RESUMEN – TRABAJO DE GRADO

AUTORES	**YESID FERNANDO QUINTANA** **WILSON SNEIDER TORRADO GONZÁLEZ**
FACULTAD	**Ingenierías**
PLAN DE ESTUDIOS	**Especialización en Auditoria de Sistemas.**
DIRECTOR	**Andrés Mauricio Puentes Velásquez**
TÍTULO DE LA TESIS	**PLANEACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA "KATALINDA SHOES"**

RESUMEN

ESTE ESTUDIO DOCUMENTA LA PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICABLE A LA EMPRESA KATALINDA SHOES, SEGÚN LA NORMA ISO/IEC 27001, RESALTANDO AQUELLOS ASPECTOS EN LOS CUALES SON PRINCIPALMENTE NECESARIOS ROBUSTECER LOS CONTROLES DE SEGURIDAD EN FUNCIÓN DE LOS RIESGOS EXISTENTES Y EL NIVEL DE CRITICIDAD DE LOS ACTIVOS DE INFORMACIÓN. SE RECOMIENDA LA MANERA MÁS EFICIENTE DE SALVAGUARDAR LOS RECURSOS INFORMÁTICOS DE CATÁSTROFES NATURALES, ROBOS, PÉRDIDAS, Y DAÑOS INTENCIONALES O NO INTENCIONALES QUE PUEDAN AFECTAR LA DISPONIBILIDAD DEL RECURSO, ASÍ COMO ESTABLECER CONTROLES QUE PERMITAN EVITAR EL ACCESO NO AUTORIZADO A LA INFORMACIÓN DE LOS SISTEMAS Y SERVICIOS UTILIZADOS POR LA EMPRESA.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:
95	0	0	1

PLANEACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA “KATALINDA SHOES”

YESID FERNANDO QUINTANA
WILSON SNEIDER TORRADO GONZÁLEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2015

PLANEACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA "KATALINDA SHOES"

YESID FERNANDO QUINTANA
WILSON SNEIDER TORRADO GONZÁLEZ

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

IS. Esp. MSc(c) Andrés Mauricio Puentes Velásquez
Director

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2015

ADVERTENCIA

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ACEPTACIÓN DEL RIESGO: decisión de asumir un riesgo.

ACTIVO: es cualquier cosa que representa o que tiene un valor para la organización.

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

ANÁLISIS DE RIESGO: uso sistemático de la información para identificar las fuentes y estimar el riesgo, con el fin de prever o corregir las vulnerabilidades que se presentan.

ARQUITECTURA DE TI: Marco integrado para evolucionar o dar mantenimiento a TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

DIRECTRIZ: descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del mismo.

GESTIÓN DEL RIESGO: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado complete de los activos.
MODELO: representación de un objeto, sistema o idea, de forma diferente al de la entidad misma.

MODELO DE GESTIÓN: esquema o marco de referencia para la administración de una entidad.

POLÍTICA: es toda intención y directriz expresada formalmente por la Dirección.

PROCEDIMIENTO: método o sistema estructurado para ejecutar algunas cosas.

REGISTRO: asiento o anotación que queda de lo que se registra.

RIESGO: probabilidad de que una amenaza cause un impacto.

RIESGO RESIDUAL: nivel restante de riesgo después del tratamiento del riesgo.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información.

TI: tecnologías de la Información.

TRATAMIENTO DEL RIESGO: proceso de selección e implementación de medidas para modificar el riesgo.

VALORACIÓN DEL RIESGO: proceso global de análisis y evaluación del riesgo.

VULNERABILIDAD: debilidad de un activo o grupo de activos que pueden ser aprovechadas por una o varias amenazas.

INTRODUCCIÓN

La auditoría de sistemas nos permite hoy en día contar con mecanismos que nos ayudan a perfeccionar el funcionamiento de los procesos y de la tecnología de una organización con miras a proyectarse como empresas líderes a futuro. Por tal motivo, la organización requiere tener el control de todos sus recursos, mantenerlos protegidos y en las mejores condiciones para poder ofrecer un servicio que llene las expectativas de sus consumidores. Esta permite valorar el estado de madurez de la empresa y determinar si hay falencias o no en el funcionamiento de la misma.

Las empresas cada día deben enfrentar nuevos retos, cambios y procesos a los cuales deben adaptarse para poder permanecer en el entorno donde desarrollan sus actividades; por este motivo es indispensable contar con herramientas tecnológicas seguras que permitan alcanzar el logro de los objetivos y metas propuestas. La gestión de la información en una empresa debe estar sometida a una constante Inspección y revisión, con el fin de verificar la preservación de las características básicas de la misma: confidencialidad, disponibilidad e integridad; todo esto, siguiendo normas y estándares definidos a nivel internacional, las auditorías son un mecanismo que provee los instrumentos para verificar dicho cumplimiento.

El presente trabajo se desarrolló con la finalidad de planear los procesos y tareas que se establecerán en el sistema de gestión de la seguridad de la información en la empresa “katalinda shoes” en la ciudad de Ocaña, teniendo en cuenta los lineamientos de la Norma NTC ISO 27001:2013. Esta propuesta reúne un compendio de controles requeridos a partir de los hallazgos encontrados en las auditorías realizadas con anterioridad.

.

1. TITULO

Planeación Del Sistema De Gestión De Seguridad De La Información Para La Empresa "Katalinda Shoes"

1.1 PLANTEAMIENTO DEL PROBLEMA

La empresa "Katalinda shoes" dedicada a comercializar calzado en Ocaña y distribuir sus productos a nivel nacional, cuenta con una serie de elementos de infraestructura tecnológica que dan soporte al procesamiento de información; estos elementos han cambiado de manera progresiva para mejorar tecnológicamente, sin tener en cuenta la necesidad de una gestión segura y eficiente de la información organizacional.

La tecnología que se ha adoptado ha permitido expandir las fronteras comerciales de la empresa, innovando en el uso y aprovechamiento del *e-commerce*, y *social media* como estrategias de comercialización y mercadeo de manera ágil y cercana a los clientes; sin embargo, esta estrategia de mercadeo con fuerte presencia en redes sociales debe acompañarse de medidas que busquen preservar la integridad, confidencialidad y disponibilidad de la información de la empresa. La empresa cuenta con sistemas de información para gestionar la información contable y financiera, como componente fundamental para la operación del negocio. A pesar de contar con esto, se han percibido falencias relacionadas con adquisición de tecnología, inexistencia de un departamento de sistemas, capacitación inadecuada del personal, problemas en la gestión de inventarios y contabilidad, información de clientes y proveedores, además de las múltiples carencias en materia de infraestructura de cómputo, redes de datos y sistemas de vigilancia.

1.2 FORMULACION DEL PROBLEMA

¿Cómo generar a través de un Sistema de Gestión de Seguridad de la Información para la empresa "Katalinda Shoes", un instrumento que permita efectivamente gestionar y mitigar al máximo los riesgos asociados al procesamiento y almacenamiento de la información?

1.3 OBJETIVOS

1.3.1 General.

Planear un sistema de gestión de seguridad de la información para la EMPRESA KATALINDA SHOES en Ocaña.

1.3.2 Objetivos específicos

- Diagnosticar los elementos organizacionales en la empresa KATALINDA SHOES a través de una auditoría pasiva con base en los controles de la norma ISO 27001

- Identificar los elementos que conforman el SGSI – Sistema de Gestión de Seguridad de la Información para la empresa KATALINDA SHOES a partir de un análisis de los controles más adecuados a las necesidades de la empresa.

- Documentar formalmente las actividades y políticas requeridas para gestionar adecuadamente la seguridad de la información en la empresa KATALINDA SHOES.

1.4 JUSTIFICACIÓN

En el presente documento se desarrolló la planeación de un Sistema de Gestión de Seguridad de la Información para la empresa "KATALINDA SHOES"; esta propuesta tiene como aporte principal los instrumentos para aumentar la cantidad y calidad de los controles informáticos, teniendo en cuenta un proceso para 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.

Teniendo presente los avances tecnológicos utilizados para las ventas en línea y el comercio electrónico, además de permitir la correcta operación de los sistemas de información con los que se cuentan hoy en día, es importante que la empresa "Katalinda shoes" cuente con métodos a la vanguardia en materia de la seguridad de la información para aportarle al negocio y permitirle enfrentarse a los mercados competitivos que existen. El contar con un grupo de Políticas aprobadas por la Gerencia se reconocería como fundamental para brindar dirección y alineamiento de la tecnología con los objetivos del negocio.

Aunque la planeación y posterior operación de un SGSI no es obligatoria para la empresa, la dirección ve la necesidad de poner en marcha este sistema, con el ánimo de dar soporte a sus procesos misionales, por esto es necesario contar con un soporte efectivo para administrar la seguridad de la información que además de brindar facilidad y agilidad en estos procesos, logre posicionarla como una organización que acata la normatividad nacional e internacional en cuanto a Seguridad de la Información.

1.5 HIPÓTESIS

El proceso de planear y documentar un Sistema de Gestión de Seguridad de la Información ajustado a las necesidades específicas de la empresa "Katalinda shoes", proveerá un instrumento que permita efectivamente gestionar y mitigar al máximo los riesgos asociados al procesamiento y almacenamiento de la información; contribuyendo al soporte informático adecuado para el cumplimiento de los objetivos misionales.

1.6 DELIMITACIONES

1.6.1 Geográficas.

Oficinas de la empresa Katalinda shoes. Ocaña, Norte de Santander.

1.6.2 Temporales

El proyecto de investigación se llevara a cabo en un lapso de 2 meses desarrollando cada objetivo propuesto, a partir de la aprobación del Anteproyecto.

1.6.3 Conceptuales.

Los conceptos se relacionan con la Seguridad Informática, Sistema de Gestión de Seguridad de la Información (SGSI), Políticas de Seguridad de la Información, Gestión de Riesgos.

NTC ISO/IEC 27001 Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). 2005.

NTC ISO/IEC 27002 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. 2005.

NTC 5254. Gestión del Riesgo. 2004.

NTC ISO/IEC 27005. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. 27005.

NTC ISO 31000. Gestión del Riesgo. Principios y Directrices. 2011

1.6.4 Operativa.

El desarrollo del proyecto desde el punto de vista operativo se soporta en los procesos principales del almacén KATALINDA SHOES.

2 MARCO REFERENCIAL

2.1 MARCO HISTORICO

La información es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros. Para este proyecto se consideran activos de información los mencionados anteriormente. Dichos activos están sujetos a ser atacados por amenazas que de no controlarse pueden causar impactos en la información y en efecto a la organización reflejándose en pérdidas económicas y de imagen. Así de esta manera, la alta dirección de cualquier organización debe ser consciente de que su información siempre se encontrará en riesgo y que debe tomar las medidas necesarias para enfrentarse a este tipo de adversidades.

2.1.1 Antecedentes

En el año 2004 se publicó la UNE 71502 titulada Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) y que fue elaborada por el comité técnico AEN/CTN 71. Es una adaptación nacional de la norma británica British Standard BS 7799-2:2002.

Con la publicación de UNE-ISO/IEC 27001 (traducción al español del original inglés) dejó de estar vigente la UNE 71502 y las empresas nacionales certificadas en esta última están pasando progresivamente sus certificaciones a UNE-ISO/IEC 27001.

La seguridad de la información toma especial relevancia en el año 1980 en donde se fundamentan las bases de la seguridad de la información, en este año, James P. Anderson escribe un documento titulado 'Computer Security Threat Monitoring and Surveillance'. Lo más interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas.

2.2 MARCO CONCEPTUAL

2.2.1 Amenaza

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

2.2.2 Apropiación

Las apropiaciones son autorizaciones máximas de gasto que el Congreso de la República aprueba para ser comprometidas durante la vigencia fiscal respectiva. Después del 31 de Diciembre de cada año estas autorizaciones expiran y en consecuencia no podrán comprometerse, adicionarse, transferirse.

2.2.3 Auditoría

Puede definirse como el proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso.

Otro concepto de auditoría definido por Echenique es, "un examen crítico que se realiza con el objeto de evaluar la eficiencia y eficacia de una sección o un organismo y determinar cursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos. El encargado de realizar las auditorias es el auditor, un auditor es la persona que evalúa la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación".

2.2.4 Auditoría Informática

Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientes los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicional de la auditoría.

2.2.5 Control

Cualquier medido que tome la dirección, el Consejo y otros, para mejorar la gestión de riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas.

2.4.6 Control interno

Todas las medidas utilizadas por una empresa para protegerse contra errores, desperdicios o fraudes y para asegurar la confiabilidad de los datos. Está diseñado para ayudar a la operación eficiente de una empresa y para asegurar el cumplimiento de las políticas de la empresa.

2.4.7 Control Interno Informático

Sistemas Integral al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

2.4.8 Disponibilidad

Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

2.4.9 Evaluación del riesgo

Proceso global de estimar la magnitud de los riesgos y decidir si un riesgo es o no tolerable.

2.4.10. Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

2.4.11. Identificación del peligro

Proceso que permite reconocer que un peligro existe y que a la vez permite definir sus características.

2.4.12. Identificación del riesgo

Proceso para determinar lo que puede suceder, por qué y cómo.

2.4.13. ISO (Organización Internacional de Normalización)

Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

2.4.14. 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.

2.4.15. Tratamiento del riesgo

Selección e implementación de las opciones apropiadas para ocuparse del riesgo.

2.4.16. Valoración del riesgo

Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

2.4.17. Vulnerabilidad

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

2.3 MARCO CONTEXTUAL

Línea de Investigación: Gobernabilidad de TI. La línea de investigación es la enmarcada en Gobernabilidad de TI, la cual tiene establecido un macro proyecto titulado: "Establecimiento de un marco conceptual de gobernabilidad de TI para las empresas colombianas", el cual se está trabajando para el contexto de Norte de Santander, en su parte inicial la Provincia de Ocaña, por sectores de empresas. Se requiere de la concepción y creación del mencionado marco conceptual, y de la realización de un proceso minucioso de validación del marco propuesto. Para la aplicación del marco conceptual se utiliza una metodología de investigación evaluativa, donde los instrumentos representan un insumo muy importante. Se definen una serie de etapas en el proceso investigativo como son: la recolección de información, diagnóstico, desarrollo de un plan de mejora y la socialización de resultados.

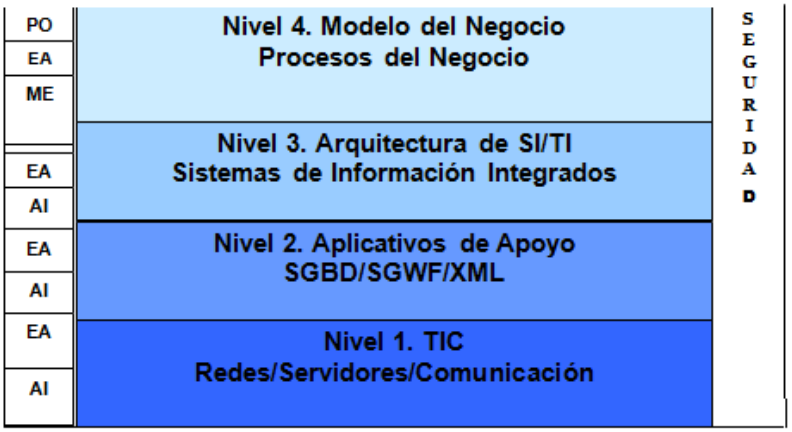
Durante muchos años la gobernabilidad ha sido vista como el futuro de las tecnologías de la información y la comunicación, a pesar del manejo de diferentes criterios de calidad en gobernabilidad de TI. El proceso de gobernabilidad de una empresa[1]se refiere al conjunto de responsabilidades y prácticas ejecutadas por el comité directivo de la misma, con el objetivo de proveer dirección estratégica a la compañía, asegurando que los objetivos definidos sean alcanzados, verificando que los riesgos sean administrados apropiadamente y que los

[1]COBIT, GovernanceInstitute Modelo ExecutiveSummary. [Versión electrónica] Extraído el 20 de Diciembre, 2008, desde http://www.isaca.org/cobit.html, 2003.

recursos utilizados sean utilizados responsablemente. La gobernabilidad de TI es parte integral de la gobernabilidad de la empresa, y comprende el liderazgo, las estructuras organizacionales y los procesos que aseguran que la organización de TI sostenga y extienda las estrategias y objetivos de la organización, siendo responsabilidad del comité directivo de la empresa y del comité ejecutivo de TI.

Inspirados en diversos elementos como: el modelo inter-empresa de Santana[2], los conceptos de madurez y los objetivos de control de COBIT[3], se diseñó un marco conceptual de Gobernabilidad de TI[4], donde se identifican los principales componentes de la organización y las maneras en que estos componentes trabajan juntos con el fin de alcanzar los objetivos del negocio. Los componentes o niveles, comprenden procesos de modelado de negocios, arquitectura de SI/TI, Aplicativos de apoyo, y Tecnologías de Información y Comunicación (Ver Figura 1).

Figura 1: Marco conceptual de Gobernabilidad de TI:



Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

[2]M. **SANTANA**. *Developing an inter-enterprise alignment maturity model: research challenges and solutions*.Technical Report TR-CTIT-07-29, Centre for Telematics and Information Technology, University of Twente, Enschede.Extraído.

[3]**COBIT 4.0**, *Governance IT*. Extraído el 3 de Enero, 2009 del sitio Web del Institute, Borrad briefingon TI governance: http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/ContentManagement/ContentDisplay.cfm, 2006.

[4]T, **VELASQUEZ**, Establecimiento De Criterios De Gobernabilidad De TI En Las Empresas Colombianas. Universidad de los Andes. Mérida. Venezuela. 2010.

Nivel 4: Modelado del negocio. Involucra la descripción de la estructura organizacional, procesos de negocios, sistemas de planeación y control, mecanismos de gobierno y administración, políticas y procedimientos de la empresa. Cada uno de estos componentes interactúa y contribuye a alcanzar las metas y objetivos del negocio y provee la base para identificar los requerimientos de los Sistemas de Información (SI) que soportan las actividades del negocio.

Nivel 3: La arquitectura de los sistemas de información. Esta arquitectura provee un modelo para el desarrollo e implementación de aplicaciones individuales, mapas de negocios y requerimientos funcionales de las aplicaciones, y muestra la interrelación entre aplicaciones. Las Aplicaciones Emergentes de Arquitectura están normalmente "orientadas al servicio". Los servicios pueden ser vistos como bloques de construcción que pueden ser ensamblados y re-ensamblados para lograr los cambios en los requerimientos del negocio, en una aproximación que maximice el re-uso y ayude a mantener la flexibilidad en las políticas de servicio para adaptarse a los cambios.

Nivel 2: Aplicativos de apoyo. Son todas las aplicaciones de apoyo a la arquitectura de aplicación como los sistemas de gestión de bases de datos (que ayudan a los procesos básicos de mantenimiento de la base de datos), la administración de los recursos de datos (esto muestra como los recursos de información están siendo administrados y compartidos en beneficio de la empresa). La Arquitectura de Información/Datos incluirá consideraciones de tecnología de almacenaje y administración del conocimiento que faciliten la explotación de la información corporativa, esto incrementará la cobertura y el contenido de la administración de datos y facilitará el acceso a la información por múltiples canales y otras herramientas como XML y SGWF. Incluye los siguientes procesos dentro de los objetivos de control.

Nivel 1: Tecnología de información y comunicación (TIC). Describe la estructura, funcionalidad y la distribución del hardware, software y los componentes de comunicación que mantienen y soportan la Arquitectura de SI/TI, conjuntamente con los estándares técnicos aplicados a ellos. Estos componentes comprenden toda la "infraestructura de TIC" de la organización. El desarrollo, documentación y mantenimiento de la arquitectura de SI del negocio, debe formar parte del proceso de pensamiento estratégico que se debe desarrollar en la organización. Incluye los siguientes procesos dentro de los objetivos de control.

Se toman de referencia los objetivos del modelo de COBIT para definir las variables del modelo propuesto para las empresas colombianas como son:

- Planificación y Organización PO
- Adquisición e Instrumentos AI

- Entrega y Apoyo DS
- Monitoreo y Evaluación ME

En cada nivel se identifican las variables encontradas de acuerdo a los controles presentes en cada objetivo (Ver Tabla 1).

Tabla 1: Objetivos de Control presentados en cada Nivel

	TIC	Aplicativos de apoyo	Arquitectura de SI/TI	Modelo de Negocio
Planificación y Organización			**X**	**X**
Adquisición e Instrumentos	**X**	**X**	**X**	
Entrega y Apoyo	**X**	**X**	**X**	**X**
Monitoreo y Evaluación			**X**	**X**

Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

Evaluación del Nivel de Madurez. En[5]se muestra un modelo de madurez basado en valores para la alineación de TI en el negocio llamado el VITALMM, el cual cubre todos los sistemas de información que en la organización se empleen, en colaboraciones de inter-empresa, así como la infraestructura tecnológica y las facilidades de soporte necesarios para ellos, identificando valores para la alineación de TI en el negocio se toma como referencia la clasificación de 0 – Inexistente, 1 – Inicial, 2 – Repetible, 3 – Definido, 4 – Manejado y 5- Optimizado.

Se elabora una guía para la aplicación del modelo conceptual en la que se define: El reconocimiento del marco conceptual de gobernabilidad de TI, reconocimiento de la

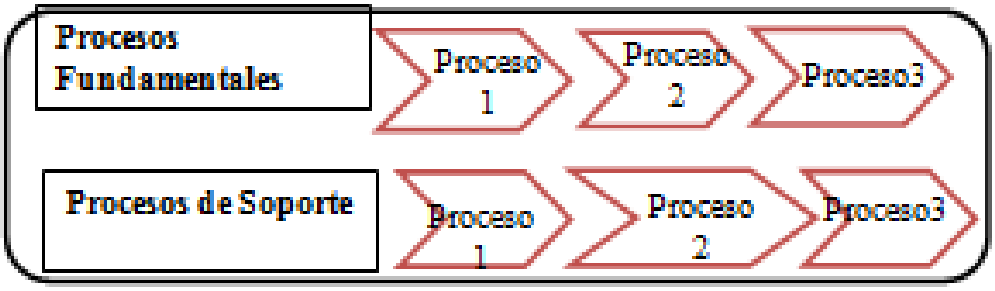
[5]M. **SANTANA**. *Developing an inter-enterprise alignment maturity model: research challenges and solutions*.Technical Report TR-CTIT-07-29, Centre for Telematics and Information Technology, University of Twente, Enschede.Extraído el 7 de mayo de 2007 desde http://eprints.eemcs.utwente.nl/9780/01/Research_challenges_(REPORT).pdf

empresa, diseño y aplicación de los instrumentos de medición, análisis de la información recogida con la elaboración del diagnóstico situacional, realizar o seleccionar los formatos requeridos dentro de la empresa, creando el marco de referencia y la Implementación de los lineamientos definidos.

Reconocimiento del marco conceptual de gobernabilidad de TI. En este punto se toma la información suministrada anteriormente.

Reconocimiento de la dependencia tecnológica. Incluye una breve historia o reconocimiento de la dependencia desarrolladora del proyecto informático, los Objetivos general y específicos, la Misión y visión de la empresa. Se determina el Diagrama de proceso: procesos fundamentales y procesos de soporte (Ver Figura 2), la Estructura orgánica de la dependencia tecnológica y la Identificación de los perfiles del personal a cargo de los procesos de la TIC como son: Director ejecutivo (CEO), Director financiero (CFO), Ejecutivos del negocio, Director de información (CIO), Propietario del proceso de negocio, jefe de operaciones, Arquitecto en jefe, Jefe de desarrollo, Jefe de administración de TI, La oficina o función de administración de proyectos (PMO) y el cumplimiento, auditoría, riesgo y seguridad.

Figura 2: Diagrama de Procesos



Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

Diseño y aplicación de los instrumentos de medición. Se necesita medir los tipos de escenarios, las variables determinadas para ser evaluadas que permitan medir el nivel de madurez en sus procesos se establecen de acuerdo al cargo desempeñado dentro de la dependencia, a través de preguntas correspondientes con su función, la existencia de un plan estratégico, la misión, visión y objetivos del proyecto, los recursos, la forma de seguimiento a los procesos, herramientas de medición, gestión y planificación.

Se revisa el nivel de madurez teniendo en cuenta las definiciones establecidas (Ver Tabla 2).

Tabla 2: Valores del Modelo de madurez

0	**No existe:** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1	**Inicial:** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2	**Repetible pero intuitiva:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3	**Proceso definido:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4	**Administrado y medible:** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5	**Optimizado:** Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Fuente. COBIT 4.0

Análisis de la información recogida con la elaboración del diagnóstico situacional. Se analiza la información de los instrumentos aplicados como entrevista y la validación de los mismos con la observación o validación respectiva, construyendo la tabla respectiva por cada nivel del modelo y los objetivos de control incluidos tomando como valor válido el observado.

A continuación se representa en una tabla el impacto de los objetivos de control de COBIT 4.1 sobre los criterios y recursos de TI.

La nomenclatura utilizada en los criterios de información para esta tabla es la siguiente: (P), cuando el objetivo de control tiene un impacto directo al requerimiento, (S), cuando el

objetivo de control tiene un impacto indirecto es decir no completo sobre el requerimiento, y finalmente ( ) vacío, cuando el objetivo de control no ejerce ningún impacto sobre el requerimiento, en cambio cuando se encuentra con (X) significa que los objetivos de control tienen impacto en los recursos, y cuando se encuentra en blanco ( ), es que los objetivos de control no tienen ningún impacto con los recursos.

Tabla 3: Objetivos de Control de COBIT

Objetivos de Control de COBIT	**Criterios de Información de COBIT**							**Recursos de TI de COBIT**			
	Efectividad	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Personas**	**Información**	**Aplicación**	**Infraestructura**
Planear y Organizar											
PO1 Definir un plan estratégico de TI	**P**	**S**						**X**	**X**	**X**	**X**
PO2 Definir la arquitectura de la información	**S**	**P**	**S**	**P**					**X**	**X**	
PO3 Definir la dirección tecnológica	**P**	**P**								**X**	**X**
PO4 Definir los procesos, organización y relaciones de TI	**P**	**P**						**X**			
PO5 Administrar la inversión en TI	**P**	**P**					**S**	**X**		**X**	**X**
PO6 Comunicar las metas y la dirección de la gerencia	**P**					**S**		**X**	**X**		
PO7 Administrar los recursos humanos de TI	**P**	**P**						**X**			
PO8 Administrar la calidad	**P**	**P**		**S**			**S**	**X**	**X**	**X**	**X**
PO9 Evaluar y administrar los riegos de TI	**S**	**S**	**P**	**P**	**P**	**S**	**S**	**X**	**X**	**X**	**X**
PO10 Administrar los proyectos	**P**	**P**						**X**		**X**	**X**
Adquirir e Implementar											
AI1 Identificar las soluciones automatizadas	**P**	**S**								**X**	**X**
AI2 Adquirir y mantener software aplicativo	**P**	**P**		**S**			**S**			**X**	

AI3 Adquirir y mantener la infraestructura tecnológica	**S**	**P**		**S**	**S**						**X**
AI4 Facilitar la operación y el uso	**P**	**P**		**S**	**S**	**S**	**S**	**X**		**X**	**X**
AI5 Procurar recursos de TI	**S**	**P**				**S**		**X**	**X**	**X**	**X**
AI6 Administrar los cambios	**P**	**P**		**P**	**P**		**S**	**X**	**X**	**X**	**X**
AI7 Instalar y acreditar soluciones y cambios	**P**	**S**		**S**	**S**			**X**	**X**	**X**	**X**
Entregar y Dar Soporte											
DS1 Definir y administrar los niveles de servicio	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
DS2 Administrar los servicios de terceros	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
DS3 Administrar el desempeño y capacidad	**P**	**P**			**S**					**X**	**X**
DS4 Asegurar el servicio continuo	**P**	**S**			**P**			**X**	**X**	**X**	**X**
DS5 Garantizar la seguridad de los sistemas			**P**	**P**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
DS6 Identificar y asignar costos		**P**					**P**	**X**	**X**	**X**	**X**
DS7 Educar y entrenar a los usuarios	**P**	**S**						**X**			
DS8 Administrar la mesa de servicio y los incidentes	**P**	**P**						**X**		**X**	
DS9 Administrar la configuración	**P**	**S**			**S**		**S**		**X**	**X**	**X**
DS10 Administrar los problemas	**P**	**P**			**S**			**X**	**X**	**X**	**X**
DS11 Administrar los datos				**P**			**P**		**X**		
DS12 Administrar el ambiente físico				**P**	**P**						**X**
DS13 Administrar las operaciones	**P**	**P**		**S**	**S**			**X**	**X**	**X**	**X**
Monitorear y Evaluar											
ME1 Monitorear y evaluar el desempeño de TI	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
ME2 Monitorear y evaluar el control interno	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
ME3 Garantizar el cumplimiento regulatorio						**P**	**S**	**X**	**X**	**X**	**X**
ME4 Proporcionar gobierno de TI	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**

Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

2.4 MARCO TEORICO

2.4.1 ISO/IEC 27001:2005

Publicada el 15 de Octubre de 2005, es la norma principal de la familia de la ISO27000[6], y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI.

2.4.2 ISO/IEC 27001:2013

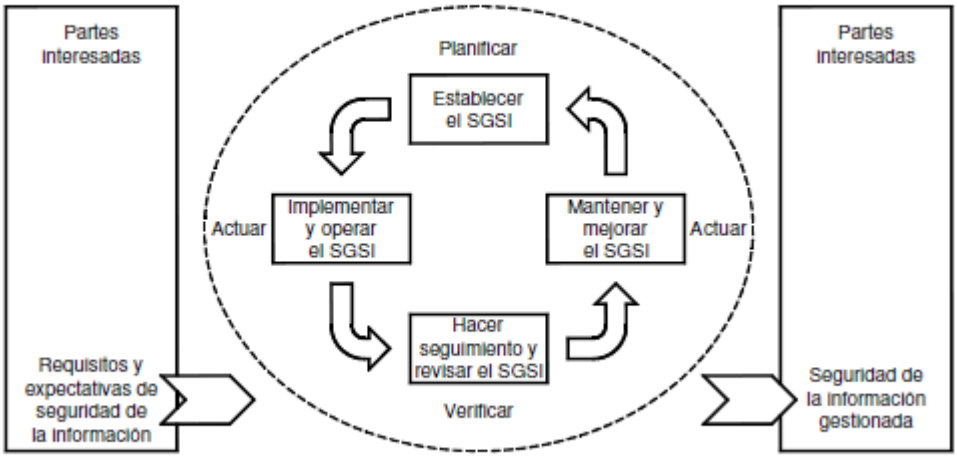
Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas. Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. La Figura 1 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas. La Figura 1. [7]

[6] INTERNATIONAL ORGANIZATION FOR STANDARIZATION ISO/IEC 27000. www.iso27000.es. 2008

[7] Norma técnica Colombiana NTC-ISO/IEC 27001

Figura 3.Modelo PVHA aplicado a los procesos SGSI



Fuente: norma técnica colombiana NTC- ISO/IEC 27001

2.4.3 ISO/IEC 27002:2005

Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, mencionados en el anexo A de la ISO 27001, 39 objetivos de control y 133 controles.
Los dominios a tratar son los siguientes:

- **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 empresa cumpla 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.

- **Modelo de valor:** Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

- **Mapa de riesgos** Relación de las amenazas a que están expuestos los activos.

- **Declaración de aplicabilidad** Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

- **Evaluación de salvaguardas** Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

- **Estado de riesgo** Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

- **Informe de insuficiencias** Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

- **Cumplimiento de normativa** Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

- **Plan de seguridad** Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

2.5 MARCO LEGAL

Tabla 4: Marco Legal

NORMA	DESCRIPCIÓN

Artículos 209 y 269, Constitución Política de Colombia 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".
Ley 1273 de 2009	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.
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.
Constitución/1991	Reitera el principio fundamental de competencia abierta., permite la inversión extranjera en el sector, y establece el carácter público del espectro electromagnético encargándole al Estado su control.
Decreto 2122/1992	Modifica algunos artículos del Decreto 1901 asignándole nuevas funciones al Ministerio de Comunicaciones y creando nuevas dependencias, entre las cuales se encuentra la Comisión de regulación de Telecomunicaciones como una Unidad Administrativa Especial.
Ley 335/1996	Modifica aspectos fundamentales de la normatividad en materia de televisión la cual estaba contenida en la Ley 14 de 1991 y en la Ley 182 de 1995.Por medio de esta Ley se permite una mayor participación del sector privado en la prestación del servicio de televisión.
Ley 689/2001	Modificó parcialmente la ley 142 de 1994 de servicios públicos domiciliarios en lo relacionado a los numerales 14.15 y 14.24 del artículo 14.

Decreto 575/2002	Mediante este decreto se reglamenta la prestación de los servicios de comunicación personal (PCS), fue modificado en el artículo 59 por decreto 576 de 2002.
Decreto 1686/2002	Se reglamenta el artículo 36 de la ley 80 de 1993, el cual establece que el término de duración de las concesiones para la prestación de los servicios y actividades de telecomunicaciones no podrá exceder de diez años, prorrogable automáticamente por un lapso igual.
Decreto 600/2003	Por medio del decreto 600 de 2003se expiden normas sobre los servicios de Valor Agregado y Telemáticos, y se reglamenta el decreto ley 1900 de 1990.
Decreto 0020/2003	En el decreto 0020 de 2003 se establece el procedimiento a seguir por el Ministerio de Comunicaciones para la fijación de las condiciones de administración del dominio.
Decreto 3055/2003	Por medio del cual se modifica el decreto 600 de 2003.
Decreto 195/2005	Por la cual se adoptan límites de exposición de las personas a campos electromagnéticos, se adecúan procedimientos para la instalación de estaciones radioeléctricas y se dictan otras disposiciones.
Decreto 075/2006	Interceptación de servicios de telecomunicaciones. Operadores de servicio móvil celular y PCS.
Decreto 1928/2006	Espectro electromagnético.

Fuente: Adaptación de los Autores del proyecto

3 DISEÑO METODOLOGICO

3.1 TIPO DE INVESTIGACIÓN

El proceso investigativo que se ha llevado sigue los parámetros de una investigación descriptiva debido a que se estudia el comportamiento independiente de unas variables, buscando especificar las propiedades de las personas que intervienen en el tratamiento de la información organizacional, con el fin de auditar las prácticas actuales y describir de manera detallada el conjunto de controles y mejoras que se deben hacer.

3.2 POBLACIÓN Y MUESTRA

Actualmente la empresa Katalinda shoes cuenta con una población manejable en cantidad, se decidió que la muestra seria el total de la población conformada por dirigentes y trabajadores de la empresa.

3.2.1 Técnicas de recolección de la información

Durante el desarrollo de este proyecto se emplearon fuentes primarias y secundarias de recolección de información para la identificación del estado actual de inseguridad desde diversos aspectos (tecnológico, financiero, recurso humano) y la selección y formulación de los controles necesarios para optimizar el tratamiento seguro de la información en la empresa.

Las fuentes primarias utilizadas en el estudio la constituyen personas de la empresa, asesores de la Universidad Francisco de Paula Santander Seccional Ocaña; se formularon y aplicaron diversos instrumentos de recolección de información como listas de chequeo, encuesta y entrevistas a los dirigentes y empleados de la empresa; todo esto para obtener información objetiva de primera mano sobre el funcionamiento de la organización, teniendo la seguridad como aspecto importante. Los diferentes instrumentos de recolección de información como: la encuesta y observación directa se pueden apreciar en los anexos. Entre las fuentes secundarias de información se cuenta con la información extraída de revistas, libros y textos de clase, documentación, bibliotecas y consultas virtuales.

4 PRESENTACIÓN DE RESULTADOS

Para el logro de los objetivos propuestos se implementaron una serie de actividades

Tabla 5: Actividades por objetivo

OBJETIVOS	ACTIVIDADES	Resultado
Diagnosticar los elementos organizacionales de la empresa Katalida Shoes a través de una auditoria pasiva con base en la norma ISO/ IEC27001	1. Recopilar la información de la empresa como: misión, visión, objetivos, procesos entre otros. 2. Diseñar instrumentos (Lista de Chequeo, Encuesta, entrevista, papeles de trabajo.) de recolección de información. 3. Auditoría	1. Modelado del Negocio. 2. Instrumentos de Recolección de Información. 3. Informe de Auditoria
Identificar los elementos que conforman el SGSI para la empresa Katalida Shoes	**3.** Consultar los elementos que estructuran un Sistema de Gestión de Seguridad de la Información **4.** Adaptar al contexto de la empresa los dominios de seguridad física y lógica	Documentos del Marco Referencial.
Documentar formalmente las actividades y políticas requeridas para gestionar adecuadamente la seguridad de la información en la empresa Katalinda Shoes.	1. Identificación de alcances y objetivos. 2. Crear una política de gestión de seguridad basada en la norma ISO 27001:2013.	

Fuente: Autores del proyecto

Figura 4.Metodología PVHA

Fuente: Adaptación de los autores del proyecto

4.1 DIAGNOSTICO

Diagnosticar los elementos organizacionales de la empresa KTALINDA SHOES a través de una auditoria pasiva con base a la norma ISO/IEC 27001:2013.

4.1.1 Modelado del negocio

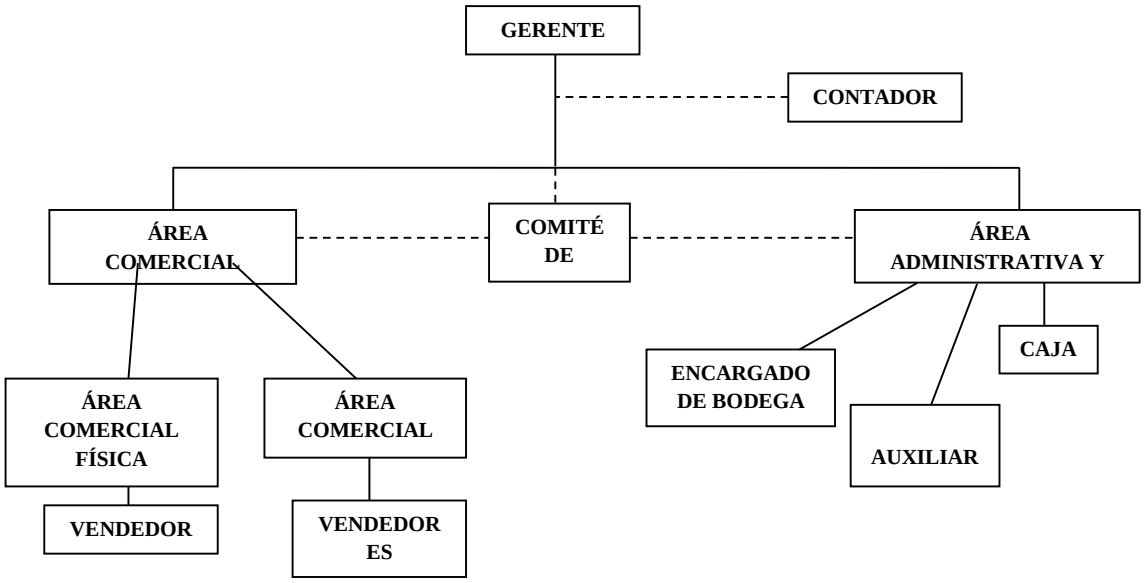
Información general de la empresa y dependencia seleccionada.

El almacén KATALINDA SHOES fue creado en mayo del año 2013 por la señora Lisney Criado como un proyecto personal de emprendimiento que sin contar con muchas herramientas financieras logro la puesta en marcha del mismo. Hoy en día la empresa cuenta con 5 personas, una empleada que comenzó a laborar desde la creación de la microempresa y cuatro empleados más que juntos con su esposo desarrollan los diferentes procesos de la

misma, además de un contador externo encargado de la parte contable y tributaria del almacén.

KATALINDA SHOES, es un almacén localizado en la calle 10 # 11-92 local 104 edificio Crediservir en la ciudad de Ocaña, que está al servicio de toda la comunidad. La empresa es atendida por su actual propietaria Lisney, quién lleva año y 4 meses al mando del creciente almacén.

Figura 1. Organigrama de la Empresa.



Fuente: Autores del Proyecto

Modelo de Objetivos. La empresa KATALINDA, vincula directamente su objetivo general con la misión y visión de le empresa. (Figura 3.)

Misión. Ofrecer calzado de moda, diseño y confort que satisfaga las necesidades, expectativas y gustos de nuestros clientes. Prestando un servicio con atención y calidad en nuestros puntos de venta.

Visión. KATALINDA para el 2016 será la tienda líder en la comercialización de calzado en la región de Ocaña. Trabajando con políticas de calidad y atención al cliente que garanticen

la preferencia y lealtad a nuestros productos, asegurando el crecimiento sostenido de nuestra empresa.

Objetivo general

Es el Crecimiento y consolidación empresarial en la ciudad de Ocaña en la comercialización de calzado.

Figura 2. Objetivos de la empresa KATALINDA.

Financiera
Incrementar los ingresos, brindando atención eficaz y eficiente a nuestros clientes, consolidando de ésta manera el marco competitivo de la empresa.

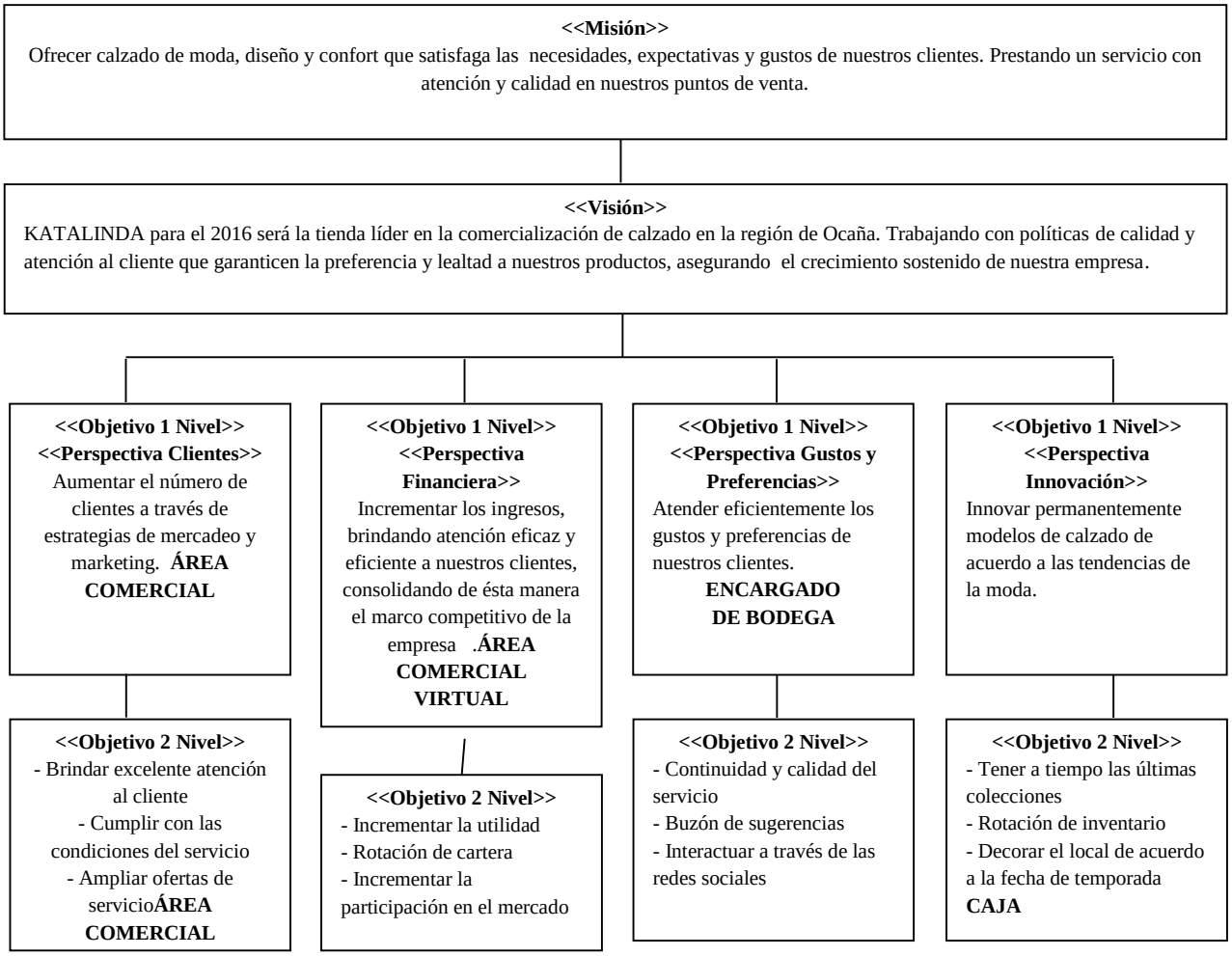
Clientes
Aumentar el número de clientes a través de estrategias de mercadeo y marketing.

Gustos y Preferencias
Atender eficientemente los gustos y preferencias de nuestros clientes.

Innovación
Innovar permanentemente modelos de calzado de acuerdo a las tendencias de la moda.

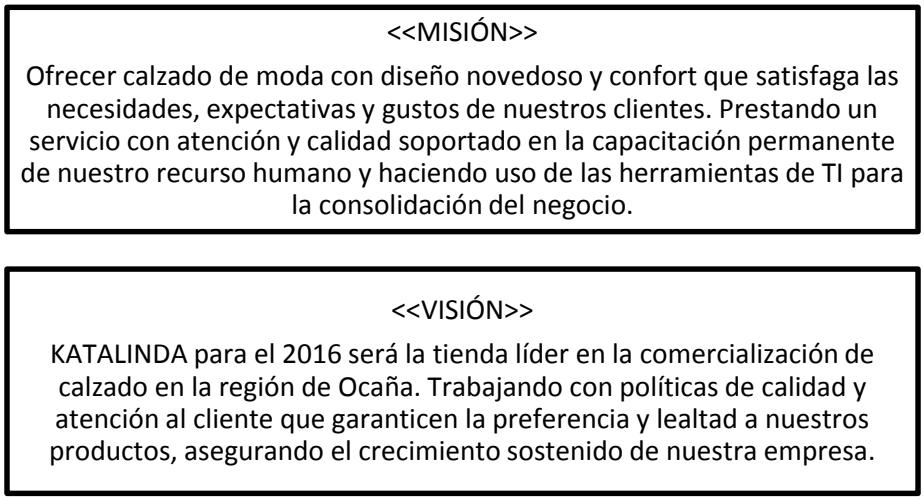
Fuente: Autores del Proyecto

Figura 3. Misión, Visión y Objetivos de la empresa KATALINDA.



Fuente: Autores del Proyecto

Figura 5: Misión y Visión Propuestas



Fuente: Autores del proyecto

Valores corporativos de "KATALINDA SHOES"

Competitividad. Desarrollar el talento y la capacidad de cada miembro de nuestra organización para que asuma con eficiencia, responsabilidad y compromiso su rol dentro de la empresa.

Compromiso. Estimular en cada miembro de la empresa, una actitud responsable y pertinente para realizar su función en forma eficiente y fomentar en cada uno, una genuina sensibilidad social y respeto por el medio ambiente.

Comunicación. Mantener una intercomunicación abierta y fluida dentro y fuera de la empresa; para transmitir los objetivos corporativos y crear una buena imagen, ante todos los que interactúan con la empresa.

Confianza. Generar y un clima de amistad con todos los que se relaciona con la empresa.

Cooperación. Proporcionar al personal de la empresa el apoyo necesario para el logro de los objetivos personales y corporativos.

Honestidad. Ejercer con integridad y transparencia todos nuestros actos.

Puntualidad. Establecer una cultura de exactitud y responsabilidad en todos nuestros compromisos.

Respeto. Fomentar una actitud de obediencia, en todas las relaciones personales y en todos los niveles de autoridad.

Responsabilidad. Ser puntual y eficaz con los compromisos adquiridos.

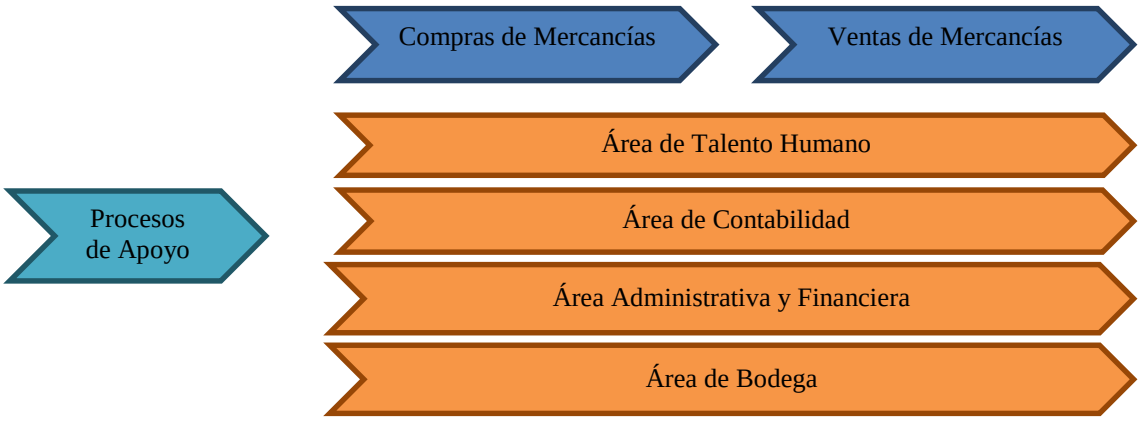
Servicio. Dar la mejor asistencia de apoyo a los demás. Nuestra promesa básica es: "Vivir para servir, y dar lo mejor de sí mismo".

Diagrama de procesos

Para realizar el diagrama de procesos se consultó la documentación presentada por la empresa KATALINDA en la cual se definen los dos procesos misionales de la empresa complementados con entrevistas.

KATALINDA realiza su principal objetivo que es la comercialización de calzado basado en dos procesos principales como las compras de mercancías y las ventas de mercancías (ilustración en la figura 4)

Figura 4. Cadena de valor de la empresa KATALINDA



Fuente: Autores del proyecto

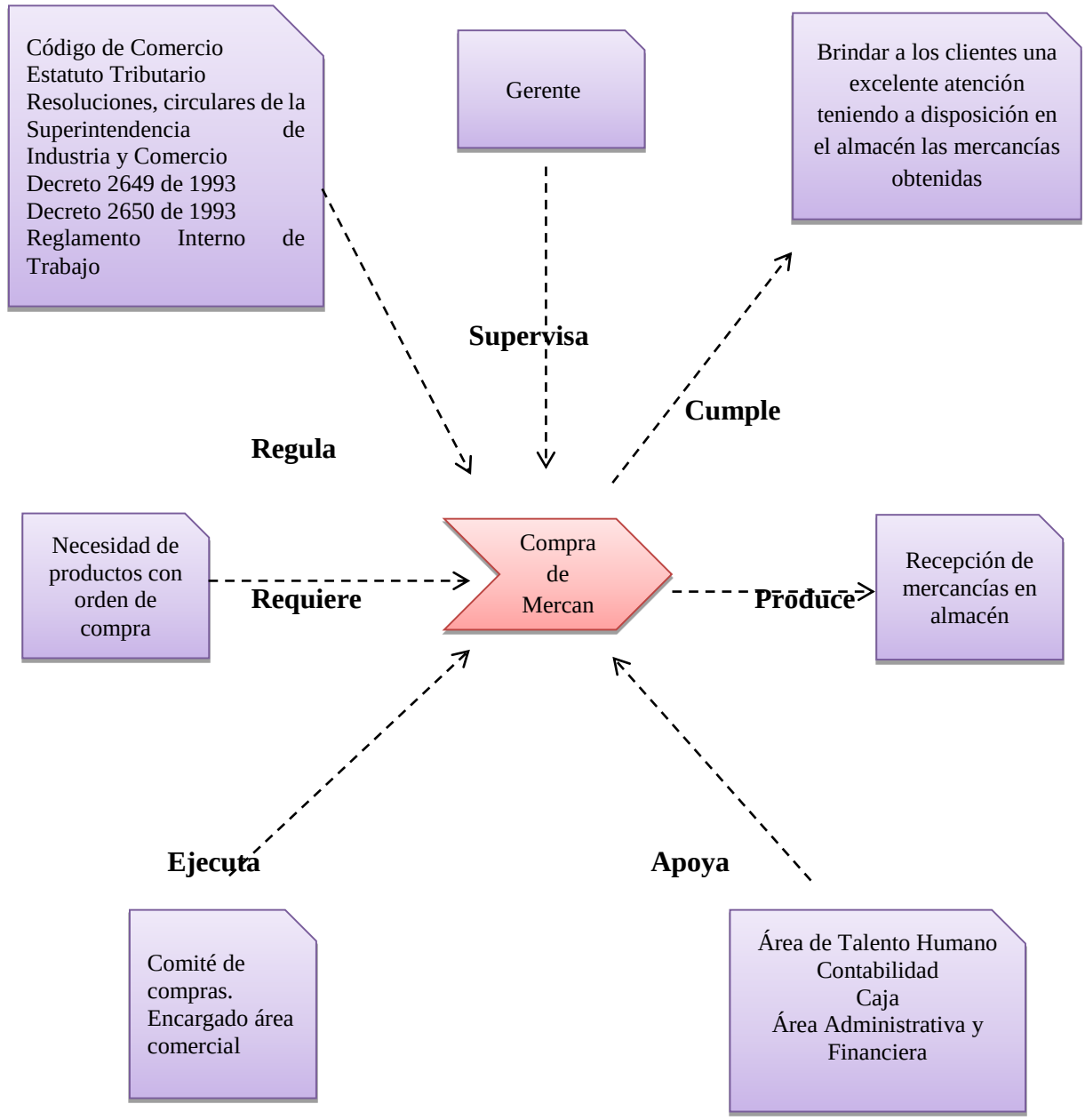
PF compra de mercancías
PF venta de mercancías

La descripción de cada uno de estos procesos misionales se presenta en diagrama de descripción de procesos de manera jerárquica.

Diagrama de descripción de procesos

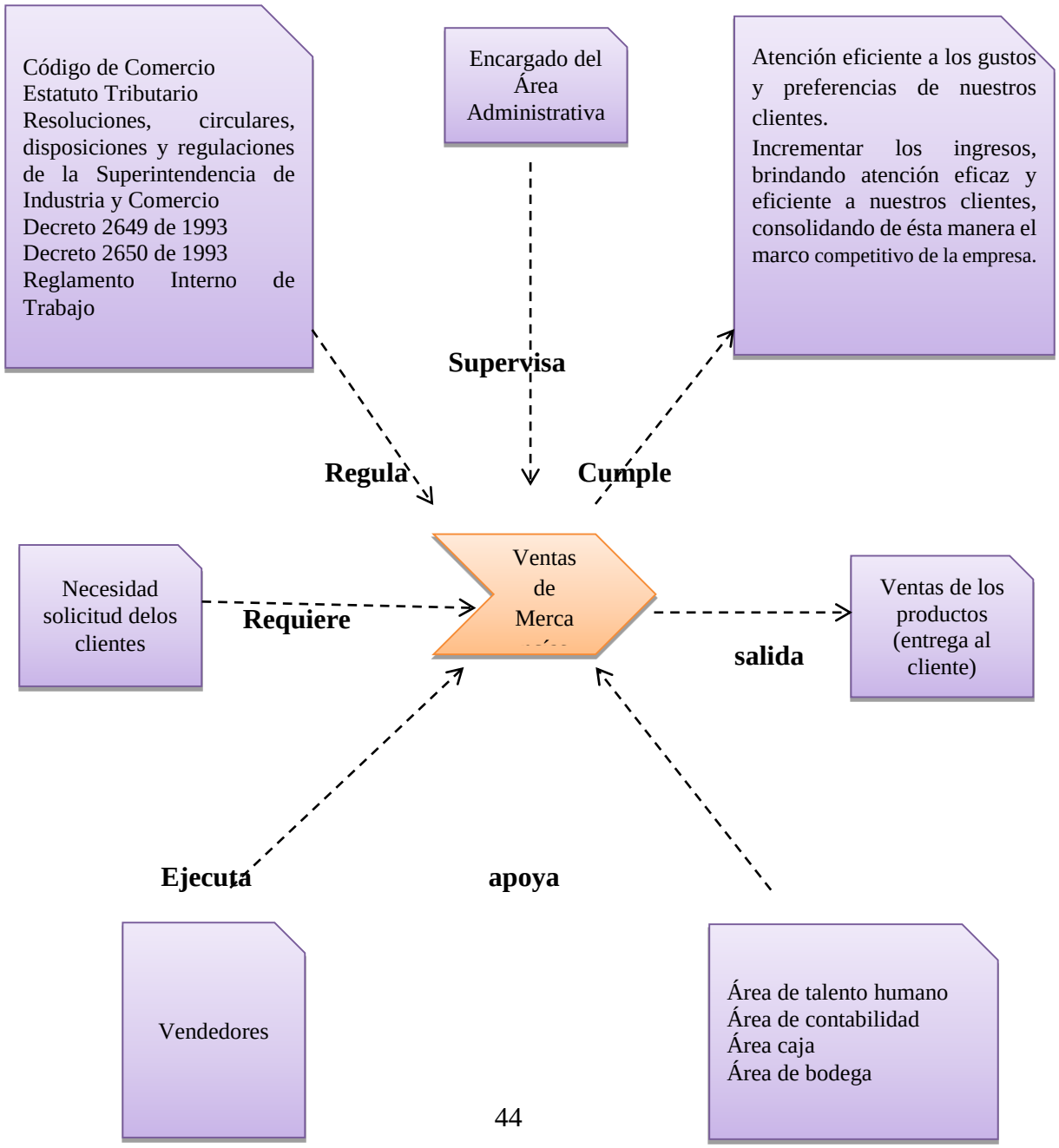
PF compra de mercancías. El proceso principal de compras de mercancías tiene como objetivo mantener la mercancía disponible en vitrinas y bodegas. (Su descripción puede verse en la figura 5).

Figura 5. PF Compra de mercancía KATALINDA.



PF Ventas de Mercancías. El proceso fundamental de ventas de mercancías tiene como objetivo llevar los productos hasta el cliente final atreves de la venta directa o virtual de los productos que se ofrecen en la empresa KATALINDA. (Su descripción se ilustra en la figura 6).

Figura 6.PF ventas de mercancías.



Tecnologías de la información y las comunicaciones en KATALINDA

Sistemas de información

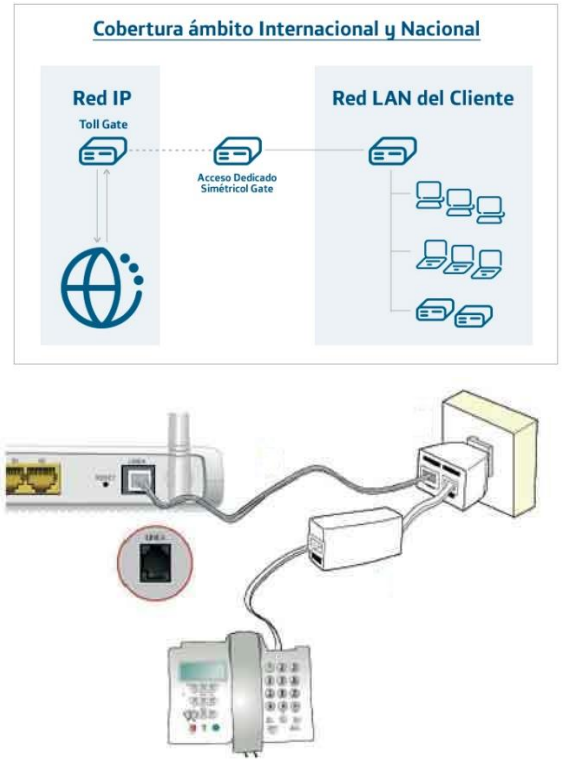
KATALINDA, cuenta con un sistema de información para el proceso de contabilidad llamado Manager ver 3.1 con licencia. Éste software contiene archivo, clientes, proveedores, archivo de proveedores punto de venta, reporte de caja, factura de venta, factura de compra ,notas débito y crédito, estado de cuentas clientes, estado de cuenta proveedores, kardex de artículos, artículos y existencias, balance general, estado de resultados.

Aplicación en los celulares VmeyeSuper (Software que nos permite visualizar las cámaras).

Infraestructura tecnológica

La empresa para el desarrollo del proceso de comercialización cuenta con la siguiente infraestructura de Red figura 7.

Figura 7. Cabecera de Red de la Empresa Movistar



Fuente: Empresa de Movistar

En la figura se observa la Topología de Red interna brindada por la empresa Movistar que llega a través de la Línea telefónica y que éste a su vez se conecta en un Punto de red de un Switch/Router.

Elementos de entrada de información. Línea Telefónica Nacional de la empresa Movistar y Sistema de cámaras de seguridad interno compuesto por un dvr de 4 canales y uno de audio más disco duro de 500, 4 cámaras domos de 720 tvl visión nocturna Y 24 leds, micrófono de alta resolución y un monitor LG de 24 pulgadas.

Elementos de Procesamiento de Señal. Switch/Router

Elementos de Salida. Portátil Lenovo G400 con procesador Intel, Celulares y Datafono adscrito la redaban.

El proceso de comercialización se apoya en la siguiente infraestructura (figura 8).

Figura 6. Infraestructura de Red proceso de Comercialización

Fuente: Autores del Proyecto

Para el funcionamiento del área comercial la empresa KATALINDA cuenta con 1 Computador Portátil, 1 Cámara IP y 1 Datafono interconectados por una Red LAN mediante un SWITCH/ROUTER de 6 puertos, que es el elemento que permite expansión de la red.

Nivel de Madurez de TIC en KATALIDA SHOES

Para identificar el nivel de madurez de TIC en el que se encuentra la empresa KATALINDA SHOES Se tuvieron en cuenta criterios como adquirir y mantener infraestructura tecnológica, adquirir recurso de TI, Garantizar la continuidad del servicio, garantizar la seguridad de los sistemas y administración del ambiente físico obtenido como resultado que la empresa KATALINDA SHOES se encuentra en el nivel inicial del nivel de madures de la escala de CMMI.

Tabla 6: Nivel 1 Tecnología de Información y Comunicación

(TIC)	**Recomendaciones**
Adquirir y mantener infraestructura tecnológica	Es necesario mejorar el proceso de adquisición y mantenimiento de la infraestructura tecnológica teniendo en cuenta las necesidades críticas del negocio.
Decisiones de adquisición	
Sistema configurado para realizar prueba / instalación	
Requerimientos de ambiente físico	
Actualizaciones de estándares de tecnología	
Requerimiento de monitoreo de sistema	
Conocimiento de la infraestructura	
Adquirir recursos de TI	Se debe desarrollar un plan de continuidad del servicio, que le permita a la empresa mantener la prestación de servicio.
Requerimientos de administración de la relación con terceros	
Artículo provisto	
Arreglos contractuales	
Garantizar la continuidad del servicio	Se requiere determinar un plan de seguridad adecuado que permita salvaguardar los elementos hardware y software y la información de la empresa
Resultados de la prueba de contingencia	
Criticidad de puntos de configuración de TI	
Plan de almacenamiento de respaldos y de protección	
Umbrales de incidente / desastre	
Requerimientos de servicios contra desastres incluyendo roles y responsabilidad	
Reportes de desempeño de los procesos	

Garantizar la seguridad de los sistemas	Diseñar un plan a mediano plazo para la administración del ambiente físico, que permita tener una adecuada instalación que soporte el área de infraestructura TI.
Definición de incidentes de seguridad	
Requerimiento específico de entrenamiento sobre conciencia de seguridad	
Reportes de desempeño del proceso	
Cambio de seguridad requeridos	
Amenazas y vulnerabilidad de seguridad	
Administración del ambiente físico	
Reportes de desempeño de procesos	

Fuente: Autores del Proyecto

4.1.2 Auditoria pasiva al almacén KATALINDA SHOES

Se desarrollo una Auditoria de Sistemas al Almacén de Calzado KATALINDA SHOES donde se aplicó la metodología acorde a las necesidades del almacén. Esta Auditoria está estructurada por un Plan de Auditoria, que comprende la fase de planeación, el Desarrollo de la Auditoria donde se evidencian las técnicas empleadas que soportan los hallazgos y por último se encuentra el Informe de Auditoría que comprende las observaciones, las conformidades, las no conformidades y el plan de mejoramiento.

Tabla 7 Informe de Auditoria

INFORME DE AUDITORIA FORTALEZAS		
N°	**PROCESO**	**DESCRIPCION**
1	Estructura organizacional	El personal que labora en KATALINDA SHOES conoce los objetivos misionales, son empleados motivados, satisfechos con su sueldo y con sentido de pertenencia por la empresa.
2	Servicio al cliente	Se evidencia una excelente atención al cliente y el almacén goza de una buena imagen en el mercado del calzado por la calidad de sus productos, garantía ofrecida, excelentes precios y variedad de diseños.

3	Herramientas Tecnológicas.	El Marketing en redes sociales como Facebook e instagram, la Promoción y venta en el comercio virtual ha sido el factor clave para el crecimiento y éxito del negocio. Se cuenta con 4 computadores de excelente calidad, 2 proveedores de servicios internet, servicio de datafono.
4	Seguridad Física y del ambiente	Se cuenta con cámaras de seguridad con el fin de tener un soporte en caso de robos y

OBSERVACIONES			
N°	**PROCESO**	**DESCRIPCION**	**ACCION DE MEJORA**
1	ESTRUCTURA ORGANIZACIONAL	La empresa KATALINDA cuenta con estructura organizacional pero dentro de la misma no existe unas funciones específicas de personal a realizar apoyo tecnológico a los proceso de la empresa. La empresa KATALINDA no cuenta en la actualidad con personal capacitado en sistemas. La empresa KATALINDA no cuenta con procesos de gestión tecnológico como apoyo los procesos misionales documentado y aprobado	Definir claramente en la estructura organizacional de la empresa funciones y responsabilidades específicas en manejo del proceso de gestión tecnológica como apoyo a Los procesos misionales de compra y venta de la empresa. Capacitar al personal asignado con funciones específicas en el manejo de sistemas. Crear un proceso definido y claro de apoyo tecnológico a los demás procesos misionales de la organización
2	ÁREA OPERATIVA	Desconocimiento del personal administrativo y técnico sobre legislación de manejo de base de datos, redes sociales y comercio electrónico.	Capacitar en temas legales de manejo de base de datos, Uso de Redes sociales a todo el personal involucrado en el manejo de comercio virtual.

3	AREA FINANCIERA	La empresa KATALINDA ejecuta parcialmente el software comercial manager 3.1 como apoyo a los procesos misionales de la empresa.	Contratar a una persona que maneje el software comercial de la empresa, con el fin de mantener actualizada la información de entradas y salidas de los proceso de compra y venta de la empresa.

NO CONFORMIDADES				
No.	**PROCESO**	**DESCRIPCION**	**CRITERIO**	**ACCIONES DE MEJORA**
1	Seguridad física e institucional	Se evidencio que no existen normas y reglamentos sobre seguridad en la organización.	**NTC ISO 27002 CONTROL 9.1.2 Controles de acceso físico**	Crear un plan de gestión en manejo de incidentes de seguridad de la empresa
2	Seguridad física	No existe un cableado estructurado de los equipo de cómputo y comunicación de la Empresa.	**NTC ISO 27002 CONTROL 9.2.3 Seguridad del cableado**	Se recomienda Proteger el cableado de la energía y las telecomunicaciones que soportan los servicios de información contra la interrupción o daño.
3	Seguridad institucional	Se evidenció que no se cuenta con Extintores ni con planta eléctrica en caso de fallas de este servicio o un incendio.	**NTC ISO 27002 CONTROL 9.2.2 Servicio de suministro**	Adquirir un extintor y una planta eléctrica En la mayor brevedad posible
4	Seguridad física	Se observó que el área de Sistemas no cuenta con una estructura física adecuada donde se	**NTC ISO 27002 CONTROL 9.1.3 Seguridad de oficinas recintos e instalaciones**	Reubicar o adaptar el espacio físico del almacén; de tal manera que se definan espacios

		puedan llevar a cabo los del mismo.		adecuados para el correcto funcionamiento del mismo.
5	Seguridad de la Información	Se evidencio que la empresa KATALINDA no cuenta con una política de seguridad de la información	**NTC ISO 27001 A.5 Políticas de seguridad de la información**	Definir e implementar una política de identificación análisis y valoración de riesgos que eviten pérdidas en la integridad, disponibilidad y confidencialidad de la información.
6	Seguridad de los Equipos	Los equipos de cómputo y comunicaciones de la empresa no cuentan con seguridad física en la áreas donde funcionan	**NTC ISO 27002** Control 9.2.1 Ubicación y protección de los equipos	Se recomienda: tener físicamente separado los medios de procesamiento de información manejados por la organización
7	Seguridad de los Equipos	La empresa KATALINDA no cuenta con un plan de mantenimiento a los equipos de cómputo y comunicaciones.	**NTC ISO 27002** Control 9.2.4Mantenimiento de los equipos	Definir e implementar un plan de mantenimiento preventivo adecuado para los equipos.

PLAN DE MEJORAMIENTO PROPUESTO				
No.	**NO CONFORMIDAD**	**ACCIONES DE MEJORA**		**RESPONSABLE**

1	Se evidencio que no existen normas y reglamentos sobre seguridad en la organización	Crear un plan de gestión en manejo de incidentes de seguridad de la empresa	GERENTE
2	No existe un cableado estructurado de los equipo de cómputo y comunicación de la Empresa.	Se recomienda Proteger el cableado de la energía a través de canaletas para proteger contra la interrupción o daño.	INGENIERO DE SISTEMAS ENCARGADO DEL DEPARTAMENTO DE SISTEMAS
3	Se evidenció que no se cuenta con extintor ni planta eléctrica en caso de fallas de este servicio o de un incendio.	Adquirir un extintor y una planta eléctrica en la mayor brevedad posible	PROPIETARIOS
4	Se observó que el Área de Sistemas no cuenta con una estructura física adecuada donde se puedan llevar a cabo los del mismo.	Reubicar o adaptar el espacio físico del almacén; de tal manera que se definan espacios adecuados para el correcto funcionamiento del mismo.	PROPIETARIOS
5	Se evidencio que la empresa KATALINDA no cuenta con una política de seguridad de la información	Definir e implementar una política de Identificación análisis y valoración de riesgos que eviten pérdidas en la integridad, disponibilidad y confidencialidad de la información.	GERENTE E INGENIERO DE SISTEMAS
6	Los equipos de cómputo y comunicaciones de la empresa no cuentan con seguridad física en la áreas donde funcionan	Se recomienda: tener físicamente separado los medios de procesamiento de información	GERENTE

		manejados por la organización.	
7	La empresa KATALINDA no cuenta con un plan de mantenimiento a los equipos de cómputo y comunicaciones.	Definir e implementar un plan de mantenimiento preventivo adecuado para los equipos.	INGENERO DE SISTEMAS.

Fuente: Autores del Proyecto

En el desarrollo de la auditoría al proceso de gestión Tecnológica de la empresa se encontraron aspectos que definen el estado actual que presenta la organización frente a esta temática. Por tal motivo, a continuación se presenta el dictamen, el cual describe situaciones encontradas y las recomendaciones pertinentes de acuerdo a los requisitos mínimos exigidos por la norma internacional NTC ISO 27001 y sus buenas prácticas referenciadas en la NTC ISO 27002. La cual se trata este dominio, con el fin de mejorar la seguridad en la organización. En esta auditoría se evaluaron los siguientes aspectos:

 Se evaluó la gestión tecnológica que soporta los procesos de compra y ventas de la empresa, considerando requisitos legales y buenas prácticas de seguridad de la información.

Durante la evaluación se informa que se observaron las siguientes situaciones: Los perímetros de seguridad física presentan deficiencias a nivel interno ya que no cuentan con una estructura física adecuada en el área de sistemas que sea amplia y con espacios adecuados para llevar a cabo procesos como ventas en línea, marketing, contabilización entre otros procesos. La parte tecnológica se encuentra descentralizada, de tal manera que los equipos tecnológicos se manipulan desde cualquier sitio, situación que presenta un riesgo para la seguridad de la información de los mismos al no tener buenas prácticas implementadas. A nivel documental, se evidencio que no existen políticas de seguridad de la información, en este caso, políticas de seguridad física y del entorno. Igualmente, desde el punto de vista operativo se identificó que no existen procedimientos, estándares y registros de control de acceso físico, manejo de medios, gestión de incidentes y en especial un sistema de gestión de riesgos de la información, que permita identificar los riesgos y los controles pertinentes para la mitigación de los mismos.
El no tener definida, documentada, aprobada, publicada e implementada las políticas, procedimientos y estándares, pone en riesgo el cumplimiento de las normas y las medidas adecuadas para la protección de la información, y en efecto, pueden existir pérdidas en la integridad, disponibilidad y confidencialidad de la misma, aunque actualmente se están desarrollando con la reestructuración de los manuales de procedimiento y la puesta en marcha

de la digitalización de archivos. La seguridad de los equipos es inadecuada porque no se realizan mantenimientos preventivos de forma permanente, de tal manera que se eviten posibles fallas que perjudiquen los procesos que se llevan a cabo en la empresa y poniendo en riesgo la integridad y disponibilidad de la información. Los servicios de suministros, son deficientes, debido a la falta de una planta eléctrica y un extintor que permita la continuidad de los procesos internos administrativos en caso de incendio, ausencia o falla de energía. La seguridad del cableado presenta deficiencias significativas por la exposición de algunos cables que se encuentran al descubierto sin canaletas y de libre acceso a los mismos. Se presenta un riesgo en la gestión de los activos ya que no se disponen de inventarios de los mismos (hardware, software, información, documentos, infraestructura,…). Se presenta un alto riesgo de cumplimiento de requisitos legales al tener parcialmente identificada la normatividad y legislación que aplica a la empresa en el manejo de base de datos, comercio virtual y manejo de redes sociales de sus clientes. De acuerdo con la evaluación realizada conforme a los criterios establecidos para esta auditoría y a los resultados obtenidos de la misma, nos permitimos hacer las siguientes recomendaciones con el fin de mitigar los riesgos y garantizar la continuidad del Negocio:

- Reubicar o Adaptar el espacio físico del almacén; de tal manera que se definan espacios adecuados para el correcto funcionamiento de los equipos que hacen parte del proceso de gestión tecnológica como apoyo a los procesos misionales de la organización que cumpla con los estándares de seguridad según las normas.
- Crear un plan de gestión en manejo de incidentes de seguridad de la empresa
- Definir y establecer una estructura organizacional adecuada a la misión de la empresa y que incluya el proceso de gestión tecnológica.
- Proteger el cableado de la energía a través de canaletas para proteger contra la interrupción o daño.
- Adquirir un extintor y una planta eléctrica en la mayor brevedad posible.
- Definir e implementar una política de identificación análisis y valoración de riesgos que eviten pérdidas en la integridad, disponibilidad y confidencialidad de la información.
- Documentar el manual de funciones con roles y cargos adecuados a las operaciones del negocio.
- Se recomienda: tener físicamente separado los medios de procesamiento de información manejados por la organización.
- Definir políticas de seguridad de la información e implementar buenas prácticas de seguridad a todas las áreas de la empresa.
- Definir e implementar un plan de capacitación y sensibilización periódica de los empleados que generen conciencia, formación y cultura organizacional en el

cumplimiento de la misión, manejo de funciones, procesos, recursos tecnológicos, seguridad de la información y cumplimiento de requisitos legales.

- Definir e implementar un plan de mantenimiento preventivo adecuado para los equipos o Establecer contacto y contratos de soporte y mantenimiento de hardware y software.
- Identificar los requisitos legales que debe cumplir la empresa y definir planes para el oportuno cumplimiento de los mismos

4.2 ELEMENTOS DEL SGSI PARA LA EMPRESA KATALIDA SHOES

4.2.1 ISO/IEC 27001:2013

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).

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

El presente sistema de gestión de la seguridad de la información (SGSI) se basa en la norma ISO/IEC 27001:2005, la cual contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. Propone un sistema basado en el Ciclo de Deming: Plan, Do, Check, Act (Planear, Hacer, Verificar, Actuar) conocido como PDCA, el cual encamina a un sistema de mejora continua con capacidad de adaptase a cambios y necesidades de su entorno de desarrollo.

Figura 7: Ciclo de Deming

Fuente: Adaptación del Ciclo de Deming por los Autores del Proyecto

A continuación se hace una breve descripción de las actividades que se deben realizar en cada una de las 4 Fases del ciclo PDCA según el estándar internacional 27001[8].

Planificar

En esta fase se define actividades susceptibles de mejora e identifican los objetivos a alcanzar, procesos y procedimientos del SGSI relevantes para mejorar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

Hacer

En esta fase se debe implementar un plan de tratamiento de riesgos, operar políticas y controles, procesos y procedimientos y la definición de métricas que permitan evaluar la eficacia de los procesos implantados.

Comprobar

[8] ISO/IEC. (2005). *Estandar Internacional 27001 - Primera edición* .

En el transcurso de esta fase se aplica diversos tipos de revisiones las cuales miden el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia.

Mejorar
Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna del SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo.

La norma ISO /IEC 27001 tiene 11 dominios de controles que cubre todos los rincones de una empresa donde debe existir seguridad de la información, los dominios están divididos en 39 objetivos de control que comprende 133 controles de seguridad.
Se seleccionan los controles para definir un SGSI que aplique a la empresa "Katalinda shoes" los cuales se encuentran en el Anexo A de la norma ISO/IEC 27001.

Fases para un sistema de gestión de seguridad de la información[9]

- Requerimientos Generales
- Establecer y manejar el SGSI
- Implementar y operar el SGSI
- Monitorear y revisar el SGSI
- Mantener y mejor el SGSI

Responsabilidad de la Gerencia
- Compromisos de la gerencia; Debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI.
- Gestión de recursos

Auditorías Internas SGSI
La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar los objetivos de control, controles, procesos y procedimientos del SGSI que cumplan;

[9] ISO/IEC. (2005). *Estandar Internacional 27001 - Primera edición* .

- Los requerimientos del estándar ISO/IEC 27001.
- Los requerimientos de seguridad de la información identificados.
- Se implementen y mantenga de manera efectiva.
- Se realice conforme a lo esperado.

Revisión gerencial del SGSI

- General: La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos 1 vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad.
- Insumos de la revisión.
- Resultados de la revisión.

Mejoramiento del SGSI

- Mejoramiento continúo.
- Acción correctiva.
- Acción preventiva.

4.2.2 ISO/IEC 27002

El ISO/IEC 27002, también conocido como ISO 17799, es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El objetivo de la norma ISO/IEC 27002 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Se trata de una norma no certificable, pero que recoge la relación de controles a aplicar para establecer un SGSI.

Para el desarrollo de la Política de Seguridad de la Información base del SGSI, se seleccionó la norma ISO/IEC 27002, porque es un marco de trabajo de mejores prácticas internacionales que establece las guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la organización. Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han salido de una evaluación de riesgos.

Estructura del estándar:

El ISO/IEC 27002 contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales. Se detallan las diferentes cláusulas con sus categorías y los objetivos que persiguen cada una de ellas:

1. Política de Seguridad
    - Política de seguridad de la información. Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

2. Organización de la Seguridad de la Información
    - Organización interna. Manejar la seguridad de la información dentro de la organización.
    - Grupos o personas externas. Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados o manejados por, grupos externos.

3. Gestión de Activos
    - Responsabilidad por los activos. Lograr y mantener una apropiada protección de los activos organizacionales.
    - Clasificación de la información. Asegurar que la información reciba un nivel de protección apropiado.

4. Seguridad de Recursos Humanos
    - Antes del empleo. Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, y reducir el riesgo de robo, fraude y mal uso de los medios.
    - Durante el empleo. Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.
    - Finalización o cambio de empleo. Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.

5. Seguridad Física y Ambiental
    - Áreas seguras. Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

- Equipo de seguridad. Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

6. Gestión de Comunicaciones y Operaciones
   - Procedimientos y responsabilidades operacionales. Asegurar la operación correcta y segura de los medios de procesamiento de la información.
   - Gestión de la entrega del servicio de terceros. Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.
   - Planificación y aceptación del sistema. Minimizar el riesgo de fallos en el sistema.
   - Protección contra el código malicioso y móvil. Proteger la integridad del software y la integración.
   - Copia de Seguridad. Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.
   - Gestión de seguridad de la red. Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
   - Gestión de medios. Evitar la divulgación no-autorizada, la modificación, eliminación o destrucción de activos y la interrupción de las actividades comerciales.
   - Intercambio de información. Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
   - Servicios de comercio electrónico. Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.
   - Monitorización. Detectar las actividades de procesamiento de información no autorizadas.

7. Control de Acceso
   - Requerimiento del negocio para el control del acceso. Controlar el acceso a la información.
   - Gestión de acceso del usuario. Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.
   - Responsabilidades del usuario. Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.
   - Control de acceso a la red. Evitar el acceso no autorizado a los servicios de la red.
   - Control del acceso al sistema operativo. Evitar el acceso no autorizado a los sistemas operativos.
   - Control de acceso a la aplicación y la información. Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

- Computación y tele-trabajo móvil. Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móvil.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
   - Requerimientos de seguridad de los sistemas de información. Garantizar que la seguridad sea una parte integral de los sistemas de información.
   - Procesamiento correcto en las aplicaciones. Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.
   - Controles criptográficos. Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.
   - Seguridad de los archivos del sistema. Garantizar la seguridad de los archivos del sistema.
   - Seguridad en los procesos de desarrollo y soporte. Mantener la seguridad del software y la información del sistema de aplicación.
   - Gestión de la Vulnerabilidad Técnica. Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

9. Gestión de Incidentes de Seguridad de la Información
   - Informe de los eventos y debilidades de la seguridad de la información. Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.
   - Gestión de los incidentes y mejoras en la seguridad de la información. Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

10. Gestión de la Continuidad Comercial
   - Aspectos de la seguridad de la información de la gestión de la continuidad del negocio. Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallos importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

11. Cumplimiento
   - Cumplimiento de los requerimientos legales. Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

- Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico. Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

Consideraciones de auditoría de los sistemas de información. Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

4.3 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Posterior a las fases de diagnóstico e identificación de los estándares pertinentes para la planeación del Sistema de Gestión de la Seguridad de la Información se procedió a documentar formalmente los elementos requeridos para condensar en una política el resultado de la presente propuesta. Dicho documento se encuentra como anexo al presente proyecto, y cuenta con la aprobación de la dirección de la empresa. Ver (anexo A).

Figura 8 Estructura de la Política del almacén KATALINDA SHOES

Fuente: Autores del Proyecto

4.3.1 Alcance del SGSI

El Sistema de Gestión para la Seguridad de la Información para la empresa "KATALINDA SHOES" aplica a toda la empresa, y a todos sus trabajadores. La empresa reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la misma.

Se hace necesario el establecimiento de las políticas de seguridad de la información que protejan, preserven y administren correctamente la información de la empresa "KATALINDA SHOES", junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

CONCLUSIONES

Nos encontramos en una era donde la tecnología ha permeado la mayoría de actividades cotidianas como conocer productos, hacer compras, comunicarnos; estas interacciones y transacciones deben tenerse en cuenta al momento de implantar soluciones tecnológicas en una organización de manera que incorporemos la seguridad como un elemento fundamental. La empresa "Katalinda shoes" está posicionada como una de las más grandes comercializadoras de calzado de Ocaña, gracias a un crecimiento jalonado en gran parte, por el acercamiento a los clientes a través de redes sociales y sistemas de información. La presente investigación demuestra la importancia de la planeación de unas medidas de seguridad para cualquier organización. En una primera etapa se obtuvo un diagnóstico a partir de varias auditorías llevadas a cabo en el último año, analizando tanto a las personas y procesos de gestión de la información, como a los componentes técnicos y tecnológicos involucrados en dicha gestión.

A partir de los hallazgos que surgieron en las diferentes auditorías, se procedió a analizar detalladamente los controles y objetivos de control adecuados al entorno particular de la empresa, para esto se contrastó lo establecido en la norma ISO 27001 y la ISO 27002. La primera proporciona un modelo para establecer, implementar, operar, monitorear, revisar y mejorar un Sistema de Gestión de Seguridad de la Información, proporcionando adicionalmente, un anexo con el listado de los dominios, los objetivos de control y los controles; la 27002 ofrece un conjunto de recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

A partir de esto, se formalizó en un documento de políticas de seguridad el compendio de controles requeridos para estar mejor preparados en la empresa ante cualquier situación que pueda afectar la imagen, la presencia en redes sociales o los activos de la organización; teniendo como finalidad proteger las características primarias de la información: confidencialidad, integridad y disponibilidad.

BIBLIOGRAFÍA

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. (06 de 04 de 2006). *NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001*. Bogotá: l Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Avila, M. F. (s.f.). *Gestion Empresarial*. Recuperado el 09 de 2015, de Gestion Empresarial: https://gestionempresarial4.wordpress.com/174-2/

Camelo, L. (s.f.). *Seguridad de la Información en Colombia*. Obtenido de Seguridad de la Información en Colombia: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html

Dhole, D. (s.f.). *blog-top com*. Obtenido de blog-top com: http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

E-CENTRO. (s.f.). *E-CENTRO.* Recuperado el 29 de 11 de 2014, de E-CENTRO: http://centrodeartigo.com/articulos-enciclopedicos/article_80922.html

Gómez Vieites, Á. (s.f.). *wikipedia*. Recuperado el 29 de 2014 de 2014, de wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

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

Pérez, Y. M. (s.f.). *Universidad Francisco de Paula Santander -UFPS.* Obtenido de Universidad Francisco de Paula Santander -UFPS: http://www.ufps.edu.co/ufps/atencionalciudadano/pdf.php?pdf=http://www.ufps.edu.co/ufpsnuevo/archivos/UFPS_Politica_de_seguridad_de_la_informacion.pdf

Públicas, M. d. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España: Ministerio de Hacienda y Admnistraciones Públicas.

SCRIBD. (s.f.). *https://es.scribd.com.* Recuperado el 28 de 11 de 2014, de https://es.scribd.com: https://es.scribd.com/doc/245012580/Normas-Iso-27000

Velasquez, P. T. (s.f.). *Modulo de Inducción* . Ocaña : www.ufpso.edu.co, 2012.

ANEXOS

ANEXO A: Políticas de Seguridad de la información para el almacén KATALINDA SHOES

TABLA DE CONTENIDO

1. ALCANCE

El Sistema de Gestión para la Seguridad de la Información para la empresa "KATALINDA SHOES" aplica a toda la empresa, y a todos sus trabajadores. La empresa reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la misma.

Se hace necesario el establecimiento de las políticas de seguridad de la información que protejan, preserven y administren correctamente la información de la empresa "KATALINDA SHOES", junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

2. SEGURIDAD DE LOS RECURSOS HUMANOS

Los siguientes controles están orientados a reducir los riesgos de error humano, comisión de ilícitos en el área de tecnológica y de sistemas contra el uso inadecuado de instalaciones.

2.1 ANTES DEL EMPLEO

2.1.1 Se verificarán los antecedentes de todos los candidatos a un empleo en KATALINDA SHOES como parte de los criterios de selección de acuerdo con las leyes, reglamentación y ética pertinentes.

2.1.2 Como parte de sus términos y condiciones iniciales de empleo, los empleados deberán conocer firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de KATALINDA SHOES.

2.2 DURANTE EL EMPLEO

2.2.1 Se desarrollará planes de capacitación de Seguridad de la Información, los cuales se realizarán periódicamente, mínimo una capacitación por semestre.

2.2.2 Todos los empleados de KATALINDA SHOES, y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la misma,

recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la seguridad de la información.

2.2.3 Todos los empleados serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

2.2.4 Los empleados de KATALINDA SHOES, al momento de tener conocimiento directo o indirecto sobre una debilidad de seguridad, son responsables de registrar y comunicar las mismas al jefe inmediato del almacén.

2.3 TERMINACIÓN Y CAMBIO DE EMPLEO

2.3.1 Cuando un empleado se retire del almacen KATALINDA SHOES, el encargado eliminará el usuario y los privilegios de acceso correspondientes al empleado y debe hacer entrega del inventario de activos, credenciales de acceso a su cargo entre otros.

3. GESTIÓN DE ACTIVOS

3.1 RESPONSABILIDAD POR LOS ACTIVOS

3.1.1 Los activos de información de KATALINDA SHOES serán identificados, clasificados y valorados para establecer los mecanismos de protección necesarios.

3.1.2 Se debe brindar a los líderes de proceso y a los encargados de cada almacén las herramientas tecnológicas y complementarias que permitan la administración del inventario garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

3.2 MANEJO DE MEDIOS

3.2.1 El funcionario se compromete a asegurar física y lógicamente los activos a su cargo a fin de no poner en riesgo la información KATALINDA SHOES contenida en el mismo.

3.3 TRATAMIENTO DE LA INFORMACIÓN DE TITULARES

3.3.1 Garantizar al titular, el derecho del habeas data.

3.3.2 Almacenar la información de forma segura impidiendo la adulteración, pérdida, consulta o acceso no autorizado.

4. CONTROL DE ACCESO

4.1 REQUISITOS DEL ALMACÉN KATALINDA SHOES PARA EL CONTROL DE ACCESO

4.1.1 Para una efectiva gestión de la seguridad de la información resulta de vital importancia, restringir los accesos y garantizar la adecuada utilización de los recursos informáticos.

4.1.2 Cada empleado y funcionario es responsable de los mecanismos de control de acceso que le sean proporcionados.

4.2 GESTIÓN DE ACCESO DE USUARIOS

4.2.1 Para la consulta de documentos y recursos cargados en el Sistemas de Información se establecerán privilegios de acceso a los funcionarios de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Jefe Inmediato.

4.2.2 El jefe del almacén KATALINDA SHOES, mantendrá y publicará los procedimientos de administración de cuentas de usuario para el uso de servicios.

5. SEGURIDAD FÍSICA Y DEL ENTORNO

5.1 ÁREAS SEGURAS

5.1.1 La protección física se llevará a cabo mediante la creación de diversas barreras o perímetros de seguridad en las instalaciones del área tecnológica y demás instalaciones administrativas que contengan información confidencial o crítica.

5.1.2 Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico y protección los que serán determinados por el jefe del alamacen, a fin de permitir el acceso sólo al personal autorizado.

5.1.3 Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas generales en materia de sanidad y seguridad.

5.2 EQUIPOS

5.2.1 El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

5.2.2 El equipamiento estará protegido y respaldado con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía funcionará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

5.2.3 El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

5.2.4 Disponer de pólizas de protección de equipos actualizadas.

5.2.5 Se establecerá un plan de mantenimiento preventivo para los equipos y velará por el cumplimiento del mismo.

5.2.6 La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento o los medios de almacenamiento que contengan material sensible.

5.2.7 Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal del almacén el cual debe estar capacitado en las políticas de seguridad y las responsabilidades personales en el uso y administración de la información Institucional.

5.3 ESCRITORIO Y PANTALLA LIMPIA

5.3.1 Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir

los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

5.3.2 Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

5.3.3 Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

6. SEGURIDAD DE LAS OPERACIONES

6.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

6.1.1 Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el jefe de KATALINDA SHOES.

6.1.2 El líder de la división de Sistemas controlará que los cambios en los componentes operativos no afecten la seguridad de los mismos ni de la información que soportan.

6.1.3 Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

6.1.4 Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

6.2 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

6.2.1 No se permite la desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por el jefe del almacén KATALINDA SHOES.

6.2.2 No se permite escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código diseñado para auto replicarse, dañar o afectar el

desempeño de cualquier dispositivo o infraestructura tecnológica de la Universidad.

6.3 COPIAS DE RESPALDO

6.3.1 Los medios que alojan copias de seguridad deben estar correctamente conservados de acuerdo a las políticas y estándares definidos por el jefe del almacén KATALINDA SHOES.

6.3.2 Se elaborará copias de seguridad diarias a los sistemas de información y las guardará en sitios bajo llave.

6.3.3 Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

7. GESTION DE INCIDENTES

Eventos aleatorios, causados por el hombre o por la naturaleza, previsibles o no, tales como el terrorismo, terremotos, fallas de la tecnología, entre otros, pueden generar interrupciones a la Universidad en la entrega de productos y servicios. La posibilidad de que se presenten estos eventos, unido a la extrema dificultad para su predicción, incentiva desde hace muchos años a las organizaciones a que establezcan lineamientos para la gestión de continuidad del negocio, con el fin de seguir entregando sus productos y servicios a un nivel aceptable. Que permitirá

- Responder a los incidentes de manera sistemática, eficiente y rápida.
- Estar preparado ante la materialización de incidentes inesperados con el fin de volver a la normalidad en poco tiempo.
- Evitar al máximo la pérdida de información y de activos relacionados con el tratamiento, procesamiento y almacenamiento de la misma.
- Trabajar continuamente por mejorar en la gestión y tratamiento de incidentes.
- Generar una base de conocimientos sobre Incidentes.
- Evitar en lo posible, incidentes repetitivos.

7.1 REPORTES DE INCIDENCIAS DE SEGURIDAD INFORMÁTICA.

Se debe comunicar cualquier incidencia a los directivos y diligenciará un formato donde quede consignados los datos de reporte del incidente y de la persona que reportó:

REPORTE DE INCIDENTES
Datos del reporte de incidencia • Número • Fecha • Hora • Descripción del incidente • Efectos Producidos • Responsable del activo afectado • Causas del incidente (se diligencia, una vez se recupere la normalidad del proceso afectado)
Datos del reportante: • Nombre • Cargo • Dependencia • Correo

7.1.1 Todos los funcionarios que son usuarios de los sistemas y servicios de información deben anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.

7.1.2 Para determinar el alcance, el encargado de Seguridad de la Información puede hacerse las siguientes preguntas:

- ¿Cuántos equipos fueron comprometidos?
- ¿Qué es lo que está en riesgo?
- ¿Se encuentran en riesgo aplicaciones críticas?
- ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
- ¿Hay otros equipos con la misma vulnerabilidad?

7.1.3 Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.

7.1.4 La **contención,** evitará que el incidente siga produciendo daños. La **erradicación** eliminará la causa del incidente y todo rastro de los daños y la **recuperación**, consiste en volver el entorno afectado a su estado original. Para llevar a cabo estas acciones, se tendrán que contar con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva. Para contar con una buena estrategia tengamos en cuenta estos agentes:

- Daño potencial de recursos a causa del incidente
- Necesidad de preservación de evidencia
- Tiempo y recursos necesarios para poner en práctica la estrategia
- Efectividad de la estrategia total o parcialmente
- Duración de las medidas a tomar
- Criticidad de los sistemas afectados

- Características de los posibles atacantes
- Si el incidente es de conocimiento público
- Pérdida económica
- Posibles implicancias legales
- Relación costo-beneficio de la estrategia
- Experiencias anteriores

7.2 CONSTITUCIÓN POLÍTICA DE COLOMBIA:

- **Artículo. 61**.- El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.
- **Ley 23 de 1982** Establece los derechos de autor.
- **Ley 1266 de 2008** (Habeas Data)
- **Ley 1273** Delitos Informáticos
- **Ley 1581** Protección de datos personales
- **Ley 488 de 1998** Se elimina el ajuste integral por inflación fiscal para los inventarios, ingresos, costos y gastos. Por expresa disposición del artículo 14 de la mencionada ley, estos cambios tienen efectos contables.
- Plan único de cuentas
- Decreto 2193 aplicativo SIHO
- Normas de auditoría generalmente aceptadas NAGA
- Decreto 2193 del MDPS
- **ISO 27002:** Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

REFERENCIAS DE LAS POLITICAS

Gobierno en Linea, M. d. (2011). *Lineamientos para la implementación del modelo de seguridad de las información.* Bogotá.

ISO 27001:2013. Sistemas de gestión de Seguridad en la Información– Requerimientos.

ISO 27001:2005. Sistemas de gestión de Seguridad en la Información– Requerimientos.

ISO/IEC 133351: 2004. Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones

ISO/IEC TR 133353: 1998. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI .

ISO/IEC 133354: 2000. Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas.

ISO 14001:2004. Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso.

ISO/IEC TR 18044:2004.Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información.

ANEXO B: Evaluación de la Misión y Visión

Misión

No.	CRITERIOS	PREGUNTAS	SI	NO	OBSERVACIÓN
1	Clientes	¿Quiénes son los clientes?	x		
2	Productos y servicios	¿Cuáles son los servicios o productos más importantes?	x		
3	Mercados	¿Compite geográficamente?	x		
4	Tecnología	¿Cuál es la tecnología básica?		x	
5	Preocupación por supervivencia, crecimiento y rentabilidad	¿Cuál es la actitud de la organización en relación con metas económicas?	x		
6	Filosofía	¿Cuáles son las creencias básicas, los valores, las aspiraciones, las prioridades éticas de la organización?		x	
7	Concepto de sí misma	¿Cuáles son las ventajas competitivas claves?	x		
8	Preocupación por la imagen pública	¿Cuál es la imagen pública a que aspira? , ¿Es responsable socialmente, ante la comunidad y el medio ambiente?		x	
9	Preocupación por los empleados	¿Son los empleados un valor activo para la organización? ¿Pone atención a los deseos de las personas claves, de los grupos de interés?	x		

Visión

No	CRITERIOS	SI	NO	OBSERVACIONES
1	¿Orientada al futuro incluso en su redacción?	x		
2	¿Es integradora?	x		
3	¿Es corta (Puede tener una descripción amplia)?		x	
4	¿Es positiva y alentadora?	x		
5	¿Es realista-posible?	x		
6	¿Es consistente con los principios y valores de la Organización?	x		
7	¿Orienta la transición de lo que es a lo que debe llegar a ser?	x		
8	¿Expresa claramente los logros que se esperan en el período?	x		
9	¿Cubre todas las áreas actuales y futuras de la organización?	x		
10	¿Está redactada en términos que signifiquen acción?	x		
11	¿Tiene fuerza e impulsa a la acción?	x		
12	¿Contiene el futuro visualizado?	x		
13	¿Es el sueño alcanzable a largo plazo?	x		

ANEXO C: Evaluación del nivel de Madurez de CMMI

Nivel 1. Tecnología de Información y Comunicación (TIC)

	Entrevista	Observado	Promedio
Adquirir y mantener infraestructura tecnológica	1,6		1,29
Decisiones de adquisición	3	3	

Sistema configurado para realizar prueba / instalación	1	1	
Requerimientos de ambiente físico	1	0	
Actualizaciones de estándares de tecnología	2	1	
Requerimiento de monitoreo de sistema	1	1	
Conocimiento de la infraestructura	2	2	
OLAs planeadas inicialmente	1	1	
Adquirir recursos de TI	3		2,3
Requerimientos de administración de la relación con terceros	3	2	
Artículo provisto	3	2	
Arreglos contractuales	3	3	
Garantizar la continuidad del servicio	0,83		0,83
Resultados de la prueba de contingencia	0	0	
Criticidad de puntos de configuración de TI	1	1	
Plan de almacenamiento de respaldos y de protección	2	1	
Umbrales de incidente / desastre	1	1	
Requerimientos de servicios contra desastres incluyendo roles y responsabilidad	1	1	
Reportes de desempeño de los procesos	0	1	
Garantizar la seguridad de los sistemas	1		1
Definición de incidentes de seguridad	1	1	
Requerimiento específico de entrenamiento sobre conciencia de seguridad	2	2	
Reportes de desempeño del proceso	0	0	
Cambio de seguridad requeridos	1	1	
Amenazas y vulnerabilidad de seguridad	1	1	
Administración del ambiente físico	2		2
Reportes de desempeño de procesos	2	2	

Promedio escala de madurez en las TIC			1,5

ANEXO D: Papeles de trabajo de la auditoria

OBJETIVO. Evaluar el grado de satisfacción de los servicios virtuales ofrecidos por la empresa KATALINDA.

INSTRUMENTO A APLICAR. Encuesta

TIPO DE PRUEBA.

Cumplimiento X **Sustantiva __** **Doble finalidad __**

PROCEDIMIENTO A APLICAR.

1. Aplicar encuestas a usuarios de la redes sociales

RECURSOS

Humanos. Usuarios redes sociales katalinda

Materiales. Formato virtual de encuesta, Equipo Portátil.

HALLAZGOS

- ✓ La empresa KATALINDA cuenta con el servicio de mercadeo y venta virtual de sus productos y podemos determinar que este es un valor agregado con que hoy cuenta la empresa.

- ✓ Se puede determinar que falta más actualización de permanente de sus productos en la página oficial de la empresa enlas redes sociales.

CAUSAS

La falta de recurso humano con labores específicas y exclusivas de mantener la actualización de las páginas.

SITUACION DE RIESGO QUE GENERAN

- ✓ Menores ventas.
- ✓ Desconocimiento oportuno de impacto de un producto nuevo.
- ✓ Acumulación de inventarios.

RECOMENDACIONES.

- ✓ Definir y asignar recurso humano con labores específicas en el manejo de las páginas de las redes sociales.
- ✓ Contratar un servicio de asesoría externa en marketing virtual.
- ✓ Establecer un procedimiento ágil y eficaz para la atención virtual de sugerencia y pedidos de los productos de la empresa.

FECHA DE REALIZACIÓN

Parte 1. 12 y 13 de Septiembre de 2014
Parte 2. 15 y 16 de Septiembre de 2014

ELABORADO POR	**REVISADO POR**
Ingeniero de Sistemas. Sneider Torrado Contadora Pública. Ana Cueto	Administrador de Empresas. Yesid Quintana

Auditores Auxiliares	Auditor Líder

Fecha: 20/09/2014	**ENTREVISTA**	Entrevistada: Lisney Criado Vergel

No.	Pregunta
Organizacionales	
1	¿Teniendo en cuenta la estructura organizacional de la empresa, conoce usted en qué nivel se encuentra? Rta/ Soy la gerente y estoy en la cabeza del organigrama, por lo tanto recae sobre mí la responsabilidad de toda la empresa.
2	¿Teniendo en cuenta que los empleados no están capacitados en el manejo de sistemas, quién realiza el mercadeo y venta virtual? Rta/ Yo misma lo hago, eso se me ha dificultado un poco ya que cuando llegan al almacén muchos clientes, tengo que atenderlos y al mismo tiempo estar pendiente de las redes sociales.
Tecnológicos	
3	¿Sí la empresa crece rápidamente, tiene algún tipo de control en cuanto al software comercial? Rta/ Claro que sí, como han aumentado tanto las ventas a través de la redes sociales, he pensado en mandar a realizar un sitio web con la característica de que los clientes compren por internet, es decir incursionar en el comercio electrónico.

ELABORADO POR	REVISADO POR
Ingeniero de Sistemas. Sneider Torrado Contadora Pública. Ana Cueto Auditores Auxiliares	Administrador de Empresas. Yesid Quintana Auditor Líder

Fecha: 17/09/2014	**LISTA DE CHEQUEO**

No.	Pregunta	Si	No
Organizacionales			
1	¿La empresa tiene definida una estructura organizacional?	x	
2	¿Cuenta con una misión la empresa?	x	
3	¿Cuenta con una visión la empresa?	x	
4	¿Se tiene definido el organigrama de la empresa?	x	
5	¿Existe un proceso de de gestión tecnológica?		x
6	¿El proceso de gestión tecnológica se encuentra documentado, aprobado y publicado?		x
7	¿Cuenta la empresa con un área de sistemas?		x
8	¿Existe en el Manual de funciones de la empresa, funciones específicas de sus empleados al proceso de gestión tecnológica como parte de apoyo a los procesos de compra y ventas?		x
9	¿Existe un manual de conducta o disciplinario de los funcionarios?	x	
10	¿Disponen de empleados capacitados en el manejo de sistemas?		x
11	¿Existe una persona responsable en la empresa del proceso de gestión tecnológica como parte de apoyo a los procesos de compras y ventas?		x
Tecnológicos			
12	¿Se maneja el comercio electrónico en el proceso de compras y ventas de la empresa?	x	
13	¿Dispone la empresa de software comercial para el proceso de apoyo tecnológico a los procesos de compra y ventas?	x	

14	¿Cuenta la empresa con equipos de cómputo y comunicaciones para soportar el proceso tecnológico de apoyo a los proceso de compra venta?	x	
15	¿Dispone de recursos financieros la empresa para el proceso de apoyo tecnológico a los procesos de compra y venta?	x	
16	¿Existe un Manual técnico del manejo del software comercial?		x
17	¿Los equipos de cómputo y comunicaciones reciben mantenimiento periódicamente?		x
18	¿Existe protección del equipamiento eléctrico y cableado de los equipos de cómputo y comunicaciones?		x
19	¿Conocen la empresa sobre normas y leyes que protegen a los usuarios en materia de base de datos y redes sociales?		x
20	¿Cuenta la empresa con un plan objetivo de usuarios y seguidores en redes sociales?	x	
21	¿Existe un manual de usuarios para el manejo de sistemas de información?		x
22	¿Existe un administrador de usuarios de software y páginas oficiales de la empresa?	x	
23	¿La empresa realiza periódicamente copias de seguridad de la información?		x
24	¿Los usuarios de la redes sociales cuentan con un ágil y eficaz repuestas a sus peticiones, pedido y reclamos?	x	
25	¿Se mantiene actualizada la página oficial de la empresa con los productos nuevos y disponibles para la venta?	x	
26	¿Existe un área física exclusivamente para el proceso tecnológico a los procesos de compra y venta?		x
27	¿El software comercial cuenta con sus respectivas licencias?	x	
Seguridad de la Información			
28	¿Existe una política de seguridad de la información de la empresa?		x
29	¿Se encuentra organizada la seguridad de la información en la empresa?		x
30	¿Se gestionan los activos de información en la empresa?		x
31	¿Se gestiona la seguridad de los recursos humanos en la empresa?	x	
32	¿Se gestiona la seguridad física en la empresa?	x	
33	¿Se controla el acceso lógico a los sistemas de información de la empresa?		x
34	¿Se gestionan las comunicaciones y operaciones de la empresa?	x	

35	¿Se controla la adquisición, desarrollo y mantenimiento de sistemas de la empresa?		x
36	¿Se gestionan los incidentes de seguridad de la empresa?		x
37	¿Dispone de planes de continuidad del negocio de la empresa?		x
38	¿Se identifican y cumplen requisitos legales, contractuales de seguridad de la información?		x
Legales			
39	¿Se tienen identificados los requerimientos legales del negocio?	x	
40	¿Se cumple la ley de protección de datos personales?		x
41	¿Se cumple la ley de derechos de autor?		x
42	¿Se cumple la ley general de archivo?		x
43	¿Se cumple la ley de comercio electrónico?		x

ELABORADO POR Ingeniero de Sistemas. Sneider Torrado Contadora Pública. Ana Cueto Auditores Auxiliares	**REVISADO POR** Administrador de Empresas. Yesid Quintana Auditor Líder

OBJETIVO. Evaluar la estructura organizacional de la empresa en todos sus procesos misionales verificando el componente tecnológico que apoya los diferentes procesos de la empresa. Igualmente evaluar la seguridad de la información en su componente tecnológico y sus conocimientos sobre asuntos legales de manejo de base de datos y redes sociales de que realiza con mercadeo y comercio virtual la empresa.

INSTRUMENTO A APLICAR. Lista de Chequeo

TIPO DE PRUEBA.

Cumplimiento X **Sustantiva __** **Doble finalidad __**

PROCEDIMIENTO A APLICAR.

2. Solicitar a la persona encargada de la empresa el diligenciamiento de la lista de chequeo.

RECURSOS

Humanos. Lisney Criado Vergel Gerente,
Personal administrativo

Materiales. Formato impreso de la Lista de chequeo, Agenda de notas, Equipo Portátil

HALLAZGOS ORGANIZACIONALES

- ✓ La empresa KATALINDA cuenta con estructura organizacional pero dentro de la misma no existe unas funciones específicas de personal a realizar apoyo tecnológico a los proceso de la empresa.
- ✓ Que la empresa KATALINDA no cuenta con procesos de gestión tecnológico documentado y aprobado.
- ✓ Que la empresa KATALINDA no cuenta en la actualidad con personal capacitado en sistemas.
- ✓ La empresa no cuenta con una persona responsable del proceso de apoyo de gestión tecnológico.

HALLAZGOS TECNOLOGICOS

- ✓ La empresa KATALINDA cuenta hoy en día con un software comercial con licencia pero que no se encuentra un Manual de gestión del mismo de igual manera en la actualidad no se ejecuta ese software como apoyo a los procesos misionales de la empresa.

- ✓ La empresa no cuenta con un plan de mantenimiento a los equipo de cómputo y comunicaciones.

- ✓ No existe un área específica dentro la empresa donde funciones los equipos de cómputo y comunicaciones del mismo.

HALLAZGOS SEGURIDAD DE LA INFORMACIÓN.

- ✓ La empresa KATALINDA no cuenta con una política de seguridad de la información.

- ✓ No cuenta con seguridad física de equipos de cómputo y comunicaciones de la empresa.

HALLAZGOS LEGALES

- ✓ La empresa no tiene conocimiento sobre legislación sobre manejo de base de datos, redes sociales y comercio electrónico.

CAUSAS

- ✓ No contar con una estructura organización definida en su manual con funciones específicas de sus empleados.

- ✓ No tener asignado un espacio físico específico dentro de la empresa para que funcionen los equipos de cómputo y comunicaciones de la empresa.

- ✓ No tener claro el concepto de seguridad de la información.

- ✓ No contar con un plan de capacitación en sistemas de su personal.

- ✓ Falta de capacitación en temas legales sobre manejo de base de datos, comercio electrónico y manejo de redes sociales.

SITUACION DE RIESGO QUE GENERA

- ✓ Desorganización administrativa.
- ✓ Falta de control a los procesos de compras y ventas de la empresa.
- ✓ Posibles problemas legales con usuarios de las redes sociales.
- ✓ Falta de seguridad, integridad y confidencialidad de la información.

RECOMENDACIONES.

- ✓ Definir políticas, procedimientos y estándares de seguridad física y de control de acceso físico.
- ✓ Asignar un espacio físico para el funcionamiento de los equipos de cómputo y comunicaciones de la empresa.
- ✓ Definir claramente en la estructura organizacional de la empresa funciones y responsabilidades específicas en manejo del proceso de gestión tecnológica como apoyo Los procesos de compra y venta.
- ✓ Capacitar al personal asignado con funciones específicas en el manejo de sistemas.
- ✓ Solicitar al proveedor del software comercial el manual de funcionamiento del mismo.
- ✓ Capacitar en temas legales de manejo de base de datos, Uso de Redes sociales a todo el personal involucrado en el manejo de comercito virtual en temas legales.
- ✓ Definir e implementar un Sistema de Gestión de Riesgo de la Información (Políticas, metodologías de identificación, análisis y valoración de riesgos y plan de tratamiento de riesgos).

FECHA DE REALIZACIÓN
20 de septiembre de 2014

ELABORADO POR Ingeniero de Sistemas. Sneider Torrado Contadora Pública. Ana Cueto Auditores Auxiliares	**REVISADO POR** Administrador de Empresas. Yesid Quintana Auditor Líder

OBJETIVO. Verificar la seguridad física donde funcionan los equipos computacionales y de comunicaciones de la empresa katalinda.
INSTRUMENTO A APLICAR. Observación
TIPO DE PRUEBA. **Cumplimiento _ Sustantiva __ Doble finalidad _X_**
PROCEDIMIENTO A APLICAR. 1. Visita a la instalaciones físicas del almacén 2. Mediante la observación verificar en que sitios y en qué condiciones funcionan los equipos computacionales y de comunicaciones de la empresa.
RECURSOS **Humanos.** Personal Administrativo katalinda
HALLAZGOS En la realización de esta prueba se puede determinar que los equipos computacionales de comunicaciones no tienen un espacio físico determinado y adecuado para el buen funcionamiento y seguridad de los mismos.
CAUSAS La falta de asignar un espacio físico dentro las instalaciones de la empresa para el funcionamiento del área.

SITUACION DE RIESGO QUE GENERA

- ✓ Amenaza física de los equipos computaciones y comunicaciones de la empresa.
- ✓ Amenaza de ingreso de personal no autorizado de los equipos computacionales.

RECOMENDACIONES.

- ✓ Definir e implementar un área física dentro de la empresa para el funcionamiento de los equipos computacionales y comunicaciones de la empresa que cuenta con seguridad física y condiciones adecuadas para el recurso humano que labora en la misma.
- ✓ Se debe definir las áreas seguras de la empresa katalinda e implementar controles de seguridad a las mismas contra el acceso no autorizado.
- ✓ Se debe implementar seguridad a los equipos de cómputo.
- ✓ Se deben definir responsables de los equipos de cómputo.
- ✓ Se debe definir procedimientos de control de acceso físico a las instalaciones donde se encuentran los equipos de cómputo.

FECHA DE REALIZACIÓN
11 de Septiembre de 2014

ELABORADO POR	**REVISADO POR**
Ingeniero de Sistemas. Sneider Torrado Contadora Pública. Ana Cueto Auditores Auxiliares	Administrador de Empresas. Yesid Quintana Auditor Líder

YSA OCANA Consulting Team

KATALINDA

OBJETIVO. Verificar la aplicabilidad del software comercial (manager) en los procesos de compra y venta de la empresa.

INSTRUMENTO A APLICAR.

TIPO DE PRUEBA.

Cumplimiento **Sustantiva _X_** **Doble finalidad __**

PROCEDIMIENTO A APLICAR.

1. Validar la integridad de la información de los reportes actuales de los procesos del software comercial de la Empresa Katalinda.

RECURSOS

Humanos. Personal administrativo katalinda.

Materiales. Formato impreso de cada proceso, Equipo Portátil.

HALLAZGOS

La empresa katalinda actualmente cuenta con un software comercial con licencia que cuenta con varia herramientas como inventarios, clientes, proveedores, caja, balance general, estado de resultados.

Que la actualidad la empresa no está aplicando el software (manager) permanentemente en los proceso de compra y venta de la empresa.

CAUSAS

La causa principal es no contar con personal con funciones específicas en el manejo de software que mantenga actualizada la información de entradas y salidas de los proceso de compra y venta de la empresa.

SITUACION DE RIESGO QUE GENERA

- ✓ Falta Control sobre los proceso de compra y venta de la empresa.
- ✓ Falta de manejo en el Control de los inventarios.
- ✓ Desconocimiento de mercancías existentes y faltantes en inventarios.
- ✓ Control deficiente sobre los ingresos, costos y gastos de la empresa.
- ✓ Desconocimiento de los resultados (pérdidas o ganancias del ejercicio)

RECOMENDACIONES.

Definir un cargo con sus funciones y responsabilidades dentro de la empresa que maneje el software comercial de la empresa.

FECHA DE REALIZACIÓN

Parte 1. 12 y 13 de Septiembre de 2014

Parte 2. 15 y 16 de Septiembre de 2014

ELABORADO POR	**REVISADO POR**
Ingeniero de Sistemas. Sneider Torrado Contadora Pública. Ana Cueto Auditores Auxiliares	Administrador de Empresas. Yesid Quintana Auditor Líder