DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA FERRETERÍA ARGENTINA DE LA CIUDAD DE PASTO

MARIBEL JAQUELINE PEREZ

MARIO FERNANDO JURADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA FERRETERÍA ARGENTINA DE LA CIUDAD DE PASTO

MARIBEL JAQUELINE PEREZ
MARIO FERNANDO JURADO

Trabado de grado Esp. Seguridad Informática
Trabajo de grado aplicado

Director: Esp. Martin Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2018

CONTENIDO

pág.

TABLAS

Pág.

Figuras

Pág.

INTRODUCCIÓN

Actualmente la información se ha convertido en uno de los activos más importantes de las empresas, es por esto que se debe preservar la integridad, disponibilidad y confidencialidad de está al ser transmitida, procesada y almacenada. Adicionalmente dada su importancia y el papel que está juega dentro de las empresas, es uno de los activos objetivo más valioso por parte de los delincuentes el cual sufre una gran cantidad de ataques a diario, con diferentes propósitos tales como robo, alteración, perdía parcial o total, lo que conlleva a las empresas, a sufrir grandes pérdidas por estas acciones. Es así como surgen los sistemas de gestión de seguridad de la información que pretende mantener los tres pilares fundamentales de la información dentro de las empresas, permitiendo que la información siempre esté disponible, que esta no sea alterada e interrumpiendo el acceso a esta, por personas no autorizadas.

El sistema de gestión de seguridad de la información, trabaja a través de la filosofía PDCA (*plan-do-check-act*), la cual dice que primero se debe empezar a planear las medidas y controles, para proteger la información, posteriormente se procede a realizar lo planeado luego se debe verificar y evaluar para finalmente actuar y repetir el ciclo, cabe destacar que un SGSI se basa en una mejora continua y constante esto quiere decir que no es necesario implementar lo en su totalidad desde un inicio; puesto que esto puede ser contraproducente para las empresas. El estudio a ejecutarse debe en sus principios realizar un inventario de los activos informáticos, el cual permita evaluar cuáles son los más importes y el lugar que estos tiene dentro de la organización, posteriormente de cada activo informático se deben elegir las variables que se desean evaluar, una vez seleccionadas las variables a evaluar se deben seleccionar los métodos de evaluación, las medidas y herramientas, se procede a realizar el análisis de los resultados y la implementación de los controles pertinentes que permitan corregir las vulnerabilidades y amenazas detectadas, este proceso debe realizarse a través de los SGSI de forma continua y progresiva lo que permitirá a la empresa tener una mejora en la infraestructura IT y su seguridad para así poder resguardar y dar un mejor manejo a la información.

Ferretería Argentina ubicada en la ciudad de Pasto que opera hace 45 años, fundada por el señor José Ávila Díaz (Q.E.D) en 1971. Hoy en día es una empresa reconocida a nivel departamental y nacional mediante la actividad comercial de la distribución de material de construcción, remodelación y artículos para el hogar; su éxito en ventas le ha permitido ganarse en este año el primer lugar frente a otras ferreterías de la región suroccidental según el estudio de la Revista Fierro, quien año tras año hace un reconocimiento a las empresas que forman parte del sector ferretero. Esta empresa cuenta con dos sedes en la ciudad de Pasto con el propósito

de abrir una tercera en esta misma ciudad, lo cual aporta al desarrollo de la ciudad, así mismo empleo a más de 100 personas. Por su crecimiento, le fue necesario implementar un sistema de información que permita mejorar su servicio a cientos de personas que le visitan y que ayude a automatizar la actividad contable y de inventario; al procesar gran cantidad de información, es estrictamente necesario contar un control en cuanto a la seguridad en este sistema de información que permita blindarlo de cualquier acción que pueda causar un daño irreparable.

El proyecto lo que pretende, es realizar un estudio a la situación actual de la seguridad informática en la Ferretería Argentina, para que a través de su estudio se pueda diseñar un sistema de gestión de seguridad de la información, de esta manera poder realizar las respectivas recomendaciones en cuanto a las amenazas y riesgos que se puedan detectar en este proceso, evitando posibles accesos no autorizados o acciones mal intencionadas que puedan afectar la prestación de servicios en la empresa.

TÍTULO

“DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA FERRETERÍA ARGENTINA DE LA CIUDAD DE PASTO”

LÍNEA DE INVESTIGACIÓN

Trabajo de aplicación en infraestructura y tecnología.

1. DESCRIPCIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La Ferretería Argentina es una empresa dedicada a la comercialización de productos para la construcción y remodelación, atendiendo las necesidades de la región sur occidental del país, la cual en los últimos años se ha modernizado sistematizando algunos de sus procesos, ésta se encuentra ubicada en la ciudad de Pasto, actualmente cuenta con dos sedes en la misma ciudad, comunicándose a través de un servicio de internet haciendo uso de ip publica, debido a esto se genera inseguridad en las transacciones que se realizan a diario siendo una arquitectura cliente/servidor, esta comunicación se puede definir como insegura al no ser encriptada sin hacer uso del protocolo VPN, poniendo en riesgo la información que es uno de los activos más importantes de esta empresa, en la toma de decisiones. Es importante mencionar que hasta la fecha Ferretería Argentina no cuenta con un sistema de gestión de seguridad de la información, el cual le permita detectar a partir de los diferentes controles, posibles riesgos, amenazas y vulnerabilidades que afecten la integridad, disponibilidad y confiabilidad de la información, ocasionando perdida de fidelización de sus clientes, así mismo su posicionamiento y ganancias que se han logrado año tras año.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un sistema de gestión de seguridad de la información apoyado en las normas ISO 27001 e ISO 27002 versión 2013, ayudaría a mejorar la calidad de los procesos que se llevan a cabo diariamente, salvaguardando la integridad, disponibilidad y confidencialidad de la información en la Ferretería Argentina?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información para la Ferretería Argentina, mediante las normas ISO 27001 e ISO 27002 versión 2013, con el fin de detectar las amenazas y vulnerabilidades, para finalmente recomendar los controles pertinentes que mejoren la seguridad de la información.

2.2 OBJETIVOS ESPECÍFICOS

- Recolectar la información de activos informáticos, procesos y servicios soportados por TI.
- Realizar el análisis y evaluación de riegos desde la metodología seleccionada.
- Verificar los controles existentes en la norma ISO 27002 que mejor se adecuen a la Ferretería Argentina.
- Diseñar el sistema de gestión de la seguridad de la información que soportará los procesos que se llevan a cabo en la Ferretería Argentina.
- Presentar el diseño del SGSI a los directivos de la Ferretería Argentina para su evaluación y posterior implementación.

3. JUSTIFICACIÓN

La implementación y el aprovechamiento de la tecnología mediante el uso de sistemas de información en las organizaciones, ha logrado mejorar cada uno de sus procesos internos, haciendo que estos sean más eficientes, obteniendo respuestas oportunas, lo cual permite tomar decisiones frente a los resultados que arroja el sistema de información. Es por ello que es necesario asegurar los activos informáticos que en una organización se utilizan para ejecutar los diferentes procesos, haciendo uso de los sistemas de gestión de seguridad de la información SGSI, estos ayudan a la infraestructura tecnológica IT de forma transversal a toda organización implementando buenas prácticas, ya que su principal función es salvaguardar estos activos, evitando la extracción de información importante por parte de personas malintencionadas, fallas en los dispositivos de almacenamiento, o en casos extremos la pérdida total de este activo, causando por fuerza mayor a un cierre parcial de la organización por ende recayendo sobre ella grandes desventajas frente a la prestación de servicios.[1]

Ferretería Argentina en los últimos años ha ido sistematizado cada uno de los procesos que se llevan a cabo, mejorando considerablemente el servicio prestado a sus clientes, lo que ha causado que se posicione como una de las mejores ferreterías a nivel regional, sin embargo desde que este proceso se ha venido implantando la empresa ha descuidado la seguridad de la información procesada por los sistemas informáticos, esto puede generar alguna desventaja frente a la competencia, la cual puede aprovechar las fallas ocasionadas por la carencia de sistemas seguros. La falta de seguridad puede ocasionar pérdida parcial o total de información, sustracción de información crítica tal como es proveedores, precios, promociones, estrategias de mercadeo entre otros.

Es por esto que el presente proyecto pretende diseñar un SGSI, el cual ayude a detectar las fallas, vulnerabilidades y riesgos los cuales pongan en peligro los activos informáticos de la Ferretería Argentina, mediante las normas ISO 027001 e ISO 27002 con el fin de determinar el impacto de estos proponiendo los controles pertinentes que mitiguen esta falencia.

[1] Véase el interesante capítulo de Manuel Castells sobre la economía informacional y el proceso de globalización en su obra La era de la información: CASTELLS, Manuel. La economía información y el proceso de globalización (cap. 5). En La Era de la Información: Economía, Sociedad y Cultura, vol. I. Madrid: Alianza Editorial, 1997, p. 93-178.

4. ALCANCE Y DELIMITACIÓN

En el presente proyecto se realizó un estudio en cada una de las áreas que pertenecen a la empresa y posteriormente se diseñó un SGSI, este SGSI se enfocó en los procesos de:

- Ventas y facturación
- Nomina
- Copias de seguridad
- Mantenimiento e instalación de equipos.
- Soporte de sistemas.
- Monitoreo de cámaras.
- Red de datos cableada
- Red de datos wifi

Para ello se aplicó la metodología Magerit para el proceso de análisis y evaluación de riesgos y los estándares ISO/IEC 27001 e ISO/IEC 27002 para el diseño del SGSI.

5. METODOLOGÍA

5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación del proyecto es descriptivo, ya que precisa las características más importantes de seguridad de la información y se obtiene datos completos y exactos; por lo tanto, el proyecto toma las medidas necesarias para la protección contra errores y vulnerabilidades de la seguridad informática, teniendo en cuenta cada fase del proceso.

5.2 PARADIGMA Y ENFOQUE DE INVESTIGACIÓN

5.2.1 Paradigma. Este proyecto es de tipo cuantitativo porque gracias a las escalas de medición, las técnicas estadísticas y el análisis de datos; se determina el grado de confidencialidad, confiabilidad e integridad de la información. Para obtener un conocimiento lo más objetivo posible del estado de la seguridad de informática y de la información de la Ferretería Argentina.

5.2.2 Enfoque. El enfoque para este proyecto es el empírico analítico, según Restrepo (1999. p. 8)[2] Empírico se refiere a la denominada investigación científica clásica, que consiste en plantear situaciones problemáticas a partir de hipótesis de trabajo para demostrarlas, además busca el dominio y conocimiento a través de la experiencia y se interesa por controlar y predecir los hechos que se estudian para ser modificados. Y analítico ya que gracias a los resultados obtenidos es posible implementar las políticas necesarias en la empresa. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

De acuerdo a esto se tomarán en cuenta las experiencias propias de los usuarios en el manejo de los diferentes activos informáticos presentes en la Ferretería Argentina y el análisis de los procedimientos que se llevan a cabo por parte de los

[2] RESTREPO, María Consuelo. Producción de textos educativos: Ediciones Bogotá D.C; Colombia. Pág. 8 .ISBN: 978-958-20-0850-4.

usuarios del sistema con el fin establecer las vulnerabilidades, amenazas y riesgos a los que se encuentra expuesto.

5.3 POBLACIÓN Y MUESTRA

5.3.1. Población. La población para este proyecto son todos los usuarios que interactúan con el sistema de información de Ferretería Argentina de acuerdo con la infraestructura tecnológica. La Tabla 1 describe la relación de usuarios del sistema.

Tabla 1 Población.

TALENTO HUMANO	VINCULADOS
Gerente	1
Administrador sede	1
Administrador de sistemas	1
Contadores públicos	4
Trabajo social	1
Auxiliar de costos	1
Compras	1
Auxiliar de compras	1
Salidas y entradas de mercancía interna	2
Auxiliar de sistemas	2
Inventario	2
Recepción	4
Cajeros	17
TOTAL ASISTENCIAL	38

Fuente: Los autores del proyecto

5.3.2 Muestra. El proyecto usa un muestreo intencional, ya que permite realizar una selección de usuarios de acuerdo al grado de experiencia y conocimiento en la empresa, para así obtener una información veraz y precisa, esta técnica es subjetiva ya que se encuentra sujeta al criterio de la persona que a través de su experiencia dentro de la empresa ayuda a seleccionar la muestra más indicada y representativa, este método es conveniente usar cuando la población no es muy grande como es el caso del proyecto.

5.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para el proyecto se hace uso de diferentes instrumentos de recolección de información entre los que se encuentran:

- **Observación directa**: Haciendo uso de este instrumento se observan características, condiciones, conductas y actividades en la empresa. En Ferretería Argentina se implementará esta técnica para colocarse en contacto con los sistemas de información existentes, y con las personas responsables de la información.

- **Entrevistas:** Se hace uso de este instrumento con la finalidad de obtener mayor información que puede ser brindada por parte de diferentes usuarios que interactúan con los procesos que se ejecutan en la empresa, posteriormente ejecutar el respectivo análisis.

- ***Check-List*:** En el proyecto se implementa este instrumento como técnica de verificación de conformidades y no conformidades en el manejo de la seguridad de la información en la Ferretería Argentina.

5.5 SECUENCIA DE ACTIVIDADES

A continuación se describe el plan de trabajo que se siguió para la ejecución del proyecto, éste se presenta en la Tabla 2 como se indica.

Tabla 2 Tabla de secuencia

ACTIVIDADES LÓGICAS ANTERIORES	ACTIVIDADES PLANIFICADAS			ACTIVIDADES LÓGICAS POSTERIORES
	ORDEN	DETALLE	DURACIÓN EN SEMANAS	
-	A	Visita y reconocimiento a la empresa	1	B

ACTIVIDADES LÓGICAS ANTERIORES	ACTIVIDADES PLANIFICADAS			ACTIVIDADES LÓGICAS POSTERIORES
	ORDEN	DETALLE	DURACIÓN EN SEMANAS	
A	B	Identificar la información y procesos de la empresa	1	C
B	C	Estudio de metodología para el análisis de riesgos y vulnerabilidades	1	D
C	D	Realizar análisis de riesgos y vulnerabilidades	2	E
D	E	Revisión documental del estándar ISO 27001 y ISO 27002	1	F
E	F	Diseñar los instrumentos de recolección de información	1	G
F	G	Aplicar los instrumentos de recolección de información	1	H
F, G	H	Elaborar la matriz de amenazas, riesgos, impacto y vulnerabilidades de la seguridad de la información	1	I
F,G,H	I	Analizar los resultados obtenidos de los papeles de trabajo aplicados a la empresa.	2	J
I	J	Determinar los controles apropiados para mitigar los riesgos, vulnerabilidades y amenazas	2	K
J,K	K	Realizar recomendaciones y planes de mejoramiento para la Ferretería Argentina	1	-

Fuente: Los autores del proyecto.

6. MARCO DE REFERENCIAL

6.1 ANTECEDENTES

Para llevar a cabo el desarrollo de este proyecto es necesario conocer proyectos que de una u otra forma tengan relación con este, para tener de cierta forma un precedente que ayude con su buena realización.

- **"SEGURIDAD EN INFORMATICA (AUDITORÍA DE SISTEMAS)"** Este proyecto se presentó por: LUIS DANIEL ALVARES BASALDÚA en México ayudara en el desarrollo del presente proyecto, ya que da una visión global de los pasos y recursos necesarios para el estudio de la seguridad informática en diferentes aspectos de un sistema de informático, con este trabajo se fundamentara el análisis a realizar en la Ferretería Argentina.

- **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE SEGURIDAD DE INFORMACIÓN EN PROCESOS TECNOLÓGICOS"** Este proyecto se presentó por: BARRANTES PORRAS CARLOS EDUARDO y HUGO HERRERA JAVIER ROBERTO en Lima – Perú, este trabajo ayudara a contextualizar y obtener criterios para realizar el análisis y posteriormente la implementación del SGSI en la Ferretería Argentina, dando una visión global de este trabajo sobre las áreas IT de las organizaciones.

- **"METODOLOGÍA DE IMPLANTACIÓN DE UN SGSI EN UN GRUPO EMPRESARIAL JERÁRQUICO"** Este proyecto fue presentado por: GUSTAVO PALLAS MEGA en Montevideo – Uruguay, este proyecto dará una visión de cómo se debe realizar la implementación de un SGSI a través de los diferentes niveles de la organización, para así poder proteger y optimizar los procesos informáticos que mejoren la seguridad de la Ferretería Argentina.

- **"DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO"** Este trabajo de grado fue presentado por: CARLOS ALBERTO GUZMAN SILVA, este proyecto ayuda a comprender la importancia y el uso de la norma ISO 27001 dentro de los procesos de implementación de un SGSI, en la Ferretería Argentina.

- **"DISEÑO DE UN MANUAL DE PROCEDIMIENTOS DEL SISTEMA CONTABLE EN LA EMPRESA FEVECOMEX S.A.S. BASADO EN LA NORMA TECNICA COLOMBIANA PARA LA SEGURIDAD DE LA INFORMACION NTC-ISO/IEC 27001/2006"** Este proyecto se presentó en la Universidad de

Cartagena por: ADRIANA PAOLA POLANCO VELEZ, este proyecto ayudara en el proceso de realizar la debida documentación para la implantación del SGSI, dentro de la Ferretería Argentina de tal forma que sea más eficiente y fácil.

- **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO".** El presente proyecto presentado por: ROBERT MARCELO TABANGO y YESID CAMILO GUERRERO está enfocado en un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño, ya que la información es un factor clave de éxito y por lo tanto su eficiente administración garantiza altos estándares de calidad y productividad. El proyecto ayudará en la aplicación de la metodología de la norma ISO 27001 e ISO 27002.

6.2 MARCO TEÓRICO

- **ISO 27000:** La ISO2700 es una familia de normas relacionadas con la seguridad informática, esta puede ser certificada; si se habla en específico de la ISO2700 se hace referencia a la certificación de dar el primer acercamiento hacia el resto de normas y es la base para el las demás; sus principales características son:

- ✓ Visión general de la familia de normas
- ✓ Introducción a los SGSI.
- ✓ Comprensión y definición de la familia de normas ISO 2700.
- ✓ Descripción del proceso de mejora continúa

- **ISO 27001:** Es primera en la familia de normas ISO27000, es la encargada de dar los lineamientos para establecer, implementar mantener y mejorar un SGSI o sistema de gestión de seguridad de la información y sus principales características son:

- ✓ Definición del alcance del SGSI
- ✓ Definición de una Política de Seguridad
- ✓ Definición de una metodología y criterios para el Análisis y Gestión del Riesgo
- ✓ Identificación de riesgos
- ✓ Evaluación de los posibles tratamientos del riesgo
- ✓ Elaboración de un Declaración de Aplicabilidad de controles y requisitos
- ✓ Desarrollo de un Plan de Tratamiento de Riesgos

- ✓ Definición de métricas e indicadores de la eficiencia de los controles
- ✓ Desarrollo de programas de formación y concienciación en seguridad de la información
- ✓ Gestión de recursos y operaciones
- ✓ Gestión de incidencias
- ✓ Elaboración de procedimientos y documentación asociada

- **ISO 27002:** Dentro de la familia de normas ISO 27000 lo referente a la norma ISO 27002 es el tratamiento de los riesgos informáticos a partir de buenas prácticas las cuales incluyen una medida de 133 controles que permiten gestionar los activos informáticos con sus respectivos riesgos. Dentro de esta norma encontramos 14 capítulos que guían en las buenas prácticas de seguridad relacionada con las siguientes áreas.

- ✓ Políticas de Seguridad de la Información
- ✓ Organización de la Seguridad de la Información
- ✓ Seguridad relativa a los recursos humanos
- ✓ Gestión de activos
- ✓ Control de acceso
- ✓ Criptografía
- ✓ Seguridad física y del entorno
- ✓ Seguridad de las operaciones
- ✓ Seguridad de las comunicaciones
- ✓ Adquisiciones, desarrollo y mantenimiento de los sistemas de información
- ✓ Relación de proveedores
- ✓ Gestión de incidentes de seguridad de la información
- ✓ Aspectos de seguridad de la información para la gestión de la continuidad de negocio
- ✓ Cumplimiento

- **SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN:** Un sistema de gestión de seguridad de la información, es una serie de pasos y reglamentos que permiten a las organizaciones mejorar la disponibilidad, integridad y confidencialidad de la información que se maneja al interior de estas, todo esto a través del buen uso de sus activos tecnológicos, el SGSI se basa en el principio de una mejora continua, ya que para poder implementar uno de estos es necesario hacerlo de una forma poco agresiva, evitando que se afecte el funcionamiento de las organizaciones, pero a su vez se debe realizar de forma continua y mejorando, esto es gracias al PDCA (*plan-do-check-act*), es decir que un SGSI debe ser coincidido desde la planeación, luego la implementación, la supervisión y la mejora. Dentro de los principales estándares para el diseño e

implementación de un SGSI en las organizaciones se encuentra la ISO 27000, esta es una familia de normas que presentan una serie de pasos, recomendaciones y metodologías para poder implementar un SGSI de forma adecuada y efectiva.

- **METODOLOGIAS DE ANÁLISIS Y EVALUACIÓN DE RIESGOS:** Dentro de las metodologías de análisis y evaluación de riesgos, más reconocidas a nivel mundial se encuentran las siguientes:

- ✓ Mehari
- ✓ Octave
- ✓ ISO/IEC 27005
- ✓ Magerit

Para el desarrollo del presente proyecto se hace uso de la metodología Magerit, ya que es una de las más famosas, esto es gracias a su forma fácil de implementarla dentro de las organizaciones, ésta se basa en la evaluación de los riesgos y amenazas que pueden vulnerar las integridad, disponibilidad y confidencialidad de la información, Magerit en primer lugar se centra en la realización de un inventario de todos los activos tecnológicos que influyen en el tratamiento de los riesgos, una vez realizado el análisis y estudio de riesgos, se debe tratar con el riesgo residual, el cual ayuda a las organización a re-evaluar, si las amenazas y los riesgos persisten, cabe destacar que estas metodologías de análisis y evaluación de riesgos son una parte fundamental para poder implementar una SGSI, ya que sin ellas sería imposible evaluar el progreso de estos.

6.3 MARCO CONCEPTUAL

- **RIESGO INFORMÁTICO:** El riesgo informático es la probabilidad estadística de que una amenaza producida por una vulnerabilidad se produzca, además se debe medir la ocurrencia del suceso mediante un periodo de tiempo para determinar su frecuencia, esto debe incluir el impacto de este suceso dentro de los activos informáticos, ya sea evaluando directamente la información afectada o los dispositivos que la gestionan. Es de vital importancia dentro de los riesgos informáticos determinar directamente cual es la amenaza que lo puede producir ya que las empresas deben evaluar la frecuencia de ocurrencia de esta y su impacto dentro de las organizaciones para contemplar así la posibilidad de implementar controles cobre esta amenaza que ayuden a prevenir, detectar o minimizar este riesgo.

Es importante considerar los riesgos dentro de las organizaciones, especialmente los riesgos informáticos ya que la infraestructura IT este inmersa dentro de la mayoría de los procesos llevados a cabo en las organizaciones de una forma transversal, y un riesgo informático puede afectar los procesos llevados a cabo dentro de las organizaciones.

- **VULNERABILIDAD:** Una vulnerabilidad se puede decir que es una falla dentro de un activo informático el cual afecte la integridad, confidencialidad y disponibilidad de la información. Este activo puede ser tanto software como hardware además cabe desatacar que una vulnerabilidad puede atacar también un control implementado para mitigar los riesgos informáticos.

  En la actualidad las grandes empresas de IT están combatiendo las amenazas mediante la publicación de las vulnerabilidades detectadas para que sean corregidas, esto se da ya que los ciberdelincuentes aprovechan las vulnerabilidades provocadas por fallos de fabricación, los cuales pueden ser comprados en una especie de mercado negro con el fin de vulnerar las organizaciones y sacar provechos económicos de esto. Tal es el caso de los *hackers* que hurtaron cientos de herramientas informáticas usadas para explotar vulnerabilidades por la NSA y las pusieron e subasta para que ciberdelincuentes puedan comprar y así usarlas con fines personales. Uno de los tipos de vulnerabilidades más conocidas en la actualidad es la *ZERO-DAY*, esta vulnerabilidad consiste en un fallo de fabricación ya sea de un software o un hardware el cual es publicado y aun así las empresas desde el momento de la publicación de esta vulnerabilidad no la combaten permitiendo que los ciberdelincuentes saquen provecho de esto desde el momento de su publicación afectando así a las organizaciones. También cabe destacar que las personas hacemos parte de los activos informáticos ya que somos las personas encargadas de manejar los recursos y los dispositivos, de esta forma en la actualidad ha surgido el concepto de ingeniería social la cual es una vulnerabilidad que ataca a las personas y afecta los activos informáticos de las organizaciones.

  Con el desarrollo del presente trabajo La Ferretería Argentina de la ciudad de pasto se verá beneficiada ya que asegurará sus procesos y así la información que estos manejan ayudando a mantener su actual posición en el mercado mejorando así los proceso presentando un mejor servicio a la clientela, además entrara en un proceso de mejora continua.

- **AMENAZA:** Se considera amanezca a todo lo que pone en riesgo algún hecho, este término llevado a la seguridad informática tiene un contexto muy importante

dado que una amenaza es algo que puede poner en riesgo la confidencialidad, integridad y confidencialidad de la información, en la actualidad existen muchas amenazas que alteran la seguridad, desde las amenazas naturales como por ejemplo incendios, fallas en construcción, inundaciones hasta amenazas provocadas por delincuentes.

6.4 MARCO LEGAL

El presente trabajo tiene como sustento legal las normas establecidas por el estado colombiano, en lo que se refiere a seguridad informática como es la ley 1273 de 2009, las cuales reglamentan el uso de datos personales y protege la información de las organizaciones en Colombia.

En concordancia con la anterior ley y sus respectivos artículos se respetó ante todo la integridad de los datos y privacidad de la información que se manejada en la Ferretería Argentina de la ciudad de Pasto, de no ser así los especialistas encargados de llevar a cabo el estudio se regirán a los castigos en la norma contemplados.

6.5 MARCO METODOLÓGICO

Para el presente proyecto se hace uso del estándar ISO 27000 y para el análisis de riesgos se implementa Magerit, con el uso de estas metodologías, se realiza un desarrollo íntegro permitiendo de esta forma mejorar la seguridad de la Ferretería Argentina mediante el diseño del Sistema de Gestión de Seguridad de la Información, que según los directivos se implementara o no.

8. RESULTADOS ESPERADOS

Una vez diseñado el Sistema de Gestión de Seguridad de la Información, se espera que la Empresa Ferretería Argentina lo implemente con el fin de que los procesos que se realiza por parte del personal no se vean afectados por algún tipo de incidencia asociada a problemas de seguridad, además se espera que se ejecuten diferentes auditorias con el fin de mejorar el SGSI mediante el proceso de mejora continua.

9. RECURSOS

9.1 RECURSOS HUMANOS

Este proyecto se llevará a cabo por los ingenieros de sistemas MARIBEL JAQUELINE PÉREZ PORTILLO identificada con C.C 1.087.414.445 de Túquerres y MARIO FERNANDO JURADO SANCHEZ identificado con C.C 1.085.266.387 de Pasto, en la Tabla 3 se describen tanto la cantidad de tiempo empleado en el proyecto y el personal requerido.

Tabla 3 Personal

No.	Descripción	Cantidad	Valor/hora	Total
2	Ingeniero de sistemas.	400 h	15000	$ 6’000.000
	TOTAL	400 h	15000	$ 6’000.000
Fuente: Los autores del proyecto.				

*Este valor incluye prestaciones sociales.

9.2 RECURSOS TECNOLOGICOS

El proyecto requiere de los elementos tecnológicos consignados en la Tabla 4 para su desarrollo.

Tabla 4 Recursos Tecnológicos.

Cantidad	Descripción
1	Computador HP Envy
1	Computador Asus
1	Cámara Fotográfica
1	Impresora
1	USB Kingston 8 Gb
1	Software Ms Office 2013
1	Conexión a internet
1	Quemador de DVD
Fuente: Los autores del proyecto.	

9.3 RECURSOS MATERIALES

La Tabla 5 describe la cantidad de materiales requeridos para el desarrollo del proyecto.

Tabla 5 Recursos Materiales

Cantidad	Descripción
2	Resma de Papel tamaño carta
2	Dvd
3	Tonners de tinta
4	Lapiceros
Fuente: Los autores del proyecto.	

9.4 RECURSOS FINANCIEROS

La Tabla 6 presenta los gastos financieros del presente proyecto, los cuales serán asumidos en su totalidad por los estudiantes.

Tabla 6 Presupuesto

Descripción	Total
Personal	$6’000.000
Materiales	$270.000
Equipos	$1’950.000
Imprevistos (10%)	$822.000
Total	$9’110.000
Fuente: Los autores del proyecto	

*El valor de este proyecto será asumido en su totalidad por los realizadores de esta investigación.

A continuación se presenta en la Tabla 7, la relación de materiales usados para la ejecución del presente proyecto.

Tabla 7 Materiales

Cantidad	Descripción	Valor/Unitario	Total
2	Resma de Papel tamaño carta	$11.000	$22.000
5	DVD	$1.A con000	$5.000
4	Tonners de tinta	$60.000	$240.000
3	Lapiceros	$1.000	$3.000
	TOTAL		**$270.000**
Fuente: los autores del proyecto.			

Por otra parte se realiza un inventario de los equipos necesarios para la ejecución del proyecto, este está consolidado en la Tabla 8-

Tabla 8 Equipos

Cantidad	Descripción	Valor Unitario	Total
1	Alquiler Computador HP Pavilon dv5	$1’000.000	$1’000.000
1	Alquiler Grabadora tipo periodista	$400.000	$400.000
1	Alquiler Cámara Fotográfica	$400.000	$400.000
1	Alquiler Impresora	$80.000	$80.000
1	USB de 8 Gb	$20.000	$20.000
1	Conexión a internet	$30.000	$30.000
1	Quemador de DVD	$20.000	$20.000
	TOTAL		**$1’950.000**
Fuente: los autores del proyecto.			

10. CRONOGRAMA

Tabla 9 Cronograma

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
Visita y reconocimiento a la empresa												
Identificar la información y procesos de la empresa												
Estudio de metodología para el análisis de riesgos y vulnerabilidades												
Realizar análisis de riesgos y vulnerabilidades												
Revisión documental del estándar ISO 27001 y ISO 27002												
Diseñar los instrumentos de recolección de información												
Aplicar los instrumentos de recolección de información												
Elaborar la matriz de amenazas, riesgos, impacto y vulnerabilidades de la seguridad de la información												
Analizar los resultados obtenidos de los papeles de trabajo aplicados a la empresa.												
Determinar los controles apropiados para mitigar los riesgos, vulnerabilidades y amenazas												
Realizar recomendaciones y planes de mejoramiento para la Ferretería Argentina												

Fuente: Los autores del proyecto

11 DESARROLLO PROPUESTA

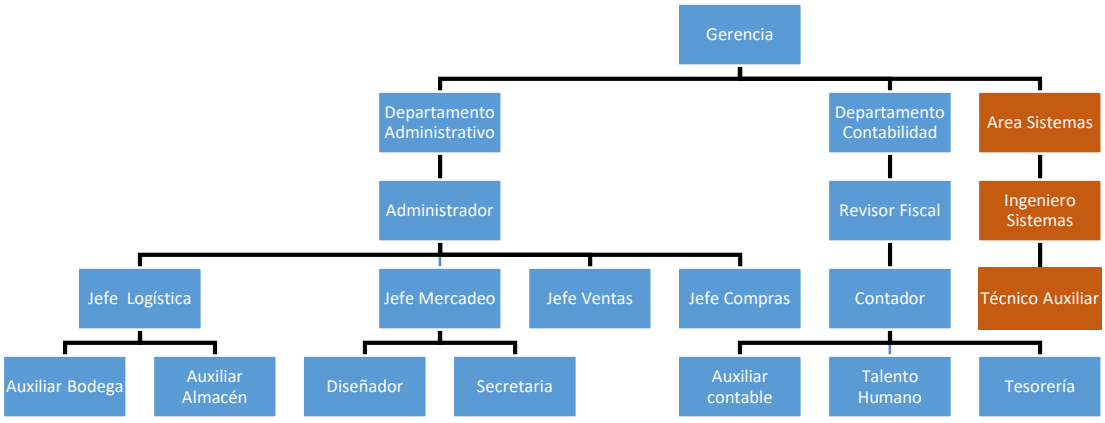
11.1 VISITA Y RECONOCIMIENTO A LA EMPRESA

- **Ubicación:** Avenida Bolívar Cll 22 # 1-140
- **Actividad comercial:** Venta de material para construcción y remodelación
- **Reseña histórica de la organización:** Más de cuarenta años en el sector hacen parte de la experiencia, que desde 1971 se fundó en la Ciudad de Pasto. Ferretería Argentina de la Avenida Bolívar es un hipermercado, con amplia zona de cargue y descargue, parqueadero para 70 vehículos, amplio espacio en el almacén para mejor comodidad de nuestra distinguida clientela. Su inauguración se llevó a cabo en 2007 y hoy forma parte de una ferretería de gran formato.

  Esta empresa envuelve una historia de más 45 años en el mercado. La necesidad de proveer herramientas, materiales de construcción, productos agrícolas y de ebanistería se convirtió en una oportunidad que fue evolucionando en el crecimiento de esta empresa. En la actualidad sus líneas de productos enmarcan un portafolio de 10 mil referencias.

11.2 ORGANIGRAMA

Figura 1 Organigrama



Fuente: Los autores del proyecto.

La figura 1 describe la organización administrativa de la ferretería argentina Pasto, con cada una de las áreas con sus respectivas dependencias a cargo.

11.3 ESTUDIO DE METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES

- **MAGERIT:** En la actualidad existen muchas metodologías para el análisis y gestión de riesgos, entre las más importantes destacan metodologías tales como magerit u octave, las cuales se enfocan a realizar un análisis profundo de los riesgos que pueden afectar la seguridad informática, algo que resalta dentro de estas metodologías es la actividad de realizar una inventario de los activos con los cuales cuentan las organizaciones, este inventario debe ser objetivo y solo se debe incluir los activos que se involucran con el manejo de la información y la seguridad, otro aspecto importante dentro de las metodologías de análisis de riesgos, es el riesgo residual, ya que el objetivo es mejorar la seguridad e una forma continua siempre se debe volver a evaluar los activos y sus riesgos para así poder comprender si estos aún están en riesgo.

  Las metodologías de análisis de riesgos ayudan a las organizaciones de una forma trasversal, ya que mediante estas se puede descubrir y analizar los riesgos potenciales que pueden poner en peligro la integridad, disponibilidad y confidencialidad de la información, sabiendo que este es uno de los activos más importantes dentro de toda organización, ya que la información y su buen manejo pueden llevar al éxito dentro de las organizaciones, también es claro destacar que gracias a estas metodologías se puede realizar una mejora continua de la seguridad mitigando los riesgos principales, a medida que con el tiempo se cubre la mayoría de estos. [3]

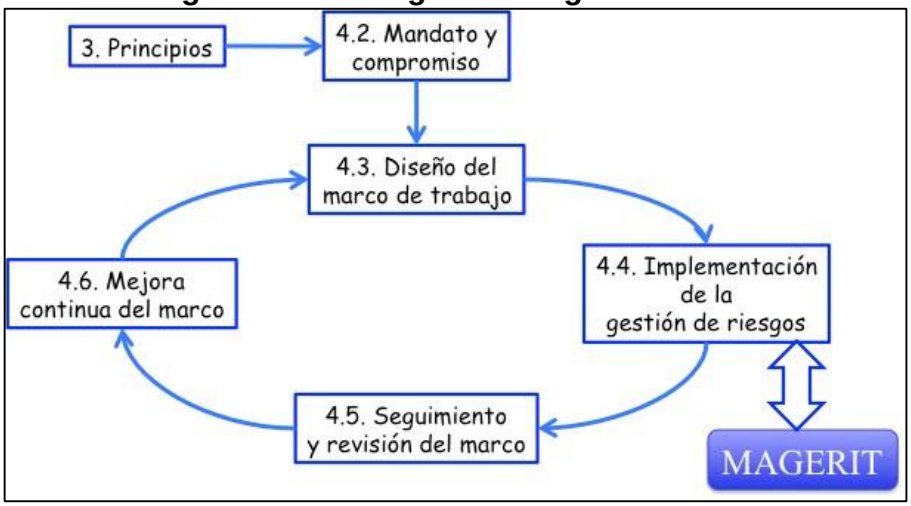
  Para el desarrollo del presente proyecto se hará uso de la metodología Magerit, ya que es una de las más famosas, esto es gracias a su forma fácil de implementarla dentro de las organizaciones, ésta se basa en la evaluación de los riesgos y amenazas que pueden vulnerar las integridad, disponibilidad y confidencialidad de la información, Magerit en primer lugar se centra en la realización de un inventario de todos los activos tecnológicos que influyen en el tratamiento de los riesgos, una vez realizado el análisis y estudio de riesgos, se debe tratar con el riesgo residual, el cual ayuda a las organización a re-evaluar, si las amenazas y los riesgos persisten, cabe destacar que estas metodologías de análisis y evaluación de riesgos son una parte fundamental para poder

[3] Ministerio de Administraciones Públicas. Madrid (2006). MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información IMétodo. Disponible en: http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

implementar una SGSI, ya que sin ellas sería imposible evaluar el progreso de estos.

11.3.1 Proceso. MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo, con esto se puede garantizar que la metodología se ha implementado de forma correcta dentro de una empresa. (ver figura 1)

Figura 2 Proceso de gestión de riesgos de Magerit



Fuente: Magerit V3 Libro 1 Pagina 7

11.3.2 Objetivos. La metodología Magerit en la actualidad es implementada por diferentes empresas para la gestión de los riesgos informáticos, este marco de trabajo presenta unos objetivos en los cuales basa su metodología los cuales son.

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

11.3.3 Dimensiones de la seguridad. El marco de trabajo presentado por Magerit se basa en la evaluación de las diferentes dimensiones de la seguridad, a través de estas variables la metodología permite realizar una evaluación a conciencia la cual permite determinar el nivel de riesgos en que se encuentra la organización, las dimensiones de la seguridad contempladas por Magerit son:

- **Disponibilidad:** esta dimensión contempla la importancia de la disponibilidad de cada uno de los activos evaluados dentro de la metodología, y el impacto o riesgo que la ausencia de estos ´pueda ocasionar en el funcionamiento correcto de la organización, esta es una de las dimensiones más importantes ya que existen activos que deben permaneces siempre disponibles para que la empresa u organización tenga un funcionamiento adecuado.

- **Integridad:** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, por personas de la entidad o ajenas a ella. Manteniendo la información tal y como se generó.

- **Confidencialidad:** es la garantía de que la información llegue únicamente a las personas que se autorice, la información debe ser protegida para que no sea divulgada sin consentimiento del personal que tenga acceso a ella.

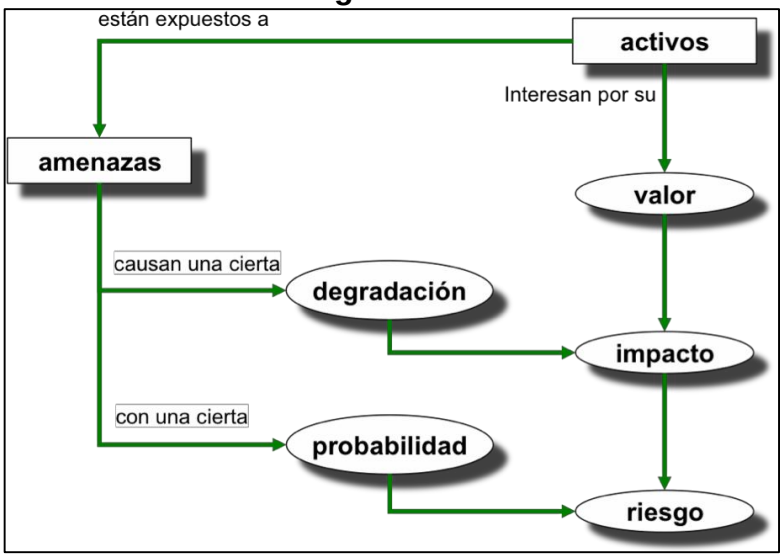
Se puede decir que las 3 anteriores dimensiones son las principales y las que siempre se deben evaluar en el marco de trabajo, sin embargo se pueden añadir dos dimensiones que permiten realizar un mejor estudio de los riesgos y la percepción que tienen de ello los usuarios como lo son: temas de información:

- **Autenticidad:** propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

- **Trazabilidad:** control para determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

11.3.4 Método de análisis de riesgos. El marco de trabajo presentado por Magerit sigue una serie de pasos, los cuales permiten evaluar los riesgos presentados en una organización, esta evaluación se realiza dentro de las dimensiones mencionadas anteriormente, además se presentan de forma ordenada y sistemática como se observa en la siguiente imagen.

Figura 3 Método de análisis de riesgos



Fuente: Magerit V3 Libro 1 Pagina 22

11.4 IMPLEMENTACIÓN DE MAGERIT DENTRO DE LA FERRETERÍA ARGENTINA DE PASTO

11.4.1 Paso 1: Activos. Para comenzar a realizar un análisis de riesgos de forma adecuada Magerit plantea como primer paso la clasificación de los activos, entendemos por activo un bien, un derecho o cualquier recurso conformado en la empresa, además Magerit permite clasificar cada uno de estos activos mediante una nomenclatura especial, la cual permite una gestión de forma más sencilla para un posterior análisis de estos. A continuación se presenta la Tabla 10 de clasificación de activos para Magerit.

Tabla 10 Clasificación de Activos Metodología Magerit

Tipo de activo		Corresponde
Nomenclatura	**Nombre**	
[D]	Datos	Copias de seguridad, archivos
[S]	Servicios	Funciones del área de sistemas que satisface a los usuarios

Tipo de activo		Corresponde
Nomenclatura	**Nombre**	
[SI]	Soporte de información	Material impreso
[SW]	Software	Aplicaciones, programas
[HW]	Hardware	Equipos que soportan la información
[COM]	Redes de comunicación	Servicios en comunicación
[AUX]	Equipamiento auxiliar	Equipos que permiten el soporte de información pero no están relacionados con los datos
[L]	Instalaciones	Espacios donde se encuentran los equipos y la información
[P]	Personal	Cada uno de los usuarios que tienen relación con el sistema de información
Fuente: Los autores del proyecto.		

De acuerdo a esta clasificación se procede a realizar el inventario de la Ferretería Argentina obteniendo como resultado el siguiente inventario.

Servicios [S]

Nomenclatura de clasificación de los servicios [S], en la Tabla 11 se realiza un breve resumen los activos que hacen parte la clasificación de servicios, que se asocian para la Ferretería Argentina.

Tabla 11 Servicios

Código	Magerit		Proceso	Servicio	Responsable
S1	S	www	Página web	Brindar información a los clientes de los productos que se vende en la ferretería	Ingeniera de sistemas
S2	S	PUB	Publicidad	Diseñar todo lo necesario para realizar la publicidad en redes sociales e impresos	Ingeniera de sistemas
S3	S	PUB	Redes sociales	Actualización constante de Instagram y Facebook	Ingeniera de sistemas
S4	S	INT	Soporte	Mantener los equipos de cada una de las dependencias, funcionando correctamente	Ingeniera de sistemas
S5	S	INT	Asesoría en manejo de sw	Asesorar al personal para el manejo un buen manejo de los	Ingeniera de sistemas

Código	Magerit		Proceso	Servicio	Responsable
				diferentes sw que hacen uso.	
S6	S	INT	Asesoría en compra de equipos y sw	Documentación de los equipos a adquirir para elegir el más apropiado y socializarlos con el Gerente	Ingeniera de sistemas
Fuente: Los autores del proyecto.					

Datos [D] y Soportes de información [SI]

Nomenclatura de clasificación de los Datos [D], en la Tabla 12 se realiza un breve resumen los activos que hacen parte la clasificación de datos, que se asocian para la Ferretería Argentina

Tabla 12 Datos

Código	Magerit			Activo de información	Responsable	Disposición final
D01	D		INT	Hoja de vida de equipos de la empresa	Ingeniera de sistemas	Área de sistemas
D02	D	ADM	INT	Copias de seguridad	Ingeniera de sistemas	Ingeniera de sistemas
D03	D		INT	Inventario de cámaras de seguridad	Ingeniera de sistemas	Área de sistemas
D04	D		INT	Publicidad	Ingeniera de sistemas	Jefe de mercadeo
Fuente: Los autores del proyecto.						

Nomenclatura de clasificación de Soporte de Información [SI], en la Tabla 13 se realiza un breve resumen los activos que hacen parte la clasificación de soporte de información, que se asocian para la Ferretería Argentina

Tabla 13 Soportes de información

Código	Magerit			Activo de información	Responsable	Disposición final
SI01	SI		PRINTED	Acta inventario	Ingeniera de sistemas	Área de sistemas
SI02	SI	COM	PRINTED	Acta entrega tablets	Ingeniera de sistemas	Área de sistemas
Fuente: Magerit						

Aplicaciones [SW]

Nomenclatura de Clasificación de las Aplicaciones [SW], en la Tabla 14 se realiza un breve resumen los activos que hacen parte de la clasificación de software, que se asocian para la Ferretería Argentina

Tabla 14 Software

Código	Magerit			Activo de información	Responsable	Disposición final
SW01	SW		OS	Windows Server 2012 R2	Ingeniera de sistemas	
SW02	SW		OS	Windows 10	Ingeniera de sistemas	PC
SW03	SW		OS	Windows 10	Auxiliar de sistemas	PC
SW04	SW		OS	Android	Ingeniera de sistemas	Área Ventas
SW05	SW			Corel Draw	Ingeniera de sistemas	Jefe de mercadeo
SW06	SW		OFFICE	LibreOffice	Ingeniera de sistemas	Recepción
SW07	SW		OFFICE	Microsoft Office	Ingeniera de sistemas	Contabilidad
SW08	SW			Sw Contable	Ingeniera de sistemas	Usuarios
SW09	SW		Backup	Cobian Backup	Ingeniera de sistemas	Ingeniera de sistemas
SW10	SW			Zkteco	Ingeniera de sistemas	Administrador
SW11	SW			Unifi 3.2.1	Ingeniera de sistemas	Ingeniera de sistemas
SW12	SW			Winbox	Ingeniera de sistemas	Ingeniera de sistemas
SW13	SW	STD	AV	Avira Free	Ingeniera de sistemas	PC
SW14	SW	STD	AV	Windows Defender	Ingeniera de sistemas	PC
SW15	SW		OFFICE	Winrar treal	Ingeniera de sistemas	PC
SW16	SW			Google Chrome	Área de sistemas	PC
SW17	SW			Microsoft Remote Desktop	Área de sistemas	
SW18	SW		OFFICE	Acrobat Reader	Área de sistemas	PC
Fuente: Los autores del proyecto.						

Hardware [HW]

Nomenclatura de Clasificación del Hardware [HW], en la Tabla 15 se realiza un breve resumen los activos que hacen parte de la clasificación de hardware, que se asocian para la Ferretería Argentina

Tabla 15 Hardware

Código	Magerit			Descripción	Responsable	Disposición final
HW01	HW	NETWORK	MODEM	Modem	Ingeniera de sistemas	Área de sistemas
HW02	HW	NETWORK	SWITCH	Switch	Ingeniera de sistemas	Área de sistemas
HW03	HW	NETWORK	ROUTER	RouterBoard	Ingeniera de sistemas	Área de sistemas
HW04	HW	NETWORK		AP	Ingeniera de sistemas	Área de sistemas
HW05	HW	MID		Tablet		Área de sistemas
HW06	HW	PC		Computador All in one	Ingeniera de sistemas	Área de sistemas
HW07	HW	PC		Computador An tower	Ingeniera de sistemas	Área de sistemas
HW08	HW	DATA		Servidor hp prolaind xeon	Ingeniera de sistemas	Área de sistemas
HW09	HW	PABX		DVR	Ingeniera de sistemas	Área de sistemas
HW10	HW			Impresora		Área de sistemas
HW11	HW	DATA		Disco duro externo	Ingeniera de sistemas	Ingeniera de sistemas
HW12	HW	PBX		Planta telefónica		
Fuente: Los autores del proyecto.						

Equipamiento auxiliar [AUX], Instalaciones [L], Comunicaciones [COM] y Personas [P]

Nomenclatura de Clasificación del Equipamiento Auxiliar [AUX], en la Tabla 16 se realiza un breve resumen los activos que hacen parte de la clasificación de equipamiento auxiliar, que se asocian para la Ferretería Argentina

Tabla 16 Equipamiento auxiliar

Código	Magerit		Activo de información	Responsable	Disposición final
AUX1	AUX	UPS	UPS	Ingeniera de sistemas	Instalación Ferretería Argentina
AUX2	AUX	CABLING	Cableado estructurado	Ingeniera de sistemas	Instalación Ferretería Argentina
AUX3	AUX	GEN	Planta eléctrica	Ingeniera de sistemas	Instalación Ferretería Argentina
AUX4	AUX	POWER	Fuentes de alimentación	Ingeniera de sistemas	Instalación Ferretería Argentina
AUX5	AUX	TV	Televisores	Ingeniera de sistemas	
Fuente: Los autores del proyecto.					

Nomenclatura de Clasificación Instalaciones [L], en la Tabla 17 se realiza un breve resumen los activos que hacen parte de la clasificación de instalaciones, que se asocian para la Ferretería Argentina

Tabla 17 instalaciones

Código	Magerit		Activo de información	Responsable	Disposición final
L1	L	BUILDING	Instalaciones Avenida Bolívar		
L2	L	LOCAL	Cuarto de seguridad	Ingeniera de sistemas	Instalación Ferretería Argentina
Fuente: Los autores del proyecto.					

Nomenclatura de Clasificación de Comunicaciones [COM], en la Tabla 18 se realiza un breve resumen los activos que hacen parte de la clasificación de comunicación, que se asocian para la Ferretería Argentina

Tabla 18 Comunicaciones

Código	Magerit		Activo de información	Responsable	Disposición final
COM1	COM	INTERNET	Internet	Ingeniera de sistemas	
COM2	COM	LAN	Red local	Ingeniera de sistemas	

Código	Magerit		Activo de información	Responsable	Disposición final
COM3	COM	PSTN	Red telefónica	Ingeniera de sistemas	
Fuente: Los autores del proyecto.					

Nomenclatura de Clasificación de Personas [P], en la Tabla 19 se realiza un breve resumen los activos que hacen parte de la clasificación de personal, que se asocian para la Ferretería Argentina

Tabla 19 personal

Código	Magerit		Activo de información	Responsable	Disposición final
P01	P	UI	Aux de sistemas		
P02	P	UI	Ingeniera de sistemas		
P03	P	UI	Contadora		
P04	P	UI	Aux. contables		
P05	P	UI	Personal de compras		
P06	P	UI	Personal de ventas		
P07	P	UI	Personal de bodega		
P08	P	UI	Personal de almacén		
P09	P	UI	Personal de inventario		
P10	P	UI	Personal logística		
P11	P	UI	Jefes de personal		
Fuente: Los autores del proyecto.					

11.4.2 PASO 2: Valoración de activos. En este paso se realiza la valoración por cada uno de los activos que hacen parte de la empresa Ferretería Argentina y que son de gran importancia. La valoración de activos se realiza a partir de la siguiente tabla en la cual se encuentra descrito cada uno de los tipos de valoración, además esta valoración debe contemplar las 5 dimensiones de la seguridad de la información (disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad).

- **VALORACIÓN CUALITATIVA:** La valoración cualitativa se debe realizar de acuerdo a la Tabla 20, donde se indica la escala con que se evaluaron los activos

de forma cualitativa, esta tabla se basa en magerit y con ella se puede obtener el valor total del activo de información.

Tabla 20 Escala valoración cualitativa

Abreviación	Ocurrencia/t	Expectativa de ocurrencia	Dificultad de ocurrencia
MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy posible	Factible
M	Media	Posible	Media
B	Baja	Poco posible	Difícil
MB	Muy baja	Muy raro	Muy difícil
Fuente: los autores del proyecto			

La valoración de la tabla se debe realizar en cada una de las dimensiones, además se debe realizar respecto a la importancia que tiene cada uno de los activos en su dimensión dentro de la organización, esto quiere decir que se debe responder las preguntas con el fin de dar respuesta y obtener la valoración. Estas preguntas se encuentran en el libro de MAGERIT versión 3.

- ✓ **Confidencialidad:** ¿qué daño causaría que lo conociera quien no debe?
- ✓ **Disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- ✓ **Integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto?
- ✓ **Autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- ✓ **Trazabilidad:** ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

Como ejemplo podemos evaluar cada una de las dimensiones a uno de los activos.

ACTIVO A EVALUAR
WINDOWS SERVER 2012 R2

Dimensión: Disponibilidad

Evaluación: MA

En este caso se asigna un valor de muy alta, ya que si se llega a vulnerar la disponibilidad del sistema operativo del servidor la Ferretería quedaría sin funcionar.

Dimensión: Confidencialidad

Evaluación: MA

En esta ocasión se da el criterio de MUY ALTA, ya que si se llega a fallar la confidencialidad del sistema operativo del servidor se expondría la información crítica del sistema contable.

Dimensión: Integridad

Evaluación: MA

Dado que los datos que se almacenan y procesan en este sistema operativo son de gran importancia, no se debería fallar en esta dimensión ya que podría ser crítico que se llegue a modificar o en tal caso borrar algún dato que se encuentra alojado en el sistema.

Dimensión: Autenticidad

Evaluación: MA

Llevar un control y un buen manejo de las cuentas de usuario junto con sus contraseñas es muy alto y más en el caso del servidor principal, impidiendo con ello el acceso de personas no autorizadas y protegiendo la información y procesos que se pueden llevar en este.

Dimensión: Trazabilidad

Evaluación: MA
Es importante llevar a cabo un control permanente de quien realiza cada una de las acciones dentro del servidor, de esta forma es posible conocer con detalle por medio de logs al momento de una falla en los procesos.

Este tratamiento se realizó con cada uno de los activos obteniendo como resultado lo indicado ver (**Anexo 1 Análisis de riesgos y vulnerabilidades, en la hoja valoración cualitativa).**

- **VALORACIÓN CUANTITATIVA:** Esta valoración de los activos se realiza acorde a la evaluación realizada en el paso anterior, ya que se debe asignar un equivalente numérico a cada uno de los valores asignados por las dimensiones estos valores son tomados de la Tabla 21.

Tabla 21 Escala valoración cuantitativa

Abreviación	Calificación activo	Probabilidad	% ocurrencia
MA	Critico	5	100
A	Importante	4	80
M	Apreciable	3	60
B	Bajo	2	40
MB	Despreciable	1	20
Fuente: los autores del proyecto			

La Tabla 22 ilustra un ejemplo de una valoración, tomando como ejemplo el activo WINDOWS SERVER 2012 R2.

Tabla 22 Ejemplo valoración

Nombre del activo	A	T	C	I	D	Valor promedio	Calificación activo
Windows Server R2	5	5	5	5	5	5	CRITICO
Fuente: los autores del proyecto							

Una vez realizada la evaluación cuantitativa se pasa a promediar y ubicar la importancia del activo en este caso es de valor critico lo que quiere decir que el activo tiene una gran importancia para la empresa, de esta forma se realiza la evaluación de los demás activos obteniendo como resultado los valores de **Anexo 1 Análisis de riesgos y vulnerabilidades, en la hoja valoración cuantitativa.**

11.4.3 PASO 3: Pruebas. Para ejecutar un análisis de riesgos es necesario obtener las pruebas necesarias de las cuales se pueda tener como evidencia las posibles vulnerabilidades que puedan ocasionar algún tipo de amenaza, estas pruebas se realizaron sobre los activos que representan mayor importancia en la empresa, esto se deduce de la valoración de los activos.

Las pruebas realizadas en este apartado no se divulgaran ya que la empresa no autorizo publicar esto, sin embargo se muestra los resultados obtenidos de los cuales se puede inferir las vulnerabilidades a las que se encuentras expuestos cada uno de los activos.

Las pruebas se realizaron sobre los siguientes aspectos

- **RED:** Para medir el nivel de vulnerabilidades en la red de la empresa se hizo uso del software nmap mediante zenmap, wireshark, arpsoof, y algunos sniffers,

estas pruebas evidenciaron vulnerabilidades tales como puertos abiertos, información sin encriptar, red no segmentada, por otra parte no se ha implementado hasta el momento de herramientas de seguridad, como son firewall, IDS que permiten dar un mayor grado de seguridad impidiendo ataques destructivos, además mediante observación directa se pudo evidenciar exposición de los cableado de voz y datos, ausencia de la norma de cableado estructurado TIA/EIA 568.

- **SERVIDOR:** Para medir la seguridad en el servidor se hizo uso de herramientas como zenmap, nessus, openvass, en estos análisis se detectó vulnerabilidades tales como puertos abiertos, ausencia de antivirus, además mediante observación directa y análisis de políticas se encontraron vulnerabilidades como usuarios sin perfiles ni restricciones, información expuesta, información sin encriptar, registro de logs expuestos, configuraciones por defecto.

- **PAGINA WEB:** En este activo se hizo uso del sistema operativo Owasp y de herramientas que permiten analizar un sitio web en busca de fallas en seguridad, las herramientas utilizadas fueron openvass y vega, encontrando como resultado que la página se encuentra expuesta a vulnerabilidades de CRSF, XSS, y además no cuenta con certificados SSL.

- **CONTRASEÑAS:** Mediante el uso de software tal como JHON THE RIPPER se analizó el uso de contraseñas, detectando que los usuarios en muchas ocasiones hacen uso de contraseñas débiles, además mediante observación directa se puede deducir que la empresa no cuenta con políticas para el uso de contraseñas seguras.

- **POLÍTICAS:** La empresa no cuenta con políticas de seguridad, lo cual evidencia que muchos procesos se encuentras expuestos, tales como dar de baja a los usuarios o uso y cambio de contraseñas seguras.

11.4.4 PASO 4: Amenazas. Una amenaza es un elemento o persona capaz de realizar o infringir alguna alteración de un activo en este caso informático, las amenazas aprovechan vulnerabilidades, ya que son estas las que dan la oportunidad de generar una falla en los activos, la cual altere uno o más dominios de la seguridad, las amenazas en este caso tienen un calificación, la cual proviene de la metodología seleccionada en este caso Magerit versión 3.

Para la identificación y evaluación de amenazas a las cuales están expuestos los activos de la Ferretería Argentina, se toma como referencia clasificación que se encuentra en el libro 2 de MAGERIT versión 3. Gracias a esta clasificación el proceso de evaluación de amenazas se facilita, ya que en ella se encuentra

determinado las amenazas que pueden afectar a cada uno de los tipos de activos, a continuación en la tabla 23 se muestra un ejemplo con las amenazas principales que se presentan para el activo WINDOWS SERVER 2012 R2

Tabla 23 Ejemplo tabla de amenazas

CATEGORIA	AMENAZA
ERRORES Y FALLOS NO INTENCIONADOS	[E.2] Errores del administrador
	[E.3] Errores de monitorización (log)
	[E.4] Errores de configuración
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
ATAQUES INTENCIONADOS	[A.3] Manipulación de los registros de actividad (log)
	[A.4] Manipulación de la configuración
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.15] Modificación deliberada de la información
	[A.26] Ataque destructivo
	[A.22] Manipulación de programas
	[A.19] Divulgación de información
Fuente: los autores del proyecto	

La información correspondiente a las amenazas de cada uno de los activos que se encuentran en la Ferretería Argentina está en el **Anexo 1 Análisis de riesgo y vulnerabilidad, en la hoja amenazas y vulnerabilidades.**

11.4.5 PASO 5: Vulnerabilidades. Una vulnerabilidad se pude decir que es una falla dentro de un activo informático el cual afecte la integridad, confidencialidad y disponibilidad de la información. Este activo puede ser tanto software como hardware además cabe desatacar que una vulnerabilidad puede atacar también un control implementado para mitigar los riesgos informáticos.

También cabe destacar que las personas hacemos parte de los activos informáticos ya que somos las personas encargadas de manejar los recursos y los dispositivos, de esta forma en la actualidad ha surgido el concepto de ingeniería social la cual es una vulnerabilidad que ataca a las personas y afecta los activos informáticos de las organizaciones.

A continuación se presenta en la Tabla 24 el análisis de vulnerabilidades de uno de los activos según el análisis realizado en la pruebas, como ejemplo se toma el activo WINDOWS SERVER 2012 R2

Tabla 24 Ejemplo análisis vulnerabilidades

CATEGORIA	AMENAZA	VULNERABILIDADES
ERRORES Y FALLOS NO INTENCIONADOS	[E.2] Errores del administrador	Falta de conocimiento en la administración de servidores Windows
	[E.3] Errores de monitorización (log)	No hay control sobre el acceso de los logs al sistema operativo.
	[E.4] Errores de configuración	Privilegios de usuarios mal asignados debido a la falta de conocimiento del administrador
	[E.15] Alteración accidental de la información	Directorios del servidor no se encuentran configurados adecuadamente
	[E.18] Destrucción de información	Directorios del servidor no se encuentran configurados adecuadamente
	[E.21] Errores de mantenimiento / actualización de programas (software)	No existe una hoja de vida del servidor con los detalles necesarios para llevar a cabo un proceso de mantenimiento y actualización
ATAQUES INTENCIONADOS	[A.3] Manipulación de los registros de actividad (log)	No hay control sobre el acceso de los logs al sistema operativo.
	[A.4] Manipulación de la configuración	Los usuarios no tienen restricción de acceso al sistema.
	[A.5] Suplantación de la identidad del usuario	La creación y control de cuentas no están configurado.
	[A.6] Abuso de privilegios de acceso	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.
	[A.11] Acceso no autorizado	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.
	[A.15] Modificación deliberada de la información	Los usuarios no tienen control sobre las acciones que realizan en el sistema.
	[A.26] Ataque destructivo	El servidor pose una ip pública.
	[A.22] Manipulación de programas	Los usuarios no poseen políticas y perfiles que limiten el uso en el sistema.
	[A.19] Divulgación de información	El sistema pose información crítica que puede ser accedida por los usuarios.
Fuente: los autores del proyecto		

De igual forma se realizó el análisis de todas las vulnerabilidades para cada una de las amenazas de los demás activos, obteniendo como resultado **Anexo 1 Análisis de riesgos y vulnerabilidades, en la hoja amenazas y vulnerabilidades.**

11.4.6 PASO 6: Análisis de riesgos. A continuación se presenta el análisis realizado a las amenazas que afectan la seguridad de la Ferretería Argentina, además de esto se incluye una estimación del impacto sobre cada una de sus dimensiones del activo y una probabilidad de ocurrencia con el fin de determinar los riesgos.

- **ESTIMACIÓN DE IMPACTO:** Como objetivo se pretende conocer el alcance del daño que puede producirse si una amenaza llega a ejecutarse en los activos de la Ferretería Argentina, la estimación del impacto se puede obtener a partir de las Tablas 25 y 26 que son de doble entrada con el fin de obtener los resultados, del impacto que será evaluado por cada una de la amenazas. Para ello se hace uso de una tabla del impacto cualitativa, la cual será transformada a su escala cuantitativa como se indica a continuación.

Tabla 25 Estimación de impacto cualitativo

Impacto		Degradación		
		1	10	100
Valor del activo	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Magerit V3, libro 3, Pag. 6

Tabla 26 Estimación impacto cuantitativo

Impacto		Degradación		
		1	10	100
Valor del activo	MA	3	4	5
	A	2	3	4
	M	1	2	3
	B	1	1	2
	MB	1	1	1

Fuente: Los autores del proyecto.

Critico (5): [MA] Impacta fuertemente en la operatividad de los procesos.
Importante (4): [A] Impacta en la operatividad de los procesos.
Apreciable (3): [M] Impacta en la operatividad del macro proceso.
Bajo (2): Impacta [B] en la operatividad del proceso.

Despreciable (1): [MB] Impacta levemente en la operatividad del proceso

El cálculo del impacto se hace dependiendo la materialización de una amenaza, como ejemplo se toma el activo WINDOWS SERVER 2012 R2 y el resultado es presentado en la Tabla 27.

Tabla 27 Ejemplo evaluación de impacto

Amenazas	Vulnerabilidades	F		D	Impacto		Riesgo
[E.2] Errores del administrador	Falta de conocimiento en la administración de servidores Windows	3	M	10	4	A	A
[E.3] Errores de monitorización (log)	No hay control sobre el acceso de los logs al sistema operativo.	2	B	10	4	A	A
[E.4] Errores de configuración	Privilegios de usuarios mal asignados debido a la falta de conocimiento del administrador	3	M	10	4	A	A
[E.15] Alteración accidental de la información	Directorios del servidor no se encuentran configurados adecuadamente	3	M	10	4	A	A
[E.18] Destrucción de información	Directorios del servidor no se encuentran configurados adecuadamente	3	M	100	5	MA	MA
[E.21] Errores de mantenimiento / actualización de programas (software)	No existe una hoja de vida del servidor con los detalles necesarios para llevar a cabo un proceso de mantenimiento y actualización	3	M	10	4	A	A
[A.3] Manipulación de los registros de actividad (log)	No hay control sobre el acceso de los logs al sistema operativo.	2	B	10	4	A	A
[A.4] Manipulación de la configuración	Los usuarios no tienen restricción de acceso al sistema.	3	M	10	4	A	A
[A.5] Suplantación de la identidad del usuario	La creación y control de cuentas no están configurado.	2	B	10	4	A	A
[A.6] Abuso de privilegios de acceso	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.	4	A	100	5	MA	MA
[A.11] Acceso no autorizado	Los usuarios no poseen perfiles que limiten el	4	A	100	5	MA	MA

Amenazas	Vulnerabilidades	F		D	Impacto	Riesgo
	acceso acorde a sus funciones.					
[A.15] Modificación deliberada de la información	Los usuarios no tienen control sobre las acciones que realizan en el sistema.	3	M	1	3	B	B
[A.26] Ataque destructivo	El servidor pose una ip pública.	3	M	100	5	MA	MA
[A.22] Manipulación de programas	Los usuarios no poseen políticas y perfiles que limiten el uso en el sistema.	2	B	100	5	MA	MA
[A.19] Divulgación de información	El sistema pose información crítica que puede ser accedida por los usuarios.	3	M	10	4	M	M
Fuente: Los autores del proyecto							

El análisis completo de cada uno de los activos se encuentra en **Anexo 1 Análisis de riesgos y vulnerabilidades, en la hoja amenazas y vulnerabilidades.**

- **ESTIMACIÓN DE LA PROBABILIDAD:** El objetivo consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir (a mayor número de vulnerabilidades, mayor probabilidad de ocurrencia de las amenazas), para ello se hace uso de la Tabla 28 la cual se basa en Magerit y fue adaptada al proyecto:

Tabla 28 Frecuencia materialización de amenazas

1	Raro	**MB**	Puede ocurrir una vez cada 2 años.
2	Muy baja	**B**	Al año.
3	Baja	**M**	En 6 meses.
4	Media	**A**	Al mes.
5	Alta	**MA**	A la semana.
Fuente: Los autores del proyecto			

En la Tabla 29 se visualiza el impacto y la frecuencia de materialización cada una de las amenazas sobre el activo ejemplo.

ACTIVO:
WINDOWS SERVER 2012 R2
Degradación: 100%

Impacto: 5 (Critico)
Tipo: Software [SW]

Tabla 29 Ejemplo frecuencia

CATEGORIA	AMENAZA	VULNERABILIDADES	Frecuencia [F]	
ERRORES Y FALLOS NO INTENCIONADOS	[E.2] Errores del administrador	Falta de conocimiento en la administración de servidores Windows	MEDIO	3
	[E.3] Errores de monitorización (log)	No hay control sobre el acceso de los logs al sistema operativo.	BAJO	2
	[E.4] Errores de configuración	Privilegios de usuarios mal asignados debido a la falta de conocimiento del administrador	MEDIO	3
	[E.15] Alteración accidental de la información	Directorios del servidor no se encuentran configurados adecuadamente	MEDIO	3
	[E.18] Destrucción de información	Directorios del servidor no se encuentran configurados adecuadamente	MEDIO	3
	[E.21] Errores de mantenimiento / actualización de programas (software)	No existe una hoja de vida del servidor con los detalles necesarios para llevar a cabo un proceso de mantenimiento y actualización	MEDIO	3
ATAQUES INTENCIONADOS	[A.3] Manipulación de los registros de actividad (log)	No hay control sobre el acceso de los logs al sistema operativo.	BAJO	2
	[A.4] Manipulación de la configuración	Los usuarios no tienen restricción de acceso al sistema.	MEDIO	3
	[A.5] Suplantación de la identidad del usuario	La creación y control de cuentas no están configurado.	BAJO	2
	[A.6] Abuso de privilegios de acceso	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.	ALTO	4
	[A.11] Acceso no autorizado	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.	ALTO	4
	[A.15] Modificación deliberada de la información	Los usuarios no tienen control sobre las acciones que realizan en el sistema.	MEDIO	3
	[A.26] Ataque destructivo	El servidor contiene una ip pública.	MEDIO	3

CATEGORIA	AMENAZA	VULNERABILIDADES	Frecuencia [F]	
	[A.22] Manipulación de programas	Los usuarios no poseen políticas y perfiles que limiten el uso en el sistema.	BAJO	2
	[A.19] Divulgación de información	El sistema contiene información crítica que puede ser accedida por los usuarios.	MEDIO	3
Fuente: Los autores del proyecto.				

- **ESTIMACIÓN DEL RIESGO:** Para obtener el riesgo de cada uno de los activos es necesario conocer la importancia del impacto, al momento de materializarse una amenaza, y la frecuencia con que se llega a presentar esta amenaza respecto al tiempo. Para esta estimación se hace uso de la Tabla 30 obtenida de Magerit versión 3, aplicando la relación entre probabilidad de ocurrencia, con el impacto de ésta sobre los activos, como resultado se obtiene el riesgo.

Tabla 30 Estimación del riesgo

		Probabilidad				
Riesgo		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	MA	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B
Fuente: Magerit V3, libro 3, Pag. 7						

Para una demostración de este proceso se continúa con el activo que se ha venido tomando WINDOWS SERVER 2012 R2, tabulando los resultados en la Tabla 31.

Tabla 31 Ejemplo estimación del riesgo

Nombre activo	Amenaza	Vulnerabilidades	F		I		R
WINDOWS SERVER 2012	[E.2] Errores del administrador	Falta de conocimiento en la administración de servidores Windows	3	M	4	A	A
	[E.3] Errores de monitorización (log)	No hay control sobre el acceso de los logs al sistema operativo.	2	B	4	A	A
	[E.4] Errores de configuración	Privilegios de usuarios mal asignados debido a la falta de conocimiento del administrador	3	M	4	A	A

Nombre activo	Amenaza	Vulnerabilidades	F		I		R
	[E.15] Alteración accidental de la información	Directorios del servidor no se encuentran configurados adecuadamente	3	M	4	A	A
	[E.18] Destrucción de información	Directorios del servidor no se encuentran configurados adecuadamente	3	M	5	MA	MA
	[E.21] Errores de mantenimiento / actualización de programas (software)	No existe una hoja de vida del servidor con los detalles necesarios para llevar a cabo un proceso de mantenimiento y actualización	3	M	4	A	A
	[A.3] Manipulación de los registros de actividad (log)	No hay control sobre el acceso de los logs al sistema operativo.	2	B	4	A	A
	[A.4] Manipulación de la configuración	Los usuarios no tienen restricción de acceso al sistema.	3	M	4	A	A
	[A.5] Suplantación de la identidad del usuario	La creación y control de cuentas no están configurado.	2	B	4	A	A
	[A.6] Abuso de privilegios de acceso	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.	4	A	5	MA	MA
	[A.11] Acceso no autorizado	Los usuarios no poseen perfiles que limiten el acceso acorde a sus funciones.	4	A	5	MA	MA
	[A.15] Modificación deliberada de la información	Los usuarios no tienen control sobre las acciones que realizan en el sistema.	3	M	2	B	B
	[A.26] Ataque destructivo	El servidor contiene una ip pública.	3	M	5	MA	MA
	[A.22] Manipulación de programas	Los usuarios no poseen políticas y perfiles que limiten el uso en el sistema.	2	B	5	MA	MA
	[A.19] Divulgación de información	El sistema contiene información crítica que puede ser accedida por los usuarios.	3	M	3	M	M

Fuente: Los autores del proyecto

Los riesgos de color rojo y naranja son aquellos que deben ser tratados de inmediato por la empresa, ya que las amenazas debido a su frecuencia pueden llegar a materializarse y provocar mayor deterioro sobre el activo o inactividad en los procesos, esto depende de que activo se pueda ver afectado. En esta ocasión para tratar los riesgos tomaremos como guía estos 2 niveles, por otra parte este análisis se realizó con el resto de amenazas y activos. **Anexo 1 Análisis de riesgos y vulnerabilidades, en la hoja amenazas y vulnerabilidades**

- **EVALUACIÓN DE RIESGOS:** La Tabla 32 presenta el comportamiento que se seguirá para cada activo de información, si el Nivel de Riesgo es despreciable, bajo, el proceso concluye, en caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles necesarios.

Tabla 32 Evaluación de riesgos

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Despreciable	Finaliza el proceso.
Bajo	Finaliza el proceso.
Apreciable	Una de las tres opciones: a. Se transfiere el riesgo por ejemplo tomando un seguro.
Importante	b. Se evita el riesgo retirando el activo de información.
Critico	c. Se reduce o mitiga el riesgo por medio de controles.
Fuente: El presente proyecto	

- **PLAN DE TRATAMIENTO DE RIESGOS:** La tabla 33 presenta el plan de tratamiento de riesgos, en este paso se asignan los respectivos tratamientos de riesgo a las amenazas que se contemplaron anteriormente, eso se hace con el fin de mitigar los riesgos que se encuentran en nivel alto y muy alto, siendo estos los que se deben mitigar lo más pronto.

Tabla 33: plan de tratamiento de riegos

Nombre de Activo	Amenaza	Vulnerabilidad	Riesgo	PTR
REDES SOCIALES	[A.5] Suplantación de la identidad del usuario	Contraseñas débiles	A	Crear políticas para la asignación de contraseñas
PEDIDOS A PROVEEDORES	[A.10] Alteración de secuencia	Omisión de las instrucciones	A	Documentar procesos de capacitación a personal

Nombre de Activo	Amenaza	Vulnerabilidad	Riesgo	PTR
	[E.9] Errores de [re-]encaminamiento	Mensajes enviados a un destino incorrecto	A	Actualización y verificación de correos a destinatarios
	[E.19] Fugas de información	Información confidencial a la competencia	MA	Realizar un contrato de confidencialidad a los empleados
	[E.14] Escapes de información	Información confidencial manejada por ex empleados	A	Realizar un contrato de confidencialidad a los empleados
	[A.5] Suplantación de la identidad del usuario	Descuido de los usuarios	A	Asignar contraseñas a usuarios del SO y disminuir el tiempo de suspensión del equipo
COPIAS DE SEGURIDAD	[I.10] Degradación de los soportes de almacenamiento de la información	Daño en el disco duro de almacenamiento de backups	MA	Realizar copias de seguridad en la nube
	[E.19] Fugas de información	Información expuesta por descuido	A	Encriptación de backups
WINDOWS SERVER 2012 R2	[E.2] Errores del administrador	Configuraciones mal realizadas	A	Capacitación en el manejo de la administración de Windows Server
	[E.3] Errores de monitorización (log)	Archivos logs eliminados	A	Realizar copias de archivos logs
	[E.4] Errores de configuración	Puertos abiertos	A	Cerrar los puertos que no se hacen uso
	[E.15] Alteración accidental de la información	Acceso no autorizado por personal no capacitado	A	Restringir el acceso de personal no autorizado a información confidencial
	[E.18] Destrucción de información	Ataques de virus o troyanos	MA	Implementar antivirus Premium
	[E.21] Errores de mantenimiento / actualización de programas (software)	Actualizaciones sin programar	A	Programar actualizaciones
	[A.3] Manipulación de los registros de actividad (log)	Alteración de los errores	A	Encriptar archivos log y hacer copias de seguridad
	[A.4] Manipulación de la configuración	Configuración sin pruebas	A	Hacer uso de una copia del SO para ejecutar pruebas después de configurar

Nombre de Activo	Amenaza	Vulnerabilidad	Riesgo	PTR
	[A.5] Suplantación de la identidad del usuario	Inicio de sesiones abiertas	A	Asignar contraseñas a usuarios del SO y disminuir el tiempo de suspensión del equipo
	[A.6] Abuso de privilegios de acceso	Usuarios no limitados en sus funciones	MA	Configurar privilegios de usuarios
	[A.11] Acceso no autorizado	Acceso no controlado de los usuarios al sistema	MA	Configurar privilegios de usuarios
	[A.26] Ataque destructivo	Ataques de rasomware, virus, troyanos	MA	Mantener copias de seguridad constantes del sistema operativo
	[A.22] Manipulación de programas	Instalación de software indebido en el servidor	MA	Restringir la instalación de software a personal no autorizado
COREL DRAW	[A.8] Difusión de software dañino	Descarga de software ilegal	A	Verificar la integridad del software a instalar
SIIGO	[E.1] Errores de los usuarios	Personal no capacitado	A	Capacitar al personal en el uso de SIIGO
	[E.2] Errores del administrador	Parametros mal configurados	MA	Capacitar al administrador en el manejo de SIIGO
	[E.15] Alteración accidental de la información	Datos ingresados de forma incorrecta	A	Capacitar al personal en el uso de SIIGO
	[E.21] Errores de mantenimiento / actualización de programas (software)	Problemas al actualizar	MA	Mantener copias de seguridad de SIIGO
	[A.6] Abuso de privilegios de acceso	Usuarios sin restricción	MA	Parametrización de usuarios dependiendo sus funciones
	[A.15] Modificación deliberada de la información	Extracción de información confidencial	A	Realizar un contrato de confidencialidad a los empleados
	[E.24] Caída del sistema por agotamiento de recursos	Recursos insuficientes para proceso de información	A	Aumentar las capacidades del servidor según la necesidad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Instalación de componentes no compatibles	MA	Capacitación al personal encargado de mantenimiento
	[I.5] Avería de origen físico o lógico.	Deterioro de componentes por el tiempo y uso	MA	Realizar mantenimiento periódicamente y

Nombre de Activo	Amenaza	Vulnerabilidad	Riesgo	PTR
				hacer verificar componentes
	[A.11] Acceso no autorizado	Control de ingreso a personal	A	Controlar el acceso de personal no autorizado
DISCO DURO EXTERNO	[I.5] Avería de origen físico o lógico.	Daño por uso inadecuado	MA	Hacer uso de un disco duro alterno
	[I.10] Degradación de los soportes de almacenamiento de la información	Deterioro de componentes por el tiempo y uso	MA	Hacer uso de un disco duro alterno
	[A.25] Robo	Perdida del activo con información importante	MA	Restringir el acceso a personal no autorizado
CABLEADO ESTRUCTURADO	[N.1] Fuego	Perdida del cableado	MA	Implementar medidas de seguridad de instalaciones físicas
	[I.7] Condiciones inadecuadas de temperatura o humedad	Deterioro del cableado	A	Adecuar la instalación de cableado a la norma
CUARTO DE SEGURIDAD	[N.7] Desastres naturales. Fenómeno sísmico.	Temblores, terremotos, erupción volcánica	A	Verificar el cumplimiento de la norma antisísmica
OPERADORES	[E.7] Deficiencias en la organización	Funciones no asignadas	A	Realizar un manual de funciones para los empleados
	[E.19] Fugas de información	Estrategias de negocio a terceros	A	Realizar un contrato de confidencialidad a los empleados
ADMINISTRADOR DE SISTEMAS	[E.2] Errores del administrador	Configuraciones del sistema mal ejecutadas	A	Capacitar al personal encargado de la administración de sistema
Fuente: Los autores del proyecto				

11.5 LISTA DE CHEQUEO

Una vez realizado el análisis de riesgos se procede a elaborar una lista de chequeo a partir de los controles estipulados en la norma ISO27002, esto ayudara a medir el grado de madurez dentro de la empresa y determinar una matriz de aplicabilidad que ayude a determinar los controles pertinentes para la empresa.

Para diseñar esta lista se debe seleccionar cada uno de los controles por dominio y formular una pregunta, cuya respuesta sea SI o NO, esto ayuda a determinar si el control se implementa o no en la empresa, por ejemplo:

En este ejemplo tomamos el DOMINIO 13. Seguridad en las telecomunicaciones, como se observa para cada uno de los controles de éste dominio se formula una pregunta, y se tiene como opciones dos respuestas que son SI o NO es decir se responde a que si la empresa aplica o no ese control. Una vez se tiene las respuestas de la lista de chequeo y de acuerdo a la respuesta de SI/NO y el total de preguntas se determina el nivel de cumplimiento o madurez para cada dominio evaluado (si hubiera 5 preguntas, 3 de respuesta SI y 2 de NO, el nivel de cumplimiento sería 3/5=0.6, se multiplica por 100 que equivale a 60% de cumplimiento para el dominio)

Para este caso el nivel de cumplimiento del dominio es de 43%, concluyendo que es necesario implementar procesos que ayuden al cumplimiento de controles respecto a la seguridad en las telecomunicaciones de la empresa. En la Tabla 34 se presenta un ejemplo de nivel de cumplimiento por control.

Tabla 34 Ejemplo nivel de cumplimiento por control

Objetivo de control	Código	Control	Descripción	Pregunta	Si	No	Nivel Cumplimiento
13.1 Gestión de la seguridad en las redes	13.1.1	Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.	La organización controla y administra la red?	X		43%
	13.1.2	Mecanismos de seguridad asociados a servicios en red	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se	La organización identifica los mecanismos de seguridad para los servicios de red?	X		

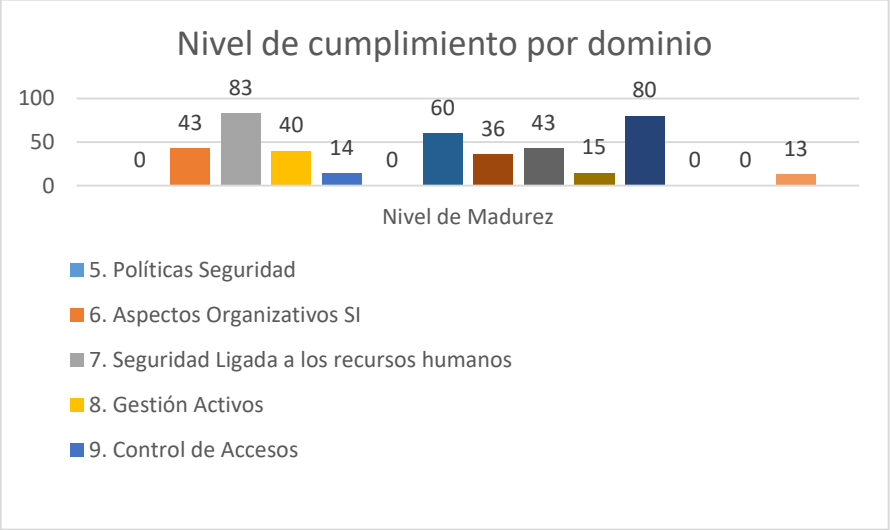
Objetivo de control	Código	Control	Descripción	Pregunta	Si	No	Nivel Cumplimiento
			entregan de manera interna o están externalizados.				
	13.1.3	Segregación de redes	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.	La organización segrega la red en funciona los empleados y servicios?		X	
13.2 Intercambio de información con partes externas	13.2.1	Políticas y procedimientos de intercambio de información	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.	La organización gestiona políticas para el intercambio de información?		X	
	13.2.2	Acuerdos de intercambio	Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.	La organización garantiza la transferencia de información entre las entidades externas a ella?		X	
	13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información referida en la	La organización tiene control sobre la	X		

Objetivo de control	Código	Control	Descripción	Pregunta	Si	No	Nivel Cumplimiento
			mensajería electrónica.	mensajería electrónica e-mail?			
	13.2.4	Acuerdos de confidencialidad y secreto	se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.	La organización identifica, revisa y documenta las restricciones para que los empleados no divulguen información confidencial?		X	
Fuente: Los autores del proyecto							

Para los dominios restantes se realizó el mismo procedimiento y se encuentra adjunto en el **Anexo 2 Declaración de aplicabilidad SOA** en la hoja que lleva el nombre de **Nivel de cumplimiento**

Una vez realizada esta medición se puede elaborar un gráfico que muestra de forma más clara la madurez por cada uno de los dominios de la norma ISO27002, como se indica en la Figura 4.

Figura 4 Nivel de madurez



Fuente: El presente proyecto

- **MATRIZ DE APLICABILIDAD:** Esta matriz es la base que ayuda a determinar, cuáles son los controles que se deben implementar en la empresa, acorde a los activos evaluados en la etapa de análisis de riesgos. El proceso que se realiza para elaborar la matriz, es verificar cada uno de los controles respecto a la lista de chequeo y decidir si éste, ya se aplica y si no describir la forma en que se debe aplicar en la empresa, adicionalmente a esto se debe justificar si el control no aplica en la empresa. Como ejemplo se toma el dominio **5. Políticas de seguridad,** en el cual se observa cómo se debería implementar los controles con el fin de cumplir con este, los resultados se tabulan en la Tabla 35.

Tabla 35 Ejemplo matriz aplicabilidad

DOMINIO	OBJETIVO DE CONTROL	CODIGO	CONTROL	Comentarios (Descripción de la implementación / Justificación de la exclusión)	Razones para la selección			
					LR	CO	BR/BP	RRA
5. Políticas Seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1	Políticas para la seguridad de la información	Diseñar políticas de seguridad a partir de un SGSI previo, en el cual se realiza un análisis de riesgos teniendo en cuenta cada uno de los activos de la empresa			X	X
		5.1.2	Revisión de las políticas para la seguridad de la información	Este control no aplica, ya que la empresa no cuenta con políticas que puedan ser revisadas				
Fuente: Los autores del proyecto								

Este proceso se documenta y realiza en el **Anexo 2 Declaración de aplicabilidad** en la hoja que lleva el nombre de **SOA**

11.6 POLITICAS DE SEGURIDAD

Para generar las políticas de seguridad se debe partir de los resultados del análisis de riesgos que sería el Plan de tratamiento de riesgos PRT y del documento de declaración de aplicabilidad SOA que es el resultado de la verificación de controles.

En el PTR se encuentra el tratamiento de los riesgos y también están definidos los controles para mitigar los riesgos encontrados, en el SOA se encuentran cuáles de los controles aplicables y que están especificados en la norma no existen en la ferretería, y partiendo de esos resultados se generan la Tabla 36, la cual presenta las siguientes políticas.

Tabla 36. PTR

PTR	Dominio	Control	Política		Costo
Realizar un manual de funciones para los empleados	6. Aspectos organizativos SI	6.1.1 Asignar responsabilidades	Realizar manual de funciones en donde se discrimine las responsabilidades de cada cargo	1. Verificar e identificar cada uno de los cargos ejercidos en la empresa 2. Listar las funciones y responsabilidades de cada uno de los cargos 3. Generar un documento con las especificaciones del cargo las funciones y responsabilidades por cada una de las áreas.	$1’000.000
Realizar un contrato de confidencialidad a los empleados	7. Seguridad Ligada a los recursos humanos	7.1.2 Términos y condiciones de contratación	Realizar contrato de confidencialidad donde se especifique las obligaciones en cuanto a seguridad de la información.	1. Determinar cuáles son los aspectos importantes relacionados con la información crítica, los cuales deben plasmarse en el contrato confidencial. 2. Especificar sanciones y multas si se llega a divulgar información confidencial por parte del personal 3. Redacción del contrato de confidencialidad por	$ 2’000.000

PTR	Dominio	Control	Política		Costo
				parte de una persona experta. 4. Aplicar el acuerdo de confidencialidad al personal que ingrese.	
Documentar procesos de capacitación a personal	7. Seguridad Ligada a los recursos humanos	7.2.2 Concienciación, educación y capacitación en SI	Generar un documento con el proceso de capacitación a empleados nuevos por cada área de la empresa.	1. Generar folletos de capacitación de personal nuevo, por cargo a ejercer 2. Asignar personal por área encargado de capacitar al empleado nuevo. 3. Dar a conocer al personal encargado de la capacitación el folleto y el proceso de esta. 4. Aplicar la capacitación a cada empleado nuevo	$ 1’000.000
Aumentar las capacidades del servidor según la necesidad	8. Gestión activos	8.1.3 Uso aceptable de los activos	Analizar las necesidades de recursos hardware para el servidor gestionando los recursos de forma óptima.	1. Analizar los recursos necesarios del servidor 2. Comprobar los recursos económicos para modificar los componentes necesarios 3. Comprar los componentes necesarios 4. Adaptar al servidor los recursos necesarios.	Esta política no se puede calcular el costo hasta tener el estudio de recursos necesarios.
Hacer uso de disco duro alterno	8. Gestión activos	8.3.1 Gestión de soportes extraíbles	Gestionar la forma de almacenar la información en	1. Analizar la cantidad de medios extraíbles necesaria	$360.000

PTR	Dominio	Control	Política		Costo
			diferentes medios extraíbles, que den soporte en caso de fallo de alguno de estos.	2. Adquirir nuevos medios extraíbles. 3. Realizar copias de seguridad en los diferentes medios extraíbles.	
Configurar privilegios de usuarios	9. Control de acceso	9.2.2 Gestión de los derechos de acceso asignados a usuarios	Gestionar los privilegios de cada uno de los usuarios quienes tengan relación con el sistema, evitando ingresos indebidos por personal no autorizado	1. Analizar las funciones de cada uno de los usuarios 2. Dependiendo las funciones que realice el usuario asignar los privilegios necesarios 3. Generar acceso de usuarios, asignando los roles correspondientes	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación.
Restringir el acceso de personal no autorizado a información confidencial	9. Control de acceso	9.2.3 Gestión de los derechos de acceso con privilegios especiales	Restringir el acceso a usuarios mediante el uso de privilegios especiales	1. Crear documento con permisos acorde al usuarios 2. Configurar los permisos 3. Aplicar permisos a usuarios antiguos	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación.
Parametrización de usuarios dependiendo sus funciones	9. Control de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios	Parametrizar los usuarios acorde a la revisión de sus permisos y funciones	1. Revisar manual de funciones 2. Crear roles y permisos de acceso acordes a las funciones 3. Asignar los roles a los diferentes empleados	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación.
Crear políticas para la asignación de contraseñas	9 Control de acceso	9.4.3 Gestión de contraseñas de usuarios	Crear un documento donde se especifique la forma de creación de contraseñas para cada	1. Hacer uso de mínimo 10 caracteres 2. Hacer uso de mínimo un carácter especial	esta política no genera costos, sin embargo se debe asignar al personal

PTR	Dominio	Control	Política		Costo
			uno de los usuarios del sistema.	3. Combinación de letras mayúsculas, minúsculas y números 4. La contraseña no debe contener nombres comunes 5. Cambiar contraseña cada 2 meses 6. Comprobar el nivel de seguridad de las contraseñas con John the ripper	adecuado para su implementación
Encriptación de backups	10. Cifrado	Política de uso de los controles criptográficos	Hacer el uso de controles criptográficos para la protección de la información	1. Elegir una herramienta PKI para encriptar la información 2. Encriptar la información 3. Realizar un checksum para resguardar la integridad de la información	Este control no tiene costos ya que se realizara con software libre, sin embargo se debe asignar al personal idóneo para que sea aplicada
Controlar el acceso a personal no autorizado	11. Seguridad física y ambiental	11.1.2 Controles físicos de entrada	Adquirir cerraduras que controlen el acceso del personal no autorizado	1. Analizar la cerradura más óptima para el acceso 2. Medir el nivel de costo de la implementación 3. Adquirir la cerradura 4. Instalar cerradura 5. Registrar empleados acorde a acceso permitido	$ 2’000.000 por cerradura
Implementar medidas de seguridad de	11. Seguridad física y ambiental	11.1.4 Protección contra amenazas externas y ambientales	Verificar periódicamente cada uno de los mecanismos que hacen parte de la seguridad	1. Hacer una lista de chequeo para donde se encuentren las características a	Esta política no se puede calcular el costo hasta tener el

PTR	Dominio	Control	Política		Costo
instalaciones físicas			física de las instalaciones de la empresa.	evaluar de los mecanismos de seguridad física 2. Aplicar la lista de chequeo de verificación 3. Analizar los resultados para ejecutar cambios de los dispositivos 4. Realizar la verificación una vez al mes	estudio de recursos necesarios.
Verificar el cumplimiento de la norma antisísmica	11. Seguridad física y ambiental	11.1.5 El trabajo en áreas seguras	Verificar que las instalaciones cumplan la norma antisísmica colombiana	1. Consultar norma antisísmica colombiana. 2. Verificar cada una de las áreas físicas que cumplan la norma. 3. Informar aquellas áreas que no cumplan con dicha norma	$4’000.000
Adecuar la instalación de cableado a la norma	11. Seguridad física y ambiental	11.2.3 Seguridad del cableado	Verificar que el cableado instalado y el cableado a instalar cumpla la norma ANSI/TIA/EIA-568	1. Inspeccionar cada área de las instalaciones de la empresa, para verificar el cumplimiento de la norma 2. Analizar los resultados encontrados después de la verificación 3. Corregir el cableado según las especificaciones de la norma ANSI/TIA/EIA-568	Esta política no se puede calcular el costo hasta tener el estudio de recursos necesarios.

PTR	Dominio	Control	Política		Costo
Asignar contraseñas a usuarios del SO y disminuir el tiempo de suspensión del equipo	11. Seguridad física y ambiental	11.2.8 Equipo informático de usuario desatendido	Protección adecuada de los equipos de cada uno de los usuarios, para prevenir el acceso no autorizado	1. Hacer uso de contraseñas 2. Configurar equipos minimizando el tiempo de suspensión	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación
Implementar antivirus Premium	12. Seguridad operativa	12.2.1 Controles contra el código malicioso	Controlar la propagación de software malicioso mediante el uso de antivirus premiun	1. Buscar un antivirus que se adecue a las necesidades 2. Adquirir licencia del antivirus 3. Instalar antivirus en los equipos 4. Configurar reglas de antivirus	$ 600.000 por 2 años y 5 equipos
Realizar copias de seguridad en la nube	12. Seguridad operativa	12.3.1 Copias de seguridad de la información	Se debe realizar copias de seguridad del sistema y los datos en caso de desastres o daños producidos por ataques externos.	1. Elegir un medio de almacenamiento en la nube, con capacidad necesaria 2. Sincronizar medios y carpetas para realizar copias de la información critica 3. El usuario debe organizar la información en carpetas cuyo nombre haga referencia a la información almacenada 4. El usuario debe realizar la copia de seguridad en el directorio sincronizado y asignado para ello	$ 5.000 por 100 GB con 10.000 accesos al mes total $ 60.000 anual con windows azure

PTR	Dominio	Control	Política		Costo
				5. Realizar pruebas de la información almacenada en las copias de seguridad	
Realizar copias de archivos logs	12 Seguridad operativa	12.4.1 Registro y gestión de eventos de actividad	Hacer copias periódicas de los registros relacionados con las actividades de los usuarios, fallas y eventos de seguridad de la información	1. Sacar una copia de seguridad de los archivos log semanalmente 2. Realizar un checksum para verificar que los archivos no estén modificados 3. Probar las copias de seguridad.	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación
Verificar la integridad del software a instalar	12. Seguridad Operativa	12.5.1 Instalación del software en sistemas en producción	Verificar el origen de paquetes de instalación para su posterior instalación.	1. Verificar software adquirido e instalado mediante suma de chequeo. 2. Realizar instalación de software que cumpla la verificación.	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación.
Restringir la instalación de software a personal no autorizado	12. Seguridad operativa.	12.6.2 Restricciones en la instalación de software	Restringir la instalación de software no autorizado al personal que opera en los sistemas.	1. Realizar una lista de software permitido por los equipos 2. Configurar equipos para bloquear la instalación de software 3. Aplicar la configuración para más equipos	Esta política no genera costos para la empresa, sin embargo se debe asignar al personal adecuado para su implementación.
Fuente: los autores del proyecto.					

CONCLUSIONES

La seguridad de la información dentro de la Ferretería Argentina de la ciudad de Pasto es de vital importancia ya que de esta dependen gran cantidad de procesos, por otra parte la ferretería manea mucha información crítica que actualmente se encuentra venerable por diferentes amenazas.

La implementación del SGSI dentro de la ferretería argentina ayudara a mitigar las amenazas de los riesgos más críticos sobre algunos de los activos dentro de la empresa, este sistema puede ser implementado por pocos, para que su impacto sobre los costos y ´personal no sea agresivo, cabe recordar que un sistema de gestión de la información es una mejora continua y requiere el compromiso de todos los empleados de la organización.

Actualmente muchos de los activos presentes en la Ferretería Argentina de la ciudad de Pasto se encuentran en un nivel de riesgo alto, es por ello que estos activos requieren una mayor atención, ya que pueden llegar a comprometer tanto la disponibilidad, integridad y confidencialidad de la información.

El análisis de amenazas y riesgos es una actividad que se debe realizar de forma constante, ya que esta ayudara a la Ferretería Argentina de la ciudad de Pasto a detectar el nivel de riesgos residual que pueden afectar a los activos, con esta actividad se garantiza el funcionamiento óptimo del sistema de gestión de la seguridad informático, además cabe resaltar que este proyecto no cubrió la totalidad de los activos en riesgos.

RECOMENDACIONES

Se recomienda implementar las políticas evaluadas dentro del proyecto, ya que a través de estas la seguridad de los activos más importantes y con ellos la información más importante aumentara disminuyendo el la probabilidad de que un riesgo se materialice y afecte la disponibilidad, integridad y confidencialidad de la información que se maneja dentro de la ferretería.

Se recomienda realizar auditorías de forma constantes posterior a la implementación del sistema de seguridad de la información, ya que estas ayudaran a detectar posibles falencias de seguridad que surjan con el tiempo las cuales pongan en riesgo los activos de la empresa y con ellos la información que estos manejan.

Obtenidos los resultados gracias al análisis de riesgos, se pudo observar que la empresa necesita implementar medidas de seguridad con el fin de salvaguardar la información, por ello se recomienda hacer uso constante de las diferentes herramientas de seguridad, de este modo poder estar mitigando posibles riesgos que puedan generarse.

BIBLIOGRAFIA

AHACEITUNO, Vicente. Seguridad de la Información. Creaciones COPYRIGHT. 2004. Barcelona. 265p. ISBN 849-33-3367-0.

AREITIO BERTOLI, Javier. Seguridad de la Información: redes, informática y sistemas de información. Paraninfo Cengage. 2008. 561p. ISBN 978-84-9732-502-8.

BARRERA, Hurtado de. El Proyecto de Investigación: Sypal; Caracas, 2008

BICHACHI, Diana Susana. El uso de las Listas de Chequeo (CheskList) como herramienta para controlar la calidad de la ley. [en línea] <http://www.claudiabernazza.com.ar/ssgp/html/pdf/check_list.pdf>, 2013

CAMARENA AUDIRAC, Carlos Augusto. ABC Del desarrollo organizacional, 2006

ERB, Markus. Seguridad de la Información y Protección de Datos. [en línea]. <https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/ > [citado 2009]

ERB, Markus. Amenazas y Vulnerabilidades. [en línea]. <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/> [citado 2009]

GARCíA ESTUDILLO, Victoriano. La información como recurso estratégico para las empresas. [en línea]. <http://www.gestiopolis.com/la-informacion-como-recurso-estrategico-para-las-empresas/> [citado en 13 de abril de 2015]

GLASS, G y STANLEY, J.S. Métodos Estadísticos Aplicados a las ciencias sociales: Prentice-Hall; México, 1996

HERNÁNDEZ SAMPIERI, Roberto y FERNÁNDEZ COLLADO, Carlos y BAPTISTA LUCIO, Pilar. Metodología de la investigación: McGraw-Hill Interamericana; México, 2010. p.80

HORNOS BARRANCO, Miguel y ARAQUE CUENCA, Francisco y ABAD, María del Mar. La información como recurso estratégico para las empresas. [en línea]. <http://www.gestiopolis.com/la-informacion-como-recurso-estrategico-para-las-empresas/> [citado en 13 de abril de 2015]

ISO27000. El portal de ISO 27001 en español http://www.iso27000.es/.

KRIPPENDORFF, K. Content analysis. An introduction to its methodology: Sage; Beverly Hills, 1980

LADINO A., MARTHA ISABEL, VILLA S., PAULA ANDREA, LÓPEZ E., ANA MARÍA. FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS.Scientia Et Technica [en línea] 2011, XVII (Abril-Sin mes): [Fecha de consulta: 27 de agosto de 2017] Disponible en:< http://www.redalyc.org/articulo.oa?id=84921327061 > ISSN 0122-1701

MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línea] 2010,6 (Junio-Sin mes): [Fecha de consulta: 27 de agosto de 2017] Disponible en:< http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VwPWyPnhDIU >

MARTíNEZ DE LA CRUZ, Sergio Alejandro. Importancia de los sistemas de información para las Pymes. [en línea]. < http://www.gestiopolis.com/importancia-sistemas-informacion-pymes/> [citado en 1 de noviembre de 2009]

MÉNDEZ, C. Metodologia, Diseño y Desarrollo del Proceso de Investigación: Mc Graw-Hill; Caracas, 2001

RESTREPO, María Consuelo. Producción de textos educativos: Ediciones Bogotá D.C; Colombia. 1999. p. 8 .ISBN: 978-958-20-0850-4.

REVISTA GERENCIA. Seguridad informática ¿Qué hacer para proteger la información? [en línea]. <http://www.emb.cl/gerencia/articulo.mvc?xid=932> [citado en noviembre de 2009]

TABANGO GOYES Marcelo, GUERRERO Camilo. Sistema de gestión de seguridad de la información basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la universidad de Nariño, San Juan De Pasto, 2014, 150h. Trabajo de Grado (ingeniero de sistemas). Universidad de Nariño. Facultad de Ingeniería. Disponible en el catálogo en línea de la Biblioteca Alberto Quijano: <http://biblioteca.udenar.edu.co>.

TAMAYO, Mario. El Proceso de la investigación científica: Limusa; México, 2001

TESCH, R. Qualitative research: analysis types and software tolos: The Falm Press; New York, 1992

UNIVERSIDAD TECNOLOGICA DE PEREIRA: Políticas de Seguridad de Activos de Información: http://media.utp.edu.co/sistema-de-gestion-de-seguridad-de-la-informacion/archivos/politicas_sgsi.pdf.

ANEXOS

Anexo 1: Análisis de riesgos y vulnerabilidades, disponible en: https://1drv.ms/x/s!Ah-q2EXORx3-jEqJe7pmhTbLyPfb

Anexo 2: Declaración de aplicabilidad SOA, disponible en: https://1drv.ms/x/s!Ah-q2EXORx3-jEsL8_gfuk1Ca6lr