UNIVERSIDAD COOPERATIVA DE COLOMBIA
SEDE ARAUCA
PROGRAMA DE INGENIERÍA DE SISTEMAS

MODALIDAD DE GRADO PARA OPTAR AL TÍTULO DE INGENIERO DE SISTEMAS

Análisis de riesgos basado en los dominios 8 y 11 de la ISO/IEC 27002:2013 para el área de Almacén e Inventarios del Centro de Gestión y Desarrollo Agroindustrial de Arauca (SENA)

Presentado por:
Bryan Mahecha Pacheco
Luis Miguel Aparicio Sanchez

Asesor de modalidad de grado:
Carlos Eduardo Puentes Figueroa

Arauca, Arauca
Mayo
2021

Notas de autor:
Correspondencia relacionada con este documento ser enviada a:
bryan.mahechap@campusucc.edu.co

Tabla de contenido

Lista de tablas

Lista de figuras

Introducción

El Centro Criptológico Nacional (CCN) desarrolló la solución PILAR como una herramienta de Entorno de Análisis de Riesgos (EAR), que soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), a través de esta herramienta se analizan los riesgos en las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. (CCN-CERT, 20).

Con esta herramienta y siguiendo los objetivos de la metodología MAGERIT, se analiza el estado actual de los procesos de información del área de Almacén e Inventarios del Centro de Gestión y Desarrollo Agroindustrial de Arauca SENA, con base a la norma ISO/IEC 27002:2013 en sus dominios 8 y 11.

Finalizado el análisis de riesgos, se evidencia cuáles son los controles que se encuentran inexistentes o muy poco desarrollados en los dominios evaluados, así que basándose en estos resultados se dan sugerencias, recomendaciones o pautas, las cuales puedan ayudar a implementar salvaguardas que permitan mitigar los riesgos que conlleva cada amenaza a los activos de información más importantes para la organización.

Palabras clave:

MAGERIT, riesgo, activos, amenaza, análisis, seguridad.

Abstract

The National Cryptological Center (CCN) developed the PILAR solution as a Risk Analysis Environment (EAR) tool, which supports the analysis and risk management of an information system following the MAGERIT methodology (Risk Analysis and Management Methodology Information Systems), through this tool the risks are analyzed in the dimensions of confidentiality, integrity, availability, authenticity and traceability. (CCN-CERT, 20).

With this tool and following the objectives of the MAGERIT methodology, the current state of the information processes of the Warehouse and Inventory area of the Center for Management and Agroindustrial Development of Arauca SENA is analyzed, based on the ISO / IEC 27002: 2013 standard. in its domains 8 and 11.

After the risk analysis, it is evident which are the controls that are non-existent or very little developed in the evaluated domains, so based on these results, suggestions, recommendations or guidelines are given, which can help to implement safeguards that allow to mitigate the risks. risks posed by each threat to the organization's most important information assets.

Keywords:

MAGERIT, risk, assets, threat, analysis, security.

1. Contexto del proyecto

1.1 Planteamiento del Problema

Hoy en día la información se ha convertido en el activo más importante para las empresas, pues, es la encargada de relacionar cada aspecto de la organización y de guiarla de forma eficiente hacia el éxito. Por tal motivo, se debe buscar y garantizar la seguridad de la información desarrollando un control en la gestión de activos, así como en la seguridad física y ambiental de los mismos.

Desde el 2020, a causa de la emergencia sanitaria provocada por el Covid-19, las empresas han tenido que migrar del trabajo presencial al trabajo remoto o Home Office, lo cual ha generado una crisis en la seguridad de la información, ya que esta modalidad de trabajo ha permitido que los activos de la información tuvieran un uso externo a las instalaciones de la entidad, comprometiendo la integridad, confidencialidad y disponibilidad de la información.

Por eso para el área de Almacén e Inventarios del Centro de Desarrollo Agroindustrial de Arauca Sena, quien es la encargada del flujo del proceso de control de bienes de la entidad, es de suma importancia determinar el nivel de riesgos en la gestión de sus activos de información y determinar el estado actual de la seguridad física y ambiental de estos, para así poder ejercer controles y medidas que permitan mejorar la seguridad de la información.

1.2 Justificación

La empresa que conoce, valora y gestiona sus activos de información esta menos expuesta a potenciales amenazas y vulnerabilidades, ya que le permite definir estrategias de seguridad a cada uno de sus activos, desarrollando planes de mitigación de riesgos. Así mismo la seguridad física y ambiental juega un papel muy importante en la protección de la información, mediante el control físico de las instalaciones de trabajo, como también en la clasificación de los factores externos que pueden llegar a generar algún riesgo sobre los activos de información.

Por estas razones mediante el análisis de riesgos que se desea desarrollar en este proyecto, se espera conocer el estado actual de los activos de información, así como reconocer y valorar las posibles vulnerabilidades que pueden llegar a comprometer la seguridad de la información. De esta forma se generaría una serie de sugerencias que permitan minimizar el impacto de los daños que se puedan causar por la ocurrencia de alguna posible amenaza.

1.3 Pregunta Problema

¿De qué manera se puede realizar el análisis de riesgos basados en los dominios 8 y 11 de las ISO/IEC 27002:2013 para el Centro de Gestión y Desarrollo Agroindustrial en su área de Almacén e Inventarios?

1.4 Objetivos

1.4.1 Objetivo General

Analizar los riesgos del área de Almacén e Inventarios con base a la norma ISO/IEC 27002:2013 en sus dominios 8 y 11 en el Centro de Gestión y Desarrollo Agroindustrial de Arauca utilizando la metodología MAGERIT.

1.4.2 Objetivos Específicos

- Caracterizar los procesos relacionados al área de Almacén e Inventarios enfocados en los dominios de Gestión de Activos (8) y Seguridad Física y Ambiental (11) de la normativa ISO/IEC 27002:2013.
- Identificar los activos de información relacionados al área de Almacén e Inventarios.
- Analizar los riesgos del área de Almacén e Inventarios aplicando la metodología MAGERIT.
- Generar propuestas de valor a partir de los resultados obtenidos del análisis de riesgos.

2. Marco teórico

2.1 Estado del Arte.

2.1.1 Nacionales

(Tova & Salguero 2018) en su estudio: Auditoría interna a los activos físicos del área TI en la Universidad Cooperativa de Colombia sede Ibagué, aplicando el estándar ISO/IEC 27002:2013. Realizaron una auditoría seguridad de la infraestructura en el área de TI, donde realizaron una investigación de los activos de información más específicamente a los activos físicos de área y como estos pueden ser expuestos a diferentes riesgos. Ellos aplicaron un checklist estableciendo los dominios 5, 8 y 11 de la ISO/IEC 27002:2013 y su conclusión fue la generación de resultados donde se mitigarían los riesgos garantizando la tríada de la norma que es la confidencialidad, integridad y disponibilidad.

(Orjuela & Ballesteros 2019) en su estudio: Análisis de riesgos al proceso de gestión de tecnología de la información para la caja de compensación familiar del Tolima Comfatolima, sede administrativa–Ibagué. Plantearon realizar el análisis de riesgos específicamente cuarto de servidores teniendo en cuenta le metodología MAGERIT y sus resultados fueron la elaboración de las conformidades y no conformidades donde la finalidad es que el departamento de T.I implante controles de seguridad, mitigue y gestiones los riesgos.

(Valencia & Orozco 2017) en su estudio: Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Formulan la importancia de las normas relacionadas a la familia de la ISO/IEC 27000. Junto con su implementación en las organizaciones, para esto ellos proponen una metodología que consta en 5 fases: Aprobación de la dirección para iniciar el proyecto (1), definir el alcance, los límites y la política del SGSI (2), análisis de los requisitos de seguridad de la información (3), valoración de riesgos y planificar el tratamiento de riesgos (4), diseñar el SGSI (5).

2.1.2 Locales

(Calderón 2015) en su estudio: Auditoria de seguridad de la información e infraestructura de ti de la empresa de energía de Arauca Enelar e.s.p. del departamento de Arauca. Tuvo como finalidad la realización de una auditoría en la entidad para poder así identificar los diferentes riesgos a los cuales se podría ver expuesto la organización, tuvo en cuenta la metodología MAGERIT y de esta forma realizó un checklist para así poder identificar los activos de información. La auditoría se basó en los dominios 5, 8, 11, 12, 13 y 14 de la normativa ISO/IEC 27002:2013. Con los resultados obtenidos estableció una serie de controles para gestionar y mitigar los riesgos.

(Pabón & Beltrán 2015) en su estudio: Estudio del análisis de riesgo acerca de la seguridad de la información a través de la gestión tecnológica en la asociación Frepaem-saravena. Utilizan la normativa ISO/IEC 27002:2005 en conjunto con la metodología MAGERIT para realizar su investigación. Determinan una serie de pasos a seguir como lo son conocer el estado actual de la empresa, analizan los riesgos con base a los activos de información, generan unos resultados donde resaltan una serie de recomendaciones las cuales son socializadas a la alta gerencia de la entidad. Cabe señalar que más allá que un estudio de análisis de riesgos como lo denominan en el titulo del documento vendría siendo más una auditoría debido a que tienen en cuenta cada uno de los dominios de la normativa.

2.2 Marco conceptual

2.2.1 Seguridad de la Información

Según la norma ISO/IEC 27001 es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confidencialidad (ISO/IEC 17799:2005). La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. (Montes, 2014)

2.2.2 Sistema de Gestión de Seguridad de la Información

La norma ISO/IEC 27002:2013, define un Sistema de Gestión de Seguridad de la Información (SGSI) como las políticas, procedimientos, directrices, y recursos asociados a actividades colectivamente gestionadas por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI, es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización, para alcanzar los objetivos propuestos. (Salamanca, 2016)

2.2.3 Activo de información

Es toda información que tenga valor para la organización. No obstante, este concepto es bastante amplio debe ser limitado por una serie de consideraciones: o El impacto que para la organización supone la pérdida de confidencialidad, integridad y/o disponibilidad de cada activo. o El tipo de información que maneja. o Sus productores y consumidores. (Mineducación , 2013)

2.2.4 Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Mineducación , 2013)

2.2.5 Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (Mineducación , 2013)

2.2.6 Norma ISO/IEC 27000.

Esta norma establece un conjunto de estándares desarrollados por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (Montes, 2014)

2.2.7 ISO/IEC 27001:2013

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en el ámbito de una organización. Esta norma incluye los requerimientos para realizar la valoración y el Tratamiento de riesgos de seguridad de la información, conforme las necesidades de una organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Cuando una organización declara conformidad con esta norma, no es aceptable excluir cualquiera de los requisitos especificados de los numerales 4 al 10. (Benavides C, 2013)

2.2.8 ISO/IEC 27002:2013

Esta norma se basa en el código de las buenas prácticas para la gestión de la seguridad. Se puede dar recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización. Esta norma también describe los objetivos de control (aspectos para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas a tomar). Al igual que el Anexo A de la norma ISO/IEC 27001, tiene los 14 dominios, 35 objetivos de seguridad y 114 controles de seguridad. (Montes, 2014)

Figura 1. Imagen de Dominios de la Norma ISO/IEC 27002: 2013

Fuente: Dominios de la Norma ISO/IEC 27002: 2013; Adaptado de Universidad Autónoma de Occidente https://red.uao.edu.co/

2.3 Metodología

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que busca gestionar de una forma sistemática los riesgos a los que se puede ver expuestos las diferentes organizaciones en temas relacionados a la seguridad informática. Esta metodología define objetivos claros trazables y alcanzables para las organizaciones y permite realizar un seguimiento exhaustivo del avance de estos. (Rojas P, 2019)

2.3.1 Objetivos MAGERIT:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.

- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.
- Ventajas de Magerit: Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles. (Ministerio de hacienda España, 2012)

2.3.2 Elementos del Análisis de Riesgos

En la realización de un Análisis y Gestión de Riesgos según MAGERIT, el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

- Activos: Recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información o dato.
- Amenazas: Determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza.
- Vulnerabilidades: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- Impactos: Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto.
- Riesgo: Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia.
- Salvaguardas (Funciones, Servicios y Mecanismos): Una salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas. (Ministerio de hacienda España, 2012)

2.3.3 Implementación de la Metodología

La metodología MAGERIT, define un paso a paso para llevar cabo de manera satisfactoria la implementación del análisis de gestión de riesgos, los cuales se describen a continuación.

- Identificación de los activos más relevantes de la organización y descripción de los servicios e información que maneja.
- La valorización de los activos se realizará de manera cualitativa, teniendo en cuenta las siguientes dimensiones: su confidencialidad, su integridad, su disponibilidad, la autenticidad, la trazabilidad y el valor por interrupción del servicio.
- Los activos son los elementos principales que una empresa posee para el tratamiento de la información. A la hora de iniciar un análisis de riesgo informático, se debe identificar los activos existentes en la organización y determinar el tipo. (Rojas P, 2019)
- Definición de vulnerabilidades del sistema
  - Vulnerabilidad natural
  - Vulnerabilidad de hardware y software
  - Vulnerabilidad de los medios y/o dispositivos
  - Vulnerabilidad humana
- Definición de amenazas del sistema
  - De origen natural
  - Del entorno
  - Defectos de aplicaciones
  - Causadas por personas
  - Sistemas de comunicación

- Valoración del riesgo: Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.
  - La probabilidad de ocurrencia la tomamos de las experiencias, históricos e informes emitidos por compañías que desarrollan la misma actividad económica.
  - El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.
  - zona 1 – riesgos muy probables y de muy alto impacto, representado por el color rojo
  - zona 2 –cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo, representado por el color naranja.
  - zona 3 – riesgos improbables y de bajo impacto, representado con el color amarillo.
  - zona 4 – riesgos improbables, pero de muy alto impacto, representado por el color verde. (Rojas P, 2019)

2.4 Contextualización de la empresa

"Somos un establecimiento público del orden nacional, con personería jurídica, patrimonio propio e independiente, y autonomía administrativa; Adscrito al Ministerio del Trabajo de Colombia. Ofrece formación gratuita a millones de colombianos que se benefician con programas técnicos, tecnológicos y complementarios que, enfocados en el desarrollo económico, tecnológico y social del país, entran a engrosar las actividades productivas de las empresas y de la industria, para obtener mejor competitividad y producción con los mercados globalizados.

Facultada por el Estado para la inversión en infraestructura necesaria para mejorar el desarrollo social y técnico de los trabajadores en las diferentes regiones, a través de formación profesional integral que logra incorporarse con las metas del Gobierno Nacional, mediante el cubrimiento de las necesidades específicas de recurso humano en las empresas, a través de la vinculación al mercado laboral -bien sea como empleado o subempleado-, con grandes oportunidades para el desarrollo empresarial, comunitario y tecnológico.

La entidad más querida por los colombianos funciona en permanente alianza entre Gobierno, empresarios y trabajadores, desde su creación, con el firme propósito de lograr la competitividad de Colombia a través del incremento de la productividad en las empresas y regiones, sin dejar de lado la inclusión social, en articulación con la política nacional: Más empleo y menos pobreza. Por tal razón, se generan continuamente programas y proyectos de responsabilidad social, empresarial, formación, innovación, internacionalización y transferencia de conocimientos y tecnologías.” (SENA, 2020)

2.4.1 Misión

El SENA está encargado de cumplir la función que le corresponde al Estado de invertir en el desarrollo social y técnico de los trabajadores colombianos, ofreciendo y ejecutando la formación profesional integral, para la incorporación y el desarrollo de las personas en actividades productivas que contribuyan al desarrollo social, económico y tecnológico del país (Ley 119/1994). (SENA)

2.4.2 Visión

En el año 2022 el SENA se consolidará como una entidad referente de formación integral para el trabajo, por su aporte a la empleabilidad, el emprendimiento y la equidad, que atiende con pertinencia y calidad las necesidades productivas y sociales del país. (SENA)

3. Caracterización de los procesos

Conocer el funcionamiento actual de los procesos dentro de la organización es fundamental al momento de realizar un análisis de riesgo, ya que permite delimitar el alcance del estudio y tener en cuenta todos los aspectos necesarios para un buen resultado. Esta sección determina el estado actual del área realizando el enfoque hacia los dominios 8 (Gestión de activos) y 11 (Seguridad Física y Ambiental) de la ISO/IEC 27002:2013. Realizando esto se da inicio a el primer objetivo planteado para el proyecto que es 'Caracterizar los procesos relacionados al área de Almacén e Inventarios enfocados en los dominios de Gestión de Activos (8) y Seguridad Física y Ambiental (11) de la normativa ISO/IEC 27002:2013. Para llevar a cabo este proceso se emplea la utilización de un checklist que es una herramienta evalúa las condiciones actuales del área.

Inicialmente se realizaron reuniones con el personal de almacén e inventarios para comprender el funcionamiento interno de área y el modo en que realizaban cada uno de sus procesos.

3.1 Checklist

Los listados de control, listados de chequeo, checklist u hojas de verificación, siendo formatos generados para realizar actividades repetitivas, controlar el cumplimiento de un listado de requisitos o recolectar datos ordenadamente y de manera sistemática. Se utilizan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el trabajador o inspector no se olvida de nada importante. (ISOTools, 2018)

Los principales de los checklist son los siguientes:

- Durante la realización de actividades en las que es muy importante que no se olvide ningún paso y deben hacerse las tareas con un orden establecido.
- Realizar inspecciones donde se deja constancia de cuales han sido los puntos inspeccionados.
- Verificar o examinar artículos.
- Examinar o analizar la localización de los defectos. Verificando las causas de los defectos.

- Verificar y analizar las operaciones.
- Recopilar datos para su futuro análisis.

El checklist aplicado evalúa los dominios 8 (Gestión de Avtivos) y 11 (Seguridad Físisca y Ambiental), del cual se eligieron cuatro objetivos de control y veintidós controles distribuidos de la siguiente manera:

- Dominio 8 (Gestión de Activos)
  - 8.1 Resposabilidad sobre los activos
    - ✓ 8.1.1 Inventario de activos
    - ✓ 8.1.2 Propiedad de los activos.
    - ✓ 8.1.3 Uso aceptable de los activos.
    - ✓ 8.1.4 Devolución de activos.
  - 8.3 Manejo de los soportes de almacenamiento
    - ✓ 8.3.1 Gestión de soportes extraíbles.
    - ✓ 8.3.2 Eliminación de soportes.
    - ✓ 8.3.3 Soportes físicos en tránsito
- Dominio 11 (Seguridad Física y Ambiental)
  - 11.1 Áreas Seguras
    - ✓ 11.1.1 Perímetro de seguridad física.
    - ✓ 11.1.2 Controles físicos de entrada.
    - ✓ 11.1.3 Seguridad de oficinas, despachos y recursos.
    - ✓ 11.1.4 Protección contra las amenazas externas y ambientales.
    - ✓ 11.1.5 El trabajo en áreas seguras.
    - ✓ 11.1.6 Áreas de acceso público, carga y descarga
  - 11.2 Seguridad de los Equipos
    - ✓ 11.2.1 Emplazamiento y protección de equipos.
    - ✓ 11.2.2 Instalaciones de suministro.
    - ✓ 11.2.3 Seguridad del cableado.
    - ✓ 11.2.4 Mantenimiento de los equipos.

- ✓ 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- ✓ 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- ✓ 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- ✓ 11.2.8 Equipo informático de usuario desatendido.
- ✓ 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

3.2 Análisis de GAP

Un análisis de brechas GAP es un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito. Gap se refiere al espacio entre "donde estamos" (el presente) y "donde queremos estar" (el objetivo a alcanzar). Un análisis de deficiencias también puede denominarse análisis de necesidades, permitiéndonos determinar lo que nos falta y los recursos necesarios para alcanzar los objetivos. (NORMA ISO 27001, 2019)

El documento creado para realizar el análisis de GAP (***véase anexo 4***) contiene una serie de preguntas tomando en consideración el Anexo A de la ISO/IEC 27001:2013 para las cuales se estableció los siguientes criterios de evaluación:

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.

No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Tabla 1. Criterios de evaluación análisis de GAP.

Fuente: Elaboración propia.

Para darle una respuesta a las preguntas planteadas por el formato se tiene que tomar en cuenta inicialmente las preguntas del checklist, ya que estas lo que hacen es indicar un panorama sobre como se encuentra el área a evaluar, posterior a ello también se toma en consideración las reuniones concretadas con el personal de almacén e inventarios, y de esta forma se puede dar una calificación para cada aspecto evaluado en el formato teniendo en cuenta lo señalado por los criterios y la información ya obtenida.

4. Análisis de Riesgo

El análisis de riesgo nos permite identificar claramente cuáles son los activos más importantes dentro de la organización y gestionar los riesgos de las diferentes amenazas y vulnerabilidades que pueden afectar a cada uno de ellos. Realizando el análisis de riesgos teniendo en cuenta lo propuesto por la metodología MAGERIT y haciendo uso del software PILAR se da inicio a lo planteado en el Objetivo Específico 2 'Identificar los activos de información relacionados al área de Almacén e Inventarios' y 3 'Analizar los riesgos del área de Almacén e Inventarios aplicando la metodología MAGERIT'.

4.1 Identificación de Activos

Mediante las entrevistas realizadas al personal de almacén e inventarios se pudo determinar la identificación de los activos más relevantes utilizados en sus procedimientos. El formato utilizado para levantar la información comprendía los siguientes puntos:

- Datos entidad.
  - Código: Identificador único del activo.
  - Dependencia: Es el lugar donde se encuentra ubicado el activo de información.
- Criterios con base en la ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información)
  - Nombre del activo de información
  - Descripción del activo de información
  - Tipología: Es el tipo de activo de información (Información, Software, Recurso Humano, Servicio, Hardware, Otros).
  - Formato: Es la forma en que se visualiza o se presenta el activo de información (Audio, Base de Datos, Documento de Texto, Hoja de Cálculo, Imagen, Video).
  - Clasificación según atributo de confidencialidad: Se selecciona la opción de acuerdo a la clasificación de la información (Clasificada, Publica, Reservada).

  - Información Publicada: Se diligencia la URL o la dependencia en donde se pueda ubicar la información en caso de que se pueda solicitar o consultar.
- Criterios con base en la ley 1581 de 2012 (Ley de protección de datos personales)
  - Datos Personales: Indica si el activo de información contiene o no datos personales.
  - Tipos Datos Personales: Si la respuesta de la columna es afirmativa, escoger la opción de acuerdo al tipo de datos personales que contiene el activo de información.
- Valoración del activo de información
  - Confidencialidad: Hace énfasis a que la información no esté disponible ni sea revelada a personas, procesos o entidades no autorizados.
  - Integridad: Hace énfasis a la exactitud y completitud de la información, desde su creación hasta su destrucción.
  - Disponibilidad: Se refiere a que la información debe ser accesible y utilizable por solicitud de los funcionarios y contratistas o proceso autorizado cuando así se requiera.
- Propiedad del activo de información
  - Propietario: El cargo del propietario del activo de información.
  - Custodio: Indicar el cargo del custodio de la información. es decir la persona que realiza el control en el acceso al activo de información.
  - Localización: Ingresar la ubicación física y/o electrónica del activo de información.
  - Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

4.2 Valoración de Activos

Este proceso se realiza en conjunto con la organización, la cual ayuda a identificar en que dimensión es valioso el activo, para así valorar correctamente el coste que supondría para la organización la destrucción del activo.

Las dimensiones definidas por Magerit para valorar las consecuencias de la materialización de las amenazas son las siguientes:

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [DP] Datos personales

La valoración de las dimensiones puede ser de forma cuantitativa o cualitativa. Para este proceso en específico se usó un sistema cualitativo con los siguientes niveles numéricos:

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Despreciable

Tabla 2. Criterios de valoración de activos.

Fuente: Elaboración propia.

4.3 Identificación de amenazas

Concluido el proceso de valoración de los activos, lo siguiente consiste en identificar las amenazas que puedan afectar a cada activo. Se entiende como amenaza a

todo suceso que pueda afectar al activo de un sistema de información, generando perdidas del activo mismo o de la información controlada por él.

En el libro II: Catalogo de elementos. MAGERIT determina como típicas las siguientes amenazas a los sistemas de información:

- De origen natural

  Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.
- Del entorno (de origen industrial)

  Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
- Causadas por las personas de forma accidental

  Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- Causadas por las personas de forma deliberada

  Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

4.4 Valoración de amenazas

Una vez identificadas las amenazas puntuales que afrontan los activos del área de Almacén e Inventarios, se valoran estas amenazas con respecto a las dimensiones a las que afectarían, con el fin de estimar la frecuencia en la que puede ocurrir y el impacto que causarían.

El formato utilizado para relacionar la valoración de las amenazas está compuesto por los siguientes elementos:

- Activo

  Presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

- Amenaza

  Presenta la amenaza.

- D – dimensión

  Se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

- I – impacto

  Se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

- R – riesgo

  Se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

5. Resultados

5.1 Objetivo 1. Caracterizar los procesos relacionados al área de Almacén e Inventarios enfocados en los dominios de Gestión de Activos (8) y Seguridad Física y Ambiental (11) de la normativa ISO/IEC 27002:2013.

5.1.1 Checklist

El checklist aplicado cuenta con tres posibles respuestas (Si, No, N/A) las cuales según las respuestas indicadas por el personal permiten concluir que tanto se aplican en la empresa los objetivos de control y controles de los dominios seleccionados. A continuación, se cuantifica los resultados obtenidos del checklist en la siguiente tabla:

Dominio	Objetivo de Control Evaluados	Controles Evaluados	Preguntas	Si	No	N/A
8. Gestión de Activos	2	7	12	6	5	1
11. Seguridad Física y Ambiental	2	15	29	12	12	5

Tabla 3. Resultados checklist.

Fuente: Elaboración propia.

Para ver las preguntas realizadas de las cuales se obtuvieron las respuestas, dirigirse al anexo 1.

La tabla 1 ilustra los resultados obtenidos en las 41 preguntas realizadas, resaltando las respuestas positivas se obtuvieron un 44%, contra las negativas que representan un 41%. Una tercera columna sería la de preguntas cuya respuesta sería no aplica las cuales obtuvieron un 15%.

Figura 2. Resultados porcentuales del checklist.

Fuente: Elaboración propia.

Realizando el balance que representa el comparar las respuestas obtenidas con el porcentaje se entiende el panorama actual del área, ya que gracias a esta información se podrá realizar un análisis de riesgos de manera correcta debido a que se conoce los mecanismos empleados por el área según los dominios evaluados.

5.1.2 Análisis de GAP

EL análisis de GAP evidencia los resultados obtenidos a partir de las preguntas que contiene el formato (***véase anexo 4***) a su vez teniendo en cuenta los criterios de evaluación (***véase tabla 1***).

5.1.2.1 General

Inicialmente se debe tomar en consideración el resultado general de los anexos evaluados.

Estado	Significado	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	9%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	5%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	9%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	36%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	18%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	23%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%
	Total	100%

Tabla 4. Resultados generales de los anexos evaluados.

Fuente: Elaboración propia.

Figura 3. Resultado gráfico de los anexos evaluados.

Fuente: Elaboración propia.

La segmentación porcentual y grafica logradas indican que a un nivel general el área evaluada se encuentra en un nivel medio; existe el 41% (sumatoria de estados optimizado + administrado) de los procedimientos que los podemos catalogar como que se encuentran en un nivel alto; existe un 36% (estado definido) de los procedimientos a los cuales se les debe realizar una serie de ajustes y poder así catalogarlos como altos; existe un 23% (sumatoria de estados inexistente + inicial + repetible) de los procedimientos catalogados como bajo lo que requiere una atención prioritaria.

5.1.2.2 Anexo 8

Seguidamente se toma en cuenta los resultados obtenidos para la gestión de activos.

Estado	Significado	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	14%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	14%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	14%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	14%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	43%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%
	Total	100%

Tabla 5. Resultados anexo A8.

Fuente: Elaboración propia.

Figura 4. Resultado gráfico del anexo A8.

Fuente: Elaboración propia.

La segmentación porcentual gráfica resultante del Anexo 8 indica que 57% de sus procedimientos se pueden catalogar como altos esto es un buen indicador ya que al ser el área de almacén e inventarios realizan una buena gestión de sus activos; el 14% de sus procedimientos están en un nivel medio; un 28% de los procedimientos se catalogan como bajo esto significa que sebe prestar atención en ciertos procedimientos en especifico para poder subir su puntuación.

5.1.2.3 Anexo 11

Por utlimo, los resultados obtenidos para el anexo 11 son los siguientes.

Estado	Significado	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	7%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	0%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	13%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	47%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	20%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	13%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%
	Total	100%

Tabla 6. Resultados anexo A11.

Fuente: Elaboración propia.

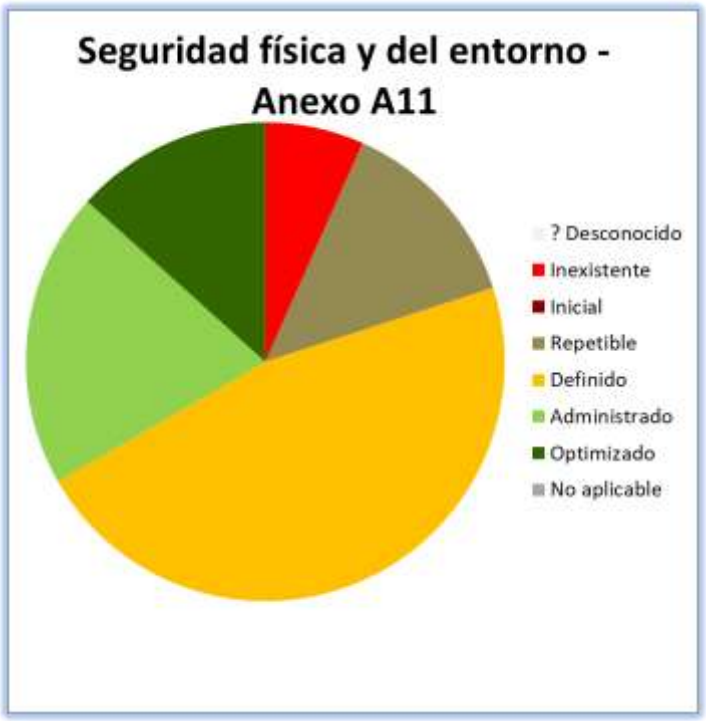

Figura 5. Resultado gráfico del anexo A11.

Fuente: Elaboración propia.

En la segmentación grafica y porcentual se encuentra un 33% de los procedimientos catalogados como alto; un 47% de los procedimientos lo cual es motivo de prestar atención ya que casi la mitad de sus procedimiento se encuentra en un rango medio por lo que se debe individualizar cada uno de los procedimientos en este rango y así poder fortalecerlos; un 20% de los procedimientos se encuentra catalogado como bajo lo que indica que se debe iniciar las labores con estos y de esta forma obtener un mejor resultado.

5.2 Objetivo 2. Identificar los activos de información relacionados al área de Almacén e Inventarios.

En las reuniones concretadas con el equipo de almacén e inventarios, se socializa la definición de activo de información (se puede definir como cualquier elemento tangible o intangible que sea de valor para la organización). De esta forma ellos identifican sus S.I (Sistemas de Información) como activos de información. Gracias a estos encuentros se

pudo recolectar la información necesaria y suministrar los datos para el formato de identificación de activos (***véase el anexo 2***).

MAGERIT en su libro II: Catalogo de elementos define los activos esenciales bajo 2 aspectos, la información que se maneja y los servicios que se prestan, a su vez realiza una clasificación de los activos (***véase el anexo 3***).

Aplicando el formato checklist preestablecido se determina cuáles son los activos esenciales que forman parte del área. Teniendo en cuenta esta clasificación se realizó el cargue de la información obtenida por el formato de identificación de activos (***véase anexo 2)*** al software de escritorio PILAR para la utilización de la metodología MAGERIT.

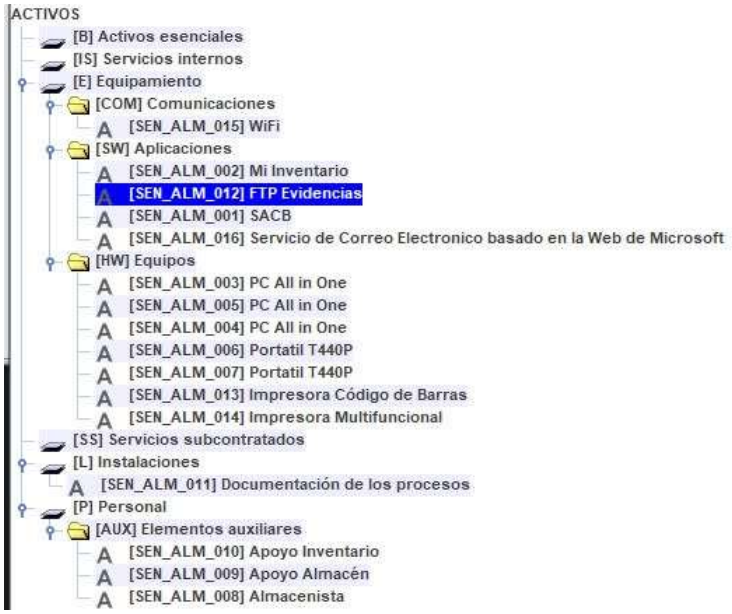

Figura 6. Activos de información

Fuente: Elaboración propia.

5.3 Objetivo 3. Analizar los riesgos del área de Almacén e Inventarios aplicando la metodología MAGERIT.

5.3.1 Valoración de activos

Siguiendo las normativas de la metodología MAGERIT, se realiza la valoración de los activos mediante la herramienta PILAR Basic 2021.1.6 de forma individual en cada una de las dimensiones establecidas, la siguiente tabla muestra a continuación los activos del área de Almacén e Inventarios y las valoraciones correspondientes:

ACTIVOS	DIMENSIONES					
	[D]	[I]	[C]	[A]	[T]	[DP]
EQUIPAMIENTO						
[SEN_ALM_015] Wifi	[8]	[2]	N.A.	N.A.	N.A.	N.A.
[SEN_ALM_002] Mi Inventario	[3]	[3]	N.A.	[7]	[2]	N.A.
[SEN_ALM_012] FTP Evidencias	[3]	[4]	N.A.	[0]	[2]	[8]
[SEN_ALM_001] SACB	[9]	[8]	N.A.	[9]	[7]	[7]
[SEN_ALM_016] Servicio de Correo Electrónico basado en la Web de Microsoft	[6]	[4]	[7]	[7]	N.A.	[6]
[SEN_ALM_013] Impresora Código de Barras	[4]	N.A.	N.A.	N.A.	N.A.	N.A.
INSTALACIONES						
[SEN_ALM_011] Documentación de los procesos	[5]	[6]	N.A.	N.A.	N.A.	N.A.
PERSONAL						
[SEN_ALM_008] Almacenista	[8]	[8]	N.A.	N.A.	N.A.	N.A.

Tabla 7. Valoración de activos.

Fuente: Elaboración propia.

5.3.2 Identificación y valoración de las amenazas

Por medio del aplicativo PILAR y del listado detallado de las amenazas del libro II de MAGERIT (***véase anexo 5***), se logran identificar las amenazas potenciales, así como también los activos a los que se le influye mayor índice de impacto y riesgo de ocurrencia, detallando en la siguiente tabla las dimensiones en las que cada amenaza afecta los activos de información.

ACTIVO	AMENAZA	D	I	R
[SEN_ALM_001] SACB	[E.24] Caída del sistema por agotamiento de recursos	D	[8]	{6,6}
	[A.24] Denegación de servicio	D	[9]	{6,6}
	[A.15] Modificación de la información	I	[8]	{6,3}
	[I.6] Corte del suministro eléctrico	D	[9]	{6,2}
	[A.18] Destrucción de la información	D	[9]	{6,2}
	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6,2}
	[E.25] Pérdida de equipos	D	[9]	{6,2}
	[E.18] Destrucción de la información	D	[9]	{6,2}
	[A.26] Ataque destructivo	D	[9]	{6,2}
	[A.8] Difusión de software dañino	D, I	[9]	{6,2}
	[I.10] Degradación de los soportes de almacenamiento de la información	D	[9]	{6,2}
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	[9]	{6,2}
	[I.1] Fuego	D	[9]	{6,0}
	[I.*] Desastres industriales	D	[9]	{6,0}
	[A.25] Robo de equipos	D	[9]	{6,0}

	[A.22] Manipulación de programas	D, I	[8]	{5,7}
	[I.5] Avería de origen físico o lógico	D	[8]	{5,7}
	[I.3] Contaminación medioambiental	D	[8]	{5,7}
	[I.8] Fallo de servicios de comunicaciones	D	[8]	{5,7}
	[I.2] Daños por agua	D	[8]	{5,4}
	[N.*] Desastres naturales	D	[9]	{5,4}
	[N.1] Fuego	D	[9]	{5,4}
	[A.23] Manipulación del hardware	D	[8]	{5,4}
	[A.28] Indisponibilidad del personal	D	[8]	{5,4}
[SEN_ALM_008] Almacenista	[A.15] Modificación de la información	I	[8]	{6,3}
	[E.24] Caída del sistema por agotamiento de recursos	D	[7]	{6,0}
	[A.24] Denegación de servicio	D	[8]	{6,0}
	[I.6] Corte del suministro eléctrico	D	[8]	{5,7}
	[A.18] Destrucción de la información	D	[8]	{5,7}
	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[8]	{5,7}
	[E.25] Pérdida de equipos	D	[8]	{5,7}
	[E.18] Destrucción de la información	D	[8]	{5,7}
	[A.26] Ataque destructivo	D	[8]	{5,7}
	[A.8] Difusión de software dañino	D, I	[8]	{5,7}
	[I.10] Degradación de los soportes de almacenamiento de la información	D	[8]	{5,7}
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	[8]	{5,7}

	[A.22] Manipulación de programas	I	[8]	{5,7}
	[I.1] Fuego	D	[8]	{5,4}
	[I.*] Desastres industriales	D	[8]	{5,4}
	[A.25] Robo de equipos	D	[8]	{5,4}
[SEN_ALM_015] Wi-Fi	[E.24] Caída del sistema por agotamiento de recursos	D	[7]	{6,0}
	[A.24] Denegación de servicio	D	[8]	{6,0}
	[I.6] Corte del suministro eléctrico	D	[8]	{5,7}
	[A.18] Destrucción de la información	D	[8]	{5,7}
	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[8]	{5,7}
	[E.25] Pérdida de equipos	D	[8]	{5,7}
	[E.18] Destrucción de la información	D	[8]	{5,7}
	[A.26] Ataque destructivo	D	[8]	{5,7}
	[A.8] Difusión de software dañino	D	[8]	{5,7}
	[I.10] Degradación de los soportes de almacenamiento de la información	D	[8]	{5,7}
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	[8]	{5,7}
	[I.1] Fuego	D	[8]	{5,4}
	[I.*] Desastres industriales	D	[8]	{5,4}
	[A.25] Robo de equipos	D	[8]	{5,4}
[SEN_ALM_016] Servicio de Correo Electrónico basado en la Web de Microsoft	[E.21] Errores de mantenimiento / actualización de programas (software)	C	[6]	{5,4}

Tabla 8. Identificación y valoración de amenazas.

Fuente: Elaboración propia.

5.4 Objetivo 4. Generar propuestas de valor a partir de los resultados obtenidos del análisis de riesgos.

5.4.1 Análisis de Gap

Gracias a la matriz de gap inicialmente realizada al área de almacén e inventarios se pudo identificar que los siguientes controles se encuentran catalogados como bajos, lo que indica que se debe iniciar a trabajar con ellos, ya que representan una vulnerabilidad a los procesos de los sistemas de información:

- A8 Gestión de activos.
  - A8.3 Manipulación de los soportes.
    - ✓ A8.3.2 Eliminación de los soportes: Creación de una política específica y documentación de obligaciones, legales o reglamentarias para la eliminación de los medios contractuales. Los datos particularmente confidenciales se deben eliminar de forma segura (borrado criptográfico, desmagnetización o destrucción física).
    - ✓ A8.3.3 Soportes físicos en tránsito: Aplicar un mecanismo de cifrado adecuado durante el proceso de transferencia de activos de información.
- A11 Seguridad física y del entorno
  - A11.1 Áreas seguras
    - ✓ A11.1.3 Seguridad de oficinas, despachos y recursos: Mejoramiento en los controles de seguridad y acceso donde se encuentran los activos de información.
  - A11.2.2 Seguridad de los equipos
    - ✓ A11.2.2 Instalaciones de suministro: Implementar un sistema de UPS que proporcione una potencia adecuada, confiable y de alta calidad para los activos de información.
    - ✓ A11.2.7 Reutilización o eliminación segura de equipos: Implementar una política de borrado seguro a los equipos puestos a eliminación.

5.4.2 Análisis de riesgos.

Basados en la información resultante de la identificación y valoración de amenazas, se recomienda la creación de salvaguardas que logren mitigar o controlar el impacto de las amenazas a los siguientes activos de información:

- [SEN_ALM_001] SACB
- [SEN_ALM_008] Almacenista
- [SEN_ALM_015] Wi-Fi
- [SEN_ALM_016] Servicio de Correo Electrónico basado en la Web de Microsoft

Esta recomendación se hace ya que estos activos son a los que se encontraron mayor número de amenazas por lo tanto es de suma importancia la mitigación de estos.

Conclusiones

- Las reuniones con las personas involucradas directamente en los procesos relacionados a las áreas que se van a analizar son de suma importancia, ya que ellos son la mayor fuente de información relevante.
- Conocer los procesos de la organización permite un mejor resultado en la identificación de los activos de información, lo cual conlleva a una valoración más exacta, permitiendo la identificación de las amenazas potenciales relacionadas a cada activo.
- El uso de la herramienta PILAR complementa el análisis de la gestión de riesgo, dando informes precisos acerca de la identificación, valoración e impacto de las amenazas, partiendo desde la información suministrada a la herramienta.
- El área de Almacén e Inventarios del Centro de Gestión y Desarrollo Agroindustrial de Arauca SENA posee aspectos que mejorar para lograr una eficiente gestión de riesgos, el análisis Gap evidencia la existencia de numerosos controles en etapas que van de inexistentes hasta definidas, las cuales deben ser mejoradas de forma inmediata para así preservar la seguridad del sistema de información.

Referentes bibliográficos

Benavides C, J. C. (2013). *Integración de la NTC ISO/IEC 27001:2013 con el Modelo de Seguridad y privacidad de la Información-MSPI del MinTIC.* Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6368/INTEGRACI%C3%93N%20DE%20LA%20NTC-ISO-IEC%2027001%20V2013%20CON%20EL%20MODELO%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACI%C3%93N-MSPI.pdf?sequence=1&isAllowed=y

CCN-CERT. (29 de Julio de 2020). *Centro Criptológico Nacional.* Recuperado de: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10388-nuevo-portal-de-pilar-la-solucion-de-analisis-y-gestion-de-riesgos-del-ccn.html#:~:text=La%20soluci%C3%B3n%20PILAR%20es%20una,de%20los%20Sistemas%20de%20Informaci%C3%B3n

ISOTools. (8 de Marzo de 2018). *¿Qué es un checklist y cómo se debe utilizar?* Recuperado de ISOTools: https://www.isotools.org/2018/03/08/que-es-un-checklist-y-como-se-debe-utilizar/

Javier Valencia-Duque, F., & Orozco-Álzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI : Revista Ibérica de Sistemas e tecnologías de Informação*, 22, 73–88. https://doi.org/10.17013/risti.22.73-88

Mina Calderón, L. (2015). *Auditoria de seguridad de la información e infraestructura de ti de la empresa de energía de Arauca Enelar e.s.p. del departamento de Arauca*. Universidad Cooperativa de Colombia, ¿Facultad de Ingenierías, Programa de Ingeniería de Sistemas, Arauca?, Colombia, 21101.

Mineducación. (2013). *Guía de evaluación de controles normas ISO 27001: 2013.* Recuperado de https://sig.mineducacion.gov.co/files/mod_documentos/documentos/PM-GU-04/PM-GU-04%20V3.pdf

Ministerio de hacienda España. (2012). Metodología de análisis y gestión de riesgos de los sistemas información. España, España.

Montes, K. (2014). *identificación de los controles de seguridad física del Centro de Datos de la Universidad Autónoma de Occidente.* Recuperado de https://red.uao.edu.co/bitstream/handle/10614/6604/T04621.pdf;jsessionid=1B28DB8A05B5CEEF32DE11799F0CF5C8?sequence=1

NORMA ISO 27001. (21 de febrero de 2019). *FASE 1 AUDITORIA INICIAL ISO 27001 GAP ANALYSIS.* Recuperado de NORMA ISO 27001: https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

Orjuela Carvajal, N., & Ballesteros Hernández, F. (2019). *Análisis de riesgos al proceso de gestión de tecnología de la información para la caja de compensación familiar del Tolima Comfatolima, sede administrativa–Ibagué.* Universidad Cooperativa de Colombia, Facultad de Ingenierías, Ingeniería de Sistemas, Ibagué.

Pabón Castrillón, L., & Beltrán Mendoza, M. (2015). *Estudio del análisis de riesgo acerca de la seguridad de la información a través de la gestión tecnológica en la asociación Frepaem-saravena*. Universidad Cooperativa de Colombia - Arauca Facultad de Ingeniería de Sistemas.

Rojas P, H. (2019). *Aplicación de la metodología Magerit para el análisis de riesgos de los sistemas de control en la estación Tenay del Oleoducto Alto Magdalena.* Recuperado

de https://repository.unad.edu.co/bitstream/handle/10596/27758/1075211684.pdf?sequence=1

Salamanca, O. (2016). *Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software*. Recuperado de https://dialnet.unirioja.es/descarga/articulo/5858358.pdf

SENA. (28 de Septiembre de 2020). *Quiénes somos.* Recuperado de SENA: https://www.sena.edu.co/es-co/sena/Paginas/quienesSomos.aspx

SENA. (s.f.). *3.1. Misión y Visión SENA.* Recuperado de SENA: https://www.sena.edu.co/es-co/sena/Paginas/misionVision.aspx

Tovar Callejas, N., & Salguero Rodríguez, A. (2018). *Auditoría interna a los activos físicos del área TI en la Universidad Cooperativa de Colombia sede Ibagué, aplicando el estándar ISO/IEC 27002:2013*. Universidad Cooperativa de Colombia, Facultad de Ingenierías, Ingeniería de Sistemas, Ibagué.

Anexos

Anexo 1. Formato de checklist.

Enlace: https://1drv.ms/x/s!AtlS6oD18ljrrEWSiPNm9VAS8XF7?e=iXV6bc

Anexo 2. Formato de Inventario de Activos.

Enlace: https://1drv.ms/x/s!AtlS6oD18ljrrEg7mrTXHULDvru1?e=afhntx

Anexo 3. Clasificación de activos MAGERIT.

Enlace: https://1drv.ms/x/s!AtlS6oD18ljrrEfWCUbELqUWmmE3?e=yblgou

Anexo 4. Análisis de GAP

Enlace: https://1drv.ms/x/s!AtlS6oD18ljrrEbwbjyCSTlwz4nW?e=eEInRk

Anexo 5. Catálogo de amenazas MAGERIT.

Enlace: https://1drv.ms/x/s!AtlS6oD18ljrrES45tPP2OfYG_2z?e=q3RR7w