física inadecuada, ya que en las Instalaciones físicas el cableado estructurado es inseguro está expuesto al poder ser pisado por los usuarios del área, así como también las instalaciones eléctricas deben ser con polo a tierra para el uso adecuado de le energía que necesitan los equipos.	3 (medio)	3 (media)	2*2= 4	9 (medio)

Fuente. Autores del proyecto.

Según los riesgos encontrados es necesario proponer controles que contrarresten tal problema y nos ayude a mejorar la situación actual, por lo tanto se propone los siguientes:

Realizar copias de seguridad, con el fin de evitar que la información se pierda, ya que esta es muy importante y se debe tratar de protegen con el objetivo de evitar problemas o inconvenientes futuros.

Mostrar con evidencias claras, los peligros que acarrea las instalaciones actuales, mostrando la exposición del cableado, esto puede llevar a accidentes, lo cual es necesario evitar por medio de oficios a los funcionarios competentes, los cuales deben tomar cartas en el asunto.

Tabla 13.

Descripción de los riesgos

DESCRIPCION DE LOS RIESGOS	CONTROL
1. Pérdida de información, por daño de equipo, porque no se cuenta con las instalaciones de seguridad necesarias para la protección de los equipos en caso de una situación inesperada.	Mantenimiento de los sistemas eléctricos y de red. Mantenimiento de la ups Adquirir tecnología que permita enfrentar fallas eléctricas. Verificar que las políticas de protección para los equipos.
2. Perdida de información, infraestructura física inadecuada, ya que en las instalaciones físicas el cableado estructurado es inseguro está expuesto al poder ser pisado por los usuarios del área, así como también las instalaciones eléctricas deben ser con polo a tierra para el uso adecuado de le energía que necesitan los equipos.	Adecuar la infraestructura física de acuerdo a los sistemas de seguridad informáticos gestionar ante los entes involucrados para el mejoramiento de la infraestructura organizar el espacio físico.

Fuente: Autores del proyecto.

Administración de problemas e incidentes

Sistema de Administración de Problemas

Objetivo de control. La Gerencia de TI deberá definir e implementar un sistema de administración de problemas para asegurar que todos los eventos operacionales que no formen parte de la operación estándar (incidentes, problemas y errores) sean registrados, analizados y resueltos oportunamente. Los procedimientos de cambios de emergencia a programas se deben probar, documentar, aprobar y reportar prontamente. Deberán emitirse reportes de incidentes en caso de problemas significativos.

Escalamiento de Problemas

Objetivo de control. La Gerencia deberá definir e implementar procedimientos de escalamiento de problemas para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el proceso de escalamiento para la activación del plan de continuidad de TI.

Seguimiento de Problemas y Pistas de Auditoría

Objetivo de control. El sistema de administración de problemas deberá proporcionar adecuadas pistas de auditoría que permitan el seguimiento de un incidente a partir de sus causas (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá

trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

Autorizaciones de Accesos Temporales y de Emergencia

Objetivo de control. Las autorizaciones de acceso temporal y de emergencia deberán ser documentadas en formularios estándar y mantenidas en archivo, aprobadas por los gerentes apropiados, comunicadas de forma segura a la función de seguridad y las mismas deberán terminarse automáticamente después de un período predeterminado.

Prioridades de Procesamiento de emergencia

Objetivo de control. La gerencia de TI debe establecer, documentar y aprobar mediante el uso de programas adecuados las prioridades de procesamiento de emergencia.

DS11: ENTREGA DE SERVICIOS Y SOPORTE

Que satisface los requerimientos de negocio de: asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Se hace posible a través de: una programación o planeación de las actividades que sea registrada y diligenciada con base en el cumplimiento de todas las actividades

Toma en consideración:

Manual de procedimiento de operaciones

Documentación para el inicio de procesos

Administración de servicios de red

Programación del personal y cargas de trabajo

Coordinación con las áreas de administración de cambios, disponibilidad y manejo continuo de negocios

Mantenimiento preventivo

Acuerdos de niveles de servicio

Operaciones automatizadas

Registro, rastreo y escalamiento de incidentes

ADMINISTRACIÓN DE OPERACIONES

Este objetivo de control está relacionado con el riesgo #2, Perdida de información, infraestructura física inadecuada, ya que en las instalaciones físicas el cabreado estructurado es inseguro está expuesto al poder ser pisado por los usuarios de la sala, así como también las instalaciones eléctricas deben ser con polo a tierra para el uso adecuado de la energía que necesitan los equipos.

Manual de Instrucciones y Procedimientos de las Operaciones de Procesamiento

Objetivo de control. La Gerencia de TI deberá establecer y documentar procedimientos estándar para las operaciones de tecnología de información (incluyendo operaciones de red). Todas las soluciones y plataformas de tecnología de información con que cuente la empresa deberán ser operadas utilizando estos procedimientos, los cuales deberán ser revisados periódicamente para asegurar su efectividad y cumplimiento.

Documentación del Proceso de Inicio y de Otras Operaciones

Objetivo de control. La Gerencia de TI deberá asegurar que el personal de operaciones esté adecuadamente familiarizado y sepa como ejecutar las tareas del proceso de inicio y con otras operaciones con base en una adecuada documentación la cual debe ser periódicamente probada y ajustada, según se requiera.

Programación de Trabajos

Objetivo de control. La Gerencia de la función de servicios de información deberá asegurar que la programación continua de trabajos, procesos y tareas sea organizada en la secuencia más eficiente, maximizando el uso de recursos y su utilización, con el fin de alcanzar los objetivos establecidos en los convenios de nivel de servicio. Las programaciones iniciales así como los cambios a estas programaciones deberán ser autorizadas apropiadamente.

Desviaciones de la Programación de Trabajos Estándar

Objetivo de control. Deberán establecerse procedimientos para identificar, investigar y aprobar la ejecución de los programas de trabajos estándar.

Continuidad de Procesamiento

Objetivo de control. Los procedimientos deberán requerir continuidad de procesamiento durante los cambios de turno de los operadores mediante la existencia de un proceso de entrega formal de actividades, actualización del estado en que se encuentran los procesos y reporte sobre las responsabilidades actuales.

Bitácoras de Operación

Objetivo de control. Los controles de la Gerencia deberán garantizar que se almacene en bitácoras suficiente información cronológica de las operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que rodean y soportan el procesamiento.

Custodia de Formularios Especiales y de Dispositivos de Salida

Objetivo de control. La gerencia deberá establecer seguridades físicas apropiadas para proteger los formularios especiales, como por ejemplo los instrumentos negociables, y los

dispositivos sensitivos de salida, como por ejemplo los cartuchos de firma tomando en consideración el apropiado registro de los recursos de tecnología de información, formularios o artículos que requieran protección adicional y administración de inventario.

Operaciones Remotas

Objetivo de control. Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la(s) instalación(es) remota(s) sean identificadas e implementadas.

Matriz DOFA. La matriz debe ser utilizada en una primera etapa para la construcción de un sistema de información. Es necesario que un SI tenga una adecuada consistencia en los datos, aunque esto no es suficiente para lograr una buena calidad, sin embargo la lógica de análisis del sistema de información da por supuesto la presencia del dato sin entrar a analizar las características de pertinencia y de correspondencia.

Matriz DOFA del sistema de información. Esta matriz permite ver las fortalezas, debilidades, amenazas y oportunidades que tiene o puede tener la institución en su entorno. Es importante desarrollarla para tener una mejor orientación en el momento de plasmar sus objetivos y planes de acción, para que sean los más cercanos a la realidad de la entidad. Ayuda a determinar qué tan capacitada esta organización para desempeñarse en el medio, esta matriz conduce al desarrollo de cuatro tipos de estrategias FO, DO, FA, DA.

Estrategia FO. Corresponde al uso de fortalezas internas de la empresa con el objeto de aprovechar las oportunidades externas.

Estrategias DO. Mejora las debilidades internas, valiéndose de las oportunidades externas.

Estrategias FA. Utiliza las fortalezas de la empresa para minimizar o evitar el impacto de las amenazas externas.

Estrategias DA. Derrotar debilidades internas y eludir amenazas tomando estrategias defensivas.

Los pasos para construir una matriz DOFA son:

Hacer una lista de fortalezas internas claves.

Hacer una lista de debilidades internas decisivas.

Hacer una lista de las oportunidades externas importantes.

Hacer una lista de amenazas externas claves.

Comparar las fortalezas internas con las oportunidades externas y registrar las estrategias.

Cruzar las debilidades internas con las oportunidades externas y registrar las estrategias.

Comparar las fortalezas internas con las amenazas externas y registrar estrategias.

Comparar debilidades internas con las amenazas externas y registrar estrategias.

Tabla 14.

Matriz DOFA

	FORTALEZAS (F)	DEBILIDADES (D)
	Es un sistema mecanizado Cuenta con herramientas y procesos bien definidos	La producción de información es deficiente con análisis limitados y sectorizados
	Algunas instituciones cuentan con sistemas de información sostenibles	El manejo de datos no es funcional en las instituciones
	Posee información para identificar aspectos a fortalecer	Falta de intercambio de información entre las empresas
	Existen objetivos, metas e indicadores estandarizados para algunas áreas, programas e intervenciones	Hay una pobre divulgación de la información El análisis de la información es limitado
	Se da importancia al adecuado manejo de información	Recursos con poca capacitación
	Existen políticas y normativas	No se tiene un proceso científicamente valido de generación o procesamiento de información
OPORTUNIDADES (O)	ESTRATEGIAS (FO)	ESTRATEGIAS (DO)
Existe interés internacional en fortalecer el sistema de información Disponer de recursos asignados por red métrica para el diagnóstico Disponer de recursos para realizar planificación	Aprovechar que el sistema es mecanizado y que las herramientas y procesos son bien definidos, disponiendo de recursos asignados por la red métrica para el diagnóstico. F1+F2+O2	El manejo de datos no es funcional, por lo que se debe aprovechar el apoyo político y financiero. D2+O4+O5

estratégica		
Apoyo político al desarrollo del diagnóstico		
Apoyo Financiero		
Existe una oferta de apoyo técnico y financiero internacional para la implantación del sistema		
Obtener más recursos y tecnificados		
AMENAZAS (A)	ESTRATEGIAS (FA)	ESTRATEGIAS (DA)
Inadecuada participación e integración de las instituciones	Se da importancia al adecuado manejo de información, logrando mejorar el inadecuada participación e integración de las instituciones. F6+A1	Se debe aprovechar los recursos sobre la capacitación y así mejorar la calidad del servicios ofrecido con el sistema de información. D6+A7
Personal rotativo afectaría la continuidad del sistema		
Puede haber importantes rezagos en la información		
Información incompleta		
El Imponer acciones particulares		
Falta de oportunidad en la información		
Falta de calidad		

Fuente: Autores del proyecto

De acuerdo a la interpretación de la matriz DOFA, se considera que el grupo de estrategias más viable es la FO, ya que se requiere a la mayor brevedad posible corregir las debilidades presentadas para lograr una mejor posición ante las amenazas visualizadas. Por lo tanto se hace necesario implementar las estrategias propuestas.

Matriz Interna-Externa (IE), del sistema de información, permite reconocer la situación general de la institución, a través de la comparación de las matrices EFI y EFE teniendo como punto de partida el impacto de las fortalezas, debilidades, oportunidades y amenazas. Los resultados de la matriz EFI se relacionan con el eje X y los de la matriz EFE con el eje Y.

Se basa está matriz en dos dimensiones claves como son los resultados totales ponderados del factor interno (EFI) ubicando en el eje X y los resultados totales ponderados del factor externo (EFE), ubicados en el eje Y.

Sobre el eje X de la matriz IE, un resultado total ponderado de 1.0 a 1.99 representa una posición interna débil; de 2.0 a 2.99 se le considera promedio y de 3.0 a 4.0 se le considera fuerte. En forma similar con el eje Y. Parámetros estratégicos de las regiones de la matriz (IE):

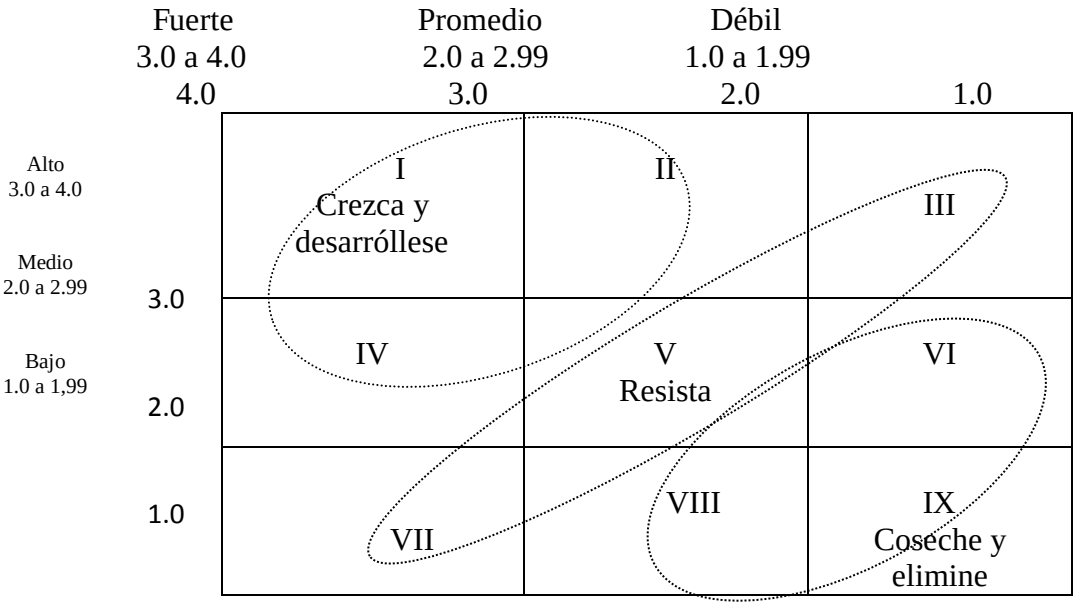


Figura 4. Categorías estratégicas de las regiones de la matriz I.E.

Fuente: Autores del proyecto

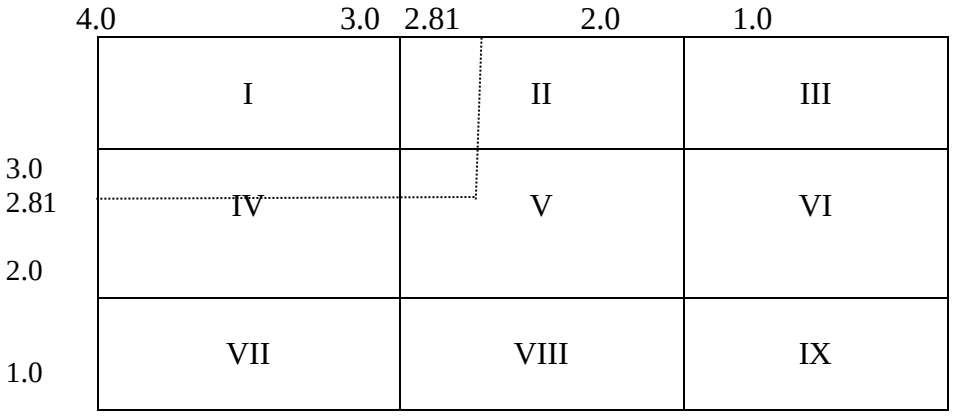


Figura 5. Aplicación de la matriz IE.

Fuente: Autores del proyecto

EFI = 2.81

EFE = 2.81

Como se observa la intersección de los resultados ponderados de la matriz IE, este se ubica en la región de las casillas I, II, IV, en el área de puesta en marcha de estrategias "Crezca y desarróllese" dentro de los cuales se pueden determinar la necesidad de crecimiento del sistema, logrando con esto abrir nuevos mercados, seguidamente mejorando la calidad de los servicios prestados, lo cual trae reconocimiento y buena imagen, se presta un servicio básico lo que le permite penetrar en otros mercados.

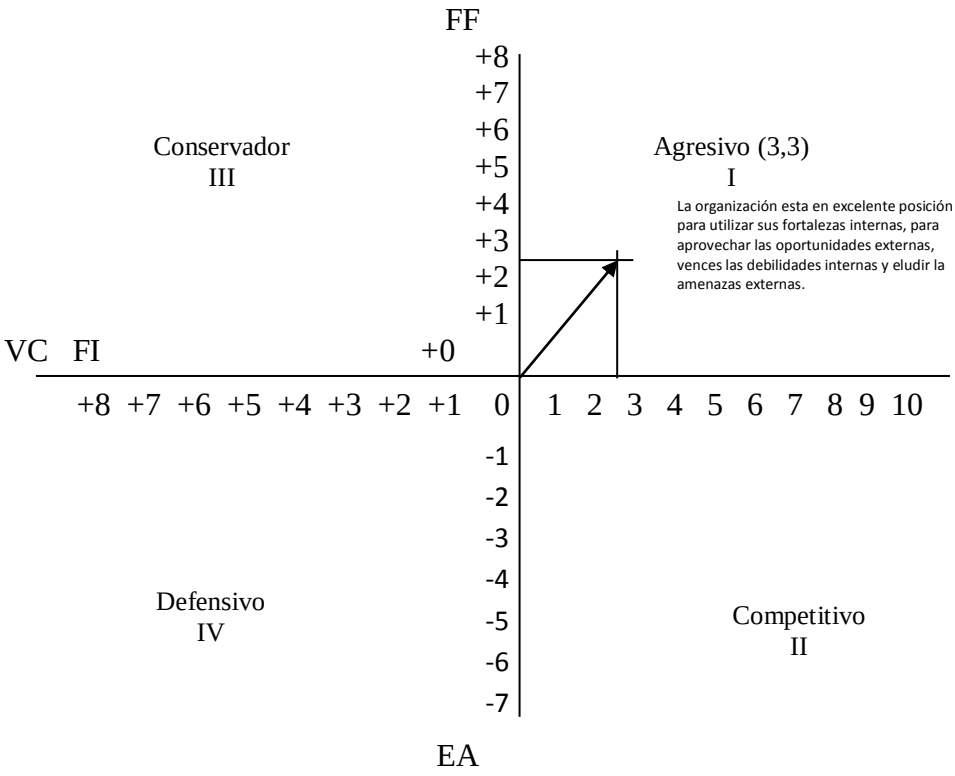


Figura 6. Representación de la matriz PEEA

Fuente: Autores del proyecto

De acuerdo con el análisis anterior, la posición estratégica del sistema, se ubica en el cuadrante agresivo, lo cual significa que debe mantener su fuerza industrial y estabilidad ambiental, aprovechando las fortalezas en cuanto a otros mercados, tecnología y competencia desleal.

Matriz de la Gran Estrategia. Permite formular estrategias acorde con la condición particular de la empresa, la metodología para elaborarla es la siguiente:

En el eje X. El eje de posición competitiva de la matriz de la gran estrategia es similar al eje de Ventaja Competitiva (VC) de la matriz PEEA. La escala de 0 a 6 de VC, anteriormente descrita para la matriz PEEA, se podría usar con la matriz PEEA, se podría usar con la matriz de gran estrategia. Recuerde que O = Posición numérico de -3 podría representar una posición competitiva promedio en la matriz de gran estrategia, así como lo represento en la matriz PEEA. El punto de intersección sobre el eje X en la matriz de gran estrategia podría ser por lo menos -3. Recuerde que +20% es igual a rápido crecimiento de mercado; -20% indica disminución rápida del mercado; el crecimiento del 0% es el punto de intersección. Un valor numérico de 0 podría por lo tanto representar el punto de intersección del eje y en la matriz de la gran estrategia.

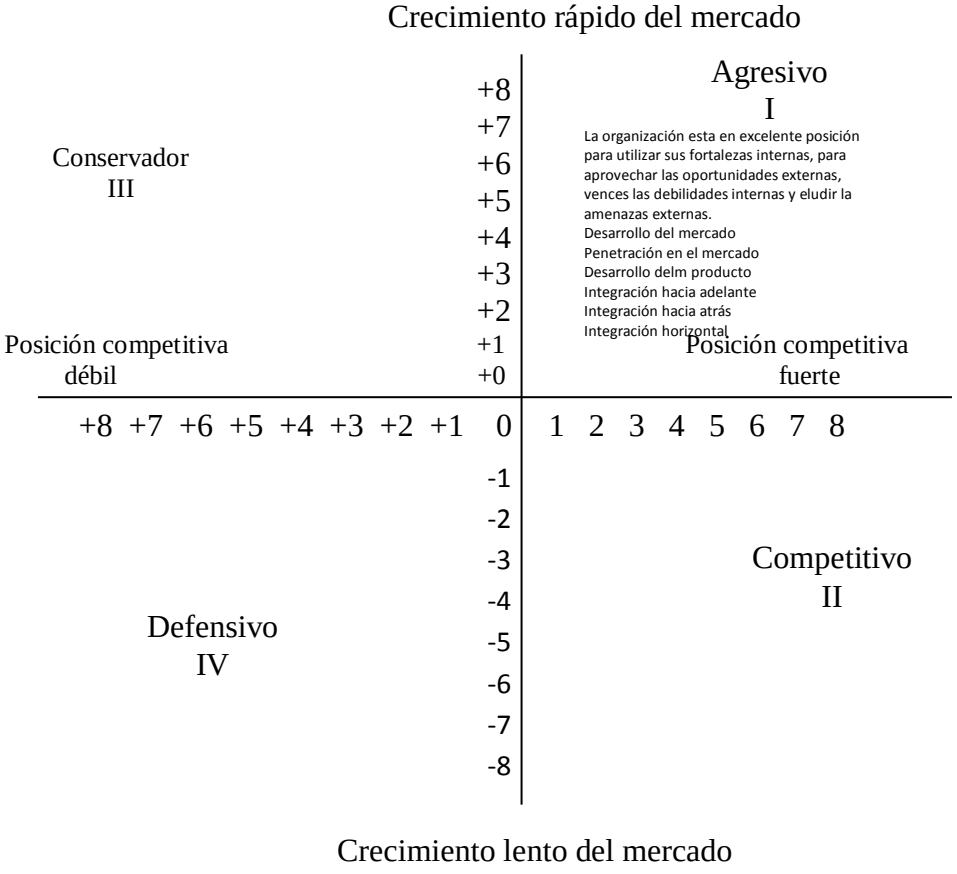


Figura 7. Presentación de la matriz de la Gran Estrategia.

Fuente: Autores del proyecto

Se recomienda estrategias de competencia en el mercado, como son campañas publicitarias y continuar capacitando para ofrecer los servicios con calidad, como también se debe aprovechar el sentido de pertenencia de los empleados hacia la empresa, la buena disposición para capacitaciones.

Empresa debe aprovechar la tecnología con la que cuenta en la actualidad, para lograr penetrar en los mercados, ya que en el cuadrante agresivo muestra el desarrollo del mercado, aprovechando la adecuada a atención al cliente con la que se cuenta.

Esta es integración hacia adelante ya que permite llevar un control o auditoria frente a las diferentes obras que se están realizando.

Capítulo 6: Conclusiones

De acuerdo a la auditoría realizada se debe decir que en la cooperativa cootransharaitama, existen algunas herramientas administrativas como son la misión, visión y organigrama, como también afirman que el personal va ingresando de forma permanente cumpliendo con la selección de personal y todo lo relacionado con la contratación de personal.

En cuanto a los posibles controles que se deben realizar se debe afirmar que teniendo en cuenta que son programas de computadora, con estructuras de datos y su documentación, que hacen efectiva la logística metodología de los requerimientos del programa. HARWARE: Son dispositivos electrónicos y electromecánicos, que proporcionan capacidad de cálculos y funciones rápidas, exactas y efectivas a las computadoras, por lo que se debe hacer constantes controles a los mismos.

El plan estratégico es muy importante para la empresa, teniendo en cuenta que en él se desarrollan una serie de matrices que permite la creación de estrategias que contribuyen al buen crecimiento de la empresa.

Y por último se debe concluir que la socialización de los resultados encontrado en la auditoria y el diseño del plan estratégico es muy importante que las personas vinculadas con la empresa conozcan y verifiquen como está la empresa y en qué aspectos es urgente que mejore.

Capítulo 7: Recomendaciones

Realizar de manera periódica auditoría en el área de sistemas de la Cooperativa Cootranshacaritama, toda vez que éstas herramientas deben ser utilizadas, teniendo en cuenta que las mismas ayudarían a encontrar procesos deficientes en el sistema, buscando de esta manera que la empresa pueda realizar la correspondiente corrección, y alcanzar así la calidad en el servicios ofrecido.

Teniendo encuentra los controles propuestos en el trabaja de grado es necesario que los directivos y asociados se reúnan y escojan la mejor opción para realizar dichos controles.

Se recomienda tener en cuenta los matrices diseñadas en el plan estratégica y así tener encuentra las estrategias planteados e implementarlas.

Se aconseja continuar realizando socialización, capacitaciones, talleres y demás con el objetivo que los empleados conozcan el manejo interno de la empresa y así entre todos contribuir a mejorar la situación encontrada en la misma.

Referencias

Aguirre, J. R. (2006). *Seguridad Informática y Criptográfica.* . Madrid. : Universidad Politécnica de Madrid.

Alcaldía de Albania Santander. (2012). *Manual de buenas prácticas política de seguridad de la información*. Obtenido de http://albania-santander.gov.co/apc-aa-files/64336435643034323334366662323433/manual-de-buenas-prcticas-sgsi.pdf

Bustamante, J. (2012). *Análisis financiero*. Obtenido de https://es.scribd.com/doc/2941779/Analisis-Vertical-y-Analisis-Horizontal-Administracion-Contabilidad

Carreón, J. (2015). *Teología de la innovación.* Chile.

Congreso de Colombia. (2010). *Decreto 1360 de 1989.* Bogotá.

Congreso de Colombia. (2010). *Ley 734 de 2002.* Bogotá.

Congreso de Colombia. (2014). *Ley 1273 de 2009.* Bogotá: Senado de la República.

Congreso de Colombia. (2014). *Ley estatutaria 1581 de 2012.* Bogotá.

Congreso de Colombia. (2015). *Decreto 1377 de 2013.* Bogotá.

Congreso de la República . (2012). *Constitución politica de Colombia.* Bogotá: Ediciones cupido.

Congreso de la Republica . (2012). *Ley 1266 de 2008.* Bogotá.

Congreso de la República. (2010). *Decreto 1474 de 2002.* Bogotá.

Congreso de la República. (2011). *Ley 1341 del 30 de julio de 2009.* Bogotá.

Congreso de la República. (2015). *Ley 603 de 2000.* Bogotá.

De Lara Haro, A. (2005). *Medición y control de riesgos financieros.* México: Limusa.

Diaz de Castro, L. (2001). *Planificación, gestión y control.* Madrid: Pearson Educación.

Echenique Garcia, J. A. (2007). *Auditoria en Informática.* 2a Edición. Mc Graw Hill.

Echenique Garcia, J. A. (s.f.). *Auditoria en Informática.* 2a Edición. Mc Graw Hill.

Educación, C. V. (25 de Noviembre de 2010). *http://www.mineducacion.gov.co/cvn/1665/w3-article-256467.html*. Obtenido de Seguridad informatica: http://www.mineducacion.gov.co/cvn/1665/w3-article-256467.html

exterior, I. C. (17 de Octubre de 2015). *https://normativa.colpensiones.gov.co/colpens/docs/acuerdo_icetex_0071_2013.htm*. Obtenido de Creditos para las graduaciones: https://normativa.colpensiones.gov.co/colpens/docs/acuerdo_icetex_0071_2013.htm

García Alvares, J. A. (21 de Junio de 2016). *http://www.asifunciona.com/electronica/af_gps/af_gps_7.htm*. Obtenido de Así funciona el GPS: http://www.asifunciona.com/electronica/af_gps/af_gps_7.htm

Gonzales, D. (2012). *Importancia de la Planeación Estratégica de TI.* Veracruz.

Guía de la Calidad. (2016). *Plan estratégico*. Obtenido de http://www.guiadelacalidad.com/modelo-efqm/plan-estrategico

Hernandez Pinto, m. G. (2006). *Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial.* Guayaquil.

Lucena López, M. J. (1999). *Criptografía y Seguridad en Computadoras.* 2a Edición, Universidadde Jaen.

Monterroso, A. (2006). *Politicas, normas y procedimientos de la infromación* . Guatemala.

Republica, P. d. (2014). *Manual de la politica dre seguridad para las tecnologias de la informacion y comunicaciones.* Bogotá.

Sanchez, K. (2012). *Politicas del sistema de información en la alcaldia de Rio de Oro Cesar.* Bogotá.

social, M. d. (2013). *Sector Administrativo de Salud y Protección Social.* Bogotá: Edición y consolidación.

Vergel Sanchez, Y. L., & Martinez Portillo, R. M. (2015). *GUÍA PRÁCTICA PARA EL CONTROL DE ACCESO DE LOS SISTEMAS DE INFORMACION DEL HOSPITAL EMIRO QUINTERO CAÑIZARES USANDO COMO HERRAMIENTA LAS ISO /IEC 27001:2005* . Ocaña: Universidad Francisco de Paula Santander.

Vergel Trigos, M., & Sepulveda Arenas, A. E. (2015). *Diseño de un manual de politcas de seguridad informatica.* Ocaña: Universidad Francisco de Paula Santander.

Villalon Huerta, A. (2004). *El Sistema de Gestión de la Seguridad de la Información.* Valencia.

Apéndice

Apéndice A. Encuesta dirigida a los empleados de la cooperativa Cootranshacarima ltda.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
INGENIERIA DE SISTEMAS

Objetivo. Diseñar un plan estratégico para la gestión segura del sistema de información de geolocalización INKCO, de la empresa Cootranshacaritama, basado en la norma ISO/IEC 270012013.

1. ¿En lugar donde se ubica el centro de cómputo está libre de inundaciones, robos o cualquier situación que pueda poner en peligro los equipos?
SI___ NO___
Por qué? _____

2. ¿Existe lugar suficiente para los equipos?
SI____ NO____
Por qué? _____

3. ¿Es adecuada la iluminación del centro de cómputo?
SI____ NO____
Por qué? _____

4. ¿Estan limpios los ductos del aire acondicionado?
SI____ NO____
Por qué? _____

5. ¿El cableado se encuestra correctamente instalado?
SI____ NO____
Por qué? _____

6. ¿Con que periodo se hace mantenimiento a los equipos?
Cada ocho días_____ cada mes____, cada tres meses____, cada año____

7. ¿Se cuenta con los manuales para cada programa y equipo?
SI___ NO____
Por qué? _____

8. De las siguientes afirmaciones clasifique cuales son las

FORTALEZAS.

Es un sistema mecanizado
Cuenta con herramientas y procesos bien definidos
Se da importancia al adecuado manejo de información
Existen políticas y normativas
Todas las anteriores

DEBILIDADES

La producción de información es deficiente con análisis limitados y sectorizados
El análisis de la información es limitado
Recursos con poca capacitación
Todas las anteriores

OPORTUNIDADES

Existe interés en fortalecer el sistema de información
Disponer de recursos para realizar planificación estratégica
Apoyo político al desarrollo del diagnóstico
Apoyo Financiero
Obtener más recursos y tecnificados
Todas las anteriores

AMENAZAS

Personal rotativo afectaría la continuidad del sistema
Puede haber importantes rezagos en la información
Información incompleta
El Imponer acciones particulares
Falta de oportunidad en la información
Falta de calidad
Todas las anteriores

Gracias.

Apéndice B. Lista de chequeo.

La siguiente lista de chequeo, tomada de (Vergel & Martinez, 2014), fue aplicada al encargado del área de sistemas, quien dio su punta de vista de acuerdo a lo tratado en las oficinas de la empresa.

LISTA DE CHEQUEO

AUDITORIA SEGURIDAD DE LA INFORMACION

1	**Existe acuerdo de confidencialidad en la empresa?**	SI ___	NO ___
2	**Ha ingresado personal nuevo a la empresa?**	SI ___	NO ___
3	**Existe política de selección de personal?**	SI ___	NO ___
4	**De los siguientes documentos, cuáles fueron sugeridos para el ingreso de los últimos trabajadores?**		
	a. Certificado Judicial Actualizado		
	b. Copia de la cédula - Libreta Militar		
	c. Referencias laborales		
	d. Motorizados: Licencia de conducción-Soat-Tarjeta de Propiedad		
5	**Los usuarios han sido creados de acuerdo al procedimiento establecido?**	SI ___	NO ___
6	**Existe inventario de los recursos informáticos de la cooperativa?**	SI ___	NO ___
7	**Se mantiene el control del ingreso del personal autorizado al área de sistemas?**	SI ___	NO ___

8	**Tratamiento de escritorio?**		
	a. Mantiene objetos innecesario en el puesto de trabajo?	SI ___	NO ___
	b. Tiene activado el protector de pantalla del monitor?	SI ___	NO ___
	c. Mantiene resguardada la información confidencial y/o restringida?	SI ___	NO ___
	d. Mantiene archivadores y/o gavetas que contiene información sensitiva bajo llave?	SI ___	NO ___
	e. Destruye el papel desechado en la forma correcta?	SI ___	NO ___
9	**Existe control del Ingreso de visitantes?**	SI ___	NO ___
10	**Existe control de ingreso de socios en horarios no hábiles**	SI ___	NO ___
11	**Existen sistemas de alarmas?**	SI ___	NO ___
12	**Se aplica la política de configuración de password?**	SI ___	NO ___
13	**Cuál es el tiempo parametrizado en el sistema de cambios de password?**		
14	**Qué versión de antivirus se maneja actualmente?**		
15	**Cada cuánto se actualiza el antivirus?**		
16	**Se lleva a cabo el procedimiento de backups?**	SI ___	NO ___
17	**Cada cuánto se realiza el backup de la información?**		
18	**Se está almacenando la copia del backups en un lugar alterno?**	SI	NO

Tomado de: (Vergel & Martinez, 2014)