RESUMEN - TESIS DE GRADO

AUTORES	**MAGDY ZULEMA ANGARITA VERA** **RITGING DAVID BERMUDEZ BECERRA** **DIANA CAROLINA TRILLOS OSORIO**
FACULTAD	**DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**Especialista YESICA MARIA PEREZ PEREZ**
TÍTULO DE LA TESIS	**DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE TRANSPORTADORES UNIDOS-COOTRANSUNIDOS LTDA SEDE OCAÑA BASADO EN LA NORMA NTC ISO/IEC 27001: 2013**

RESUMEN
(70 palabras aproximadamente)

EL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE TRANSPORTADORES UNIDOS – COOTRANSUNIDOS LTDA SEDE OCAÑA CON BASE EN LA NORMA ISO/IEC 27001:2013 BRINDARÁ UNA HERRAMIENTA QUE FACILITE Y AYUDE A CONCIENTIZAR A CADA UNO DE SUS FUNCIONARIOS ACTIVOS, SOBRE LA IMPORTANCIA DE RESGUARDAR LA INFORMACIÓN, GARANTIZANDO LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA MISMA, PARTIENDO DE UN DIAGNÓSTICO DE LA POSTURA DE SEGURIDAD PARA DETERMINAR EL NIVEL DE MADUREZ DE LA COOPERATIVA HASTA LLEGAR A UN MARCO DE TRABAJO QUE FACILITARÁ LA IMPLEMENTACIÓN DEL SISTEMA EN LA ENTIDAD..

CARACTERÍSTICAS

PÁGINAS: 93	PLANOS:	ILUSTRACIONES: 6	CD-ROM: 1

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE TRANSPORTADORES UNIDOS-COOTRANSUNIDOS LTDA SEDE OCAÑA BASADO EN LA NORMA NTC ISO/IEC 27001: 2013

MAGDY ZULEMA ANGARITA VERA

RITGING DAVID BERMUDEZ BECERRA

DIANA CAROLINA TRILLOS OSORIO

Proyecto desarrollado como requisito para optar el título de Especialista en Auditoria de Sistemas

IS. Esp. MSc (c) YESICA MARIA PEREZ PEREZ

Directora

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERIAS

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

Ocaña, Colombia **Octubre de 2016**

Glosario

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Auditoría de Sistemas: Está dirigida a evaluar los sistemas y procedimientos de uso en una empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse. (Prezi.com, 2014)

Autenticación: Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Modelado de negocio: El modelo de negocio es una representación simplificada de la lógica del negocio, es decir, es la descripción de la forma como cada negocio ofrece sus productos o servicios a los clientes, como llega a éstos, su relación con ellos y cómo la empresa gana dinero.

Continuidad del Negocio: Describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.

Contraseña: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Control de Acceso: Consiste en la verificación de si una entidad (una persona, ordenador) solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

Incidente de seguridad: Es cualquier evento que puede tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

Información. Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

Política de Seguridad. Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. (Reynolds, 1991 Julio)

Riesgo: Se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños.

Seguridad de la información. Es la preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI o ISMS, de sus siglas en inglés (Information Security Management Systems), es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información.

Sistema de información: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Índice

Lista de tablas

Lista de figuras

Lista de apéndices

Resumen

El diseño de un sistema de gestión de seguridad de la información para la cooperativa de transportadores unidos – Cootransunidos Ltda sede Ocaña con base en la norma ISO/IEC 27001:2013 brindará una herramienta que facilite y ayude a concientizar a cada uno de sus funcionarios activos, sobre la importancia de resguardar la información, garantizando la confidencialidad, integridad y disponibilidad de la misma, partiendo de un diagnóstico de la postura de seguridad para determinar el nivel de madurez de la cooperativa hasta llegar a un marco de trabajo que facilitará la implementación del sistema en la entidad.

Introducción

La información se constituye en un insumo relevante para el alcance de los objetivos de toda Organización. Sin embargo, se encuentra expuesta a riesgos en su seguridad; por tal motivo, las empresas actuales se preocupan por mitigarlos y evitar que pongan en peligro su normal funcionamiento.

Una empresa bien estructurada garantiza una prolongada continuidad en un entorno cambiante y riesgoso, razón por la cual debe integrar cada uno de los detalles que se convierten en insumos para sus procesos misionales. En esta medida, como punto a favor hoy en día se cuentan con diversas herramientas que sirven de orientación para las perspectivas de cada entidad; una de ellas es la norma NTC-ISO-IEC 27001:2013, la cual genera un importante compromiso con la seguridad de la información, permitiendo grandes alcances en cada una de las áreas estructurales de la empresa.

Así mismo, como toda organización, la Cooperativa de Transportadores Unidos de Ocaña – Cootransunidos Ltda, busca que su funcionamiento se realice con seguridad, eficiencia y transparencia; sin embargo, su atención se centra en otros aspectos, desconociendo que el manejo de la información también se constituye en un eje fundamental para el adecuado ejercicio de su labor.

Conforme a lo anterior, el presente trabajo se desarrolló con la finalidad de brindar una herramienta basada en la norma NTC-ISO-IEC 27001:2013, que facilite y ayude a concientizar a

cada uno de los funcionarios activos de Cootransunidos Ltda Ocaña, sobre la importancia de resguardar la información, de igual manera que contribuya a desempeñar sus labores de una manera óptima, garantizando la confidencialidad, integridad y disponibilidad de la misma.

Capítulo 1. Diseño de un sistema de gestión de seguridad de la información para la cooperativa de transportadores Unidos-Cootransunidos Ltda. Sede Ocaña basado en la norma NTC-ISO-IEC 27001: 2013

1.1 Descripción del problema

Ante los diferentes retos a los cuales todas las organizaciones deben enfrentarse diariamente, éstas logran tomar mayor conciencia que la información se constituye en un insumo relevante para el alcance de sus objetivos.

Una vez verificada el área administrativa y operativa de la Cooperativa Cootransunidos Ltda. Sede Ocaña se puede evidenciar que los controles relacionados con la seguridad de la información que manejan, no están acordes para garantizar la confidencialidad, disponibilidad e integridad de la misma, desde el punto de vista del factor tecnológico, al igual que el del factor humano que labora en la Empresa.

Como toda organización, la Cooperativa de Transportadores Unidos de Ocaña – Cootransunidos Ltda, busca que su funcionamiento se realice con seguridad, eficiencia y transparencia; sin embargo, su atención se centra en otros aspectos, desconociendo que el manejo de la información también se constituye en un eje fundamental para el adecuado ejercicio de su labor.

En consecuencia, aunque actualmente la Cooperativa cuenta con nuevas y modernas instalaciones, que restringe el fácil acceso de personal externo a sus áreas privadas, carece de políticas de seguridad de la información que permita concientizar a cada uno de sus funcionarios sobre el cauteloso manejo de la misma, razón por la cual se expone a la fuga y pérdida de información importante, amenazando el normal funcionamiento de la entidad sino se toman las medidas necesarias para remediar esta situación.

Formulación del problema

¿Un sistema de gestión de seguridad de la información para la Cooperativa de Transportadores Unidos-Cootransunidos Ltda. Sede Ocaña, basado en la norma NTC-ISO-IEC 27001:2013, permitirá reducir los riesgos asociados al almacenamiento y utilización de la información?

1.2 Objetivos

1.2.1 **Objetivo general**. **Diseñar** un sistema de gestión de seguridad de la información para la Cooperativa de Transportadores Unidos-Cootransunidos Ltda. sede Ocaña, basado en la norma ISO/IEC 27001:2013

1.2.2 Objetivos específicos. Definir el alcance del diseño del sistema de gestión de seguridad de la información, en la Cooperativa de Transportadores Unidos de Ocaña Ltda - COOTRANSUNIDOS.

Realizar un diagnóstico de la postura de seguridad de la información de los procesos incluidos en el alcance del diseño del SGSI para Cooperativa de Transportadores Unidos-Cootransunidos Ltda. Sede Ocaña.

Construir el marco de trabajo para facilitar la implementación de un sistema de gestión de seguridad de la información basado en la norma NTC-ISO-IEC 27001:2013, aplicable en la cooperativa de transportadores unidos-Cootransunidos Ltda. Sede Ocaña.

1.3 Justificación

Una empresa bien estructurada garantiza una prolongada continuidad en un entorno cambiante y riesgoso, razón por la cual debe integrar cada uno de los detalles que se convierten en insumos para sus procesos misionales.

Dentro de dichos insumos se encuentra la información, que consiste en uno de los cimientos sobre los cuales se estructura toda Organización. Sin embargo, se encuentra expuesta a riesgos en su seguridad; por tal motivo, las empresas actuales se preocupan por mitigarlos y evitar que pongan en peligro su normal funcionamiento.

Como punto a favor hoy en día se cuentan con diversas herramientas que sirven de orientación para las perspectivas de cada entidad; una de ellas es la norma NTC-ISO-IEC 27001, la cual genera un importante compromiso con la seguridad de la información, permitiendo grandes alcances en cada una de las áreas estructurales de la empresa.

De igual manera, la Cooperativa de Transportadores Unidos de Ocaña – Cootransunidos LTDA, no es ajena a ello, día a día se preocupa por implementar mejores prácticas que le permitan fortalecerse. Con el diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma NTC-ISO-IEC 27001:2013, se le brindará una herramienta que facilite y ayude a concientizar a cada uno de sus funcionarios activos, sobre la importancia de resguardar la información, de igual manera que contribuya a desempeñar sus labores de una manera óptima, garantizando la confidencialidad, integridad y disponibilidad de la misma.

1.4 Hipótesis

Con el diseño de un sistema de gestión de seguridad de la información para la Cooperativa de Transportadores Unidos - Cootransunidos Ltda. Sede Ocaña, basado en la norma NTC-ISO-IEC 27001:2013, se facilitarán herramientas que le permitan asegurar y salvaguardar la información que se genera constantemente dentro de la empresa, garantizándole la continuidad del negocio de una manera segura y confiable.

1.5 Delimitaciones

1.5.1 Geográfica. Este estudio tuvo lugar en la Cooperativa de Transportadores Unidos-COOTRANSUNIDOS LTDA, sede Ocaña Norte de Santander.

1.5.2 Conceptual. Los conceptos que se trataron en este proyecto están relacionados con la Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI),

Políticas de Seguridad de la Información, Controles, Continuidad del Negocio y Gestión de Riesgos.

1.5.3 Temporal. El proyecto se llevó a cabo en un plazo de 10 semanas, desarrollando cada objetivo, a partir de la aprobación del anteproyecto

1.5.4 Operativa. El desarrollo del proyecto visto desde la parte operativa, se soportó en los procesos de la Cooperativa de Transportadores Unidos - Cootransunidos Ltda Sede Ocaña, conformado por las áreas de gerencia, secretaria general, tesorería, cartera, contabilidad, agencias, despachos de pasajes y encomiendas.

Capítulo 2. Marco referencial

2.1 Marco histórico

La seguridad ha existido desde los anales de la historia y su evolución ha ido ligada de una manera u otra a la del ser humano en todo su ámbito de actuación.

En la antigüedad el hombre se enfrentaba a diversos peligros que ponían en riesgo su supervivencia, de tal forma que centró sus esfuerzos en poner todos los medios necesarios para salvaguardarla. Debido a ello generó herramientas de protección ante los peligros que le acechaban, principalmente peligros naturales, como fuego, inundaciones, ataques de animales, entre otros, dando lugar a las primeras armas para protegerse, creadas con elementos naturales como piedras o madera. De forma natural estaba desarrollando la primera seguridad: la física.

Esta preocupación inicial de preservar la vida, se convirtió en una necesidad obligatoria para salvaguardar la especia y evitar su extinción. Desde este momento el ser humano se ha enfrentado a toda clase de amenazas durante su largo camino en busca de la seguridad.
Hoy en día el objetivo de la seguridad ha evolucionado, dejando atrás el único objetivo de preservar la especie humana y diversificándolo buscando otros orientados a la seguridad en diferentes ámbitos. De la misma forma que los objetivos de la seguridad han ido evolucionando, la evolución de la seguridad en las empresas no ha quedado atrás y ha experimentado un cambio sustancial desde sus inicios, principalmente motivado por los avances tecnológicos a los que se ha visto expuesta.

En la década de los 70, la seguridad en las empresas estaba centrada en garantizar el buen uso de la información por parte de los empleados confiando en el sentido común para garantizar la seguridad de la organización. Sin embargo y debido a la inclusión y evolución de la tecnología, aparecieron nuevos riesgos que hicieron que esta "seguridad" quedara obsoleta. Uno de los principales motivos por los que el avance de la tecnología propulsó un cambio en la tendencia de seguridad de las empresas vino motivado principalmente por los virus que se convirtieron en los principales motores de crecimiento para la Seguridad de la Información a nivel mundial debido a la globalidad de sus objetivos. (Norma Técnica Colombiana NTC-ISO/IEC 27001, 2006)

Existen antecedentes de proyectos relacionados con Sistemas de Gestión de Seguridad de la Información, entre los que cabe destacar:

Sistema de gestión de seguridad de la información para la oficina de control y vigilancia en la corporación autónoma de la frontera nororiental "Corponor" territorial Ocaña. Se propone un sistema de gestión de seguridad de la información para la oficina de control y vigilancia de CORPONOR territorial Ocaña; esta propuesta tiene como fin aportar a la corporación a aumentar la cantidad y calidad de los controles informáticos, a detectar los niveles de madurez tanto de las características físicas como lógicas que dan soporte al proceso y almacenamiento de la información, a dejar sentados los elementos conceptuales y teóricos que les permitirán a las personas que allí trabajan tomar las decisiones adecuadas para utilizar adecuadamente la tecnología y contribuir a disminuir los niveles de inseguridad de la información de la organización. (Juárez, F. M. (s.f.)., s.f)

Sistema de gestión de seguridad de la información (SGSI) para el área de contabilidad de la E.S.E. hospital local de rio de oro cesar. Mediante un SGSI – Sistema de Gestión de Seguridad de la Información, el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (UFPSO, 2015)

2.2 Marco conceptual

A continuación se relacionan algunas definiciones inherentes al Sistema de Gestión de Seguridad de Información que se pretende diseñar:

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Auditoría de Sistemas: Está dirigida a evaluar los sistemas y procedimientos de uso en una empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse. (Prezi.com, 2014)

Autenticación: Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Modelado de negocio: El modelo de negocio es una representación simplificada de la lógica del negocio, es decir, es la descripción de la forma como cada negocio ofrece sus productos o servicios a los clientes, como llega a éstos, su relación con ellos y cómo la empresa gana dinero.

Continuidad del Negocio: Describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.

Contraseña: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Control de Acceso: Consiste en la verificación de si una entidad (una persona, ordenador) solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

Incidente de seguridad: Es cualquier evento que puede tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas

físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

Información. Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

Política de Seguridad. Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. (Reynolds, 1991 Julio)

Riesgo: Se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños.

Seguridad de la información. Es la preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI o ISMS, de sus siglas en inglés (Information Security Management Systems), es la parte de un sistema global de

gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información.

Sistema de información: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

2.3 Marco teórico

2.3.1 ISO/IEC 27001: 2005 – 2013. ISO **27001** es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Este 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). (INTERNATIONAL ORGANIZATION, 2008)

Los dominios que trata esta norma, once (11) en total, se describen a continuación:

Políticas de Seguridad: Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI.

Organización de la seguridad de la información: Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

Gestión de activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.

Seguridad de los recursos humanos: Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información. Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

Seguridad física y ambiental: Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

Gestión de comunicaciones y operaciones: Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

Control de accesos: El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

Sistemas de información, adquisición, desarrollo y mantenimiento: Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

Gestión de incidentes de seguridad de la información: Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de administración de incidentes, que es básicamente definir de forma clara pasos, acciones, responsabilidades, funciones y medidas correctas.

Gestión de continuidad del negocio: Lo que considera este control es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

Cumplimiento: Busca que las empresas cumplan estrictamente con las bases legales del país, evitando cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad. A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

2.3.2 ISO 22301:2012. La ISO 22301 es la norma internacional para la ISO 22301: Gestión de la Continuidad de Negocio, que se basa en el éxito de la Norma Británica BS 25999 y otras normas regionales. Está diseñada para proteger la empresa frente a cualquier posible problema. Esto incluye inclemencias meteorológicas extremas, incendio, inundación, desastres naturales, robo, interrupción de servicios de TI, enfermedad del personal o ataque terrorista. El sistema de gestión ISO 22301 permite identificar las amenazas relevantes y las funciones empresariales críticas que podrían sufrir consecuencias. También permite establecer planes con antelación para asegurarse de que la empresa no detiene su actividad.

2.3.3 Sistema de gestión de seguridad de la información (SGSI). Un Sistema de Gestión de la Seguridad de la Información *(SGSI)* es un conjunto de políticas de administración de la información. El término se denomina en inglés "Information Security Management System" (ISMS).

El término SGSI es utilizado principalmente por la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission.

La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua:

- Plan *(planificar)*: es una fase de diseño del SGSI de evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- Do *(hacer)*: es una fase que envuelve la implantación y operación de los controles.
- Check *(controlar)*: es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- Act *(actuar)*: en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

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".

2.4.2 Leyes en Colombia relacionadas con Información

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.

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.

Ley 1341 de 2009. 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.

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.

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.

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

El proyecto se realizó a través de una investigación descriptiva-cualitativa que es aquella que describe de modo sistemático las características de una población, situación o área de interés. En esta fase se diseñan los instrumentos de recolección de la información, se aplican, se tabulan y se analizan con el fin de obtener información necesaria para el desarrollo y posterior cumplimiento de los objetivos.

Con la aplicación de este método de investigación se pretendió obtener un diagnóstico situacional de la Cooperativa de transportadores unidos-Cootransunidos Ltda. Sede Ocaña.

3.2 Población y muestra

La población objeto de estudio, estuvo conformada en su medio interno por el gerente general de la Cooperativa de Transportadores Unidos-Cootransunidos Ltda. Sede Ocaña y sus ocho (8) empleados en el área administrativa, así como dos (2) despachadores del área operativa (pasajes y encomiendas).

Tabla 1.

Relación de empleados Cootransunidos Ltda. Área administrativa y operativa Sede Ocaña

NOMBRE	CARGO
Román Alberto Jácome Pérez	Gerente General
Andrea Estefanía Meza	Secretaria General
Marla Torres	Jefe de Recursos Humanos
Martha Patricia Yaruro	Contador Público
Mayerly Paola Serrano Guerrero	Auxiliar Contable
Eliana Marcela Trujillo	Auxiliar Agencias
Jenny Karina Ortiz	Auxiliar Agencias
Johana Gallardo	Auxiliar Cartera
Elena Pacheco Sepúlveda	Tesorera
Magaly Rincón Ortiz	Despachadora de encomiendas - Ocaña
Fabio David Sanjuan	Despachador de pasajes - Ocaña

Fuente: Autores del proyecto.

Para el desarrollo del proyecto de investigación se hizo necesario trabajar con el 100% de la población, por lo tanto no se requirió de la aplicación de la fórmula estadística.

3.3 Técnicas e instrumentos de recolección de información

La recolección de la información se llevó a cabo a través de la elaboración y aplicación de los diferentes instrumentos de auditoria, como lo son la entrevista, la encuesta y la lista de chequeo, aplicadas al gerente general y a los empleados de la empresa respectivamente.

Capítulo 4. Presentación de Resultados

Para el cumplimiento de cada uno de los objetivos, se desarrollaron una serie de actividades tal como se evidencia en el cuadro 2, que permitieron conocer el estado situacional a nivel de seguridad de la información de la Cooperativa de Transportadores Unidos – COOTRANSUNIDOS LTDA, como también establecer las pautas para la futura implementación del SGSI.

Tabla 2.

Actividades por objetivos

OBJETIVOS	ACTIVIDADES	ENTREGABLES
Definir el alcance del diseño del sistema de gestión de seguridad de la información.	Reunión con gerencia Identificar los procesos de misión crítica, que van a incluirse dentro del alcance.	Modelado de negocio
Realizar un diagnóstico de la postura de seguridad de la información de los procesos incluidos en el alcance del diseño del SGSI para Cooperativa de Transportadores Unidos-Cootransunidos Ltda. Sede Ocaña.	Diseñar los instrumentos de recolección de información basados en la norma NTC-ISO 27001:2013 Aplicar los instrumentos diseñados Análisis GAP (Tomar como referente anexo A de la norma NTC-ISO 27001:2013 y ejecutar una auditoria a los procesos definidos dentro del alcance).	Diagnóstico a través de la presentación de resultados (niveles de cumplimiento)
Construir el marco de trabajo para facilitar la implementación de un sistema de gestión de seguridad de la información basado en la norma NTC-ISO-IEC 27001:2013, aplicable en la cooperativa de transportadores unidos-Cootransunidos Ltda. Sede Ocaña.	Seleccionar los controles de la norma NTC-ISO 27001:2013, en los aspectos necesarios de la Cooperativa. Elaborar el documento de declaración de aplicabilidad de los controles de la norma NTC-ISO 27001:2013 Elaborar la guía para la implementación de un sistema de gestión de seguridad de la información basado en la norma NTC-ISO-IEC 27001:2013, en Cootransunidos Ltda.	Guía para la implementación del SGSI en la Cooperativa de Transportadores Unidos Ltda.

Fuente. Autores del proyecto

4.1 Alcance del SGSI

El alcance del Sistema de Gestión para la Seguridad de la Información de la Cooperativa Cootransunidos Ltda. estará enmarcado en los procesos de misión crítica que involucran el *transporte de pasajeros* así como los *giros y encomiendas*, definidos por la Gerencia de la Cooperativa, como la razón de ser de la Empresa sin los cuales no podría funcionar.

Esto involucra tanto los empleados que laboran en la parte administrativa y agencias así como los sistemas de información, en el caso de la Cooperativa, software comercial que soporta la operación de estos procesos, generando información valiosa como principal activo de la Empresa, la cual se debe proteger, preservar y administrar a través de las tecnologías utilizadas para su procesamiento, de las diversas amenazas internas y externas a las cuales está expuesta, garantizando las características propias de confidencialidad, integridad, disponibilidad, confiabilidad y no repudio.

El modelo de negocio de la Cooperativa ofrece una perspectiva de lo anteriormente expuesto:

Cootransunidos LTDA.

Misión. Prestar un servicio público de transporte terrestre automotor de pasajeros urbano, intermunicipal, mixto y veredal, al igual que los servicios conexos, para que los habitantes de la región y su área de influencia se movilicen de manera adecuada segura y eficiente, mejoren su calidad de vida y se alcance un desarrollo sostenible. Se tendrá como base el respeto, eficiencia y calidad y se implementarán

mecanismos de participación orientados a generar progreso en la región y sentido de pertenencia entre nuestros Asociados.

Visión. Seremos una empresa modelo, autosuficiente, innovadora, creativa y con tecnología de punta reconocida por sus altos estándares de desempeño, que genere confianza a los usuarios dentro de parámetros de excelencia y eficiencia.

Todas nuestras actividades llevaran un sello de calidad y compromiso. Brindaremos un óptimo servicio a nuestros clientes con respeto y entusiasmo.

Integraremos a nuestro proceso a la comunidad, a las entidades públicas y Privadas y adaptaremos, a conveniencia las experiencias exitosas que se den.

Objetivo General. Suministrar a la comunidad en general el servicio de transporte automotor por carretera y servicios conexos, con radio de acción nacional ya sea con vehículos de la empresa o de sus Asociados, que se encuentren en buenas condiciones técnico-mecánicas.

Objetivos de la Entidad (Primer Nivel)

1. Planear, organizar, dirigir, controlar, integrar y motivar para prestar los servicios de interés común para los Asociados y de beneficio para la comunidad.
2. Facilitar a los Asociados el suministro de los artículos que sean necesarios para el normal desarrollo y funcionamiento de la industria del transporte en forma solidaria.
3. La Cooperativa será ente regulador de tarifas de nuestros servicios
4. Propiciar la educación e integración cooperativa

5. Organizar servicios especializados aprovechando los recursos humanos y técnicos disponibles.
6. Fomentar la cultura propia y el espíritu cívico y patriótico.
7. Suministrarle a la comunidad en general los servicios del transporte de conformidad a las normas vigentes.

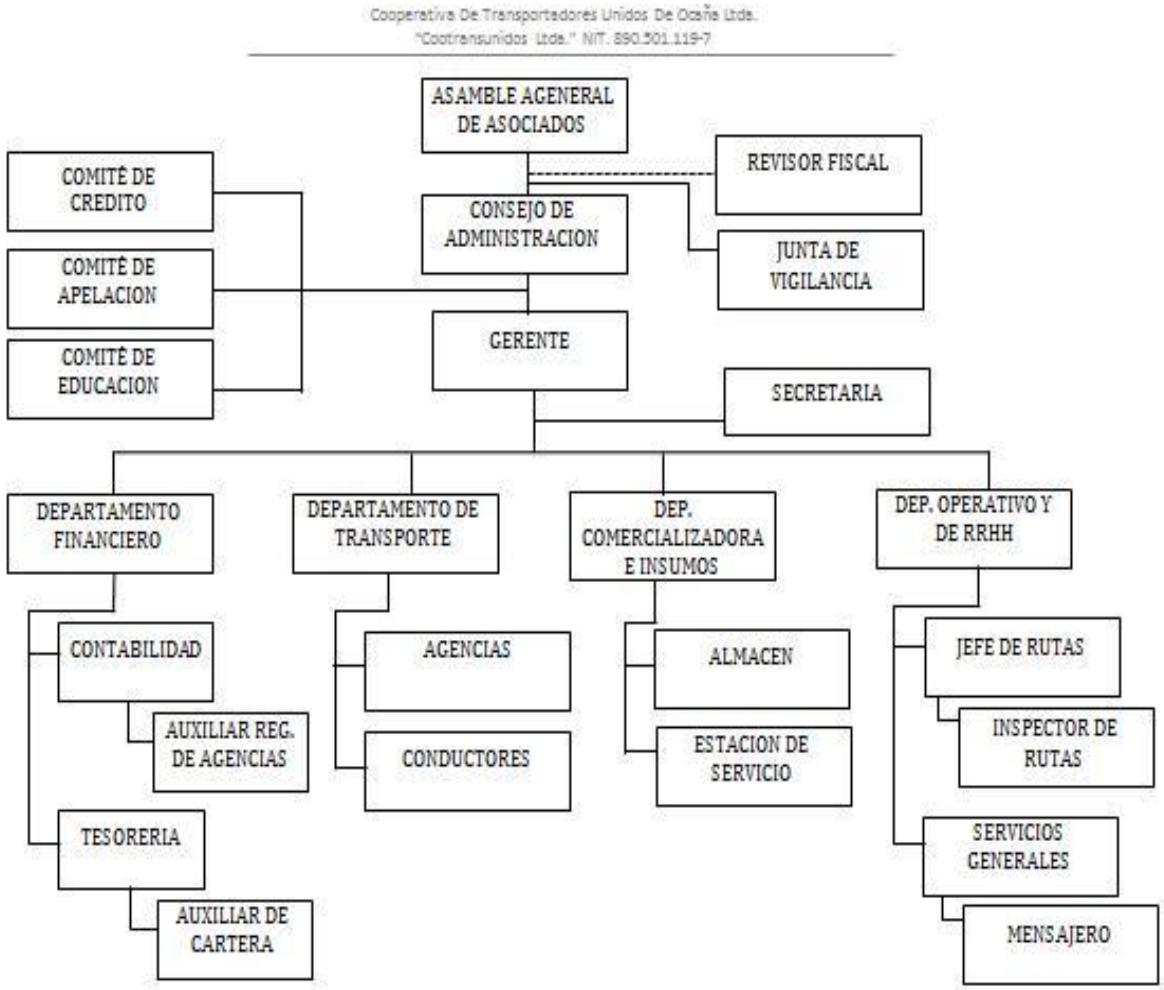

Figura 1. Organigrama de la entidad
Fuente. Autores del proyecto

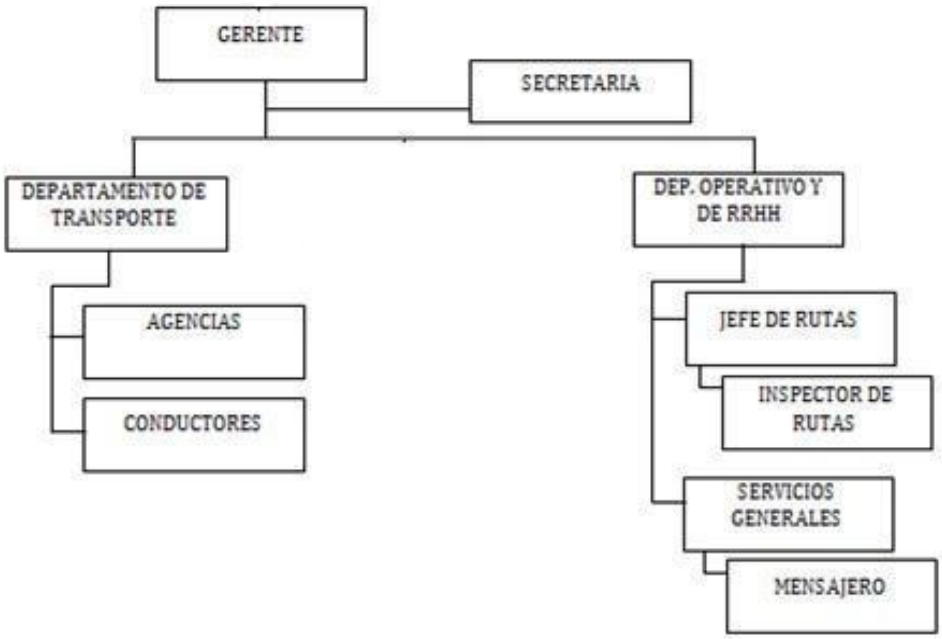

Figura 2. Enmarcación dependencias
Fuente. Autores del proyecto

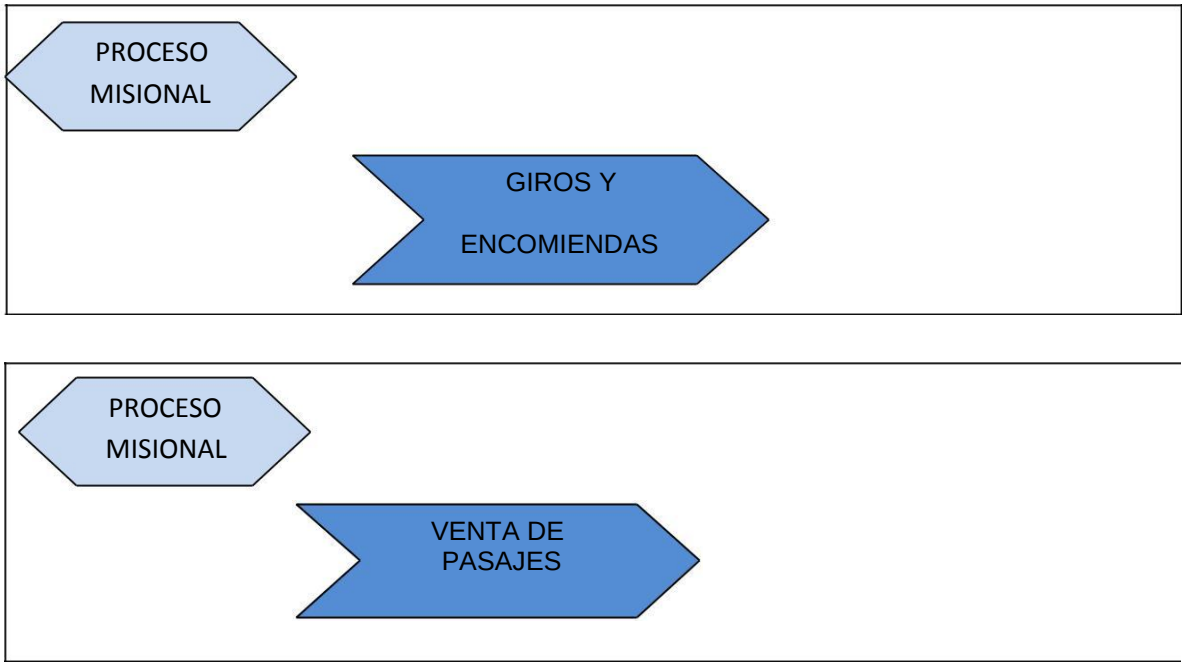

Figura 3. Diagrama de procesos de la dependencia
Fuente. Autores del proyecto

Como Cooperativa tienen dos alcances generales: transporte de pasajeros y servicio de mensajería express representados en los procesos de Venta de Pasajes y envíos de Giros y Encomiendas respectivamente. Estos procesos se manejan desde las Agencias de Despacho y su funcionamiento se soporta y administra en el sistema SILOG, software comercial adaptado a las operaciones de la Cooperativa.

PF Giros y Encomiendas. La persona llega a la agencia para:

- Recepción de encomiendas y giros
- Entrega de giros y encomiendas

Para ambos casos: encomiendas y giros, se necesitan los mismos datos del destinatario y remitente, para ingresar al sistema SILOG:

- Cédula
- Nombre
- Dirección
- Teléfono

Al destinatario, si va a domicilio se exige dirección, pero si reclama en oficina, ésta no se exige.

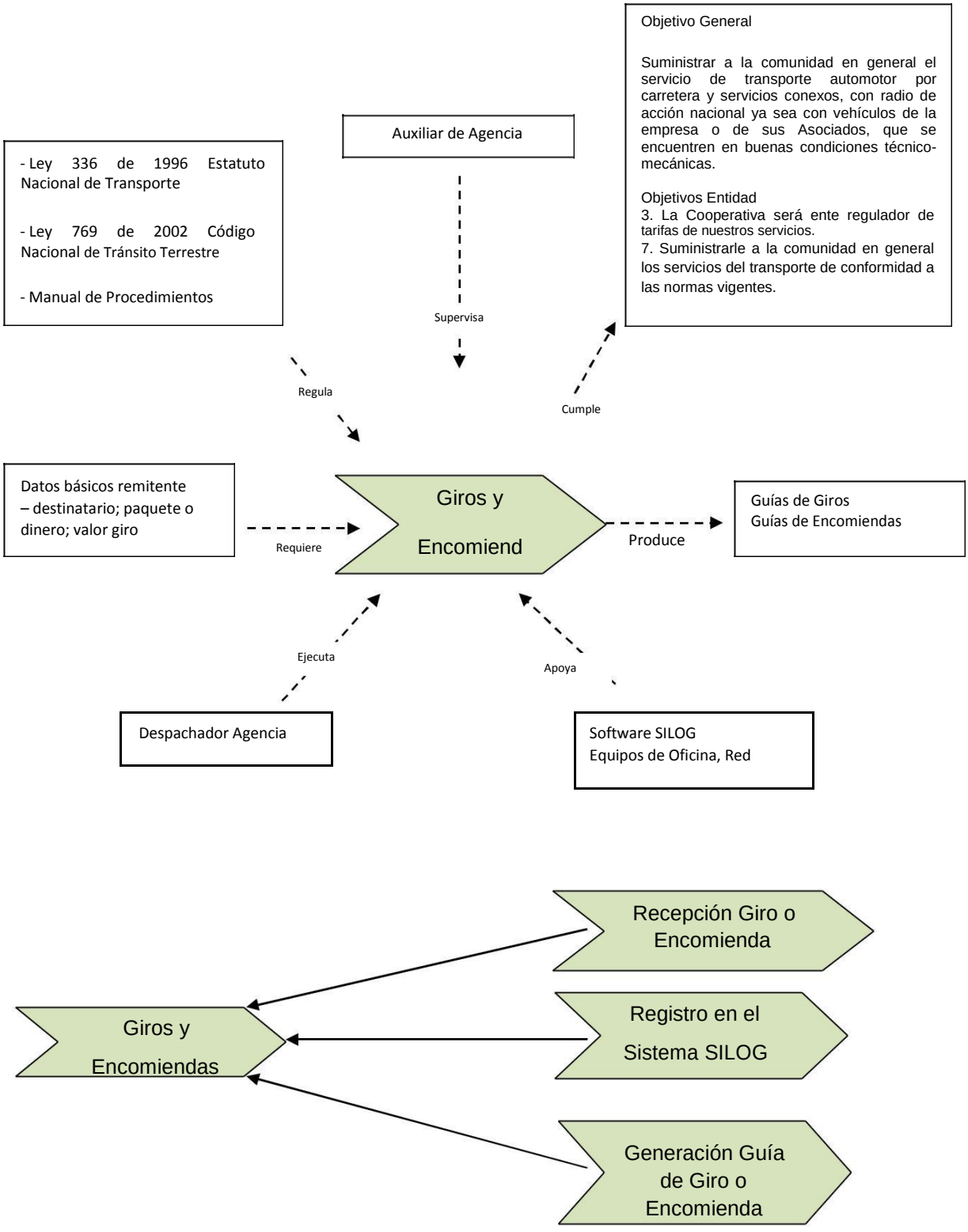

Figura 4. Descripción de Proceso Giros y Encomiendas
Fuente. Autores del proyecto

Recepción Giro o Encomienda: Una vez diligenciados los datos en el sistema, se recibe la encomienda, se revisa su estado. La encomienda recibida pasa a un lugar para su reposo para ser entregado al conductor que vaya de salida.

Al llegar a la ciudad destino, la agencia que recepciona, lo hace en la zona de descargue, quien almacena las encomiendas y queda atento a la llegada del destinatario de cada una de ellas.

Registro en el Sistema SILOG: Se registran en el sistema los datos básicos del emisor y el receptor (Cedula, Nombre, Dirección, Teléfono). Cuando el receptor va a reclamar la encomienda, éste debe identificarse obligatoriamente con su cédula, la cual es verificada en el sistema para identificar en qué vehículo se transportó y hacer entrega de la misma. En el caso de los giros, automáticamente se registra el giro en la agencia, el receptor puede reclamarlo en el destino identificándose con su cédula.

Generación de Guía de Giro o Encomienda: En el sistema van quedando las guías de las encomiendas recibidas. Con una hora de anticipación cada conductor debe acercarse a la agencia para el cargue de las encomiendas, en ese momento se procede a elaborarse la planilla de encomiendas, en las que se asignan las respectivas guías disponibles para ser transportadas, y en la zona de cargue se le hace entrega de las respectivas encomiendas.

PF Venta de Pasajes. El cliente se acerca e indica el destino a donde quiere dirigirse, cada hora se despachan carros. Se solicitan los datos de cédula, nombre, dirección, teléfono para registro en el SILOG, (si ya está registrado solo se confirman los datos, en el evento de que se requiera actualizarse).

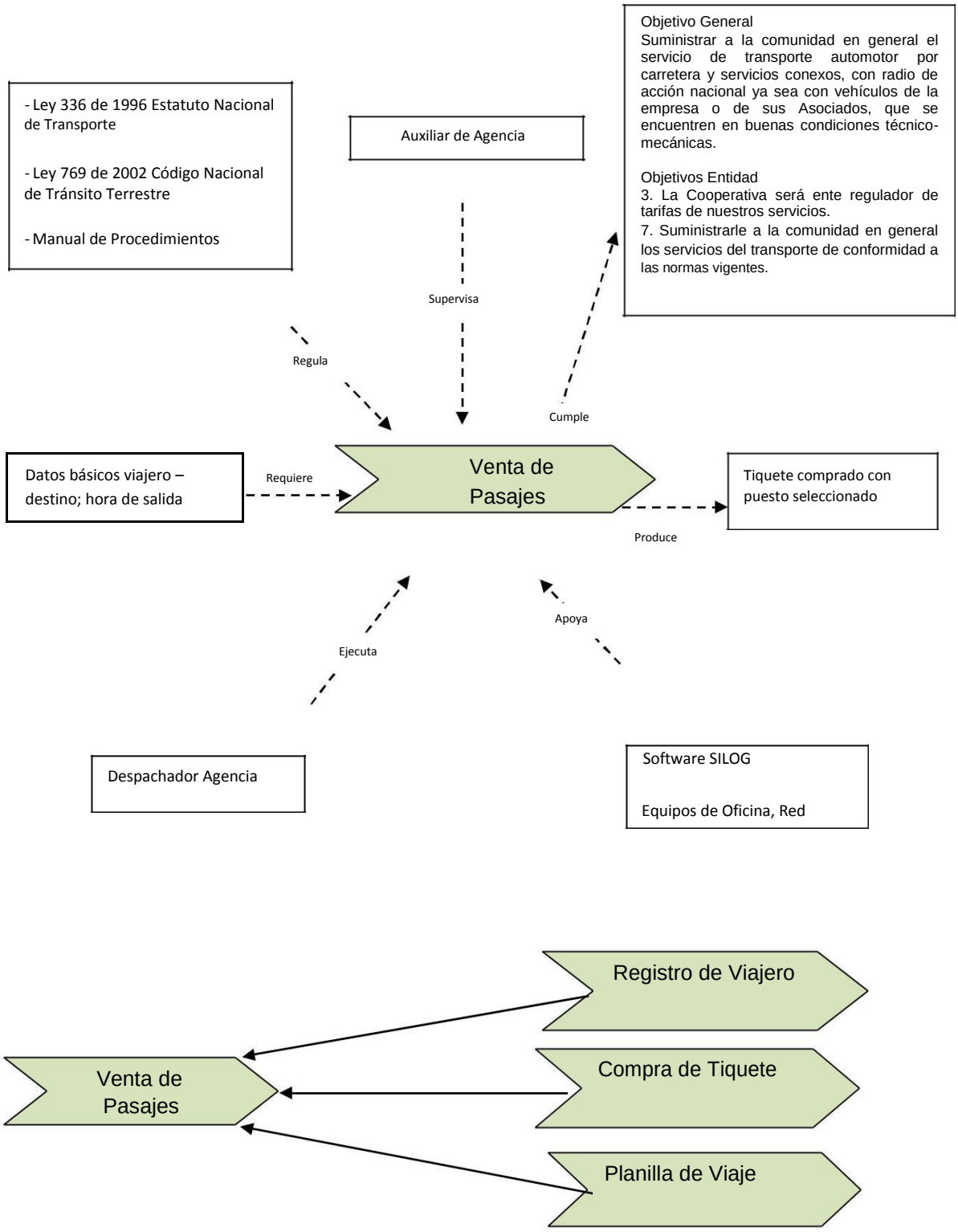

Figura 5. Descripción de Proceso Venta de Pasajes
Fuente. Autores del proyecto

Registro de Viajero: Se registran en el sistema SILOG los datos básicos del viajero (Cedula, Nombre, Dirección, Teléfono). Si ya está registrado solo se confirman los datos, en el evento de que se requiera actualizarse.

Compra de Tiquete: El sistema permite visualizar qué puestos están disponibles, para que el usuario lo escoja. La compra de tiquetes se puede hacer por vía telefónica y presencialmente, con la salvedad que vía telefónica tienen tiempo estipulado para la cancelación del mismo, de lo contrario se libera del sistema para ser vendido nuevamente.

Planilla de Viaje: El carro que esté en el clavijero (orden de despacho) se le asignan los tiquetes comprados, en su respectiva planilla de viaje. El carro se despacha cumpliendo su horario habitual, así no hayan pasajeros. El conductor cancela el valor de la planilla (valor fijado por la gerencia y el consejo) de donde se distribuyen los respectivos ingresos para la agencia y la empresa. Esas planillas están distribuidas por porcentajes, que cubren los rubros de seguros, ingreso agencia, ingreso empresa.

El valor de la planilla varía de acuerdo con la capacidad del vehículo (4, 8,12, 15 pasajeros) y la ruta a cubrir.

Área tecnológica de la entidad. La Cooperativa Cootransunidos Ltda. no cuenta con un área tecnológica, por ende no existe un encargado de los sistemas de información o un Jefe de Sistemas.

Tabla 3.
Sistemas de Información de la Entidad

NOMBRE	DESCRIPCIÓN
SILOG	Software Administrativo y Operativo ajustado a las necesidades de la Cooperativa con soporte directo del proveedor en cuanto a mantenimiento, solución de problemas y actualizaciones de manera presencial y virtual. De uso en red en las Agencias y con acceso desde Internet.
SIIGO	Software contable comercial, ajustado a las necesidades de la Cooperativa, con soporte directo del proveedor en cuanto a mantenimiento, solución de problemas y actualizaciones. De uso local por la Contadora

Fuente. Autores del proyecto

Tabla 4.
Inventario recursos tecnológicos

Gerencia	10 computadores
	2 impresoras normales y 3 impresoras de punto
	10 teléfono y 1 celular
	3 máquinas sumadoras
Agencias	Cada agencia posee computadores, teléfonos fijos y celulares e impresoras.

Fuente. Autores del proyecto

Tabla 5.
Equipos de cómputo y de comunicación propios

ARTICULO	REFERENCIA	CANTIDAD	ESTADO
Computador	No 5CM1320368	1	BUENO
Impresora EPSON	680Y2424	1	BUENO
Teléfono PANASONIC	TS500LX	1	BUENO
A.P.C 350		4	BUENO
Telefono	33F2019	1	BUENO
Impresora HP 1320	CNFC5530JC	1	BUENO
Impresora		1	REGULAR
Computador	4CS22608GD	1	BUENO
Impresora HP	CNB9R44378	1	BUENO
Impresora EPSON	NUGY00869	1	BUENO
Impresora LX 300	G8DY239715	1	BUENO
Impresora LX 300	G8DY241137	1	BUENO
Impresora EPSON	G8DY329442	1	REGULAR
C.P.U	MXX9440LF	1	BUENO
C.P.U	MXX1130525	1	BUENO
C.P.U	101SN88541	1	BUENO
C.P.U	MXX84304JC	1	BUENO
C.P.U		1	BUENO
Servidor		1	BUENO

Telefono ALCATEL	3138RB	1	BUENO
Telefono	ODKRCO40772	1	BUENO
Telefono	80223193	1	BUENO
Telefono	8GCTB836289	1	BUENO
Telefono	60278054	1	BUENO
Camaras		11	BUENO
Computador	MXX2100JRJ	1	BUENO
Impresora HP	SNPRB	1	BUENO
Computador	HACER	1	BUENO
Computador	HP	1	BUENO
Computador	SAMSUNG	1	BUENO
Computador	COMPAQ	1	BUENO
Computador	4CS22608GD	1	BUENO
Computador	SCMB20368	1	BUENO
Computador	MXX2100KRJ	1	BUENO
Plantas telefónicas		2	BUENO

Fuente. Autores del proyecto

4.2 Diagnóstico de la postura de seguridad de la información de los procesos incluidos en el alcance del diseño del SGSI para Cootransunidos Ltda. Sede Ocaña

Como toda organización, la Cooperativa de Transportadores Unidos de Ocaña – Cootransunidos Ltda, busca que su funcionamiento se realice con seguridad, eficiencia y transparencia; sin embargo, su atención se centra en otros aspectos, desconociendo que el manejo de la información también se constituye en un eje fundamental para el adecuado ejercicio de su labor.

Una vez verificada el área administrativa y operativa de la Cooperativa Cootransunidos Ltda. Sede Ocaña se puede evidenciar que los controles relacionados con la seguridad de la información que manejan, no están acordes para garantizar la confidencialidad, disponibilidad e

integridad de la misma, desde el punto de vista del factor tecnológico, al igual que el del factor humano que labora en la Empresa.

Una vez establecido un acercamiento directo con el gerente general de la Cooperativa y sus empleados, y realizada la entrevista respectiva, basada en los controles de la norma NTC-ISO-IEC 27001:2013, se logra identificar que la empresa se encuentra débil en lo que a seguridad en la información se refiere.

El gerente es consciente de la necesidad de implementar dichos controles que ayuden a organizar la entidad, protegiendo la información de fugas y usos maliciosos, ya sea por parte del personal interno o externo a la entidad.

Teniendo en cuenta el análisis GAP realizado en la Cooperativa, se logra identificar en los diferentes ciclos de la metodología PHVA lo siguiente:

Tabla 6.
Planear

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA
1	La Cooperativa cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI?	No cumple	No se está haciendo
2	La Cooperativa creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	No cumple	No existe
3	La Cooperativa contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	Cumple parcialmente	Se definió y aprobó pero no está documentado
4	La Cooperativa ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la	No cumple	No se está haciendo

	información?		
5	La Cooperativa ha identificado las partes interesadas, necesidades y expectativas de éstas respecto al Sistema de Gestión de Seguridad de la Información?	No cumple	No se está haciendo
6	La Cooperativa ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	Cumple parcialmente	Se realiza pero no bajo la norma
7	En la Cooperativa se ha definido un Cómite de Seguridad de la Información?	No cumple	No existe
8	La Cooperativa cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	No cumple	No existe
9	En la Cooperativa existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No cumple	No existe
10	En la Cooperativa existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	No cumple	No existe
11	La Cooperativa tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	No cumple	No se está haciendo
12	La Cooperativa ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	No cumple	No existe
13	La Cooperativa ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	No cumple	No se está haciendo
14	La Cooperativa tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	No cumple	No existe
15	La Cooperativa tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple	No existe

Fuente. Autores del proyecto

Se evidencia que existe toda la intención de mejorar y comenzar a implementar un sistema de seguridad de la información, de una meta del 30%, solo un 1.5% se está cumpliendo; dichos resultados se pueden establecer sosteniendo que existe la aprobación por parte del superior

jerárquico de iniciar el proyecto, de igual manera, ha evaluado los objetivos y necesidades que tienen con respecto a la implementación de dicho sistema.

No obstante por el momento no cuenta con ningún factor relevante, tales como un comité de seguridad de la información, ni documentos con políticas, roles, responsabilidades, y autoridades en seguridad; así mismo, no tiene establecido ningún proceso para identificar, analizar, valorar y tratar los riesgos en cuanto a seguridad de la información se refiere.

Tabla 7.
Hacer

	ANEXO	ESTADO	EVIDENCIA
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**		
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		
A5.1.1	Políticas para la seguridad de la información	No cumple	No existe
A5.1.2	Revisión de las políticas para la seguridad de la información.	No cumple	No existe
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A6.1	Organización interna		
A6.1.1	Roles y responsabilidades para la seguridad de la información	No cumple	No existe
A6.1.2	Separación de deberes	No cumple	No se está haciendo
A6.1.3	Contacto con las autoridades	No cumple	No se está haciendo
A6.1.4	Contacto con grupos de interés especial	No cumple	No se está haciendo
A6.1.5	Seguridad de la información en la gestión de proyectos.	No cumple	No existe
A6.2	Dispositivos móviles y teletrabajo		
A6.2.1	Política para dispositivos móviles	Cumple parcialmente	El acceso a la red a través de dispositivos móviles, está restringido, pero no se encuentra documentado
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A7.1	Antes de asumir el empleo		
A7.1.1	Selección	Cumple parcialmente	Existe un perfil para cada cargo, pero no está documentado y actualizado en su totalidad
A7.1.2	Términos y condiciones del empleo	Cumple parcialmente	Existen claúsulas de confidencialidad de la información en los contratos de los empleados, pero no está documentado de manera completa
A7.1	Durante la ejecución del empleo		
A7.2.1	Responsabilidades de la dirección	Cumple parcialmente	Conocen de la importancia de la seguridad de la información, pero no está documentado formalmente
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Cumple parcialmente	Conocen de la importancia de la seguridad de la información, pero no está documentado formalmente
A7.2.3	Proceso disciplinario	Cumple parcialmente	Una fuga de información, puede ocasionar la terminación del contrato
A7.3	Terminación y cambio de empleo		

A7.3.1	Terminación o cambio de responsabilidades de empleo	Cumple parcialmente	Cada empleado es responsable del manejo de la información de acuerdo con la claúsula de confidencialidad, una vez terminado el contrato, pero no existe un control
A8	**GESTIÓN DE ACTIVOS**		
A8.1	Responsabilidad por los activos		
A8.1.1	Inventario de activos	Cumple parcialmente	Existe un inventario de activos con características incompletas e informal
A8.1.2	Propiedad de los activos	Cumple parcialmente	A la hora de asignación de cargos se hace entrega de los equipos, los cuales deben ser entregados mediante acta una vez finalice la contratación, sin embargo, no está formalmente documentado
A8.1.3	Uso aceptable de los activos	Cumple parcialmente	Cada uno es responsable del procesamiento de la información y del uso que le dé a los equipos asignados, no obstante, no se encuentra formalmente documentado
A8.1.4	Devolución de activos	Cumple satisfactoriamente	Una vez finalizada la labor contractual, cada uno hace entrega de los equipos asignados mediante un acta.
A8.2	Clasificación de la información		
A8.2.1	Clasificación de la información	Cumple parcialmente	La información manejada contiene una reserva clasificada a nivel externo (restringido), e interno (empleados y asociados), siendo libre el acceso a la información para los empleados y personalizada para cada uno de los asociados
A8.2.2	Etiquetado de la información	No cumple	No existe un conjunto de procedimientos para el etiquetado de la información
A8.2.3	Manejo de activos	No cumple	No existe procedimiento para el manejo de activos
A8.3	Manejo de medios		
A8.3.1	Gestión de medio removibles	No cumple	No existe restricción del uso de medios removibles.
A8.3.2	Disposición de los medios	No cumple	No existe un control, ni procedimientos formales, para el uso de la información cuando ya no se requiera
A8.3.3	Transferencia de medios físicos	No cumple	No existe un control, ni procedimientos formales, para el uso de la información
A9	**CONTROL DE ACCESO**		
A9.1	Requisitos del negocio para el control de acceso		
A9.1.1	Política de control de acceso	No cumple	No existe política de control de acceso
A9.1.2	Acceso a redes y a servicios en red	Cumple parcialmente	Se asignan unos perfiles a los usuarios del Software SILOG de acuerdo con las funciones que desempeñan, sin embargo, no está documentado formalmente
A9.2	Gestión de acceso de usuarios		
A9.2.1	Registro y cancelación del registro de usuarios	Cumple	Se asignan unos perfiles a los usuarios del Software SILOG de

		parcialmente	acuerdo con las funciones que desempeñan; sin embargo, no está documentado formalmente
A9.2.2	Suministro de acceso de usuarios	Cumple parcialmente	El acceso al software SILOG se hace previa autorización del gerente o del agente encargado, no obstante, no se hace de manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas
A9.2.3	Gestión de derechos de acceso privilegiado	Cumple parcialmente	El acceso al software SILOG se hace previa autorización del gerente o del agente encargado, no obstante, no se hace de manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas
A9.2.4	Gestión de información de autenticación secreta de usuarios	Cumple parcialmente	El acceso al software SILOG se hace previa autorización del gerente o del agente encargado, no obstante, no se hace de manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas
A9.2.5	Revisión de los derechos de acceso de usuarios	No cumple	Una vez asignados los perfiles a los usuarios del Software, no se vuelve a hacer ningún control sobre los mismos
A9.2.6	Retiro o ajuste de los derechos de acceso	Cumple parcialmente	Una vez finalizada la labor contractual, cada uno hace entrega de los equipos asignados mediante un acta. Así mismo se deshabilita los permisos y usuarios para el acceso al Software
A9.3	Responsabilidades de los usuarios		
A9.3.1	Uso de información de autenticación secreta	No cumple	A pesar de que existe una claúsula de confidencialidad al momento de la contratación, no existe una política que oriente el uso de información secreta
A9.4	Control de acceso a sistemas y aplicaciones		
A9.4.1	Restricción de acceso a la información	No cumple	No existe política de control de acceso
A9.4.2	Procedimiento de ingreso seguro	No cumple	No existe política de control de acceso
A9.4.3	Sistema de gestión de contraseñas	No cumple	El ingreso a los computadores no exige contraseñas. Para el ingreso al software en el cual sí se requiere contraseña, no existe sistema de gestión de las mismas
A9.4.4	Uso de programas utilitarios privilegiados	No cumple	No está restringido la instalación y uso de estos programas
A9.4.5	Control de acceso a códigos fuente de programas	No cumple	No está restringido el acceso a los códigos fuentes
A10	**CRIPTOGRAFIA**		
A10.1	Controles criptográficos		
A10.1.1	Política sobre el uso de controles criptográficos	No cumple	No existe política para la protección de la información
A10.1.2	Gestión de llaves	No cumple	No existe política para la protección de la información
A11	**SEGURIDAD FISICA Y DEL ENTORNO**		
A11.1	Áreas seguras	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido

A11.1.1	Perímetro de seguridad física	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A11.1.2	Controles de acceso físicos	Cumple parcialmente	El área de información se encuentra ubicada de manera segura, sin embargo, no está formalmente documentada
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Cumple parcialmente	El área de información central cuenta con una estructura física nueva diseñada, para la prevención de riesgos naturales. Cabe señalar, que las agencias están expuestas ya que sus estructuras físicas no cuentan con las mismas características de la Edificación principal
A11.1.4	Protección contra amenazas externas y ambientales.	No cumple	No existen procedimientos para trabajo en áreas seguras
A11.1.5	Trabajo en áreas seguras.	Cumple parcialmente	Tanto la nueva estructura física, como la de las demás agencias están diseñadas con áreas que permiten el aislamiento de personas no autorizadas y ajenas a la entidad que puedan afectar el procesamiento de la información.
A11.1.6	Áreas de carga, despacho y acceso público	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A11.2	Equipos		
A11.2.1	Ubicación y protección de los equipos	Cumple satisfactoriamente	Cada equipo se encuentra ubicado de manera segura en las instalaciones, para evitar el fácil acceso de personal no autorizado
A11.2.2	Servicios de suministro	No cumple	No existe protección para los equipos ante cualquier interrupción o fallas en el suministro de la energía
A11.2.3	Seguridad en el cableado.	Cumple parcialmente	El cableado se encuentra canalizado en la nueva edificación (gerencia - área administrativa), sin embargo, en las agencias de despacho, éste no se encuentra protegido.
A11.2.4	Mantenimiento de los equipos.	Cumple parcialmente	Sólo se hacen mantenimientos correctivos
A11.2.5	Retiro de activos	Cumple parcialmente	Ningún equipo se retira sin autorización, sin embargo, no existe un formato de solicitud de retiro establecido
A11.2.6	Disposición segura o reutilización de equipos	No cumple	No existe restricción del uso de medios removibles.
A11.2.7	Equipos de usuario desatendido	No cumple	No existe protección alguna a los equipos desatendidos.
A11.2.8	Política de escritorio limpio y pantalla limpia	No cumple	No existe política de escritorio limpio, cada uno personaliza el escritorio a su manera.
A12	**SEGURIDAD DE LAS OPERACIONES**		
A12.1	Procedimientos operacionales y responsabilidades		
A12.1.1	Procedimientos de operación documentados	No cumple	No existe documentación para los procedimientos de operación.

A12.1.2	Gestión de cambios	No cumple	No existe control alguno sobre los cambios que surjan en la organización.
A12.1.3	Gestión de capacidad	No aplica	No posee ambientes de desarrollo y pruebas
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No aplica	No posee ambientes de desarrollo y pruebas
A12.2	Protección contra códigos maliciosos		
A12.2.1	Controles contra códigos maliciosos	No cumple	No existe una política claramente definida que permita tomar conciencia y restrinja el acceso a fuentes que vulneren los sistemas de información
A12.3	Copias de respaldo		
A12.3.1	Respaldo de la información	No cumple	No se realizan copias de seguridad regularmente del sistema y menos puestas a prueba
A12.4	Registro y seguimiento		
A12.4.1	Registro de eventos	No cumple	No se controlan los eventos y las fallas de la seguridad de la información.
A12.4.2	Protección de la información de registro	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A12.4.3	Registros del administrador y del operador	No cumple	No existe revisiones ni registros para la actividades desarrolladas
A12.4.4	Sincronización de relojes	No cumple	No existe sincronización referente a tiempo en los sistemas de procesamiento de información
A12.5	Control de software operacional		
A12.5.1	Instalación de software en sistemas operativos	No cumple	No existe una política de seguridad que restrinja la instalación de software en los sistemas operativos.
A12.6	Gestión de la vulnerabilidad técnica		
A12.6.1	Gestión de las vulnerabilidades técnicas	No cumple	No se tienen plenamente identificadas las vulnerabilidades que puedan afectar el normal funcionamiento de los sistemas de información
A12.6.2	Restricciones sobre la instalación de software	No cumple	No existen reglas que orienten la instalación de software por parte de los usuarios.
A12.7	Consideraciones sobre auditorias de sistemas de información		
A12.7.1	Controles de auditorías de sistemas de información	No cumple	No se realizan actividades de auditoría.
A13	**SEGURIDAD DE LAS COMUNICACIONES**		
A13.1	Gestión de la seguridad de las redes		
A13.1.1	Controles de redes	No cumple	No existe gestión y control en la red de la Cooperativa para

			proteger la información
A13.1.2	Seguridad de los servicios de red	No cumple	Existe exposición y vulnerabilidad de los servicios de red, no existen mecanismos de seguridad
A13.1.3	Separación en las redes	No cumple	No se evidencia separación en la red de los servicios de información y usuarios.
A13.2	Transferencia de información		
A13.2.3	Mensajería Electrónica	No cumple	Manejan un solo correo electrónico para toda la cooperativa, no se evidencia control para lo enviado y recepcionado.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Cumple parcialmente	Existen cláusulas de confidencialidad de la información en los contratos de los empleados, pero no está documentado de manera completa, no obstante no se realiza una revisión periódica, para verificar el funcionamiento de la misma.
A14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	No cumple	No existen requisitos relacionados con la seguridad de la información.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	No cumple	No existen requisitos relacionados con la seguridad de la información.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	No cumple	No existe documentado los protocolos de protección de transacciones
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		
A.14.2.1	Procedimientos de control de cambios en sistemas	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.2	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.3	Restricciones en los cambios a los paquetes de software	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.4	Principio de Construcción de los Sistemas Seguros.	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.5	Ambiente de desarrollo seguro	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.6	Desarrollo contratado externamente	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.7	Pruebas de seguridad de sistemas	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.8	Prueba de aceptación de sistemas	No aplica	No posee área de desarrollo de aplicaciones
A14.3	Datos de prueba		
A.14.3.1	Protección de datos de prueba	No aplica	No posee área de desarrollo de aplicaciones
A15	**RELACIONES CON LOS PROVEEDORES**		
A15.1	Seguridad de la información en las relaciones con los proveedores.		
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Cumple parcialmente	Existe un contrato de confidencialidad con el proveedor del software, sin embargo se han visto afectados por situaciones

			que involucran la seguridad de la cooperativa.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Cumple parcialmente	Existe un contrato de confidencialidad con el proveedor del software, sin embargo se han visto afectados por situaciones que involucran la seguridad de la cooperativa.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Cumple parcialmente	El software está diseñado con parámetros de seguridad que permitan la minimización de los riesgos asociados a la información, se encuentra definido con el proveedor pero no se gestiona
A15.2	Gestión de la prestación de servicios de proveedores		
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Cumple parcialmente	Solo se hace de manera correctiva, en el evento de que sucede cualquier anomalía.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Cumple parcialmente	De acuerdo a las necesidades del negocio se conviene con el proveedor sobre las mejoras a realizar para que el software sea actualizado y optimizado.
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		
A16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A16.1.1	Responsabilidades y procedimientos	No cumple	No están definidos las responsabilidades y procedimientos para garantizar una respuesta rápida ante posibles incidentes en la información
A16.1.2	Reporte de eventos de seguridad de la información	No cumple	No existe un canal de gestión donde se puedan registrar los eventos de seguridad de la información.
A16.1.3	Reporte de debilidades de seguridad de la información	Cumple parcialmente	Cualquier eventualidad es informada por los usuarios del sistema, sin embargo no se encuentra un procedimiento formalmente definido
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	No cumple	No existen políticas de seguridad de la información
A16.1.5	Respuesta a incidentes de seguridad de la información	No cumple	No existen políticas de seguridad de la información
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	No cumple	No existe un canal de gestión donde se puedan registrar los eventos de seguridad de la información.
A16.1.7	Recolección de evidencia	No cumple	La organización no tiene procedimientos definidos para el manejo de la información
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**		
A17.1	Continuidad de Seguridad de la información		
A17.1.1	Planificación de la continuidad de la seguridad de la información	No cumple	No existe un plan de contingencia para la continuidad del negocio, en el evento de ser afectado por algún incidente

			interno o externo.
A17.1.2	Implementación de la continuidad de la seguridad de la información	No cumple	No existe un plan de contingencia para la continuidad del negocio, en el evento de ser afectado por algún incidente interno o externo.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No cumple	No existe un plan de contingencia para la continuidad del negocio, en el evento de ser afectado por algún incidente interno o externo.
A17.2	Redundancias		
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	No aplica	La Cooperativa no posee este tipo de instalaciones
A18	**CUMPLIMIENTO**		
A18.1	Cumplimiento de requisitos legales y contractuales		
A18.1.1	Identificación de la legislación aplicable.	No cumple	No existe documentación explícita relacionada con los sistemas de información y su reglamentación legal
A18.1.2	Derechos propiedad intelectual (DPI)	No aplica	La Cooperativa no posee patentes de software de desarrollo propio, utiliza software comerciales para su operación
A18.1.3	Protección de registros	No cumple	No existe documentación explícita relacionada con los sistemas de información y su reglamentación legal
A18.1.4	Privacidad y protección de información de datos personales	No cumple	A pesar de que se protege la información, no se hace siguiendo parámetros legales claramente definidos
A18.1.5	Reglamentación de controles criptográficos.	No aplica	No aplica para la Cooperativa por la naturaleza del servicio
A18.2	Revisiones de seguridad de la información		
A18.2.1	Revisión independiente de la seguridad de la información	No cumple	No existe una política para la seguridad de la información, que permita su posterior revisión
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Cumple parcialmente	Desde la Gerencia de la Cooperativa se revisa lo relacionado con el procesamiento en los sistemas de información pero no bajo las normas de seguridad apropiadas, no se documenta.
A18.2.3	Revisión del cumplimiento técnico	Cumple parcialmente	Los sistemas de información SILOG y SIIGO que utiliza la cooperativa se revisan pero no se documenta

Fuente. Autores del proyecto

Empíricamente existen procesos que ayudan a proteger en un mínimo porcentaje la información, entre esos los siguientes: El acceso a las redes a través de los dispositivos móviles, están restringidos, existe un perfil para cada cargo, el cual es tenido en cuenta a la hora de la selección, existen cláusulas de confidencialidad de la información en los contratos de los empleados. Conocen de la importancia de la seguridad de la información y hacen énfasis en ello. De igual manera, tienen claro que una infracción en términos de fuga de información, puede ocasionar la terminación del contrato, por tal razón, cada uno es responsable del manejo de la información de acuerdo con la cláusula de confidencialidad, una vez terminado el contrato, pero no existe un control.

Se logra evidenciar que existe un inventario de activos con características incompletas e informales. A la hora de asignación de cargos se hace entrega de los equipos, los cuales deben ser devueltos mediante acta una vez finalice la contratación; cada uno es responsable del procesamiento de la información.

Así mismo, la información manejada contiene una reserva clasificada a nivel externo (restringido), e interno (empleados y asociados), siendo libre el acceso a la información para los empleados y personalizada para cada uno de los asociados

El acceso al software SILOG se hace con previa autorización del gerente o del agente encargado, no obstante, no se hace de manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas.

Con relación al acceso físico, el área de manejo de información se encuentra apartada al acceso de personal externo y de manera segura; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido.

Es interesante resaltar que el área de información central cuenta con una estructura física nueva diseñada, para la prevención de riesgos naturales, sin embargo, las agencias están expuestas ya que sus estructuras no cuentan con las mismas características de la edificación principal.

Todo lo anterior se encuentra establecido, pero no está formalmente documentado.

Tabla 8.
Verificar y actuar

VERIFICAR			
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de la Información?	Cumple parcialmente	La Cooperativa no tiene la metodología documentada pero si realiza seguimiento a la seguridad de la información
2	La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?	No cumple	La Cooperativa no tiene un SGSI implementado
3	La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	La Cooperativa no tiene un SGSI implementado
4	La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	No cumple	La Cooperativa no tiene un SGSI implementado

5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	No cumple	La Cooperativa no tiene un SGSI implementado
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple	La Cooperativa no tiene un SGSI implementado
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoría?	No cumple	No se está haciendo
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	No cumple	No se está haciendo
9	La entidad revisa la eficacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	No cumple	No se está haciendo
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información después de las acciones tomadas?	No cumple	No posee SGSI
11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	No cumple	No se está haciendo
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	No cumple	No posee SGSI

Fuente. Autores del proyecto

Al no existir un Sistema de seguridad de la información implementado, estas fases del proceso poco se pueden observar; sin embargo, al hacer énfasis al verificar, cumple con un 1.3%, teniendo en cuenta que la Cooperativa no tiene la metodología documentada pero si realiza seguimiento a la seguridad de la información de manera empírica.

Tabla 9.
Diagnóstico consolidado

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	1,5%
LOGRO2	HACER	40%	7,8%
LOGRO3	VERIFICAR	15%	1,3%
	ACTUAR	15%	0,0%
	TOTAL	100%	10,6%

Fuente. Autores del proyecto

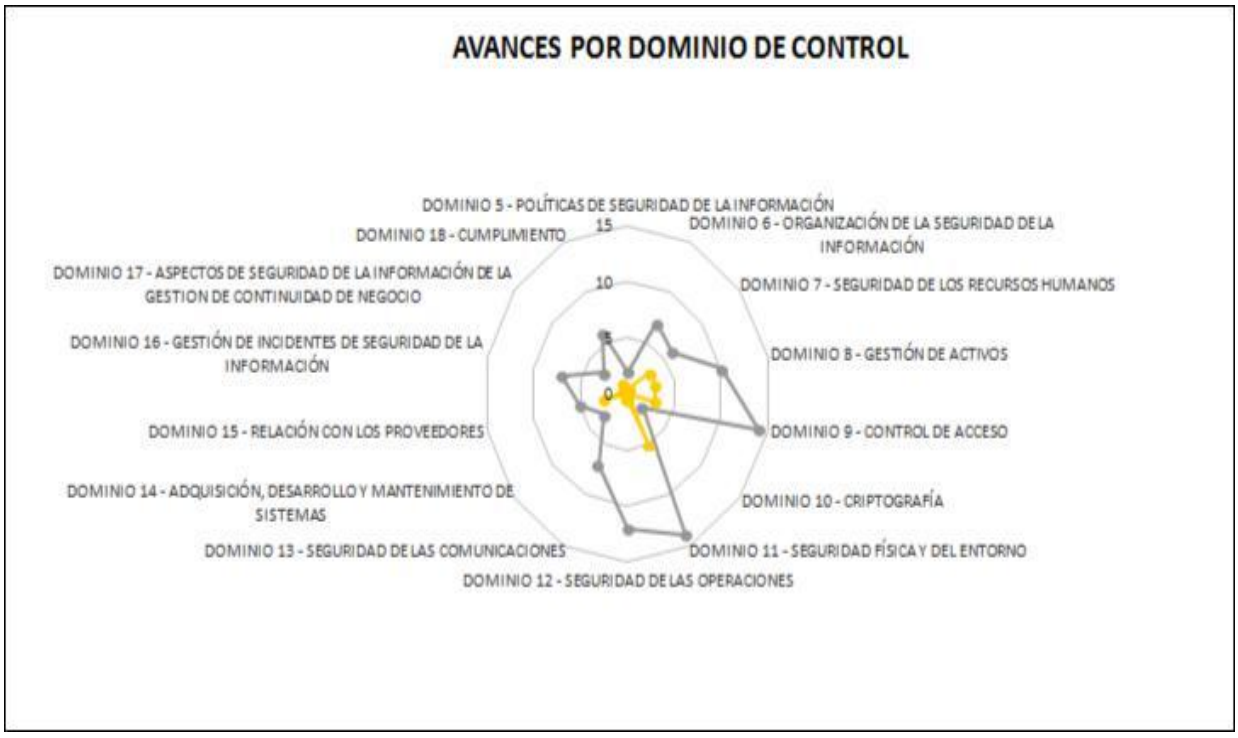

Figura 6. Gráfico de Radar
Fuente. Autores del proyecto

Tabla 10.
Por dominio de control

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	**CONTROLES QUE APLICAN**	**PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS**	**IMPLEMENTADOS**	**PARCIALMENTE**	**NO CUMPLE**	**NO APLICA**
DOMINIO 5 - POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	2	0	0	0	2	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	0,5	0	1	5	0
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	6	3	0	6	0	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	10	3	1	4	5	0
DOMINIO 9 - CONTROL DE ACCESO	14	3	0	6	8	0
DOMINIO 10 - CRIPTOGRAFÍA	2	0	0	0	2	0
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	14	5	1	8	5	0
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	12	0,5	0	1	11	2
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	7	0,5	0	1	4	0
DOMINIO 14 - ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	3	0	0	0	3	9
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	5	2,5	0	5	0	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	0,5	0	1	6	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	3	0	0	0	3	1
DOMINIO 18 - CUMPLIMIENTO	6	1	0	2	4	2
	98					

Fuente. Autores del proyecto

En síntesis, una vez identificada la postura de seguridad para los procesos de misión crítica de la Cooperativa definidos en el alcance, se aclara la visión de construcción de un marco para la implementación de un SGSI en Cootransunidos, teniendo en cuenta las debilidades encontradas, que permita materializar las intenciones de dar un manejo seguro a la información, reduciendo las posibles vulnerabilidades a las que se enfrenta a diario.

4.3 Marco de Trabajo para facilitar la implementación del SGSI en Cootransunidos

Para orientar el proceso de implementación del SGSI en la Cooperativa se hace necesario en primer lugar, entender el alcance de los dominios de seguridad de la norma ISO 27001, que se definen así:

- Política de seguridad: Documento en el cual se estipulan las políticas con respecto a la seguridad de la información de la entidad.
- Organización de la seguridad: Estructura del departamento de seguridad que le permita gestionar la seguridad de la información dentro de la organización: roles, compromisos, autorizaciones, acuerdos, manejo con terceros, entre otros.
- Gestión de activos: Procedimientos para la identificación de los activos de información y los requerimientos de estos en cuanto a confidencialidad, integridad y disponibilidad.
- Seguridad del Recurso Humano: Procedimientos para asegurar que empleados, contratistas y terceros entienden sus responsabilidades y son idóneos para los roles a desempeñar minimizando los riesgos relacionados con personal.

- Seguridad Física y del entorno: Procedimientos y controles para prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la entidad y a su información.
- Gestión de comunicaciones y operaciones: Procedimientos y controles para garantizar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica)
- Control de acceso: Procedimientos y controles para garantizar que el acceso a los activos de información este restringido a personal autorizado.
- Adquisición, desarrollo y mantenimiento de sistemas de información: Procedimientos y controles para asegurar la inclusión de los controles de seguridad en los nuevos sistemas de información (infraestructura, aplicaciones, servicios, etc.) o por cambios a los mismos.
- Gestión de incidentes de seguridad: Procedimientos y controles que buscan que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado.
- Gestión de la continuidad del negocio: Procedimientos y controles enfocados en reaccionar en contra de interrupciones de la función del negocio y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo.
- Cumplimiento: Procedimientos y controles que buscan prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

A continuación se presentan los pasos o actividades para la implementación del SGSI en la Cooperativa Cootransunidos Ltda Ocaña:

4.3.1 Solicitud del interlocutor. Para poder iniciar la actividad de generación del SGSI de la Cooperativa, se debe identificar al interlocutor que acompañará al consultor de seguridad durante todo el proceso de consultoría e implementación del SGSI. El rol de interlocutor lo debería tener el Jefe de Sistemas si la Cooperativa contara con un área de sistemas, pero como no existe dicha área, este rol será asumido por la persona más afín al sistema de información (Software de Aplicación SILOG) de la compañía. Este rol se formalizará a través del formato Nª 1 - FORMATO PARA DESCRIPCIÓN DE ROLES Y FUNCIONES que está anexo.

4.3.2 Obtención de la lista de usuarios del sistema de información y sus roles. Consiste en solicitar al interlocutor la lista de trabajadores de la Cooperativa que tienen acceso al sistema de información y los roles que desempeñan dentro de la empresa, con el objetivo de determinar cuáles de ellos están asociados al sistema de información de la compañía y correlacionarlos con los roles definidos en el esquema seleccionado.

4.3.3 Establecimiento del nivel de madurez. Esta fase ya fue definida en el diagnóstico de la postura de seguridad donde se conoció el nivel de madurez actual de la Cooperativa y el nivel de cumplimiento de los controles de seguridad del SGSI, estableciendo cuales cumplen o no así como cuales no aplican.

Para determinar el nivel de madurez actual de la compañía se determinará primero el nivel de cumplimiento de un control. Este nivel de cumplimiento se establece para todos los controles que componen el SGSI. Una vez establecido el nivel de cumplimiento de seguridad de cada control, se puede establecer el nivel de cumplimiento de seguridad para toda la empresa.

Con base en lo anterior, se establecieron los controles que se deben implementar en el SGSI de la Cooperativa para garantizar un nivel de seguridad óptimo, los cuales se describen a continuación:

Políticas de la seguridad de la información

Orientación de la Gerencia para la gestión de la seguridad de la información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuidad.

Organización de la seguridad de la información

Organización interna. Se debe crear un Área de Sistemas, encargada de la administración del manejo de la información, creando roles y responsabilidades entre los empleados participantes.

Seguridad de los recursos humanos

Antes de asumir el empleo

- Documentar el perfil de cada cargo
- Seleccionar las hojas de vida, teniendo en cuenta el perfil solicitado
- Revisar antecedentes judiciales de los aspirantes, teniendo en cuenta las leyes, reglamentaciones y ética pertinente
- Crear documento de confidencialidad para el uso de la información de manera formal, incluyéndolo dentro del contrato laboral

Durante la ejecución del empleo

- Elaborar acta de entrega del inventario físico puesto a disposición del nuevo empleado
- Cada empleado deberá ser responsable de la información que se maneje dentro de la Cooperativa
- Realizar constantes capacitaciones sobre actualización y concientización del manejo de la información; así mismo, sobre nuevos programas a ejecutar para las diferentes operaciones
- Ante cualquier eventualidad de fuga de información o mal manejo de la misma, cada uno de los empleados tendrá la responsabilidad de comunicar al área de sistemas o gerencia, para lo pertinente, relacionado con las acciones en contra de los empleados que hayan cometido una violación a la seguridad de la información.

Terminación y cambio de empleo. El empleado deberá presentar un acta haciendo entrega del inventario físico puesto a su disposición para el desempeño de sus funciones

Se procederá a desactivar los roles y perfiles asignados para el uso de los sistemas de información en la Cooperativa.

Gestión de activos

Responsabilidad por los activos. Se debe elaborar de manera formal un inventario de activos, para facilitar su correcto manejo. Así mismo, deberá estarse efectuando periódicamente revisión del estado de los mismos, y actualización de éstos.

Asignar a cada dependencia los activos necesarios para el normal desempeño de sus actividades, quienes deberán responder por los mismos

Clasificación de la información. La información se deberá clasificar de acuerdo a su grado de confidencialidad, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada, para establecer los mecanismos de protección necesarios.

Manejo de medios. Cada funcionario es responsable del manejo que le dé a la información, y responderá disciplinariamente por ello.

Los medios removibles que sean utilizados dentro de la organización será para uso interno y relacionado con la labor del funcionario.

La información que no se requiera deberá ser archivada de manera segura, y se deberá disponer de ella utilizando procedimientos formales cuando se requiera.

Control de acceso

Requisitos del negocio para el control de acceso. Solo se deberá permitir el ingreso al área de manejo de información del proceso misional (Administrativa) a personal autorizado, entendiéndose por ello, funcionarios y personas externas previa autorización.

Solo tendrán acceso al Software los funcionarios autorizados por el área de sistemas, para el desempeño de sus funciones, y los perfiles asignados serán ejecutados teniendo en cuenta las funciones que cada uno ejerza. Cada uno responderá por los privilegios otorgados.

Gestión de acceso de usuarios. Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso

Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

Responsabilidades de los usuarios. Cada uno responderá por los privilegios otorgados de acuerdo a su perfil, para el desempeño de sus funciones

Control de acceso a sistemas y aplicaciones. Cada empleado deberá generar una contraseña personal para el ingreso al sistema desde el escritorio, la contraseña contendrá unos parámetros de seguridad

Seguridad física y del entorno

Áreas seguras

- Las áreas seguras de Cootransunidos deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado
- El área de sistemas será ubicada en una zona segura con mínimos riesgos de ser afectada por vulnerabilidades de tipo natural, social y del ambiente (ataques maliciosos o accidentes).
- Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
- Se deben diseñar y aplicar protección física contra desastres naturales, incendios, inundaciones, ataques maliciosos o accidentes a los que se esté expuesto.

Equipos

- Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
- Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
- El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
- Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas, razón por la cual se deben estar haciendo mantenimientos preventivos.
- Los equipos, información o software no se deben retirar de su sitio sin autorización previa, a través de un formato formalmente diseñado.
- Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
- Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

Seguridad de las operaciones. Procedimientos operacionales y responsabilidades

- Los procedimientos de operación identificados en esta política, se deben documentar y poner a disposición de todos los usuarios de Cootransunidos que los necesitan.

- Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

- El líder o coordinador del área de sistemas de Cootransunidos, deberá controlar que los cambios en los componentes operativos, no afecten la seguridad de los mismos.

Protección contra códigos maliciosos

- Se deben implementar controles de detección, de prevención y de recuperación, antivirus licenciado, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Copias de respaldo

- Se deberán hacer copias de respaldo de la información diariamente, y ésta será resguardada en sitios seguros bajo la responsabilidad de la persona encargada, siguiendo los estándares de la Gerencia de Cootransunidos Ltda.
- Las copias se deben guardar en un sitio diferente, garantizando la seguridad de las mismas.

Registro y seguimiento

- Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
- Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

Relaciones con los proveedores. Seguridad de la información en las relaciones con los proveedores.

- Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
- Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Gestión de la prestación de servicios de proveedores

- Cootransunidos debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

- Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la re-evaluación de los riesgos.

Gestión de incidentes de seguridad de la información

Gestión de incidentes y mejoras en la seguridad de la información

- Se debe exigir a todos los empleados y contratistas que usan los servicios y software de Aplicación de la Cooperativa, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
- Canalizar todos los incidentes relacionados con seguridad de la información a través del Área de Sistemas.

Aspectos de seguridad de la información de la gestión de continuidad de negocio

Continuidad de Seguridad de la información

- Ante cualquier eventualidad de tipo natural, social, o maliciosa, que afecte el normal funcionamiento de la entidad para el cumplimiento de su proceso misional, se deberá crear un plan de contingencia, que se pondrá en marcha con el fin de no crear traumatismos en la normal prestación de los servicios.

Cumplimiento

Cumplimiento de requisitos legales y contractuales

- Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la Cooperativa para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.

Revisiones de seguridad de la información

- El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
- El SILOG se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

4.3.4 Nivel de madurez deseable. En condiciones normales el valor inicial para un peso será de 0.50 unidades, para restar importancia al criterio el valor del peso se reducirá a 0.25 y para eliminarlo se establecerá un valor de 0. En caso de querer darle mayor importancia se llevará a 0.75 y si el factor se considera fundamental para el sistema, se puede subir el valor del peso a 1.

4.3.5 Identificación de activos

Es posible hacer la siguiente clasificación de activos de acuerdo a los que maneja la Cooperativa, la metodología indica que no pueden ser tan especificados.

Tabla 11.
Clasificación de activos

Tipo activos	Descripción Activo	Propietario	Coste	Valor Estratégico
Activos esenciales				
Datos de carácter personal				
Arquitectura del sistema				
Datos / Información				
Claves criptográficas				
Servicios				
Software - Aplicaciones informáticas				
Equipamiento informático (hardware)				
Redes de comunicaciones				
Soportes de información				
Equipamiento auxiliar				
Instalaciones				
Personal				

Fuente. Autores del proyecto

4.3.6 Obtener o renovar el certificado de cultura de seguridad. El procedimiento que indica la metodología para el establecimiento de una cultura de seguridad consiste en la realización de una serie de cuestionarios de seguridad asociados a los reglamentos del SGSI con el objetivo de dar a conocer y mejorar la cultura de seguridad de la Cooperativa, sin incurrir en costes altos de mantenimiento, la idea principal radica en que al momento de aprobar el cuestionario se emite un certificado de cultura de seguridad. Este certificado se debe renovar

periódicamente para garantizar que se mantiene dicho nivel de seguridad, el certificado puede ser retirado si el usuario incurre en una falta y el puntaje de su certificado llega a ser mejor de 50 puntos en una escala de 1 a 100.

4.3.7 Realización del test de cultura de seguridad. **El** objetivo de esta actividad, es la de realizar una evaluación de los conocimientos que un usuario tiene del sistema de seguridad de la Cooperativa, determinando así si está preparado o no para acceder al mismo, esta limitación al acceso es un control adicional que permite mitigar riesgos obligando a los usuarios a incrementar su cultura de seguridad de una manera progresiva y a un costo bajo. Cada vez que se suspenda el examen se debe volver a hacer estudio del sistema como tal hasta aprobarlo y cumplir con los conocimientos adecuados para acceder al sistema, en el marco de trabajo se presenta el siguiente cuestionario como propuesta del mismo para poder realizar este test:

- Indique la vigencia y el periodo de actualización de los certificados de cultura de seguridad en la Cooperativa.
- Liste los activos a los cuales está usted asignado como responsable.
- Liste los tipos de activos disponibles en la Cooperativa
- Nombre los reglamentos que se tienen para proteger los equipos de computación y comunicaciones móviles en la Cooperativa.
- Indique el conjunto de responsabilidades que tiene usted sobre los activos de la Cooperativa.
- Nombre las actividades que tiene usted prohibidas ejecutar sobre la información de la Cooperativa. ¿Conoce usted las reglas que se tienen sobre la divulgación de la información en la Cooperativa?

- Nombre el conjunto de actividades que se tienen prohibidas realizar dentro de la red de la Cooperativa.

4.3.8 Gestionar el cuadro de mandos de seguridad. Esta actividad permite darle seguimiento al cumplimiento del SGSI y tiene efecto de subir o bajar el nivel de seguridad sobre los controles en la Cooperativa. El cuadro de mandos permite que la entidad tenga capacidad de tomar decisiones de seguridad a corto plazo sin depender de la periodicidad de las auditorías las cuales deberían tener un intervalo aproximado de dos años y permitir visualizar qué controles se han degenerado con el tiempo. La existencia de este cuadro de mando de controles permite que en todo momento el responsable de seguridad sepa que controles requieren mayor supervisión y tomen las medidas correctivas necesarias.

4.3.9 Gestionar la periodicidad de los procedimientos. a finalidad de esta actividad es dotar de los procedimientos de control de una periodicidad mínima en el cual deben ser ejecutados para poder tener de forma periódica un control sobre el SGSI, en el marco de trabajo inicialmente se propone un tiempo de un mes para todos los procedimientos pero que puede ser afinado dependiendo del criterio del responsable de seguridad.

4.3.10 Gestionar las violaciones de seguridad. El encargado de seguridad debe realizar la gestión de las violaciones de seguridad lo que se traduce a penalizar los controles asociados que se han violado en caso de que el mismo considere que efectivamente ha existido una violación, esta actividad es la que se activa al momento de la finalización del seguimiento a la activación de un procedimiento de denuncia o general.

4.3.11 Realización de auditorías periódicas. La necesidad de estas auditorías nace del poder realizar una calibración de los controles del SGSI. Como resultado de las auditorías se presentará una lista de cumplimiento de los controles el cual permitirá al encargado de seguridad realizar dicha calibración, el periodo determinado para esta auditoría recomendada por la metodología es de dos años, lo cual permite ahorrar en costos ya que las medidas a cortos plazos se toman mediante el tablero de cumplimiento de controles. En los anexos se incluyen los formatos necesarios para realizar esta auditoría.

Capítulo 5. Conclusiones

A través de un modelado de negocio se logró identificar los procesos críticos misionales de la Cooperativa, permitiendo establecer el alcance del SGSI a implementar en la Cooperativa.

Por medio de la herramienta de Análisis GAP basada en la norma ISO NTC IEC 27001:2013 se obtuvo una radiografía del estado de seguridad de la información en la Cooperativa, identificando falencias que ponen en riesgo la continuidad del negocio.

El presente proyecto permitió analizar mediante los controles y objetivos de control de la norma NTC-ISO-IEC 27001:2013 aplicables para la Cooperativa, cuáles son sus puntos débiles relacionados con la falta de la implementación de un Sistema General de Seguridad en la Información, que podrían convertirse en una fuerte amenaza para el normal cumplimento de sus procesos misionales.

Con base en lo anterior, se pudo generar un marco de trabajo que servirá de guía para la implementación del SGSI en la Cooperativa de forma sostenible y evaluable en el tiempo.

Capítulo 6. Recomendaciones

Priorizar la seguridad de la información en la Cooperativa por parte de la Gerencia, lo que implica inversión, seguimiento, considerándola como el principal activo de la misma.

Concientizar y capacitar desde la Gerencia de la Cooperativa a los empleados en los temas relacionados con la seguridad de la información para ir creando cultura y modos de trabajo eficaces.

Realizar auditorías internas una vez se implemente el SGSI en la Cooperativa con frecuencia mínima anual con el fin de favorecer la mejora continua en los procesos de misión crítica.

Referencias

INTERNATIONAL ORGANIZATION, F. S. (2008). *ISO/IEC 27000.* Recuperado el 9 de mayo de 2016, de www.iso27000.es.

Juárez, F. M. (s.f.). (s.f). *Obtenido de normas ISO/IEC 27001.* Recuperado el 15 de junio de 2016, de http://norma07.blogspot.com.co/2014/09/bienvenidos-todos.html

Norma Técnica Colombiana NTC-ISO/IEC 27001. (2006). *l Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).* Bogotá: NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001.

Prezi.com. (2 de mayo de 2014). *Auditoría de sistemas.* Recuperado el 9 de mayo de 2016, de https://prezi.com/q-i08kniv6rb/auditoria-de-sistemas/

Reynolds, J. (1991 Julio). *P. Holbroo.* RFC 1244: Site Security Handbook.

UFPSO. (2015). *Repositorio Institucional Trabajos de Grado Especialización Auditoria de Sistemas* . Ocaña .

Apéndices

Apéndice A. Entrevista

Objetivo: Evaluar el nivel de seguridad de la información en la Cooperativa de Transportadores Unidos-Cootransunidos Ltda. Sede Ocaña

Nombre: Román Alberto Jácome Pérez **Cargo**: Gerente

1. ¿Cada cuánto se realiza mantenimiento a los recursos informáticos de la Empresa y que evidencia se tiene de los mismos?

2. ¿Cómo cree usted que se encuentra Cootransunidos LTDA con referencia a la seguridad de la información? Por qué?

3. ¿Qué tipo de capacitación brinda a sus empleados, en el tema de seguridad de la información?

4. ¿Teniendo en cuenta la seguridad, que políticas maneja para preservar la seguridad de la información?

5. Además de su personal, ¿quién más tiene acceso a cualquiera de sus Sistemas de Información administrativos?

6. ¿Dónde se almacenan las copias de respaldo o backups de la información que se generan en los sistemas de información, cada cuanto se realizan y con qué frecuencia se prueban para ver si funcionan?

7. ¿Cómo se encuentra la empresa económicamente para asumir los retos que demanda la seguridad de la información?

8. ¿Cuáles son las políticas y procedimientos para la selección del personal que ingresará a laborar en la Cooperativa?

9. Cuando se termina la vinculación laboral de un empleado, ¿Cómo se realiza la desvinculación del mismo en lo relacionado con el acceso a los sistemas de la Empresa?

10. ¿Cómo garantiza la continuidad del negocio ante un eventual siniestro?

Apéndice B. Encuesta

Objetivo: Evaluar el nivel de seguridad de la información en la Cooperativa de Transportadores Unidos-Cootransunidos Ltda. Sede Ocaña

Nombre: **Cargo**:

1. Las copias de respaldo de la información es almacenada en:

☐ Caja Fuerte o Bóveda
☐ Estantes o Gavetas
☐ Muebles con cerradura o Archivador
☐ Fuera de la Organización (para prevenir pérdida de datos en el caso de incidencias)
Otras _____

2. La Empresa cuenta con:

Vigilancia	Sí __ No__
Infraestructura sólida y segura	Sí __ No__
Ruta de Evacuación	Sí __ No__
Cámaras de Vigilancia	Sí __ No__
Alarmas	Sí __ No__
Extintores	Sí __ No__
Ruta de Evacuación	Sí __ No__
Instalaciones eléctricas ideales	Sí __ No__

3. El equipo de cómputo a su disposición, cuenta con:
Contraseña, para permitir el acceso de usuarios a los sistemas Sí __ No__ Algunos__
Antivirus, actualizado
Sí __ No__ Algunos__
Software, con licencia
Sí __ No__ Algunos__
Restricción de accesos a páginas web (redes sociales, etc)
Sí __ No__ Algunos__
Acceso restringido a las aplicaciones, luego de varios intentos
Sí __ No__ Algunos__
Requerimientos necesarios para la realización optima de sus labores

Sí __ No__ Algunos__

4. ¿Con qué frecuencia el equipo de cómputo a su disposición recibe mantenimiento preventivo?

- ☐ Mensualmente
- ☐ Trimestralmente
- ☐ Semestralmente
- ☐ Anualmente
- ☐ Cuando lo requiere
- ☐ Nunca

5. ¿En qué medio respalda la información elaborada desde su puesto de trabajo?

- ☐ CD
- ☐ DVD
- ☐ Memorias USB
- ☐ Impresiones
- ☐ Disco Duro
- ☐ Ninguno

Otras _____

Apéndice C. Lista de chequeo

LISTA DE CHEQUEO COOTRANSUNIDOS LTDA			
DESCRIPCION DEL CONCEPTO	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
POSEE UNA INFRAESTRUCTURA FÍSICA ADECUADA PARA EL DESEMPEÑO LABORAL			
CUENTA CON EQUIPOS DE CÓMPUTO APTOS PARA EL DESARROLLO DE LAS ACTIVIDADES			
EL SISTEMA DE RED SE ENCUENTRA ESTRUCTURADO DE MANERA ACORDE			
SE REALIZA MANTENIMIENTO PREVENTIVO AL SISTEMA DE RED DE DATOS Y ELÉCTRICA			
LA EMPRESA TIENE SERVIDORES DE RESPALDO PARA EL ALMACENAMIENTO DE INFORMACIÓN			
LOS EQUIPOS CUENTAN CON PROGRAMAS ANTIVIRUS ACTUALIZADOS			
LAS CONEXIONES DE PROTOCOLO DE INTERNET (IP) ESTÁN PROTEGIDAS POR UN FIREWALL			
EL ACCESO A LOS EQUIPOS DE CÓMPUTO SE REALIZA POR USUARIO Y CONTRASEÑA			
SE EXIGEN NIVELES DE SEGURIDAD PARA LA CREACIÓN DE CONTRASEÑAS			
LA EMPRESA TIENE DENTRO DE SU ESTRUCTURA UN PLAN DE CONTINGENCIA			
CUENTA CON ELEMENTOS DE CONTROL DE EMERGENCIAS POR INCENDIO			
CUENTA CON UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DOCUMENTADA Y PUBLICADA			
LOS EQUIPOS DE CÓMPUTO ESTÁN DEBIDAMENTE DISTRIBUIDOS DE ACUERDO A LA FUNCIONALIDAD DE EMPRESA			
EXISTE INVENTARIO ACTUALIZADO DE TODO EL HARDWARE Y SOFTWARE DONDE SE PROCESA INFORMACIÓN			
EL SOFTWARE DE LOS EQUIPOS DE CÓMPUTO SE ACTUALIZAN PERIODICAMENTE			
SE REALIZA CON FRECUENCIA COPIAS DE SEGURIDAD A LA INFORMACIÓN DE LOS EQUIPOS DE CÓMPUTO			
LA EMPRESA CUENTA CON UN SISTEMA ELÉCTRICO ALTERNO			
SE REALIZA MANTENIMIENTO PREVENTIVO A LOS EQUIPOS DE CÓMPUTO			
LA EMPRESA CUENTA CON UN CONDUCTO REGULAR			

PARA EL MANEJO DE LA INFORMACION CONFIDENCIAL			
SE DESHABILITAN LOS USUARIOS DE SISTEMA DE LOS EMPLEADOS QUE TERMINAN RELACIÓN LABORAL CON LA EMPRESA			
LA EMPRESA CUENTA CON CÁMARAS DE SEGURIDAD			
CUENTA CON UNA PLATAFORMA VIRTUAL QUE CONECTE LA OFICINA PRINCIPAL CON LAS AGENCIAS			
CUENTA LA EMPRESA CON UNA BASE DE DATOS DE CLIENTES			

Apéndice D. Formatos

FORMATO PARA DESCRIPCIÓN DE ROLES Y FUNCIONES	CÓDIGO	
	VERSIÓN	
	FECHA	
	PÁGINA	1 DE 2
ELABORO:	CARGO:	

DESCRIPCIÓN DEL CARGO

Cargo		
Gerencia a la que pertenece		
Rol en el SGSI		
Área		
Nivel de Responsabilidad	Cargo del jefe directo	
	Cargos que dependen	
	Equipos, bienes o dinero bajo su responsabilidad:	

PRINCIPALES RESPONSABILIDADES Y FUNCIONES

Funciones Principales

FORMATO PARA ACTIVACION DE PROCEDIMIENTO GENERAL	CÓDIGO	
	VERSIÓN	
	FECHA	
	PÁGINA	
ELABORO:		
NOMBRE DEL USUARIO:	CARGO:	
DESCRIPCIÓN DEL PROCEDIMIENTO		
Nombre del procedimiento		
Activo implicado		
Descripcion del procedimiento		

Notas:

Se realiza reporte.

PLAN DE AUDITORÍA	CÓDIGO	
	VERSIÓN	
	PÁGINA	1 DE 5
	CLASIFICACIÓN	

INFORMACIÓN GENERAL

FECHAS DE AUDITORIA			
NOMBRE DEL PROCESO AUDITADO		NOMBRE DEL RESPONSABLE DEL PROCESO	
CARGO DEL RESPONSABLE DEL PROCESO		ÁREAS A AUDITAR	

INFORMACIÓN DE LA AUDITORÍA

AUDITOR LÍDER			
GRUPO AUDITOR		CRITERIOS DE AUDITORIA [1]	
OBJETIVOS DE LA AUDITORÍA		ALCANCE DE LA AUDITORÍA	

FECHA	HORA	ACTIVIDAD / PROCESO	RESPONSABLE

ACTA DE REUNIÓN DE APERTURA – AUDITORÍA	CÓDIGO	
	VERSIÓN	
	PÁGINA	4 DE 5
	CLASIFICACIÓN	

NOMBRE DEL PROCESO/ELEMENTO AUDITADO								
FECHA				HORA INICIO		HORA FIN		
PARTICIPANTES								
NOMBRE				CARGO/ROL				

DESARROLLO DE LA REUNIÓN		
OBJETIVO		
1. Comunicar que se está realizando la auditoría al procedimiento de revisión por la dirección		
2. Explicar la naturaleza de la auditoria		
TEMAS A DESARROLLAR		
	SI	NO
1. Presentación del equipo auditor		
2. Confirmación de los objetivos, alcance y criterios de la auditoría		
3. Confirmación del plan de auditoría		
4. Presentación de los métodos de auditoría		
5. Confirmación de los canales de comunicación formal entre el equipo auditor y el auditado		
6. Confirmación de que, durante la auditoría, el auditado será informado del progreso de la misma		

ACTA DE REUNIÓN DE CIERRE – AUDITORÍA	CÓDIGO	
	VERSIÓN	
	PÁGINA	5 DE 5
	CLASIFICACIÓN	

NOMBRE DEL PROCESO/ELEMENTO AUDITADO							
FECHA				HORA INICIO		HORA FIN	

PARTICIPANTES	
NOMBRE	CARGO/ROL

DESARROLLO DE LA REUNIÓN		
OBJETIVO		
1. Presentar los hallazgos y las conclusiones de la auditoría		
TEMAS A DESARROLLAR		
	SI	NO
1. Aclarar que la evidencia de la auditoría recopilada se basó en una muestra de la información disponible		
2. Presentación de los hallazgos y conclusiones de la auditoria de tal manera que se comprendan y se reconozcan por el auditado		
3. Cualquier otra opinión relativa a los hallazgos		