Modelo de políticas de seguridad de la información bajo la norma ISO 27001 para la administración de activos de información en las cooperativas de trabajo asociado (CTA)

Oscar Javier Parra Avellaneda

Asesor

Manuel Antonio Sierra Rodríguez

Universidad Nacional Abierta y a Distancia-UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2026

Agradecimientos

Agradezco a la gran comunidad de la Universidad Nacional Abierta y a Distancia así mismo como agradezco al creador por ser parte de está, ya que ha sido parte esencial para mi crecimiento personal y profesional, espero seguir siendo miembro activo de la comunidad Unadista, adicionalmente deseo agradecer a todos los directivos, docentes y tutores de la universidad ya que gracia a ellos he adquirido muchos conocimientos y me invitan a ser más ambicioso en mi desarrollo intelectual.

Dedicatoria

Dedico este trabajo y este esfuerzo a mi familia ya que son los que han sido testigos de la voluntad y compromiso que he puesto para sacar adelante esta meta, espero ser un gran ejemplo para ellos de constancia y perseverancia.

Resumen

La presente monografía de recopilación de información está encaminada a la recolección de información para el agrupamiento de datos que sean teórico prácticos, pertinentes, válidos, aplicables y que aporten parámetros puntuales para que se pueda llevar a cabo un diseño de un modelo para la implementación de políticas de seguridad de la información que tenga como enfoque la administración de los activos de información de las cooperativas con la modalidad del trabajo asociado todo ello a partir de los estándares de la norma ISO 27001. En un entorno empresarial cada vez más divulgado y con una amenaza ante ciberataques las Cooperativas de Trabajo Asociado (CTA) están enfrentando desafíos críticos para proteger tanto la confidencialidad, la integridad y la disponibilidad de los datos sensibles de los miembros y clientes como y el proteger sus activos de información que son pieza fundamental en los procesos y procedimientos establecidos para cumplir las metas organizacionales.

Este trabajo se centra en el diseño de un modelo para la eficacia de la implementación de políticas de la seguridad de la información conforme a la norma ISO/IEC 27001 de acuerdo con el contexto de las Cooperativas de Trabajo Asociado. La norma ISO 27001 contempla un procedimiento sistemático y estructurado para el establecimiento, implementación, operación, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). Se hace necesario comenzar por la evaluación de la situación actual de las Cooperativas, en materia de gestión de sus activos de información, de la identificación de sus riesgos, amenazas y las brechas de seguridad que poseen. Posteriormente, a partir de la evaluación, se diseña un conjunto de políticas y procedimientos acordes a ISO 27001 que se correspondan con la naturaleza y las necesidades de este tipo de entidades.

El modelo que se describe a continuación se basa en el ciclo de Planificar-Hacer-Verificar-Actuar (PHVA) de la norma ISO 27001 y se necesita incidir en la importancia de una cultura de la seguridad que involucre a la totalidad de los miembros y empleados de la Cooperativa.

Se definen controles concretos que van desde la gestión de accesos, la seguridad física y lógica, hasta la formación y la toma de conciencia en materia de seguridad.

Por último, se muestran las guías para la implementación y mantenimiento del modelo, garantizando que las Cooperativas no solo puedan conseguir, sino también lograr la certificación ISO 27001, consolidando con ello su interés por la protección de los activos de información y fortaleciendo la confianza entre los socios y los Stakeholders.

Palabras clave: Seguridad de la información, Cooperativas de Trabajo Asociado, norma ISO 27001, gestión de riesgos, MAGERIT.

Abstract

This information-gathering monograph is aimed at collecting and grouping theoretical and practical, relevant, valid, and applicable data. It provides specific parameters to design a model for implementing information security policies focused on managing the information assets of associated work cooperatives, all based on the ISO 27001 standard. In an increasingly interconnected business environment facing constant cyberattack threats, Associated Work Cooperatives (AWCs) face critical challenges in protecting the confidentiality, integrity, and availability of sensitive member and client data. They must also protect their information assets, which are fundamental components of the processes and procedures established to achieve organizational goals.

This work focuses on designing a model to ensure the effective implementation of information security policies in compliance with the ISO/IEC 27001 standard, tailored to the context of Associated Work Cooperatives. The ISO 27001 standard provides a systematic and structured approach to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). It is necessary to begin by assessing the current situation of these cooperatives regarding their information asset management, identifying their risks, threats, and existing security gaps. Subsequently, based on this assessment, a set of policies and procedures aligned with ISO 27001 is designed to correspond with the nature and specific needs of these entities.

The model described below is based on the Plan-Do-Check-Act (PDCA) cycle of the ISO 27001 standard and emphasizes the importance of a security culture involving all cooperative members and employees. Specific controls are defined, ranging from access management, physical, and logical security to training and security awareness. Finally, guidelines for the

implementation and maintenance of the model are presented, ensuring that cooperatives can not only achieve but also maintain ISO 27001 certification, thereby consolidating their commitment to protecting information assets and strengthening trust among members and stakeholders.

Keywords: Information security, Associated Work Cooperatives, ISO 27001 standard, risk management, MAGERIT.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La época digital va asociada a la existencia de las tecnologías de la información y la comunicación en todos los espacios. Dicha época está transformando la forma en la que las organizaciones hacen las cosas y gestionan sus activos. Las Cooperativas de Trabajo Asociado, parte fundamental de la economía de las organizaciones de economía solidaria, no están fuera de esta corriente. Por ser entidades cuya forma de asociación hace muy eficientes las acciones para dar tráfico a los flujos de información, las Cooperativas de Trabajo Asociado requieren estrategias sólidas para defender y asegurar sus datos. Es en este sentido entonces se presenta la propuesta de implementar modelos de gestión que puedan hacer frente a los desafíos de los sistemas informáticos, pero que a la vez se alineen a los estándares aceptados y reconocidos a nivel internacional.

La norma ISO/IEC 27001 se convierte en una referencia internacional en este sentido, esta proporciona un modelo práctico para la creación, implementación y mantenimiento de un sistema de gestión de la seguridad de la información (SGSI) que responda a la protección de activos y la gestión de riesgos. Sin embargo, su implementación requiere un proceso de adaptación y de contextualización.

Dentro de este marco, el presente trabajo titulado "Modelo de Políticas de Seguridad de la Información bajo la Norma ISO 27001 para la Administración de Activos de Información en Cooperativas de Trabajo Asociado" se propone como un esfuerzo encaminado a la recolección de información teórica practica que permita establecer bases sólidas para plantear un diseño de políticas de seguridad de la información dirigido a los activos de información, que busque tender un puente entre los lineamientos de la ISO 27001 y la realidad operativa y organizacional de las

Cooperativas de Trabajo Asociado en Colombia. Ya sea que el propósito de la compañía sea implementar el modelo de seguridad de la información para sus sistemas actuales o en un futuro pretenda realizar una estructuración de sus sistemas de información, según Kosutic (2016), es importante en los nuevos sistemas de información identificar los requisitos necesarios en materia de seguridad aplicables a la información, esto es posible a través de la realización de un análisis que permita identificar claramente el propósito del sistema, así como los tipos de información que se procesaran, las responsabilidades que debe tener cada usuario, entre otros aspectos.

Ya que las cooperativas de trabajo asociado son consideras en la economía actual como organizaciones generadoras de empleo se debe tener en cuenta que la norma ISO 27001 es aplicable a estas tanto, así como los pasos iniciales en los que se aborda la evaluación y tratamiento de los riesgos, Cuervo Álvarez (2017), señala los siguientes pasos a seguir para implementar efectivamente la norma:

1. Obtener el apoyo de la dirección.
2. Utilizar una metodología para gestión de proyectos.
3. Definir el alcance de la SGSI.
4. Redactar una política de alto nivel sobre seguridad de la información.
5. Definir la metodología de evaluación de riesgos.
6. Realizar la evaluación y tratamiento de los riesgos.

Esta tarea se fundamentará, por un lado, en un diagnóstico situacional de las Cooperativas y su gestión de los activos de información, por el otro, en unas directrices que permitan el establecimiento de un diseño de modelo de acuerdo con las características de la organización y unas directrices de cómo llevar a cabo la implementación de dicho modelo. De este modo, se espera contribuir al fortalecimiento de las prácticas de seguridad de la información

las cuales son: preservación de la **confidencialidad,** la **integridad** y la **disponibilidad** de la información a través de la optimización de la protección de sus activos y consolidando una cultura de seguridad integral.

Definición del Problema

Antecedentes del Problema

Hoy en día, en esta era orientada hacia la digitalización, la seguridad de la información representa una preocupación de suma importancia para todos los tipos de organizaciones, independientemente de su tamaño y organización. En este sentido, las Cooperativas de Trabajo Asociado (CTA) juegan un papel importante porque unen sus características propias de organización cooperativa con el deber de controlar y proteger información sensible de los asociados y los clientes, además administrar y gestionar grandes cantidades de información y de datos críticos indispensables para el funcionamiento de la organización. Por otra parte, a medida que crece el volumen y la complejidad de la información digital, particularmente crecen las amenazas a la confidencialidad, la integridad, y la disponibilidad de la información, siendo esto un factor de vital importancia para que las CTA pongan en práctica estándares y buenas prácticas de seguridad de la información para la protección de sus activos de información, ya que la materialización de un incidente de seguridad puede tener consecuencias fatídicas, no solo económicamente hablando, sino que provocaría una crisis de confianza y reputación muy difícil de recuperar.

Formulación del Problema

La información es, por tanto, el activo más importante de las organizaciones, no tanto por su valor en términos económicos, sino por su significado y el papel que desempeña en el marco de la gestión de las operaciones que lleva a cabo la organización, y es por esta razón que ha de ser custodiada. Las políticas de seguridad animan a las organizaciones a implementar iniciativas proactivas en la búsqueda de mejoras continuas de la misma, de tal modo que la protección de la

información se realice desde el momento de su creación y registro hasta la eliminación, evitando con ello filtraciones, robos o modificaciones inapropiadas.

El estándar ISO 27001 es un marco universalmente reconocido por la comunidad internacional para gestionar y proteger los activos de información, mediante la implementación de los sistemas de gestión y seguridad de la información (SGSI). Este estándar ha sido utilizado con éxito por diferentes organizaciones en todo el mundo, es así que su implementación permitirá a las Cooperativas de Trabajo Asociado obtener importantes ventajas estratégicas y operativas a través de la transformación de la seguridad de la información en un proceso metódico y controlado, independientemente del tamaño y el propósito social de este tipo de organizaciones pertenecientes al sector solidario.

En este sentido, Rea-Guaman et al. (2018) señalan que se ha superado la noción de que la problemática de la ciberseguridad atañe únicamente a las organizaciones de gran envergadura. En el contexto actual, la creciente interconectividad en tiempo real sitúa a cualquier organización, independientemente de sus dimensiones, en una posición de exposición directa a las amenazas cibernéticas y al consecuente riesgo para sus activos.

La Norma ISO 27001, ofrece un enfoque sistemático y completo para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI):

Por lo tanto, surge la pregunta central:

¿En qué medida un modelo de políticas de seguridad de la información, adaptado a las CTA, facilita la categorización de activos y la gestión de sus riesgos asociados?

Justificación

La aplicación de políticas efectivas para la seguridad de la información que permitan la gestión y protección de los activos de información en las Cooperativas de Trabajo Asociado (CTA) son de vital importancia en la realidad digital actual. Es preciso tener en cuenta la continuada interconexión de sistemas, la proliferación de las amenazas cibernéticas y la medida de la evolución de los ataques en el momento en que se defina la implementación de medidas de seguridad informática, con objeto de proteger los activos de información en una organización.

Según Newmeyer (2015), en los últimos años se ha evidenciado que el nivel de ataques informáticos ha tenido una evolución peligrosa, ya que se ha pasado de simplemente vulnerar funcionalidades de un sitio web a sofisticados ataques relacionados con actividades de espionaje. Un ejemplo de esto el gusano informático Stuxnet, el cual demostró que puede causar daño tanto en datos como en infraestructuras de alto valor.

El aumento progresivo de la cantidad de datos sensibles hace que la seguridad de la información sea un imperativo estratégico para las organizaciones de todo tipo, incluidas las CTA. Esta justificación aborda la relevancia y necesidad de llevar a cabo un trabajo de investigación centrado en el diseño de un "Modelo de Políticas de Seguridad de la Información Bajo la Norma ISO 27001 para la Administración de Activos de Información en las Cooperativas de Trabajo Asociado (Cta)"

El estado colombiano en estos últimos años ha demostrado su interés por promover a las empresas del sector público y privado la adaptación de metodologías suficientes para proteger sus activos de información es así como a través de sus entidades gubernamentales promueve diferentes planes y proyectos para hacer esto posible.

> El Ministerio de Tecnología y las Comunicaciones (MinTIC) tiene desplegado a nivel nacional y territorial el modelo de seguridad y privacidad para apoyar la gestión e implementación de buenas prácticas y estándares para proteger los activos críticos de información, infraestructura tecnológica, y sistemas de información y comunicaciones, fomentando la mejora continua. (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020, p. 81)

Importancia de la Seguridad de los activos de Información en CTA: Las CTA representan una parte esencial de la economía global y en especial en el territorio colombiano en las cuales son una importante fuente de empleo para sus asociados, su éxito depende en gran medida en la confianza que puede generar para sus miembros y colaboradores ya que estos son los directamente beneficiados por el crecimiento integral de este tipo de organizaciones. Soriano Cortés (2021) explica que la relación entre asociados y cooperativa se enfoca en ofrecer oportunidades laborales a sus miembros a través de esfuerzos personales directos, ya sea a tiempo parcial o completo, organizando conjuntamente la producción de bienes o servicios para terceros. Además, pueden incluir socios colaboradores en este proceso.

Además, es esencial garantizar a los clientes de estas cooperativas que existen procesos y procedimientos que permiten gestionar de forma segura la información que se utiliza para los procesos internos de estas organizaciones. La pérdida de datos, la revelación no autorizada o ciertos incidentes de la seguridad pueden tener un impacto nefasto en la reputación y/o la continuidad operativa de estas organizaciones. Por lo tanto, es válido indicar que estas CTA deben desarrollar prácticas de seguridad rígidas para proteger los activos de información.

Desafíos específicos de las CTA: Las CTA presentan características específicas, como la toma de decisiones participativa y la estructura cooperativa, lo que precisa orientaciones de

seguridad de la información específicas para su propia naturaleza. Con frecuencia, las políticas y los estándares de la seguridad de la información adoptados para empresas tradicionales no son del todo adecuados para las necesidades de las CTA, lo que demuestra la necesidad existente de orientación.

Norma ISO 27001 como marco internacionalmente reconocido: La Norma ISO 27001 es un marco de referencia aceptado a nivel internacional en la gestión de la seguridad de la información. Al respecto, Calder (2017) indica que el estándar representa una descripción ideal para el sistema de gestión, en el cual se emplea una terminología basada en compromisos con el fin de cumplir los parámetros requeridos para satisfacer las auditorías internas o externas.

Su adopción brinda a las organizaciones un enfoque sistemático y efectivo para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Sin embargo, a pesar de sus beneficios, muchas CTA enfrentan obstáculos significativos al intentar implementar esta norma debido a su complejidad y a la falta de orientación específica.

Beneficios del modelo a plantear: La formulación de un modelo específico de desarrollo e implementación de políticas de seguridad de la información de la ISO 27001 en la gestión de activos de información en las CTAs respondería directamente a las necesidades de estas organizaciones, logrando proporcionar una guía concreta adaptada para ellos, haciendo posible su antesala a la implementación de políticas de seguridad de la información y, en último término, lograr la seguridad de los datos y aumentar la confianza en las CTA.

Contribución a la comunidad científica y empresarial: El planteamiento de este modelo no solo beneficiarían a las CTA, sino que también enriquecerían el cuerpo de conocimientos en

el campo de la seguridad de la información, proporcionando una solución concreta a un problema que afecta a muchas organizaciones en la actualidad.

La presente monografía de recopilación entiende su fundamento en la gran aportación que supone para la recolección, análisis y síntesis de la información de la bibliografía que se considere relevante y que sea de utilidad por el hecho de que sea objeto de estudio y comprensión y que conlleve la elaboración de un modelo orientado a la mejora de la seguridad de la información en las CTA y para hacer frente a los problemas peculiares de las mismas. El modelo que se elabore conseguirá ser una herramienta útil y práctica para ayudar a estas organizaciones en la implementación de políticas eficaces de seguridad de la información en sus activos de información y garantizar la seguridad de los datos relevantes generando confianza y una seguridad adecuada en entornos digitales que están en constante evolución.

Además, esta monografía persigue como fin agrupar, ordenar y sintetizar la información académica teoría-práctica que permita a través de su estudio y entendimiento establecer los parámetros esenciales que fortalezcan la forma en la que se desarrollará un modelo práctico que pueda dotar a las CTA de una guía para poder implementar las políticas de seguridad de la información referidas a la norma ISO 27001 que permitan gestionar y proteger los activos de información de las CTA, pero sin olvidar los intereses de quienes forman parte de la organización y de los propios clientes, al mismo tiempo que sirva como una forma de incrementar la confianza en las CTA en el marco de la economía de la información de hoy en día.

Objetivos

Objetivo General

Proponer un modelo teórico de políticas de seguridad de la información, a través de una compilación de información enfocada a los principios de aplicabilidad de la norma ISO 27001, para la administración de los activos de información de las cooperativas de trabajo asociado en Colombia.

Objetivos Específicos

Caracterizar la normatividad aplicable en Colombia a las cooperativas de trabajo asociado, en relación con gestión de activos de información, para el proceso de clasificación y organización siguiendo los parámetros de la norma ISO 27001.

Establecer las pautas a seguir para el análisis y valoración critica de los riesgos asociados a la gestión de activos de información en cooperativas de trabajo asociado, bajo lineamientos con base en la metodología MAGERIT.

Plantear un modelo de políticas de seguridad de la información, basado en la gestión de activos de información y el análisis de riesgos, con el propósito de mejorar la protección de los activos de información en las cooperativas de trabajo asociado en Colombia.

Marco Referencial

Marco Teórico

Seguridad de la Información

En toda entidad que desee adoptar las acciones imprescindibles para la protección de sus activos pertenecientes a la información es primordial tener presente el concepto de seguridad de la información, y como éste se convierte en el fundamento para la protección de estos activos en tales entidades, es esa la razón por la que la gestión de la seguridad de la información tiene que ser concebida como uno de los elementos básicos a la hora de establecer un marco de gobernanza de las tecnologías de la información, ya que su objetivo es conseguir estrictamente la mejor protección y conservación de los activos de información y, en consecuencia, del valor que tienen en todas y cada una de las etapas del ciclo de vida natural de los mismos.

Queda claro, entonces, que la gestión de la seguridad de la información no es un elemento aislado, según Calder (2017), esta disciplina constituye “el subconjunto del gobierno de TI que se centra en proteger y asegurar los activos de la información” (p. 11), lo que reafirma su papel central dentro del marco de gobernanza.

El propósito principal que busca la seguridad de la información es preservar la confidencialidad, integridad y disponibilidad de la información durante su ciclo de vida, independientemente de la forma en se presente, se utilice o se soporte.

La confidencialidad de la información es uno de los tres principios de seguridad de la información, ya que a través de ella se debe garantizar que los datos solo puedan ser accesibles por aquellas personas, entidades o procesos que estén debidamente autorizados para ello, según Cortés (2025) la implementación de la confidencialidad requiere de la existencia de un Sistema de Seguridad de la Información (SGSI) que gestione los niveles de acceso y, por consiguiente,

proteja aquel tipo de información confidencial contra los accesos no deseados o las divulgaciones indebidas.

La integridad, en el ámbito de la información, hace referencia al nivel de protección de la manipulación o bien del cambio de los datos-información de forma no autorizada. Este es uno de los tres conceptos fundamentales en la seguridad de la información. La no implementación de sistemas de seguridad de la información puede comprometer gravemente la integridad de los datos no solo porque personas no autorizadas puedan acceder a dichos datos. También puede comprometerse la integridad de la información dado que los datos pueden ser creados o modificados por personas autorizadas que pueden dañar la integridad bien porque lo hacen conscientemente o bien porque lo hacen inconscientemente.

El concepto de disponibilidad de la información implica la posibilidad de poder acceder a los datos cuando sea necesario y únicamente a aquellas personas que tengan el permiso adecuado. La disponibilidad de la información es un concepto fundamental para garantizar que se disponga de acceso para aquellos que lo necesitan, pero que al mismo tiempo se mantenga la información encriptada y bajo custodia. La falta de disponibilidad implicaría violaciones de la información y otros problemas. Por ejemplo, una interrupción del sistema o un ataque de red podría provocar situaciones de pérdida de disponibilidad y que la información no esté disponible para aquellos que la necesitan. Como se puede observar es importante poder garantizar que existan datos disponibles cuando sean necesarios y solamente para aquellos que tienen el permiso adecuado para acceder a ellos.

Los tres elementos principales de la seguridad de la información se preservan por medio de la gestión de las amenazas desde un Sistema de Gestión de la Seguridad de la Información (SGSI), y esta es la base del estándar ISO 27001, dirigido a proteger la información y los

sistemas que permiten el acceso a ella de usos, destrucciones o revelaciones no autorizadas. Se concibe mediante un enfoque sistemático en la gestión de la información sensible de una organización para protegerla, tomando en consideración a personas, procedimientos y sistemas tecnológicos, y desarrollando una gestión continua de los riesgos (Organización Internacional de Normalización & Comisión Electrotécnica Internacional [ISO/IEC], 2022).

El objetivo principal de un sistema de seguridad de la información es proteger la información contra el acceso no autorizado, el uso, la divulgación o la modificación. La falta de implementación de sistemas de seguridad de la información puede comprometer la integridad de los datos no solo debido al acceso de personas no autorizadas, sino también porque los datos pueden ser comprometidos debido a cambios no deseados, eliminación o porciones de datos por parte de una persona autorizada. Por lo tanto, es extremadamente importante cumplir con ISO 27001, que proporciona una guía precisa para la gestión de sistemas de seguridad.

Análisis del Riesgo

El análisis de riesgos es un proceso fundamental en la implementación de un sistema de seguridad de la información, ya que permite identificar amenazas y otros eventos adversos que pueden afectar los activos de información, así como desarrollar medidas de seguridad adecuadas para mitigarlos. Según Kosutic (2016), el propósito principal de la ISO 27001 es ser una suite para la asistencia y tratamiento del riesgo, por lo tanto, el análisis de riesgos es una parte importante de la implementación de la norma ISO 27001 y de cualquier sistema de seguridad de la información.

Proceso de Análisis de Riesgo en un Sistema de Gestión de Seguridad de la Información (SGSI). Este análisis está compuesto por lo siguiente:

Identificación del Contexto. Antes de entrar de lleno en el análisis en sí mismo, es fundamental saber cuál es el contexto de la organización. De este modo, habrá que averiguar cuáles son las necesidades y exigencias de seguridad, quiénes son los interesados y sus partes correspondientes, y cuál es la organización y la función del sistema de información.

Identificación de Activos. Todo SGSI se basa en la protección de activos "cualquier bien que tiene valor para la organización, que le permite llevar a cabo su normal operación y que es susceptible de ser atacado deliberada o accidentalmente reduciendo así su valor inicial" (Sevillano Jaén & Beltrán Pardo, 2021, p. 44). Los activos pueden ser físicos, como servidores o laptops, o intangibles, como datos o software. La organización debe hacer un inventario de todos sus activos y determinar su valor o importancia.

Identificación de Amenazas y Vulnerabilidades. La identificación es fundamental porque permite comprender y gestionar los riesgos de manera efectiva, lo que ayuda a proteger los activos de una organización:

- Amenazas: Factores o agentes externos que podrían causar daño a los activos, como hackers, malware, desastres naturales, etc.
- Vulnerabilidades: Debilidades inherentes al sistema o a los activos que podrían ser explotadas por amenazas. Pueden incluir configuraciones defectuosas, falta de actualizaciones, fallos en el software, entre otros.

Evaluación de Riesgos. Es el proceso de comparar el nivel de riesgo detectado durante el proceso de identificación con criterios de riesgo previamente establecidos.

Ayuda a determinar la magnitud de los riesgos y si es aceptable o si es necesario tratarlo, de acuerdo con Andrade Talero (2021), es necesario realizar una evaluación de riesgos, ya que al llevar a cabo este proceso se obtendrán los soportes necesarios que permitirán demostrar que se tiene una correcta precaución (p. 30).

Los criterios de evaluación del riesgo deberán ser coherentes con el contexto de la gestión de riesgos en el exterior y en el interior, como con los tipos de objetivos de la organización y con las opiniones de los stakeholders. En la evaluación del riesgo, la base principal de la decisión se restringe a cuánto riesgo es tolerable. Sin embargo, la posible consecuencia y la probabilidad y la confianza en la identificación y en el análisis de los riesgos son también aspectos por considerar. La combinación de algunos riesgos discretos que sean menores o moderados puede producir un riesgo total a nivel del criterio de evaluación de este que podría en un principio parecer inofensivo, pero que en la suma de varios elementos podría ser elevado y, por tanto, prisionero de una forma adecuada de atención.

Priorizar los Riesgos. Para priorizar los riesgos identificados en una organización, se deben seguir los siguientes pasos:

- Evaluar la probabilidad de que ocurra el riesgo: Es importante evaluar la probabilidad de que ocurra cada riesgo identificado. Esto implica determinar la posibilidad de que ocurra el riesgo y la frecuencia con la que podría ocurrir.
- Evaluar el impacto del riesgo: Después de evaluar la probabilidad de que ocurra el riesgo, es necesario evaluar el impacto que tendría en la organización si ocurriera. Esto implica determinar el daño potencial que podría causar el riesgo y la magnitud del impacto.
- Asignar una prioridad al riesgo: Después de evaluar la probabilidad y el impacto del riesgo, es necesario asignar una prioridad al riesgo. Esto implica determinar la importancia

del riesgo en relación con otros riesgos identificados y asignar una prioridad en función de su importancia.

- Desarrollar medidas de seguridad: Una vez que se han priorizado los riesgos, es necesario desarrollar medidas de seguridad para mitigarlos. Estas medidas pueden incluir la implementación de controles de acceso, la capacitación de los empleados en seguridad de la información, la implementación de software de seguridad, entre otros.
- Monitorear y revisar: Es importante monitorear y revisar regularmente las medidas de seguridad implementadas para asegurarse de que sigan siendo efectivas y de que se estén cumpliendo los objetivos de seguridad de la información de la organización.
- Cálculo del Riesgo: Riesgo: Impacto x Probabilidad. Este cálculo ayuda a priorizar los riesgos en función de su gravedad.

Evaluación y Decisión. Cuando se han determinado los riesgos, se deben evaluar en función de unos criterios que previamente se hayan establecido para decidir cuáles de ellos deberán ser objeto de tratamiento. No todos los riesgos deben ser tratados; algunos riesgos pueden ser aceptables y otros pueden requerir medidas de tratamiento o mitigación.

Tratamiento del Riesgo. Existen varias estrategias para tratar el riesgo, indican Sevillano Jaén & Beltrán Pardo (2021), que el proceso de gestión de riesgos contempla cuatro estrategias fundamentales de respuesta: la aceptación consciente, la evitación, la mitigación del impacto o la probabilidad, y la transferencia (o compartición) del riesgo a terceros, también señalan que este enfoque debe aplicarse a las diversas tipologías de riesgo que enfrenta una organización, tales como los estratégicos, financieros, operativos o de cumplimiento normativo, a continuación se describe cada estrategia:

- Mitigación: Implementar controles para reducir el impacto o la probabilidad.

- Transferencia: Trasladar el riesgo a otra parte, como mediante la compra de un seguro.
- Aceptación: Decidir aceptar el riesgo sin medidas adicionales.
- Evitación: Cambiar la situación para evitar completamente el riesgo.
- Documentación: Todo el proceso de análisis de riesgo debe ser documentado para asegurar la transparencia y la revisión futura. También proporciona evidencia para auditorías.

Revisión Periódica. El entorno tecnológico es dinámico, las amenazas y vulnerabilidades cambian con el tiempo. Por ello, es esencial revisar y actualizar regularmente el análisis de riesgo para garantizar que el SGSI sigue siendo relevante y eficaz.

Este proceso es una parte esencial del SGSI según la norma ISO/IEC 27001 y asegura que la organización tiene un enfoque estructurado y metódico para gestionar los riesgos relacionados con la información.

Marco Conceptual

Activos de Información

Son todos aquellos datos, documentos o sistemas informáticos que tienen valor para una organización, según Andrade Talero (2021) “se denomina así a cualquier elemento o información de valor o indispensable para el cumplimiento de los objetivos organizacionales”. (p. 12). Pueden ser tangibles (hardware, documentos físicos, personas) o intangibles (software, datos electrónicos, conocimiento).

Seguridad de la Información

Se refiere a la protección de la información contra el acceso no autorizado, su divulgación, modificación, destrucción o interrupción. Su objetivo es garantizar la

confidencialidad, integridad y disponibilidad de los datos, independientemente de su forma: electrónica, impresa u otro tipo (Cuervo Álvarez, 2017, p. 20).

Cooperativas de Trabajo Asociado

Organizaciones democráticas, autónomas y voluntarias formadas por personas que buscan satisfacer sus aspiraciones y necesidades económicas, sociales y culturales comunes a través de una empresa conjunta de propiedad conjunta y democráticamente controlada (Horta-Solano, 2018, pp. 2-3).

Norma ISO/IEC 27000

La norma ISO 27000 se dedica a ofrecer una perspectiva completa sobre los sistemas de administración de seguridad de la información, e incluye directrices adecuadas para todas las normativas dentro su familia ISO 27000.

Norma ISO/IEC 27001

La norma ISO/IEC 27001 se ha consolidado como el estándar de referencia para la gestión de la seguridad de la información, gracias a que provee un marco sistemático para la implementación, mantenimiento y mejora continua de un SGSI. Al respecto, Cuervo Álvarez (2017) la define como un estándar internacional emitido por ISO que especifica la metodología para gestionar la seguridad de la información de forma organizada en una empresa (p. 6). Esta capacidad de estandarización es la clave de su amplia adopción global.

En ella se especifican los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI, proporcionando un enfoque basado en riesgos para garantizar la confidencialidad, integridad y disponibilidad de la información.

Se enfoca en garantizar la información frente al acceso no autorizado, uso, divulgación o modificación, pone énfasis en garantizar la confidencialidad, integridad y disponibilidad de la

información, sirve para mejorar el estado de preparación de la empresa para poner en marcha la norma y para medir este estado de preparación. Es muy utilizada en todo el mundo para garantizar la seguridad de la información en las organizaciones.

Según Watkins (2022) la estructura de la norma sigue una secuencia lineal, desde el establecimiento inicial del SGSI hasta su revisión y ajuste. No obstante, no es obligatorio abordar los requisitos en ese orden específico. En versiones anteriores, la norma estaba alineada con el reconocido modelo de mejora continua, Planificar-Hacer-Verificar-Actuar (PHVA), sugiriendo que era el mejor enfoque para diseñar, desarrollar e implementar un SGSI efectivo. Aunque esta metodología ya no es un requisito estricto en la ISO 27001, sigue siendo un enfoque válido y eficaz. Es la norma principal dentro de la serie 27001, ya que cubre todas las especificaciones relevantes para el sistema de administración de seguridad de la información. Posee un Anexo A que esboza brevemente los propósitos de los dominios y sus controles, tal como se describen en la ISO 27001:2022, para facilitar su aplicación en las organizaciones al estructurar los SGSI (ISO/IEC, 2022).

Norma ISO/IEC 27002

Es reconocida como la guía de prácticas óptimas que detalla todos los propósitos de control sugeridos y las valoraciones propuestas vinculadas a la protección de la información. En su edición más reciente, incluye 93 controles clasificados en 4 dominios; organizacionales, de personas, físicos y tecnológicos (ISO/IEC, 2022).

Norma ISO/IEC 27003

Es una normativa global que ofrece orientación para la instauración de un SGSI. Está diseñada para quienes desean implementar un SGSI y también para consultores en su labor cotidiana, ya que aborda algunos temas que anteriormente no contaban con un enfoque

estandarizado (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2017).

Evaluación de Riesgos

Proceso de identificación, clasificación y priorización de riesgos. Se basa en la comprensión de la probabilidad y el impacto potencial de un evento no deseado en la confidencialidad, integridad o disponibilidad de la información. Según Watkins (2022), para que la evaluación de riesgos sea eficaz la organización debe considerar todas las probabilidades de que algo falle en relación con la información que el SGSI pretende proteger.

Políticas de Seguridad

Documentos formales que delinean las directrices y prácticas específicas de una organización en cuanto a la gestión y protección de la información. Establecen un marco de comportamientos, expectativas y responsabilidades para empleados, miembros y terceros.

Es responsabilidad de la alta dirección establecer políticas que: Sean apropiadas para la organización, agregue objetivos de seguridad de la información, incluya compromiso para cumplir los objetivos acordes a garantizar la seguridad de la información, busquen la mejora continua del sistema de gestión de seguridad de la información, sea información documentada disponible (ISO/IEC, 2022, p. 9).

Magerit

Estrategia diseñada para el análisis y manejo de riesgos, desarrollada por el Consejo Superior de Administración Electrónica, surgida de la necesidad de las sociedades que se apoyan en las tecnologías de la información para alcanzar sus objetivos. Esta metodología se asocia estrechamente con la adopción tecnológica, aportando beneficios significativos a la población. Según Valencia Valderrama (2019), define una secuencia de acciones que comienza con el

reconocimiento de los recursos y cómo se relacionan entre sí en la empresa, después, es esencial identificar las posibles amenazas que puedan afectar dichos recursos.

Gracias a esta metodología es posible identificar riesgos que sea posible mitigar mediante implementaciones de seguridad que proporcionen confianza. Dicha estrategia incluye acciones orientadas hacia los recursos que una entidad utiliza para procesar la información.

Sistema de Gestión de Seguridad de la Información

Un SGSI es un sistema global que está constituido por políticas, procedimientos y directrices, además de recursos y actividades, con las cuales la organización gestiona y reúne el objetivo de asegurar sus activos de información críticos. Para el estándar internacional ISO/IEC 27001, un SGSI es un método sistemático para lograr establecer, poner en marcha, realizar el seguimiento y mejorar de forma continua la seguridad de la información de una organización, logrando los objetivos de negocio o de servicio.

El SGSI puede ser de toda la organización o de alguna parte de ella. Resulta central puesto que la información es vista como un valioso activo que debe ser asegurado, de acuerdo con la disponibilidad, confidencialidad o integridad. De hecho, la organización puede incorporar medidas de seguridad adicionales como autenticidad y trazabilidad, según sus necesidades o requisitos.

Un Sistema de Gestión de la Seguridad de la Información debe incluir Requisitos Generales documentados, la formulación y administración del SGSI, su puesta en marcha y funcionamiento, así como su monitoreo y revisión. También es crucial que incorpore actualizaciones y mejoras para mantenerse al día y eficiente ante los rápidos avances tecnológicos. Este sistema ayuda a proteger a la entidad de diversas amenazas, garantizando la

confidencialidad, integridad y acceso a sus activos informativos, al respecto, Argüezo Ramírez (2019)afirma que el propósito principal del SGSI es:

> Garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (pp. 38-39)

Tratamiento de Riesgo

El Ministerio de Hacienda y Administraciones Públicas (MINHAP, 2012), define este concepto como:

> Proceso destinado a modificar el riesgo. Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario. (p.10)

Marco Histórico

Orígenes de la Seguridad de la Información

El término seguridad de la información no es ningún término nuevo, desde el momento en el que el ser humano pudo registrar y almacenar información se han buscado alternativas para proteger la misma. En las civilizaciones antiguas, la información se guardaba en tablillas de arcilla o en papiros y se resguardaba de la forma más segura posible. Con la llegada de la imprenta y, posteriormente, con el desarrollo de las tecnologías de la información, la necesidad de proteger la información se puso de manifiesto.

Evolución de la Seguridad Informática

Con la llegada de las primeras computadoras en la década de 1950 y 1960, la seguridad informática comenzó a tomar forma. Las organizaciones empezaron a darse cuenta de la importancia de proteger la información digital. En las décadas de 1970 y 1980, con la popularización de las computadoras personales y las redes, surgieron los primeros virus y malware, lo que llevó a la creación de las primeras soluciones de seguridad informática.

Nacimiento de la Norma ISO/IEC 27001

La Norma ISO/IEC 27001 tiene sus raíces en el estándar británico BS 7799, publicado por primera vez en 1995 por la British Standards Institution (BSI). Tras ser adoptado por la ISO y la IEC EN 2005, se consolido como el referente global; al respecto, Calder (2017)menciona que “La norma internacional sobre la gestión de la seguridad de la información se publicó en 2005 y se actualizó en 2013, se está volviendo muy conocida y segura” (Calder, 2017, p. 18).

Cooperativas de Trabajo Asociado en Colombia

Las cooperativas de trabajo asociado en Colombia tienen una larga tradición, que se remonta a mediados del siglo XX. Estas entidades, que promueven la solidaridad y el trabajo conjunto, han jugado un papel fundamental en el desarrollo socioeconómico del país. Sin embargo, su evolución también las ha llevado a enfrentar desafíos en términos de gestión y protección de la información.

Adopción de Tecnologías de la Información en Cooperativas

A finales del siglo XX y principios del siglo XXI, las cooperativas de Colombia, como la mayoría de las organizaciones a nivel internacional, empezaron a incorporar las tecnologías de la información para mejorar sus operaciones. Este proceso de transformación digital acerco nuevos desafíos en términos de seguridad de la información que han llevado a muchas de estas

organizaciones a buscar marcos y estándares que les ayuden a proteger sus activos de información.

Antecedentes o Estado Actual

En el proyecto de Argüezo Ramírez Edgar Daniel, que presenta a la Facultad de ingeniería de la Universidad de Huanaco Perú un trabajo de suficiencia profesional titulado *"Propuesta de un sistema de gestión de seguridad de la información para la protección de activos de la información basado en la norma ISO 27001 en el área de informática de la municipalidad provincial de Huanaco" (Argüezo Ramírez, 2019),* como requisito para optar al título de ingeniero de sistemas e informática.

El estudio se enfoca en la elaboración y diferenciación de un Sistema de Gestión de Seguridad de la Información para una entidad gubernamental municipal, específicamente la Municipalidad de Huanaco. En este contexto, se propone una metodología PDCA dividida en 5 etapas en las cuales se establece el contexto en la cual se establecen objetivos, alcance y políticas del sistema de gestión de seguridad de la información , en la segunda etapa en la cual se busca la identificación de riesgos se adopta la metodología MAGERIT en lo que se destaca la identificación y valoración de activos, para la tercera etapa se busca el análisis de riesgos identificando amenazas, vulnerabilidades y controles, en una cuarta etapa se tiene como objetivo realizar la evaluación de los riesgos estableciendo su frecuencia e impacto, para la quinta y última etapa se propone establecer un plan de tratamiento de riesgos y determinar los controles que apoyaran con la reducción de los riesgos finalmente se presentan los resultados para los objetivos propuestos.

La contribución de Argüezo al proyecto actual radica en su análisis profundo sobre el desarrollo de la norma ISO 27001 como herramienta guía para la protección de los activos de

información. Es esencial subrayar el valor de realizar correctamente un inventario de activos de información permitirá establecer todos los escenarios posibles en que un determinado riesgo pueda afectar la seguridad de la información, en este proyecto se propone utilizar la metodología MAGERIT para proyectar correctamente los posibles riesgos que puedan llegar a impactar en los activos de información (Argüezo Ramírez, 2019).

El trabajo de Rafael Suarez, que presenta a la Escuela de ciencias básicas tecnología e ingeniería de la Universidad Nacional Abierta y a Distancia para preferir Título Profesional de Especialista en Seguridad Informática, en tesis que lleva de nombre *"Análisis de Activos de información Para un Sistema misional basados en la metodología MAGERIT V3 y la norma ISO 27001:2013"* (Suárez González, 2018).

Este trabajo establece los lineamientos básicos para analizar los activos de información, haciendo un correcto uso de la metodología MAGERIT e implementación de la norma ISO 27001:2022 con la finalidad de una correcta gestión de riesgos con el propósito de establecer una necesaria política de seguridad informática. Está monografía tiene como objetivo identificar y clasificar los activos de la entidad caso de estudio, permitiéndose determinar el nivel de impacto, riesgo y vulnerabilidades a través de la valoración de activos de información, con la meta de proponer controles que la entidad pueda implementar en base al ANEXO A de la norma ISO 27001.

La metodología aplicada en está monografía corresponde a una investigación descriptiva en la cual las entrevistas a personal expertos en el área de tecnología fue el método utilizado para la recolección de información con una muestra del 10% de las personas funcionarias de la entidad Caso Estudio.

El proceso de desarrollo de la presente monografía está conformado inicialmente por una evaluación del estado actual de la entidad Caso Estudio, en la cual se realiza una descripción detallada de la estructura organizacional de la entidad, una descripción de su estructura tecnológica y una descripción de sus sistemas de información.

Posteriormente se realiza una clasificación de los activos de información de la entidad Caso Estudio, para seguir con el uso de la Metodología MAGERIT para realizar la clasificación de los activos según su valoración por dimensiones, posterior a esto se realizar la identificación de las vulnerabilidades y amenazas a los que se encuentran expuestos los activos de información de la entidad Caso de Estudio, continuando con la identificación de riesgos para llegar finalmente a la formulación de controles de los activos de información, como recomendaciones finales se recomienda fortalecer los proceso de manejo de activos de información, a través de políticas formales que den pautas para el manejo adecuado de la información y sus activos.

Está monografía aporta al proyecto el detallado proceso expuesto sobre el uso de la metodología MAGERIT para el análisis y gestión de riesgos, hallazgos de vulnerabilidades e implementación de controles que permitan proteger los activos de información (Suárez González, 2018).

Marco Científico o Tecnológico

Antecedentes Científicos

Norma ISO 27001. Estándar internacional reconocido que establece los criterios para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona un enfoque sistemático para proteger la confidencialidad, integridad y disponibilidad de la información, mediante la identificación de riesgos y la implementación de controles de seguridad adecuados.

Gestión de Activos de Información. Las investigaciones previas han demostrado la importancia de gestionar adecuadamente los activos informativos de una organización, considerándolos como esenciales para su operación y valor estratégico. Se puede resumir su evolución de la siguiente manera:

1. Fase 1. Hardware Enfocado (Años 70 - 80): En la época de los grandes ordenadores, "gestión de activos" era igual a la gestión de los activos fijos:

- Enfoque: El contenedor.
- Activo Principal: El ordenador central (el hardware).
- Preocupación: Costo de adquisición, mantenimiento físico y depreciación contable.
- Analogía: Proteger la caja fuerte. El valor residía en la pesada y costosa caja fuerte física.

2. Fase 2. Gestión de los Activos de TI (Años 90): Una vez llegó el PC y las redes de área local (LAN), el manejo del software ya no estaba centralizado, el matiz del software empezaba a desplazarse hacia el hardware:

- Orientación: El contenedor y su conjunto de herramientas.
- Activo clave: PCs, servidores, y muy principalmente, licencias de software.
- Preocupación: Mantener el control del inventario de máquinas distribuidas y evitar multas por licenciamiento del software (gestión del cumplimiento de software).
- Analogía: Mantener protegidas las cajas fuertes (ahora más pequeñas y distribuidas) y gestionar las llaves (licencias).

3. Fase 3. El Nacimiento de la Seguridad de la Información (Años 2000): El crecimiento descontrolado de Internet, del comercio electrónico y los primeros ciberataques de

masas deberían dar un vuelco. Estándares como ISO 27001 (en sus primeras versiones) formalizan entonces un nuevo concepto:

- Enfoque: El contenido (los datos).
- Activo Principal: La información, los datos (bases de clientes, propiedad intelectual) se han popularizado como un activo porque tienen valor propio.
- Preocupación: La Tríada CIA (Confidencialidad, Integridad y Disponibilidad). Se desarrolla la necesidad de identificar y clasificar la información para saber qué proteger.
- Analogía: Evidenciar que lo que hay dentro de la caja fuerte es lo realmente importante.

4. Fase 4. Gobernanza de Datos y Valor Estratégico (Años 2010 - Presente): El Big Data, la analítica y la nube están marcando esta etapa, además de que la gestión de los activos de información se une a la estrategia del negocio y a la exigencia de cumplimiento normativo:

- Enfoque: El valor estratégico y el riesgo del contenido.
- Activos Principales: La información como motor del negocio, la privacidad de los datos personales y los algoritmos.
- Preocupaciones: Surge la necesidad de cumplir con las leyes como el GDPR (en Europa) o el CCPA (en California) con el propósito de no sufrir sanciones superiores a los millones de euros o dólares por una mala gestión de los datos personales. Ya no es una opción gestionar los activos, sino que se debe hacer por ley, así mismo se toma como estrategia de valor los datos con los cuales las compañías los pueden aprovechar para predecir el comportamiento del cliente, para optimizar las operaciones internas o crear nuevas ofertas.

- Analogía, El dinero (los datos) ya no solo se guarda: se invierte, se presta, genera intereses (valor). Si se hace mal, la multa del regulador puede provocar la quiebra de la empresa (riesgo).

Antecedentes Tecnológicos

Sistemas Integrados de Gestión. Las tecnologías actuales permiten la integración de múltiples sistemas de gestión en una sola plataforma, facilitando la implementación y monitoreo de políticas y protocolos de seguridad.

Herramientas de Identificación y Evaluación de Riesgos. Existen en el mercado diversas soluciones tecnológicas que facilitan el proceso de identificación, evaluación y tratamiento de riesgos asociados a los activos de información. Las cuales se encuentran clasificadas de la siguiente forma:

- Plataformas de gobernanza riesgo y cumplimiento: Entre las cuales se encuentra Service Now GRC, indica Acosta (2024), que ServiceNow opera de forma centralizada para la automatización de tareas empresariales, proporcionando servicio absolutamente a todas las funciones departamentales, desde TI y recursos humanos a la gestión de riesgos, a la auditoría y al servicio al cliente.
- Escáneres de Vulnerabilidades: En este apartado se puede incluir a OpenVas, el cual afirma Barquero Pastor (2024), que es un completo programa de análisis de vulnerabilidades con funcionalidades fundamentales, desde escaneos autenticados o no autenticados, hasta la máxima optimización del rendimiento para redes de gran tamaño. Su arquitectura implica contar con un lenguaje de programación propio para identificar cualquier brecha de seguridad, y es también la herramienta que más protocolos industriales y de internet sostiene.

- Software de gestión de riesgos: En este caso se encuentra RiskWatch el cual es una plataforma de software de gestión de riesgos con el cual las organizaciones pueden identificar, evaluar y mitigar riesgos de manera sistemática, este puede seguir marcos como NIST o ISO 27001.

Estado Actual en Bogotá

Desarrollo Tecnológico. Bogotá como principal centro económico y tecnológico de Colombia, cuenta con un ecosistema digital en constante evolución, impulsado por el crecimiento del sector TIC y la necesidad de adaptarse a las dinámicas de la economía digital.

Ciberseguridad en Cooperativas. Aunque Bogotá es una ciudad donde existe la alta disponibilidad tecnología, muchas cooperativas no han implementado políticas de seguridad de la información eficaces, exponiéndose así a un entorno creciente de ciberamenazas, está afirmación encuentra respaldo en los hallazgos de Calle-Piedrahita, Malavera-Pineda y Portilla-Rosero (2022). Estos autores, tras estudiar el sector solidario durante el año 2020, concluyeron que la inversión tecnológica en el sector no está orientada a mejorar el desempeño social o a mitigar riesgos, sino que se concentra casi exclusivamente en la fidelización de los clientes actuales, dejando de lado aspectos fundamentales como la ciberseguridad. Esta brecha evidencia que el enfoque tecnológico de las cooperativas es reactivo y comercial, no estratégico ni preventivo. Los mismos autores advierten, en sus conclusiones, que una correcta transformación digital requiere, entre otros elementos, "mejorar la ciberseguridad e incrementar la competitividad y productividad" (Calle-Piedrahita et al., 2022, p. 8).

Desarrollos Recientes y Tendencias

Automatización y Machine Learning. Las nuevas tecnologías permiten la automatización de procesos de seguridad y la implementación de sistemas de aprendizaje automático para detectar anomalías o amenazas en tiempo real.

Adopción de la Nube. Las cooperativas están migrando sus sistemas y datos a soluciones en la nube, lo que implica nuevos desafíos y consideraciones en términos de seguridad de la información.

Retos y Desafíos

Formación y Concienciación. Es esencial promover una cultura de seguridad en todos los niveles de la cooperativa, capacitando a los empleados sobre las mejores prácticas y responsabilidades.

Adaptabilidad. Las políticas y soluciones tecnológicas deben ser flexibles y adaptarse a un entorno en constante cambio, garantizando que las cooperativas estén preparadas para enfrentar amenazas emergentes.

Marco Legal

Ley Estatutaria 1266 de 2008. "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" (Congreso de la República de Colombia, 2008).

Ley Estatutaria 1581 de 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales, Congreso de la República de Colombia (2012) afirmo:

> La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Ley 1273 de 2009. Establece las conductas relacionadas con el delito informático y su sanción, lo que refuerza la necesidad de mantener sistemas de información seguros y protegidos (Congreso de la República de Colombia, 2009).

Ley 79 de 1988. Esta ley le permite al sector cooperativo contar con un marco jurídico que le brinde condiciones legales para su constitución, crecimiento y funcionamiento, reconociendo al sector cooperativo como parte importante de la economía colombiana (Presidencia de la República de Colombia, 1990).

Constitución Política de Colombia. La Carta Magna garantiza el derecho a la privacidad y a la protección de datos personales, estableciendo la base legal para la gestión de la seguridad de la información en cualquier organización dentro del territorio colombiano.

Normatividad Aplicable en gestión de activos de información para las Cooperativas de Trabajo Asociado

La normativa vigente en Colombia relacionada con la administración de activos de información en el sector solidario se basa en la Política General de Seguridad y Privacidad de la Información emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así mismo la Superintendencia de la Economía Solidaria, se encarga de fiscalizar y velar por el cumplimiento de las leyes por parte de las organización del sector de la economía solidaria esto incluye a las cooperativas de trabajo asociado. Es así como una de las funciones de la Supersolidaria es supervisar que las organizaciones de economía solidaria cumplan con las leyes gubernamentales relacionadas con la gestión y seguridad de la información (Presidencia de la República de Colombia, 2004).

Las leyes, resoluciones y decretos que rigen a las cooperativas de trabajo asociado en lo relacionado con la gestión de activos de información son las siguientes:

La estructura normativa enfocada a la seguridad de la información en el sector solidario ha tenido una transición de un enfoque puramente jurídico a un esquema de gestión más técnico e integral. En este contexto, las entidades como las Cooperativas de Trabajo Asociado (CTA) tienen como tarea integrar las normativas restrictivas de las Leyes 1581 de 2012 y 594 de 2000 —las cuales tienen como propósito proteger los datos y la memoria institucional— con los lineamientos estratégicos del Decreto 1008 de 2018 y la Resolución 500 de 2021; ya que las primeras establecen el nivel mínimo de cumplimiento legal para no recibir sanciones administrativas, y las segundas actúan como marcos técnicos de referencia que determinan la capacidad operativa y la competitividad en el actual entorno digital, a pesar de haber sido creadas con enfoque al sector público.

A continuación, se hace un análisis detallado de la situación.

Leyes

- Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”. Esta prohíbe la práctica no autorizada en el país de cualquier tratamiento de datos personales, poniendo de manifiesto los principios y obligaciones para tener en cuenta por las empresas y/o entidades con el fin de llevar a cabo el procesamiento de los datos personales, es decir, nombres, identificación, contactos, preferencias, etcétera. Las empresas/u otras entidades, antes de proceder al tratamiento de datos personales, deben contar con la autorización expresa, informada de los titulares de los datos con un propósito determinado, y garantizar el ejercicio de los derechos de acceso, rectificación, actualización y supresión de los datos e información, su finalidad es garantizar el proceso de recogida y tratamiento de datos a la persona física titular de los datos para que tenga el control de su información personal (Congreso de la República de Colombia, 2012).

En el caso concreto de las Cooperativas de Trabajo Asociado (CTA), la aplicabilidad de esta norma adquiere un tono diferenciador debido al doble papel del asociado. Dado que son organizaciones donde el trabajador es a la vez como gestor y propietario (Soriano Cortés, 2021), el flujo de datos personales no se limita a una relación laboral convencional, sino que se extiende al ámbito de la copropiedad y la gobernanza. Por ello, las CTA deben diseñar sus Políticas de Tratamiento de Información (PTI) para que se protejan los datos sensibles que provienen de las compensaciones ordinarias, los registros de seguridad social y los perfiles de competencias profesionales.

Esta obligación implica que la cooperativa, como responsable del tratamiento, debe establecer protocolos de seguridad digital para impedir que terceros —e incluso otros asociados sin

competencia administrativa— accedan a la información privada de sus pares. Del mismo modo, ya que estas organizaciones funcionan bajo los principios de autogestión, la transparencia en el ejercicio de los derechos de acceso y rectificación pasa a ser un pilar de la confianza institucional. El incumplimiento de estas disposiciones no solo expone a la cooperativa a las sanciones pecuniarias de la Superintendencia de Industria y Comercio, sino que vulnera el principio de solidaridad y protección mutua que rige al sector, poniendo en riesgo la integridad del patrimonio colectivo frente a posibles fugas de información o incidentes de ciberseguridad.

- Ley 594 de 2000: "Por la cual se dicta la ley General de Archivos y se dictan otras disposiciones". Es la norma reglamentaria que establece el deber que tiene el estado colombiano de administrar su información documental de la manera más organizada, efectiva y transparente posible. Determina el recorrido de un documento desde que se origina en una oficina hasta que se convierte en patrimonio histórico o se elimina de forma controlada, ejecutando así la gestión documental como un recurso disponible a la administración y a la ciudadanía (Congreso de la República de Colombia, 2000).

De manera particular en el ámbito solidario, y más específicamente en las Cooperativas de Trabajo Asociado (CTA), la Ley 594 de 2000, se despoja de su dimensión estatal para transformarse en una norma de gestión de activos críticos de información. Con el principio de que estas organizaciones tienen una función social y manejan recursos e información de interés público —como los registros de seguridad social, compensaciones y aportes de sus asociados—, la norma les exige que garanticen la integridad, autenticidad y disponibilidad de sus archivos a lo largo de todo su ciclo de vida.

En una CTA, aplicar los lineamientos del Archivo General de la Nación (AGN) no es solamente una recomendación técnica, es una garantía de seguridad jurídica. El carácter

obligatorio se expresa en la elaboración y aplicación de las Tablas de Retención Documental (TRD), que permiten clasificar la información asociativa y laboral, de tal manera que pueda ser recuperada cuando se requiera en auditorías de la Supersolidaria o en exigencias judiciales. En el contexto digital del 2026, esta ley se alinea con las normas de ciberseguridad para garantizar que la transición del papel al documento electrónico no afecte el valor probatorio de la memoria institucional. De esta manera, la gestión documental bajo la Ley 594 se erige como la base de la continuidad del negocio, salvaguardando el patrimonio documental de la cooperativa frente a los riesgos de pérdida, deterioro o acceso no autorizado, asegurando que la historia y los derechos de los asociados permanezcan inalterables en el tiempo.

Resoluciones

- Resolución 500 del 2021: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", expedida por el Ministerio de Tecnologías de la información y las comunicaciones (MinTIC), Su principal objetivo "establecer lineamientos generales para la implementación del modelo de seguridad y privacidad de la información – MSPI" (Ministerio de Tecnologías de la Información y las Comunicaciones, [MinTIC], 2021), el énfasis de la presente resolución consiste en proteger la información y los servicios digitales del estado velando por la confidencialidad, integridad y disponibilidad de los datos, a partir del fortalecimiento de la ciberseguridad nacional con la capacidad de hacer frente a las crecientes amenazas digitales. Las cooperativas de trabajo asociado pueden tomar como guía los lineamientos establecidos por esta resolución para la implementación de su MSPI, dada que su cumplimiento puede ser exigido por la Supersolidaria en supervisiones, con el fin de que sus organismos vigilados garanticen la seguridad de la información.

Aunque la Resolución 500 de 2021 inicialmente se aplica a los sujetos obligados de la Política de Gobierno Digital, es decir, a las entidades públicas, su impacto en las Cooperativas de Trabajo Asociado (CTA) es muy importante y aunque no las obliga directamente, sí está vinculada indirectamente. Para estas organizaciones, la resolución pasa de ser un marco opcional para convertirse en un requisito técnico exigido por la Superintendencia de la Economía Solidaria, la cual utiliza los dominios del MSPI como estándar de evaluación para el componente de gestión de riesgos y control interno. En este sentido, la obligatoriedad para la CTA, surge de la necesidad de resguardar la resiliencia operativa frente a infraestructuras críticas, en especial cuando la cooperativa administra compensaciones, aportes y datos sensibles de sus asociados que, de verse comprometidos, afectarían la estabilidad financiera y social de la entidad.

Estos lineamientos, cuando se aplican en una CTA, conducen a la incorporación de controles de seguridad rigurosos desde el diseño y por defecto. Esto obliga a la organización a realizar una clasificación exhaustiva de sus activos de información —siguiendo la metodología del MSPI— para proteger el ciclo de vida de los datos esenciales del trabajador asociado. De igual manera, bajo este marco, la CTA debe establecer protocolos de respuesta ante incidentes y esquemas de autenticación robustos, alineando su operación con los niveles de madurez digital que el estado colombiano exige a este tipo de organizaciones. En definitiva, la Resolución 500 otorga a las entidades del sector solidario la estructura requerida para convertir el cumplimiento legal pasivo en una estrategia activa de ciberseguridad, protegiendo así el patrimonio colectivo y la confianza institucional frente al complejo entorno de amenazas digitales actuales.

Decretos

- Decreto 1008 de 2018: En el cual se establecen, lineamientos generales de la política de gobierno digital, con el cual se pretende el aprovechamiento de las tecnologías de la

información y la comunicación, ya que su énfasis es facilitar la realización de trámites para los ciudadanos a través del aprovechamiento de las nuevas tecnologías usando el internet como medio de accesibilidad y comunicación entre las entidades y los ciudadanos (Presidencia de la República de Colombia, 2018).

Dentro del sector solidario, y específicamente para las Cooperativas de Trabajo Asociado (CTA), la aplicabilidad del Decreto 1008 de 2018, no solo se sitúa en el ámbito público, sino que se erige como facilitador de interoperabilidad y eficiencia operativa. Si bien el decreto se dirige principalmente a entidades y organizaciones del sector público, su impacto en las CTA es determinante en dos dimensiones: la relación con el asociado como ciudadano digital y la integración técnica con las plataformas de supervisión. Dentro del componente "TIC para la Sociedad" la cooperativa debe alinear sus canales digitales para que el trabajador asociado pueda acceder a servicios, a trámites internos y consultas de información de forma segura, accesible y transparente, emulando los estándares de confianza digital que promueve el Estado.

De igual manera, la adopción de estos lineamientos permite que la CTA fortalezca su infraestructura tecnológica para cumplir con los requerimientos de reporte ante la Supersolidaria y demás entidades gubernamentales, facilitando el intercambio de datos mediante estándares abiertos y seguros. En tal sentido el Decreto 1008 incentiva a las cooperativas a que se motiven hacia un modelo de arquitectura empresarial donde la seguridad de la información no es un proceso aislado sino un componente transversal que garantiza la disponibilidad de los servicios digitales. Como CTA, el aprovechamiento de estas tecnologías, bajo el amparo de la política de Gobierno Digital, significa una reducción de brechas burocráticas y un fortalecimiento de la gobernanza democrática, posibilitando que la autogestión y la toma de decisiones se apoyen en sistemas de información robustos, íntegros y centrados en el usuario.

Guías

Así mismo las cooperativas de trabajo asociado cuentan con guías y políticas que brinda directrices de apoyo para la gestión de los activos de información:

- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital: Establece una hoja de ruta fundamental para determinar cómo se protege a Colombia en el entorno digital. La ruta considera la creación de un ecosistema digital seguro y resiliente para el aprovechamiento de los beneficios que ofrece la tecnología a los ciudadanos, empresas y el Estado, y para que se reduzcan al mínimo los riesgos que atañen a las ciberamenazas. El documento sirvió de base para el establecimiento de normas posteriores más concretas como por ejemplo la resolución 500 de 2021 del MinTIC.

En el contexto de las Cooperativas de Trabajo Asociado (CTA), el CONPES 3854 de 2016 se aplica de manera estratégica y preventiva, basada en la gestión proactiva del riesgo digital. Aunque este documento de política pública define acciones para el Estado, su relevancia para el sector solidario es que establece los estándares de ciberseguridad y ciberdefensa que el país exige a las organizaciones que custodian los activos críticos de información. Para una CTA, que no solo administra el patrimonio financiero sino también la identidad digital y datos prestacionales de sus asociados, el CONPES 3854 se constituye como el marco de referencia para transitar de una seguridad de la información estática a una resiliencia digital activa.

El seguir los lineamientos de este documento permite que las CTA se conecten con el ecosistema nacional de seguridad digital, promoviendo el desarrollo de capacidades internas para identificar, proteger, detectar, responder y recuperarse de incidentes cibernéticos. Dentro de este enfoque, la aplicabilidad radica en la necesidad de que la cooperativa no solo esté en regla con la legislación vigente, sino que asuma su rol como parte de la infraestructura que sustenta la

economía social del país. Así, el CONPES 3854 incentiva a estas organizaciones a invertir inteligentemente en tecnología y cultura digital, asegurando que el modelo de trabajo asociado sea resiliente frente a amenazas globales como el ransomware o el phishing, protegiendo la confianza de los asociados y la continuidad de sus operaciones en un entorno cada vez más hostil.

- Guía para la gestión y clasificación de activos de información Guía No.5, MINTIC: constituye una guía práctica para la manera como las entidades deben elaborar un inventario de su información, categorizarla en función de su importancia y a, partir de esta clasificación, implementar las medidas de protección adecuadas. Es el primer paso para construir un programa de seguridad de la información a la vez sólido y eficiente que este alineado con las mejores prácticas internacionales.

La aplicabilidad de la Guía núm. 5 de MinTIC pasa de ser un cumplimiento formal en las Cooperativas de Trabajo Asociado (CTA) a convertirse en una herramienta de supervivencia institucional. Dado que en estas organizaciones el patrimonio y la información son propiedad colectiva de los asociados, la clasificación de activos permite a la administración diferenciar entre la información de uso público y aquellos datos críticos o sensibles –como el registro de compensaciones, historias laborales y estados financieros– que necesitan niveles de protección superiores. Con esta metodología, la CTA garantiza la trazabilidad e integridad de sus activos y asegura la asignación proporcional de recursos tecnológicos y humanos al valor real de la información que custodia.

De igual manera, el desarrollo de esta guía permite que las cooperativas estén alineadas con los requisitos de la Supersolidaria que exige una gestión de riesgos basada en la identificación clara de los activos sobre los que se soporta la operación. Para una CTA, el

inventario detallado de activos de información no solo facilita el cumplimiento de la Ley 1581 de 2012, sino que también refuerza la confianza de los socios al mostrar una gobernanza digital transparente y profesional. En conclusión, la Guía N. 5 aporta la terminología técnica que requiere para que la seguridad de la información deje de ser un concepto abstracto y se convierta en un proceso cuantificable y verificable, protegiendo la continuidad del modelo cooperativo frente a posibles fugas o pérdidas de datos que pongan en riesgo su estabilidad reputacional.

- Lineamientos Para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional. Versión 5 (MinTic): Dirigida a las entidades del Estado, constituyen el recurso práctico que emplea Colombia para mapear y proteger sus sistemas críticos, facilitando la transición de la teoría a la acción concreta en ciberseguridad nacional, asegurando que el Estado se enfoque en la protección de aquellos elementos más relevantes para el país.

Estos lineamientos para inventario y clasificación de activos, en cuanto a su aplicabilidad en las Cooperativas de Trabajo Asociado (CTA), adquieren una relevancia estratégica en el marco de la seguridad nacional y la continuidad del negocio. Aunque el documento está pensado para el sector público, su adopción en el sector solidario resulta crucial para aquellas organizaciones que, por su volumen transaccional o por la naturaleza de los servicios que prestan (en especial salud, transporte o servicios financieros), pueden ser consideradas parte de la infraestructura crítica indirecta del país. Para una CTA, aplicar la Versión 5 de estos lineamientos implica subir el nivel de gestión de sus activos a un nivel de ciberdefensa, lo que le permitirá saber qué sistemas son vitales para la subsistencia de la cooperativa y cuáles, de fallar, pueden tener un impacto sistémico en los derechos de sus asociados.

De igual manera, la implementación de estos lineamientos permite la alineación con el CONPES 3854, lo que posibilita que la cooperativa se conecte de forma segura a las cadenas de suministro digital del Estado. En un escenario donde las CTA operan muchas veces como contratistas o aliadas de las entidades gubernamentales, demostrar que su inventario y clasificación de activos sigue los estándares de la Infraestructura Crítica Cibernética, pasa a ser un diferencial competitivo y un requisito de confianza técnica. En conclusión, la aplicación de estos lineamientos en el sector solidario permite que la seguridad de la información pase de ser un proceso aislado de administración a ser una estrategia de protección de activos nacionales, blindando el capital social y financiero de los asociados frente a ataques de alta sofisticación capaces de comprometer la soberanía de sus datos.

- Norma Internacional ISO/IEC 27001: Es el estándar internacional de referencia para la gestión de la seguridad de la información. Proporciona un enfoque sistemático para identificar riesgos, aplicar controles y mejorar de forma continua e ininterrumpida, protegiendo así la información y la reputación de una organización, convirtiéndose en una herramienta de gestión estratégica orientada.

Dentro de las Cooperativas de Trabajo Asociado (CTA) la aplicabilidad de la norma ISO/IEC 27001, va más allá del cumplimiento de la legalidad local, para convertirse en un diferencial de competitividad y confianza. Si bien leyes como la 1581 de 2012 imponen requisitos mínimos de protección de datos, esta norma internacional ofrece un marco de resiliencia operativa basado en el ciclo de mejora continua (PHVA: Planear, Hacer, Verificar, Actuar). Para una CTA, el seguimiento de este estándar implica proteger la relación contractual a través de la protección técnica de la tríada de la información (confidencialidad, integridad y

disponibilidad), garantizando que los procesos de toma de decisiones y el manejo de excedentes y compensaciones estén protegidos por medio de controles de clase mundial.

Si vemos la evaluación desde una perspectiva comparativa, la ISO 27001 constituye el nexo de unión entre el sector público y el privado. En el sector público colombiano, esta norma constituye la base técnica obligatoria sobre la cual se construye el Modelo de Seguridad y Privacidad de la Información (MSPI) exigido por la Resolución 500 de 2021. Por el contrario, en el caso de una CTA (sector privado), su implementación es voluntaria, aunque altamente aconsejable, y pasa a ser obligación contractual cuando la cooperativa brinda servicios a grandes empresas o entidades estatales. En fin, la ISO/IEC 27001 permite que la cooperativa migre de un modelo de "cumplimiento por sanción" hacia uno de "gestión por riesgo", convirtiendo a la seguridad de la información en una ventaja estratégica que garantice la sostenibilidad del patrimonio colectivo en un mercado digital globalizado.

Características y Articulación de la Normatividad Aplicable

La sistematización normativa expuesta en la Tabla 1 da cuenta de la existencia de un marco normativo y técnico suficientemente definido que enmarca la gestión de los activos de información en el contexto colombiano, un insumo básico en la defensa, categorización y explotación de la información y que se vuelve imprescindible para las organizaciones del sector solidario y entidades que buscan la seguridad y la continuidad del negocio.

Tabla 1

Características Principales de la Normatividad

Documento	Tipo y jerarquía	Propósito central	Aplicabilidad para el sector solidario
Ley 1581 de 2012	Ley estatutaria	Regular el tratamiento de datos personales.	Obligatoria para entidades, públicas y privadas (Incluido el sector solidario).
Ley 594 del 2000 – Ley general de archivos	Ley régimen archivístico	Regulaciones para organización, conservación y acceso de archivos.	Obligatoria para entidades públicas, funciona como guía para entidades del sector solidario.
Resolución 500 de 2021-MinTIC	Resolución	Lineamientos para implementar EL MSPI.	Obligatoria para entidades públicas, funciona como guía para entidades del sector solidario.
Decreto 1008 de 2018 – política de Gobierno Digital	Decreto	Lineamientos de gobierno digital para generar valor público.	Obligatoria para entidades públicas, funciona como guía para entidades del sector solidario.
CONPES 3854 DE 2016-Política Nacional de Seguridad Digital	Política Pública	Definir la Política Nacional de Seguridad Digital con enfoque de riesgos.	Orientadora funciona como guía para entidades del sector solidario.
Guía MinTIC No. 5 – Gestión y Clasificación de Activos de Información	Guía técnica	Brindar metodología para inventario y clasificación de activos de información.	Recomendatorio sector solidario, pero puede ser exigible en Gobierno Digital sector público.
Lineamientos V5 – Inventario y Clasificación de Activos e Infraestructura Crítica	Lineamientos técnicos	Precisar lineamientos para activos e infraestructura crítica cibernética.	Recomendatoria/sectorial; aplicable en seguridad digital estatal, funciona como guía para entidades del sector solidario.
ISO/IEC 27001:2022 (Sistemas de Gestión de	Norma internacional (certificable)	Establecer requisitos para un ISMS basado	Voluntaria, pero certificable y exigible contractualmente.

Documento	Tipo y jerarquía	Propósito central	Aplicabilidad para el sector solidario
Seguridad de la Información – ISMS)		en riesgos y mejora continua.	

Nota. Esta tabla describe cada uno de los documentos normativos aplicables al sector solidario en materia de gestión de activos de información.

Establecida la caracterización general de los documentos técnicos y legales, resulta crucial proceder con una jerarquización del marco normativo, en función de su naturaleza vinculante e impacto de su falta de aplicabilidad en el sector. En la tabla 2 se muestra una comparación estructural que agrupa las normas obligatorias (Hard Law), híbridas y recomendados (Soft Law). Esta clasificación permite identificar la transición desde el cumplimiento de las leyes estatutarias con el propósito de evitar sanciones administrativas y legales hasta la adopción voluntaria de acogerse a marcos de referencia internacionales. Así se hace posible que para las organizaciones del sector solidario el valor estratégico de la norma no está exclusivamente en evitar la penalización, sino en la construcción de una infraestructura digital resiliente que garantice la continuidad del negocio y la protección del patrimonio de los asociados.

Tabla 2

Jerarquización de Marcos Legales y Técnicos

Categoría	*Normas Relacionadas*	*Consecuencia del Incumplimiento*	*Valor Estratégico*
Obligatorias (Hard Law)	• Ley 1581 de 2012 • Ley 594 de 2000	Sanciones administrativas, multas pecuniarias (SIC) y procesos disciplinarios.	Garantiza la legalidad y el respeto a los derechos fundamentales de los asociados.
Híbridas (Exigibles por Supervisión)	• Resolución 500 de 2021 • Decreto 1008 de 2018	Hallazgos en auditorías de la Supersolidaria y requerimientos de mejora.	Estandariza la operación bajo los niveles exigidos por el Estado colombiano.
Recomendadas (Soft Law)	• ISO/IEC 27001:2022 • CONPES 3854 de 2016 • Guías y Lineamientos MinTIC	Pérdida de competitividad, vulnerabilidad ante ciberataques y desconfianza del asociado.	Proporciona resiliencia, madurez digital y reconocimiento internacional.

Nota. Esta tabla muestra la jerarquización de los marcos legales y técnicos, realizando una comparativa entre la obligatoriedad y los marcos recomendados para llegar a una madurez viable en seguridad informática.

El análisis de la Tabla 2 pone en evidencia una estructura de cumplimiento multinivel donde se entrelazan la gestión estratégica y la coerción legal. Se destaca el cumplimiento obligatorio, encabezado por la Ley 1581 de 2012 y la Ley 594 de 2000, es el sustento primordial para el funcionamiento; su observancia no está sujeta a la voluntad administrativa, sino a un mandato constitucional de garantía de derechos. Pero el hallazgo más significativo está en la categoría de normas híbridas, donde los instrumentos como la Resolución 500 de 2021 y el Decreto 1008 de 2018 funcionan como mecanismos de convergencia. Si bien formalmente surgen del sector público, su exigibilidad en el sector solidario se da a través de la supervisión de

la Supersolidaria, que incorpora estos lineamientos a sus protocolos de auditoría. Finalmente, el segmento marcos recomendados, encabezado por la ISO/IEC 27001, se posiciona no como un requisito sancionatorio sino como el estándar de madurez digital necesario para mitigar riesgos sistémicos. De esta manera, se pone en evidencia que una gestión de seguridad de la información sólida en una CTA requiere pasar del cumplimiento reactivo de la normativa a una cultura proactiva basada en marcos de referencia internacionales.

Establecida la jerarquía de las normas de acuerdo con su fuerza vinculante, es indispensable analizar como leyes, resoluciones y guías aplican de forma distinta dependiendo de la función de la naturaleza del sujeto obligado. Lo que sí se debe tener muy claro es que, si bien el inicio de gran parte de la normatividad técnica en Colombia —como el Decreto 1008 de 2018 o la Resolución 500 de 2021— está en la Política de Gobierno Digital orientada al fortalecimiento del aparato estatal, su despliegue en el sector privado solidario obedece a una lógica de adaptabilidad y gestión del riesgo. Con esta premisa, la Tabla 3 muestra un ejercicio comparativo que permite diferenciar el rol de cada documento según el sector de aplicación, mostrando cómo son mandatorios para la administración pública y se transforman en herramientas de excelencia y guías de buenas prácticas para las Cooperativas de Trabajo Asociado. Este ejercicio de contraste resulta vital para demarcar los límites de la responsabilidad institucional en el ecosistema de la seguridad digital nacional.

Tabla 3

Aplicabilidad del Sector Público Versus el Sector Privado

Documento / Guía	Aplicabilidad en el Sector Público	Aplicabilidad en el Sector Privado (Solidario)
Ley 1581 de 2012	Obligatorio (Estatutario): Mandato constitucional para proteger el derecho al Habeas Data del ciudadano.	Obligatorio (Estatutario): Requisito ineludible para el tratamiento de datos de asociados, empleados y terceros.
Ley 594 de 2000	Mandatorio: Régimen integral para la administración, conservación y acceso de toda la información estatal.	Híbrido: Obligatorio para documentos de interés público (Seguridad social, contratos estatales) y guía de orden administrativo.
Decreto 1008 de 2018	Mandatorio: Es el eje rector de su transformación digital y eficiencia administrativa.	Referencial: Marco estratégico para lograr la interoperabilidad con el ecosistema del Estado.
Resolución 500 de 2021	Obligatorio: Requisito de ley para implementar el Modelo de Seguridad y Privacidad (MSPI).	Guía Técnica: Modelo metodológico para estructurar la seguridad digital y proteger el patrimonio.
Guía No. 5 y Lineamientos V5	Estándar Mínimo: Obligatorio para inventariar y clasificar activos de información estatal.	Mejor Práctica: Metodología recomendada para identificar y priorizar la protección de datos sensibles.
CONPES 3854 de 2016	Política de Estado: Obliga a la ciberdefensa y seguridad digital institucional.	Visión de Riesgo: Alineación voluntaria con la estrategia de seguridad nacional y resiliencia.
ISO/IEC 27001:2022	Base Técnica: Cimiento técnico sobre el cual el sector público construye su MSPI obligatorio.	Certificable: Meta de madurez institucional que garantiza confianza y competitividad global.

Nota. Los criterios de aplicabilidad se han definido bajo el marco de la Política de Gobierno Digital y las directrices de supervisión de riesgos de la economía solidaria.

La articulación de la normativa nacional y la ISO/IEC 27001 descrita en la Tabla 4 proporciona un marco normativo complementario que apoya la gestión de los activos de información y se convierte en una fuerte referencia aplicable en los procesos a desarrollar en las cooperativas de trabajo asociado en su propósito de mejorar la seguridad de la información.

Tabla 4

Articulación de la Normatividad con los Activos de Información e ISO 27001

Documento	Relevancia para activos de información	Relación con la ISO/IEC 27001
Ley 1581 de 2012	Define datos personales como activos críticos.	Complementa controles de privacidad.
Ley 594 del 2000 – Ley general de archivos	Documentos y expedientes como activos de información.	Complementa en gestión documental a la ISO 27001.
Resolución 500 de 2021-MinTIC	Exige inventarios, riesgos e incidentes sobre activos de información.	Alineada con la ISO 27001.
Decreto 1008 de 2018 – política de Gobierno Digital	Incorpora gestión de información como habilitador.	Exige adopción de lineamientos de seguridad (MSPI/ISO).
CONPES 3854 DE 2016-Política Nacional de Seguridad Digital	Enfatiza gestión de riesgos sobre activos e infraestructura.	Promueve adopción de estándares internacionales.
Guía MinTIC No. 5 – Gestión y Clasificación de Activos de Información.	Núcleo: inventario y clasificación de activos de información.	Complementa controles de inventario y clasificación de ISO 27001.
Lineamientos V5 – Inventario y Clasificación de Activos e Infraestructura Crítica.	Refuerza prácticas de inventario y clasificación, infraestructura crítica.	Alinea con ISO 27001 y gestión de infraestructura crítica.
ISO/IEC 27001:2022 (Sistemas de Gestión de	Requiere inventario, propietarios, clasificación y controles.	Norma base para SGSI (Sistema de Gestión de Seguridad de la información); referencia global.

Seguridad de la Información – SGSI).

Nota. Aplicabilidad o relación de la normatividad con el estándar ISO/IEC 27001.

Análisis de los Componentes Estructurales del SGSI (Cláusulas 4, 5, 6 y 10)

El éxito de un SGSI (Sistema de Gestión de la Seguridad de la Información) en las organizaciones del sector solidario está determinado por la capacidad de integración en la estructura orgánica de la organización. A diferencia de los modelos corporativos tradicionales, las CTA requieren un enfoque que combine la eficiencia operativa con los principios de autogestión y propiedad colectiva.

- Contexto de la Organización (Cláusula 4): Para la CTA, el análisis del contexto, de acuerdo con la norma ISO/IEC 27001:2022, requiere reconocer dos componentes importantes: contexto externo, con la presión regulatoria de la Superintendencia de la Economía Solidaria y la Ley 1581 de 2012, y componente interno, caracterizado por la Propiedad Cooperativa. En este escenario, el SGSI en su alcance debe resguardar no sólo los activos tecnológicos, sino el flujo de información que garantiza la transparencia frente al asociado, quien hace las veces a la vez de gestor y propietario del capital social. Por lo tanto, el contexto organizacional se entiende como un ecosistema donde la seguridad de la información garantiza la autonomía administrativa.

- Liderazgo (Clausula 5): En las organizaciones del sector solidario el liderazgo de la seguridad de la información deja de estar sólo en manos de un oficial de seguridad y pasa a la gobernanza democrática. El Consejo de Administración y la Asamblea General deben asumir un compromiso explícito a través de la aprobación de políticas que no se perciban como imposiciones técnicas, sino como directrices estratégicas para proteger el patrimonio común. El liderazgo, desde esta perspectiva, se expresa a través de la asignación de recursos y la promoción

de una cultura de formación permanente, en la cual el asociado reconozca que su deber respecto a los activos de información es intrínseco a su condición de socio.

- Planificación y gestión de riesgos (Clausula 6): El ejercicio de proporcionalidad y gestión del riesgo debe constituir la base sobre la que se asiente la planificación del SGSI en las Cooperativas de Trabajo Asociado. Estas organizaciones funcionan con un capital variable, y por ello la pérdida o alteración de la información financiera o de compensaciones puede poner en riesgo la estabilidad del modelo solidario. La aplicación de esta cláusula implica que la identificación de amenazas no se detenga en los fallos de hardware, sino que se amplíe a los riesgos reputacionales y legales que afecten a la Confianza entre los socios. Con metodologías como MAGERIT la trazabilidad permite que la planificación sea un proceso preventivo alineado con la visión de sostenibilidad de la cooperativa.
- Mejora continua (Clausula 10): La seguridad en la información es un proceso cambiante que exige resiliencia. La cláusula de mejora continua impone a la CTA la adopción del ciclo PHVA (Planear-Hacer-Verificar-Actuar) como un mecanismo de aprendizaje organizacional. Debido a la evolución de las ciberamenazas y los cambios en la normatividad aplicable, las cooperativas de trabajo asociado deben evaluar periódicamente la efectividad de sus medidas de protección y subsanar vulnerabilidades. La mejora continua en el sector solidario asegura que el sistema de gestión se vaya adaptando a la par que la organización, velando por que esté vigente técnicamente la protección del acervo informativo institucional.

Con el propósito de realizar un análisis más profundo de la articulación técnica y estratégica, la Tabla 5 ofrece una trazabilidad entre los componentes estructurales de la norma ISO/IEC 27001:2022 y el marco legal vigente. Este ejercicio permite superar la visión puramente operativa de la gestión de activos e integrar elementos fundamentales como el liderazgo

institucional y la mejora continua, asegurando que el SGSI responda a la cambiante naturaleza del riesgo digital.

Tabla 5

Trazabilidad de Componentes Estructurales del SGSI y el Marco Normativo

Cláusula ISO 27001:2022	Control Anexo A (Referencial)	Marco Normativo Articulado	Objetivo Estratégico en la CTA
Cláusula 4: Contexto de la organización	5.34: Privacidad y protección de datos.	Ley 1581 de 2012	Definir el alcance del SGSI considerando al asociado como parte interesada y dueño del dato.
Cláusula 5: Liderazgo y compromiso	5.1: Políticas para la seguridad de la información.	Decreto 1008 de 2018	Vincular al Consejo de Administración en la aprobación de políticas, asegurando gobernanza democrática.
Cláusula 6: Planificación (Riesgos)	5.9: Inventario de información y otros activos.	Guía MinTIC No. 5	Transformar el inventario de activos en una herramienta para el tratamiento de riesgos críticos.
Cláusula 10: Mejora continua	5.37: Gestión de incidentes de seguridad.	Resolución 500 de 2021	Establecer ciclos de revisión (PHVA) para adaptar la seguridad ante la evolución de las ciberamenazas.

Nota. Matriz de trazabilidad estratégica elaborada para articular los requisitos de gestión con las obligaciones legales del sector solidario.

ISO 27001 – Clasificación y Categorización de Activos de Información

Este procedimiento inicial está dirigido a realizar la imprescindible actividad de clasificación y organización de los activos de información y para ellos, es necesaria una buena comprensión del proceso inicial, así como ser consciente de la importancia de desarrollar un procedimiento eficiente y de calidad que lleve a conocer el estado actual de los activos a clasificar, sin perder de vista el hecho de que los activos de información representan el punto inicial, son una cuestión fundamental de los aspectos a tener en cuenta a la hora de la implantación de un sistema de gestión de seguridad informática para cualquier empresa.

Abordaremos cómo las habilidades analíticas juegan un papel fundamental en la identificación y categorización de los activos de información. Este enfoque no solo nos permite comprender mejor la estructura y el valor de la información que manejamos, sino que también garantiza que las medidas de protección aplicadas sean las más adecuadas y efectivas.

Y también, ahondaremos en los criterios y los parámetros que la norma ISO 27001 establece como guía internacional. Una guía para la gestión de los activos de información, con ejemplos y con un análisis que definirá su carácter práctico para implementar en muchas organizaciones pertenecientes al sector de las cooperativas de trabajo asociado y, por tanto, de la seguridad y la gestión de la información.

Inventario Activos Siguiendo Norma ISO 27001

El objetivo principal establecer una agrupación inicial de los activos de información de acuerdo con los criterios y parámetros establecidos por la norma ISO 27001, con el fin de garantizar obtener una visión clara y completa de todos los activos de información que posee la organización, incluyendo hardware, software, datos, documentación y recursos intangible.

Borrero Ochoa (2018) sugiere llevar a cabo una recolección inicial de información o diagnóstico para establecer una base metodológica desde la cual iniciar el proyecto. Esto permite realizar una comparación más detallada entre el estado inicial antes de iniciar las actividades y el producto final obtenido tras la ejecución.

La categorización de la información presenta atributos específicos y tiene en cuenta la cultura y el funcionamiento interno de las empresas con el fin de satisfacer los criterios definidos en la normativa ISO 27001:2022.

Se deben crear grupos los recursos requeridos en los controles y/o políticas de seguridad, para examinar en qué medida cada conjunto afecta o tiene influencia en el funcionamiento de la empresa y su protección. de aquellos recursos que posteriormente se les requiere aplicar los mismos controles y políticas de seguridad. Es importante examinar cómo cada conjunto identificado afecta o influye en la operación de la empresa y asegurarse de su protección.

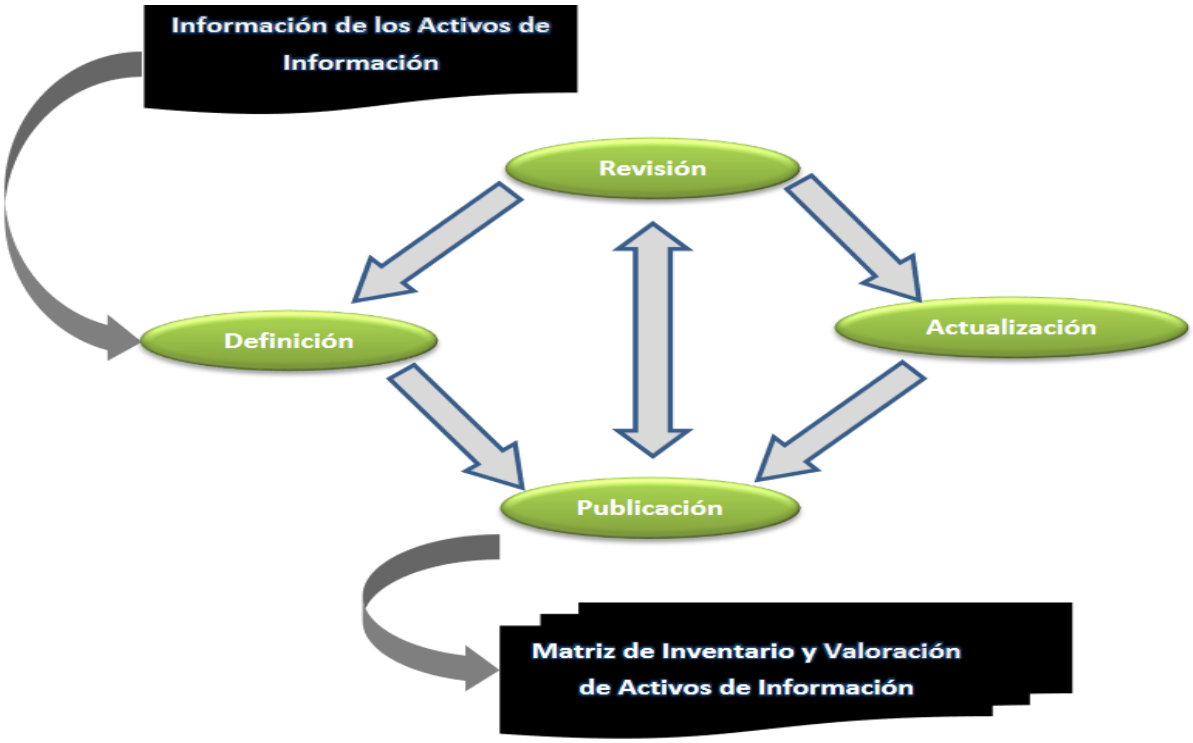
Identificación de Activos. El proceso debe realizarse de acuerdo con lo expuesto en el numeral 5.9 de la norma NTC ISO/IEC 27002:2022 (ISO/IEC, 2022), donde se establece que “se debe desarrollar y mantener un inventario de información y otros activos asociados incluidos los propietarios”. Según lo que expone la norma implicaría crear y mantener un registro detallado de todos los activos de información y otros activos relevantes (como hardware, software, documentación, etc.) que son importantes para la seguridad de la información dentro de la organización.

Siguiendo los parámetros establecidos en la norma ISO 27001 y las pautas de orientación que brinda el (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, [MinTIC], 2016) la parte inicial del proceso conlleva identificar el inventario de activos de

información con la finalidad de clasificar aquellos activos que requieren una protección más intensiva, ya que de manera clara establece sus características y su función dentro de un proceso.

Figura 1

Procedimiento Para Inventario de Activos



Nota. Procedimiento establecido para realizar inventario de activos. Tomado de. Guía para la gestión y clasificación de activos de información (GUIA No. 5), Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
(2016) https://gobiernodigital.mintic.gov.co/portal/715/articles-172093_recurso_1.pdf

Definición del Inventario. La definición implica determinar qué activos de información deben formar parte del inventario. Para llevar a cabo esta tarea, se requiere un equipo encargado de la gestión de activos de información dentro de la organización. Además, el líder de cada

proceso (o quien lo reemplace, como un líder en gestión de calidad) debe colaborar en esta actividad.

Según el Ministerio de las Tecnologías, la Información y las Comunicaciones (MinTIC, 2016), en una segunda etapa, los líderes de procesos tienen la obligación de adjuntar una solicitud a fin de proponer que la persona designada como propietario del activo de información, el custodio y el correspondiente usuario del activo revisión de la definición de los activos de información a fin de validar y revisar si las partes interesadas o los miembros de la organización son representativos de los roles que deben desempeñar, siendo recomendable que realicen este procedimiento, por lo menos, una vez por año.

Información Básica. Esta se refiere a los atributos esenciales del activo, y para llevar a cabo la fase de definición, podría abarcar al menos lo siguientes aspectos:

- Identificador: Número único que identifica al activo.
- Proceso: Nombre del proceso al que pertenece el activo.
- Nombre activo: Nombre con el cual se logra referenciar al activo dentro del proceso.
- Descripción: Es un lugar destinado a detallar el activo de tal manera que sea fácilmente reconocible por todos los participantes del proceso.
- Tipo: Establece la categoría a la que pertenece el activo. En este campo, se emplean los términos establecidos en la Tabla 6.

Tabla 6

Tipificación de Activos de Información

Inventario de activos	Detalles
Información -datos	A este tipo se relacionan datos e información que se almacenan o procesan en forma física o electrónica, como bases de datos, archivos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes de continuidad de negocios, acuerdos de retiro y registros de auditoría, entre otros.
Software	Aplicaciones que posibilitan la gestión de la información.
Recurso Humano -Personal	Individuos que, debido a su experiencia, conocimientos y relevancia para el proceso, se consideran activos de información.
Servicio	Servicios relacionados con la informática y las comunicaciones, como Internet, páginas de búsqueda, carpetas compartidas y redes internas (Intranet). servicios de red, correo electrónico, Administración de proceso de usuario.
Hardware	Dispositivos de informática y comunicaciones que, debido a su importancia, se consideran activos de información, y no solo activos fijos. computador, servidor, router, etc.
Otros	Activos de información que no encajan en ninguna de las categorías mencionadas previamente, pero que deben evaluarse para determinar su nivel de importancia dentro del proceso.

Nota. Tipos de activos de información con el fin de establecer a la categoría que pertenecen.

- Ubicación: Informa la ubicación electrónica y física del activo.

- Clasificación: Se refiere a la protección de información según su disponibilidad, integridad y confidencialidad.
- Justificación: En cada evaluación, explica las consecuencias que resultarían de la pérdida de propiedad (Confidencialidad, Integridad y Disponibilidad), o la razón por la cual se asignó esa evaluación.
- Criticidad: Según la clasificación de la información, se realiza un cálculo para determinar el valor general del activo:
    - Alta: Se refiere a activos de información en los que la calificación de la información en dos o todas las características (confidencialidad, integridad y disponibilidad) es de un nivel elevado.
    - Media: Esto se refiere a activos de información en los que la calificación de la información es alta en una de sus propiedades (confidencialidad, integridad o disponibilidad), o al menos una de ellas tiene un nivel medio.
    - Baja: Se trata de activos de información en los que la calificación de la información en todos sus aspectos es de un nivel bajo.

Propiedad. En este apartado se debe tener un responsable o encargado.

- Propietario: Corresponde a una sección específica de la organización, un puesto, un procedimiento o un equipo que tiene la responsabilidad de asegurar que la información y los activos vinculados al proceso se categoricen de manera apropiada. Deben establecer y revisar de forma regular las restricciones y clasificaciones de acceso.
- Custodio: Se refiere a una entidad, rol, proceso o equipo particulares para poder aplicar las restricciones y clasificaciones de acceso definidas por el propietario. En el caso de sistemas de información o información almacenada el rol en general recae en el departamento de

Tecnología de la Información (TI); en el caso de información física los custodios pueden ser varias personas o el proceso de archivo o correspondencia y suele definirse según donde se encuentre el activo original.

Acceso. Usuarios: Se refieren a aquellos individuos que producen, adquieren, modifican, almacenan, eliminan o emplean información, ya sea en formato físico o digital, de manera presencial o a través de redes de datos y sistemas de información.

Gestión. Fecha de ingreso: Fecha de entrada del activo de información en el Inventario. Fecha de salida: Fecha de salida del activo de información del registro del Inventario.

Revisión. La actividad destinada a la revisión implica la inspección que se lleva a cabo con el propósito de establecer si un activo de información debe permanecer en el inventario o si, por el contrario, es necesario ajustar los valores de evaluación que se fijan en el inventario y en la clasificación de activos de información. Desde una perspectiva general, el inventario de activos puede ser revisado o validado en todo momento cuando lo solicite el responsable del proceso (o la persona que este determina en su defecto), o cuando así lo determine la gestión de los activos, ya sea al responsable de un proceso o al oficial de la seguridad de la información.

Actualización. El tener claros las modificaciones o cambios que se requieren en el inventario desde cada proceso, se procede a realizar la actualización del inventario de activos de información.

Publicación. El registro de activos de información debe ser considerado como un documento de alto nivel de confidencialidad y no debe poseer atributos que permitan su alteración por parte de usuarios no autorizados. La capacidad de modificar este documento solo debe estar en manos del líder del proceso, previa autorización del oficial de seguridad de la información o su representante.

La implicación de la dirección y de los responsables de cada proceso es crucial a la hora de llevar a cabo el levantamiento de los activos de la información, dado que será la fuente de información fundamental para obtener los datos de los activos de la información y el modo de obtener dicha información es mediante la realización de entrevistas o encuestas que podrían facilitar el levantamiento de los activos, ya que estos , como antes hemos comentado, son los propios equipos y los medios digitales o los productos intangibles como los de un software o una persona con especialización(Calder, 2024).

Identificación Activos de Información Caso de Estudio Cooperativa AGM SALUD CTA. Como ejemplo podemos analizar el inventario de activos de información de una cooperativa de trabajo asociado enfocada al gremio médico en la cual por la gran cantidad de asociados que realizan su contribución laboral en la CTA, se requiere de un sistema robusto enfocado a la gestión documental de la gran cantidad de hojas de vida e historia de afiliación de cada asociado, adicional a esto los sistemas de información de la organización deben ser la base ideal para soportar un arduo proceso de gestión de talento humano, ya que por la naturaleza de la cooperativa su principal núcleo de operación es los procesos relacionados con selección de personal, gestión de la nómina, gestión de seguridad salud en el trabajo, gestión documental de información en medio digital y físico, adicional a los procesos normales que requiere una organización de esta índole.

Matriz de Inventarios Caso de Estudio. En el Apéndice A se puede observar el inventario de activos de información de una cooperativa de trabajo asociado clasificado según su tipo de activo, en este caso la matriz corresponde al tipo de activo de información tipificado como hardware.

La tipificación de activos de tipo información corresponden a datos e información almacenada o procesada electrónicamente, en el Apéndice B se relacionan los activos de información que corresponden a este tipo.

Dentro de la tipificación de activos de información es importante clasificar los medios de transmisión de datos existentes en este caso como se puede visualizar en el Apéndice C, se ha tipificado como Infraestructura de red los medios de transmisión de datos existentes.

Es necesario clasificar y tipificar al personal que ya sea por su conocimiento, experiencia o criticidad son indispensables en el proceso de gestión de activos, este se denomina tipo de activo Recurso Humano, tal cual como se observa en el Apéndice D.

Los programas, aplicativos, sistemas de información, que por su funcionalidad soportan las actividades de la organización, se pueden observar en el Apéndice E

Al finalizar esta parte del diagnóstico del sistema se logró identificar los siguientes activos de información:

10 activos tipo de Hardware.

11 activos de tipo de información.

3 activos de recurso humano.

6 activos de tipo de redes.

19 activos de tipo de Software.

Clasificación de Activos

De acuerdo con la norma ISO 27001, se pueden distinguir dos categorías de activos: los principales y los secundarios. Los principales, según esta norma, abarcan los procesos e información que son más críticos y sensibles para la organización. Mientras que los activos secundarios son aquellos que brindan el respaldo necesario a estos activos principales.

Con el objetivo de realizar una clasificación apropiada de los activos de información, se siguieron las pautas de la ISO 27001 y las recomendaciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2016), ”El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo”, tal como se describe a continuación:

Confidencialidad

Esto se refiere a la necesidad de evitar que la información sea accesible o divulgada a personas no autorizadas. Esta cuestión se aborda utilizando la clasificación proporcionada por el sistema integrado de gestión o calidad de la empresa, como referencia para realizar esta clasificación se puede observar la Tabla 7.

El MINHAP (2012) define la importancia de la confidencialidad de la siguiente manera:

> La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. (p. 9)

Tabla 7

Clasificación de la Confidencialidad

Tipo de información	Descripción
Información restringida	La información que está exclusivamente disponible para un proceso específico de la organización puede causar consecuencias adversas en términos operativos, financieros, legales o incluso en la reputación de la empresa si es accedida por alguien no autorizado.
Información privada	La información que está al alcance de los procesos internos de la empresa y que, si es accedida por una persona no autorizada, podría causar efectos adversos en los procedimientos internos.
Información pública	La información que está disponible para tanto el personal de la organización como para personas externas, sin limitaciones, y cuyo conocimiento no causa ningún daño a la empresa, sus operaciones o individuos.

Nota. Clasificación de la confidencialidad para los activos de información. Adaptado de. Guía para la gestión y clasificación de activos de información (GUIA No. 5), Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016) https://gobiernodigital.mintic.gov.co/portal/715/articles-172093_recurso_1.pdf

La integridad, según la ISO 27000, se relaciona con la precisión y totalidad de la información. Esta característica garantiza que la información sea exacta, consistente y completa desde su origen hasta su eliminación o disposición final asegurando su integridad en todo

momento. En esta guía se sugiere adoptar un esquema de clasificación con cuatro niveles tal como se observa en la Tabla 8.

Tabla 8

Clasificación de Integridad

Clasificación	Descripción
A-ALTA	La información cuya pérdida en términos de precisión y completitud podría resultar en consecuencias negativas en aspectos legales, financieros, en la continuidad de las operaciones o incluso en una pérdida significativa de la reputación empresarial.
M-MEDIA	Información cuya falta de precisión y exhaustividad podría tener repercusiones adversas en términos económicos y legales, así como retrasar las actividades y operaciones de los procesos, y también causar una disminución moderada en la imagen de la empresa entre sus empleados.
B-BAJA	Información que, en el caso de experimentar una disminución en su precisión y exhaustividad, tendría un impacto poco importante en el funcionamiento de la organización y en las partes relacionadas.
NO CLASIFICADA	Se está hablando de los activos de información que deben formar parte del inventario, incluso si todavía no han sido categorizados de manera precisa. Estos activos deben ser tratados como activos de integridad elevada.

Nota. Aspectos claves para clasificar la integridad de la información. Adaptado de. Guía para la gestión y clasificación de activos de información (GUIA No. 5), Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
(2016) https://gobiernodigital.mintic.gov.co/portal/715/articles-172093_recurso_1.pdf

Disponibilidad

Se refiere a que la información debe estar disponible y utilizable en todo momento para ser consultada por personas autorizadas según sus necesidades y en el momento que lo necesiten, es primordial determinar esta clasificación como se observa en la Tabla 9.

Tabla 9

Clasificación de Disponibilidad

Disponibilidad	Descripción
1-ALTA	La falta de disponibilidad es sumamente perjudicial para la organización.
2-MEDIA	La falta de disponibilidad que la información debe mantener puede tener consecuencias adversas en aspectos económicos y legales, así como en la interrupción y retraso de las actividades operativas, y también puede causar una disminución moderada en la imagen corporativa.
3-BAJA	La falta de disponibilidad de la información puede impactar en la continuidad de las operaciones de la empresa o entidades asociadas, aunque no conlleva implicaciones legales, económicas ni una degradación de la imagen corporativa.
4 -NO CLASIFICADA	Estos son los activos de información que deben formar parte del inventario y que aún no han sido categorizados, los cuales deben ser administrados considerándolos activos de información con alta disponibilidad.

Nota. Tipos de clasificación de disponibilidad de la información. Adaptado de. Guía para la gestión y clasificación de activos de información (GUIA No. 5), Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
(2016) https://gobiernodigital.mintic.gov.co/portal/715/articles-172093_recurso_1.pdf

Estos recursos se estiman basándose en su urgencia y relevancia en relación con las bases de la seguridad informática, conforme a los estándares que se describen a continuación en Tabla 10.

Tabla 10

Valor Criterios Activos de Información

Atributo	Criterio	Valor	Descripción
Confidencialidad	Alto	3	Datos reservados para un proceso de AgmSalud Cta que, si son revelados a terceros sin el debido permiso, pueden resultar en consecuencias adversas legales, operacionales, de reputación o financieras.
Confidencialidad	Medio	2	Datos reservados para todos los procesos de AgmSalud Cta y que, en caso de ser relevados a terceros sin el debido permiso, pueden resultar en consecuencias que lleven a un impacto negativo para sus procesos. Esta información es propia de Agm salud Cta de terceros y todos los empleados de la cooperativa pueden usarla para tareas relacionadas con los procesos, pero no debe ser revelada a terceros sin el consentimiento del dueño.
	Bajo	1	Datos que se pueden compartir o divulgar libremente a cualquier individuo, tanto dentro como fuera de Agm salud Cta, sin que esto resulte en perjuicio para terceros o para las operaciones y procedimientos de Agm salud Cta.
Integridad	Alto	3	Datos cuya inexactitud o incompletitud puede resultar en consecuencias adversas legales o financieras, demorar sus actividades o causar daños significativos a la reputación de Agm salud Cta.
	Medio	2	Datos cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones o generar pérdida de reputación moderada a funcionarios de Agm salud Cta.
	Bajo	1	Información cuya pérdida de exactitud y completitud conlleva unimpacto no significativo para Agm Salud Cta o entes externos.
Disponibilidad	Alto	3	La falta de acceso a la información puede resultar en consecuencias adversas legales o financieras, demorar sus actividades o causar daños significativos a la reputación de organizaciones externas.
	Medio	2	La falta de acceso a los datos puede provocar repercusiones legales o financieras, retrasar sus operaciones o causar un daño moderado a la reputación de *Agm salud Cta.*
	Bajo	1	La no disponibilidad de la información puede afectar la operación normal de *Agm salud Cta* o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

Nota. Valoración de los criterios que debe tener cada atributo de los activos de información. Adaptado de. Guía para la gestión y clasificación de activos de información (GUIA No. 5), Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016) https://gobiernodigital.mintic.gov.co/portal/715/articles-172093_recurso_1.pdf

La evaluación de los activos se lleva a cabo midiendo su relevancia y urgencia para la organización, y su valor se determina según el perjuicio que podría resultar al comprometer su confidencialidad, integridad y disponibilidad. Los resultados son la suma de los puntos otorgados en cada criterio, que se consolidan en lo indicado en la Tabla 11.

Tabla 11

Nivel Categorías de los Activos

Categoría	Nivel	Color
Alto	8,9	Rojo
Medio	5,6, 7	Naranja
Bajo	3, 4	Verde

Nota. Niveles de categorías de los activos según su calificación en relación con confidencialidad, integridad y disponibilidad.

Evaluación

Los criterios de valoración de activos de información son pautas o estándares que se utilizan para determinar la importancia y la sensibilidad de los activos de información en una organización. Estos criterios son esenciales para priorizar la implementación de medidas de seguridad y asignar recursos adecuadamente.

La tabla por desarrollar se compone de lo siguiente:

Figura 2

Modelo Asignación Criterio Activos

Código del Activo	Confidencialidad	Integridad	Disponibilidad	Valor

Nota. Formato asignación de criterio para activos de información.

Código del Activo: Identificación del Activo de información dentro del inventario de activos indicando a que grupo de activos pertenece.

Confidencialidad. Evalúa la importancia de la confidencialidad de un activo de información, los criterios pueden considerar si la divulgación no autorizada de la información tendría un impacto significativo en la organización, como la pérdida de datos sensibles, violaciones de la privacidad o riesgos legales.

Integridad. Determina la relevancia de la integridad de un activo de información. Se evalúa si la modificación no autorizada de la información podría causar daños o pérdida de confianza en la precisión y fiabilidad de los datos.

Disponibilidad. Mide la necesidad de que la información esté disponible cuando se requiera. Se considera si la falta de acceso a la información en momentos críticos podría afectar la continuidad del negocio o causar pérdidas financieras.

En cada criterio se le debe asignar un puntaje de 1 a 3 teniendo presente la categoría en que se debe catalogar según su nivel de impacto en la organización siendo 3 el valor más alto y 1 el valor más bajo.

Clasificación activos de información caso estudio cooperativa AGM SALUD CTA

La clasificación de los activos de información de la cooperativa CTA se visualiza en el Apéndice F, en el cual realizo como muestra la identificación del inventario y su respectiva asignación de criterios, calificando los criterios de confidencialidad, integridad y disponibilidad en cada uno de ellos.

Para el caso de ejemplo se realiza la identificación total de cincuenta y cuatro (54) activos de información de los cuales después de su respectiva clasificación, cincuenta y uno (51) los encontramos en valoración alta y tres (3) en valoración medio.

Pautas Para el Análisis y Valoración Critica de los Riesgos de Activos de Información con Base en la Metodología MAGERIT

Hay diversas formas de enfocar el análisis de riesgos en los sistemas TIC, desde consultas no estructuradas, hasta sistemas por métodos o herramientas de apoyo. Todas ellas tienen como fin hacer más objetivo el análisis de riesgos, determinando con más precisión la seguridad (o inseguridad) de los sistemas para evitar equivocaciones en nuestro juicio. El verdadero inconveniente con estos enfoques se halla en la complejidad del problema, existiendo un excesivo número de factores a considerar e incluso, si la aproximación metodológica es muy laxa, los resultados pueden ser muy poco fiables. De ahí que MAGERIT haya optado por una aproximación metodológica con reglas precisas que eviten improvisaciones y que reduzcan la subjetividad del analista.

Según Watkins (2022), es crucial identificar y evaluar los riesgos para la organización de manera que los resultados de la evaluación sean comparables y reproducibles. La severidad asignada a cada riesgo debe reflejar el costo total que la organización enfrentaría si dicho riesgo se materializara, incluyendo el costo de reposición, las repercusiones en los procesos involucrados y el impacto en la reputación de la organización. Generalmente, esta evaluación es mejor realizada por aquellos directamente involucrados en los procesos de negocio pertinentes.

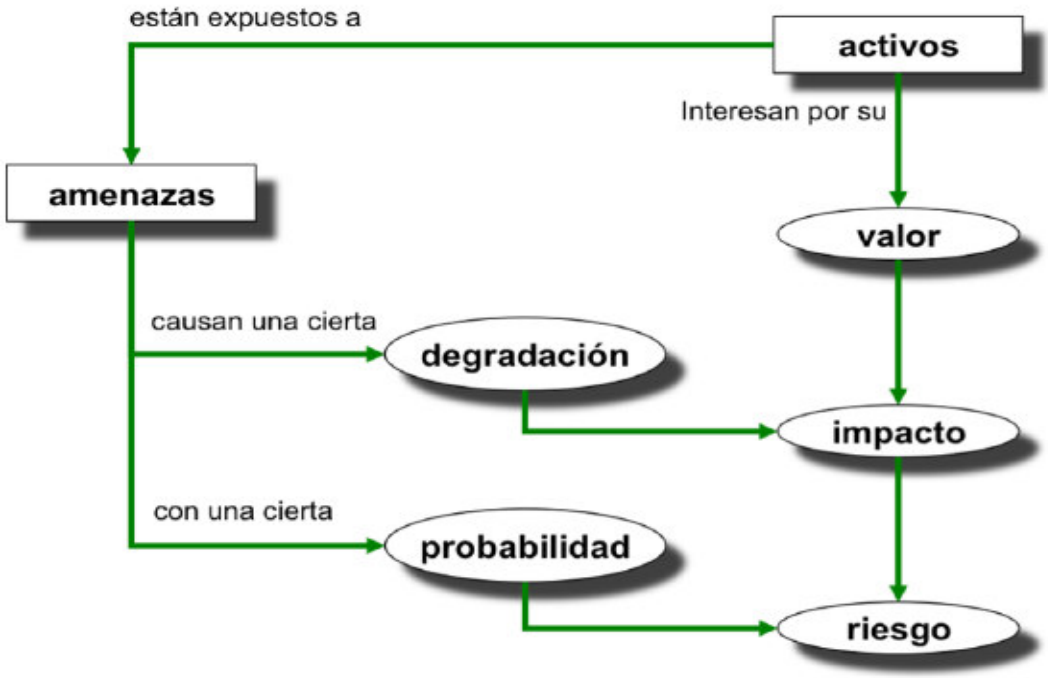
La seguridad se define como la habilidad de las redes o sistemas de información para soportar, con un grado específico de eventos, incidentes o actos ilícitos o maliciosos que pongan en riesgo la disponibilidad, autenticidad, integridad y confidencialidad de los datos guardados o transmitidos, así como de los servicios proporcionados o facilitados por estas redes y sistemas.

El análisis de riesgos facilita la evaluación del estado actual, el valor y el nivel de protección del sistema. Al alinear las acciones para el manejo de riesgos con los objetivos, la

estrategia y las políticas de la organización, se puede desarrollar un plan de seguridad. Una vez implementado y funcionando, este plan debe cumplir con los objetivos establecidos y estar acorde con el nivel de riesgo que la dirección está dispuesta a aceptar. Todas estas actividades conforman lo que se conoce como el Proceso de Gestión de Riesgos, en la Figura 3 se puede observar diagrama que nos refleja la ruta a seguir para el análisis de riesgos potenciales.

Figura 3

Elementos del Análisis de Riesgos Potenciales



Nota. Diagrama sobre los elementos que conforman el análisis de riesgos potenciales en activos de información. Tomado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012)https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Identificación de los Activos Relevantes en la Organización

En el sistema hay una jerarquía o un orden de importancia entre los activos. Los activos esenciales serían aquellos con mayor prioridad, posiblemente debido a su valor, su papel en las operaciones críticas, o su sensibilidad.

Bajo esta premisa fundamental, es posible identificar la relación activos importantes:

- Datos, representación tangible de la información.
- Servicios de soporte necesarios en la organización del sistema.
- Software necesario para administrar la información.
- Hardware sobre el reposan datos, software y servicios informáticos.
- Los dispositivos que se utilizan para almacenar datos, como soportes de información.
- Los dispositivos auxiliares que integran el material informático.
- Las redes de comunicaciones por las cuales se transmiten datos e información.
- Las instalaciones físicas en las que se resguardan los equipos de comunicaciones e informática.
- El personal que administra y opera todo el software, dispositivos, equipos y elementos relacionados anteriormente.

Dependencias

Los activos forman una red de dependencias, similar a un árbol o grafo, donde la seguridad de los activos "superiores" depende de los activos "inferiores". Esto indica una estructura en la que los activos fundamentales están soportados por otros activos más básicos o funcionales.

MINHAP (2012) explica la dependencia de activos con estas palabras:

> Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos. (p. 23)

Los activos inferiores actúan como pilares que sostienen la seguridad de los activos superiores. Esto destaca la importancia crítica de asegurar los activos en todos los niveles.

Las amenazas o daños pueden propagarse a través de estas estructuras de dependencia. Un incidente que afecte a un activo inferior puede tener consecuencias significativas en los activos superiores, resaltando la importancia de asegurar todos los niveles de activos.

La seguridad de un activo superior está asociada con la seguridad de los inferiores, ya que cualquier riesgo de un activo inferior puede afectar la integridad, la disponibilidad o la confidencialidad de un activo superior.

Valoración

La valoración de un activo en términos de seguridad está directamente relacionada con su importancia: a mayor valor de un activo, mayor es el nivel de protección requerido.

El valor de un activo puede ser que sea intrínseco o que sea acumulativo, donde los activos de menor valor de la jerarquía de dependencia incrementarán su valor a medida que aumenten, ya que ofrecen soporte a los activos que tienen un valor mayor que ellos. Los activos vitales o fundamentales, especialmente servicios e información que un sistema posee y lo proporciona como activo, son los que tienen un valor máximo y el resto de los activos se orientan a proteger y a servir de soporte para el tipo de activo fundamental.

En los sistemas de información, la explotación de datos para proporcionar servicios, ya sean internos o externos, resalta la importancia de una serie de datos necesarios para la prestación de estos servicios. La seguridad de la información y los servicios define, en gran

medida, la funcionalidad y la operatividad de una organización. Por último, las interdependencias entre los activos son fundamentales para comprender cómo la seguridad de un activo puede afectar a otros, estableciendo así un ecosistema de seguridad interconectado donde la protección de los activos esenciales es prioritaria.

Dimensiones

La relevancia de determinar y medir diversos aspectos o características de un activo dentro de una organización o sistema es proponer y llegar a añadir varios atributos o propiedades de un activo que resultan de interés para su valoración, gestión y salvaguarda: estas dimensiones podrían ser, por citar algún ejemplo, la confidencialidad, la integridad, la disponibilidad, la criticidad de las operaciones del negocio, su vulnerabilidad a riesgos concretos, entre otros.

Se debe analizar y determinar el grado o nivel en que cada una de estas características está presente o requiere atención. Por ejemplo, en el caso de un sistema de información, podríamos calibrar su confidencialidad (cómo de sensible es la información que contiene) valoración típica de los datos, su disponibilidad (qué tan crítico es que esté operativo continuamente) valoración típica de los servicios y su integridad (la importancia de que la información no sea alterada indebidamente) valoración típica de los datos que pueden estar manipulados.

Es importante mencionar que los activos esenciales también se deben analizar:

- Autenticidad: Valoración típica de los servicios en relación con autenticidad del usuario y valoración típica de los datos autenticidad de quien accede escribir o consultar la información.
- Trazabilidad del uso del servicio.
- Trazabilidad de acceso a los datos.

En aplicación de la metodología MAGERIT se agrega la autenticidad y concepto de trazabilidad términos técnicos, esto significa preservar la integridad y confidencialidad de ciertos activos del sistema, como pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad, entre otros.

Valoración de los Activos

El proceso de valoración implica calcular cuánto costaría a una organización recuperarse de un evento dañino que destruyera o comprometiera seriamente un activo específico. En este contexto, un "activo" puede ser cualquier recurso valioso para la organización, como información, infraestructura tecnológica, datos, etc.

“La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo” (MINHAP, 2012, p. 26).

Factores por estudiar:

- lucro cesante,
- coste de mano de obra,
- coste de reposición,
- capacidad de operar,
- daño a otros activos,
- daño a personas,
- daños medioambientales; y
- sanciones por incumplimiento de ley u obligaciones contractuales.

Valoración Cualitativa

Este tipo de escala se emplea para clasificar y valorar los activos de una manera que no es numérica o cuantitativa, sino basada en cualidades o características. Por ejemplo, los activos pueden clasificarse en categorías como 'bajo', 'medio', 'alto'.

La mayor desventaja del presente procedimiento es que provoca una no correcta comparación que sólo contempla el orden relativo, o dicho de otra manera, no se pueden realizar cálculos exactos y/o sumar las cifras para obtener un total. Esto puede llegar a inhibir la capacidad de realizar la siguiente serie de cálculos para realizar un examen más pormenorizado o una comparación más concreta.

Valoración Cuantitativa

Realizar valoraciones numéricas absolutas, que involucran asignar valores monetarios o cuantitativos específicos a activos o riesgos, requiere un esfuerzo considerable. Esto se debe a la necesidad de recopilar datos precisos, realizar análisis detallados y a menudo complejos, y tener en cuenta múltiples factores y variables.

Una gran ventaja de este enfoque es que permite sumar, comparar y agregar valores. Esto es particularmente útil en el contexto de la gestión de riesgos o la evaluación de activos, ya que facilita el entendimiento del impacto total o combinado de varios riesgos o la valoración conjunta de múltiples activos.

Si la valoración se realiza en términos monetarios, también es posible llevar a cabo análisis económicos que comparen lo que está en riesgo con el costo de la solución, abordando preguntas como:

- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿Vale la pena invertir tanto dinero en esta salvaguarda?

- ¿Cuánto es razonable que cueste una prima de seguros?
- ¿En qué plazo de tiempo se recupera la inversión?

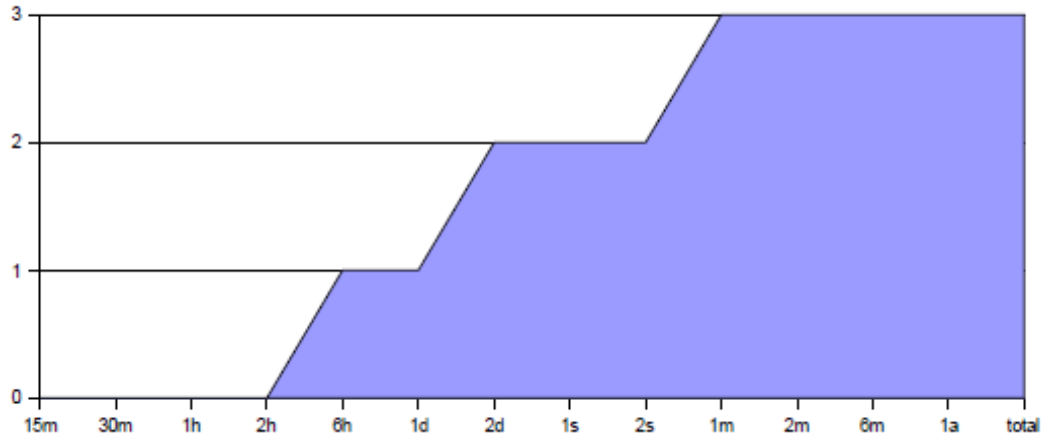
Valor de la Interrupción del Servicio

La disponibilidad del activo no se ha valorado en los pasos anteriores antes de enfocarnos en este atributo se debe tener presente lo siguiente:

El efecto de una interrupción en un servicio depende de cuánto tiempo dura. Una interrupción de una hora podría tener un impacto mínimo o incluso ser irrelevante, mientras que una interrupción de un día ya podría causar un daño moderado. Sin embargo, si la interrupción se extiende a un mes, podría ser lo suficientemente grave como para poner fin a la actividad o al negocio. Si se quiere valorar la disponibilidad de un activo, como ejemplo podemos tomar la Figura 4.

Figura 4

Coste de la Interrupción de la Disponibilidad



Nota. Diagrama sobre el coste de interrupción por tiempo de inactividad. Tomado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012)

https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Tomando como referencia la Figura 4 se puede analizar que interrupciones después de las 6 horas representan perdida de operación en la compañía, lo que se traduce en signos de alerta, ya que significa que es importante invertir para minimizar y evitar estas situaciones, ya que si no se toman medidas pueden causar después de dos meses la pérdida total de su capacidad de operar.

Amenazas

Sigue el proceso que determinará las amenazas que pueden afectar al activo, una amenaza es cualquier tipo de potencial peligro que puede causar un detrimento o un efecto negativo de algún tipo sobre los activos, cualquier dato, sistema, red, software, hardware e incluso procesos y personas que tienen un valor para la organización. Las amenazas pueden tener distintas manifestaciones y pueden comprometer la confidencialidad, integridad o disponibilidad de la información.

Identificación de las Amenazas

- De origen natural: Eventos como terremotos, inundaciones, incendios, que pueden dañar físicamente los activos de información, como los centros de datos y el hardware. (MINHAP, 2012)
- Del entorno: Existen catástrofes industriales, como la contaminación y cortes de electricidad, en las que los sistemas de información se ven afectados de manera indirecta; sin embargo, esto no significa que debamos estar desprotegidos frente a tales incidentes, a pesar de ser afectados de forma pasiva.(MINHAP, 2012)

- Defectos de las aplicaciones: Existen dificultades que se originan directamente en el equipo debido a fallos en su diseño o en su puesta en marcha, las cuales pueden tener impactos negativos potenciales sobre el sistema.
- Causadas por las personas de forma accidental: Los errores cometidos por empleados o usuarios, como la introducción accidental de datos erróneos, la eliminación inadvertida de archivos importantes, o el envío de información sensible a destinatarios incorrectos.
- Causadas por las personas de forma deliberada: Amenazas provenientes de empleados o exempleados que abusan de su acceso a los sistemas de la organización para robar, modificar o destruir información.

Valoración de las Amenazas.

Se debe valorar la influencia en el valor del activo en dos sentidos:

- Degradación: Que tanto perjudicado resultaría el valor, la degradación generalmente se define como una porción del valor total del activo, llevando a expresiones como que un activo ha sido “completamente degradado” o “degradado solo en una pequeña parte”. En situaciones donde las amenazas son no intencionales, suele ser suficiente conocer la parte del activo que ha sufrido daños físicos para determinar la correspondiente pérdida de su valor. Sin embargo, en casos de amenazas intencionales, no se puede aplicar este criterio de proporcionalidad, ya que un atacante puede infligir daños significativos de manera selectiva y desproporcionada.
- Probabilidad: Que tan probable o improbables es que se ejecute la amenaza, la probabilidad de ocurrencia de la amenaza por lo general se modela cualitativamente como se puede observar en la Tabla 12.

Tabla 12

Probabilidad de la Amenaza

Nomenclatura	Categoría	Valoración
MA	Prácticamente Seguro	5
A	Probable	4
M	Posible	3
B	Poco Probable	2
MB	Muy Raro	1

Nota. Asignación de valores para la probabilidad de ocurrencia de amenazas que afecten activos de información. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012) https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

También es posible realizar su modelación numéricamente como una frecuencia de ocurrencia Tabla 13, tomando como referencia un año en tiempo, recurriendo a la tasa anual de ocurrencia como parámetro de la probabilidad de que algo suceda:

Tabla 13

Frecuencia de Ocurrencia

Nomenclatura	Categoría	Frecuencia	Ocurrencia
MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Nota. Frecuencia de ocurrencia de una amenaza modelado numéricamente. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012) https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Determinación Impacto Potencial

La determinación de impacto potencial se refiere al proceso de evaluar y estimar las posibles consecuencias que podría tener un evento específico, como un incidente de seguridad, un desastre natural, un fallo técnico, o cualquier otro tipo de riesgo, sobre una organización, sistema, individuo o proceso.

En el contexto de la gestión de riesgos y la seguridad de la información, este proceso es crucial para comprender la gravedad de los diferentes tipos de amenazas y cómo podrían afectar los activos críticos, calificando el daño sobre el activo en el instante en que se hace realizada una amenaza.

Impacto Calculado

Calculo sobre un activo en el que se debe referenciar:

- su valor acumulado,
- las amenazas a que está expuesto.

Indica el MINHAP (2012), “El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada” (p. 29). El cálculo de este impacto acumulado ayuda a las organizaciones a comprender la magnitud total del riesgo asociado con diferentes amenazas, lo que a su vez facilita la priorización de medidas de

mitigación y la toma de decisiones en la gestión de la seguridad de la información y la planificación de la continuidad del negocio.

El impacto aumenta en proporción al valor intrínseco o acumulado que tiene un activo, cuanto más grande sea el daño sufrido por un activo atacado, mayor será el impacto resultante.

Al calcular el impacto acumulado en base a los activos que sostienen el sistema de información, es posible identificar las medidas de protección necesarias para los recursos de trabajo, como la seguridad de los equipos, la realización de copias de seguridad, entre otros.

Impacto Repercutido

Las consecuencias o efectos secundarios que se producen de forma "a posteriori" de un acontecimiento primigenio, sobre todo en un contexto donde dicha consecuencia se expande o afecta a otros sistemas, áreas u otros modos de procesos de la realidad, más allá del propio punto de origen. En lo concerniente a la gestión de riesgos, esta idea es de gran importancia puesto que se entiende que un evento dado en una parte determinada de un sistema o de una organización tiene la posibilidad de tener otras manifestaciones en forma de ramificaciones.

Se calcula sobre un activo teniendo como referencia:

- Valor del activo según sus propias características.
- Las amenazas que pueden impactar los activos superiores a él.
- El análisis del impacto se debe realizar tomando en cuenta tres dimensiones:
    - Por cada activo, se debe evaluar individualmente cada componente del sistema.
    - Por cada amenaza, se debe considerar cada riesgo potencial específico.
    - Por cada dimensión de valor, se debe analizar en los distintos criterios de valor ejemplo: económico, operativo, estratégico, etc.

Mientras mayor el valor del activo así mismo mayor el valor del impacto, entre más degradación del activo atacado así mismo el impacto es mayor y entre mayor dependencia del activo atacado así mismo el impacto es mayor.

Al calcular el impacto repercutido en activos con valor intrínseco, se facilita la evaluación de cómo los incidentes técnicos afectan la función del sistema de información. Esto proporciona una perspectiva gerencial útil para tomar decisiones críticas en el análisis de riesgos, como la aceptación de un nivel específico de riesgo.

Agregación de Valores de Impacto

Condiciones sobre las que se debe agregar los impactos singulares:

- El impacto que se nos da puede acumularse sobre varios activos, el efecto original de un problema en un activo puede extenderse y afectar a los otros activos, de tal manera que el impacto total viene dado por la combinación de los efectos de cada activo.
- El Impacto acumulado puede agregarse sobre activos que no dependan entre sí y que no hereden valor de un activo superior común, es posible sumar o acumular los impactos individuales en varios activos dentro de una organización, incluso si estos activos no están directamente relacionados o interconectados, y no derivan su valor de un mismo activo superior.
- El impacto acumulado no debe agregarse sobre activos que no sean independientes, al incluir en varias ocasiones el valor acumulado de activos superiores se generaría sobre ponderación.
- El impacto de diferentes amenazas puede agregarse puede sobre un mismo activo, se recomienda considerar en qué medida son independientes y recurrentes las diferentes amenazas.
- En diferentes dimensiones es recomendable agregar el impacto de una amenaza.

Determinación de Riesgo Potencial

El riesgo se define como la medida de afectación probable de un sistema, cuya valoración se fundamenta en dos componentes esenciales: la probabilidad de ocurrencia de una amenaza y el impacto resultante sobre los activos.(Suárez González, 2018)

El riesgo se incrementa con la probabilidad y el impacto:

$$Riesgo\ potencial = Frecuencia\ x\ Impacto$$

Frecuencia de ocurrencia: Que tan seguido se espera que ocurra la amenaza.

Impacto acumulado: Caul es el daño total que sufre el activo si la amenaza ocurre.

Lo que permite identificar una serie de zonas que se deben tener presentes en el instante del tratamiento del riesgo:

- Zona 1: Riesgos altamente probables y de muy alto impacto.
- Zona 2: Situaciones que van desde improbables y de medio impacto, hasta situaciones improbables y de impacto bajo o muy bajo.
- Zona 3: Riesgos improbables y de bajo impacto.
- Zona 4: Riesgos improbables, pero de impacto muy alto.

Al identificar de forma sistemática las amenazas que se encuentran en la Zona 1, la organización logra priorizar de manera eficiente los recursos financieros y humanos, de tal manera que el tratamiento del riesgo no sea visto como un gasto administrativo, sino como una inversión estratégica en resiliencia organizacional. Este cálculo de riesgo inherente actúa, finalmente, como el punto de partida insustituible para la trazabilidad requerida por los evaluadores y estándares internacionales, facilitando una transición razonada hacia un riesgo residual técnica y éticamente aceptable para los órganos de gobierno democrático.

La Zona 4 está caracterizada por riesgos de impacto muy alto pero baja probabilidad de ocurrencia, y representa escenarios de crisis extrema o eventos catastróficos para la estabilidad de la organización. Estos riesgos en las Cooperativas de Trabajo Asociado (CTA) se vinculan a eventos de baja frecuencia, pero que, por su naturaleza, son devastadores, tales como incendios en centros de cómputo, desastres naturales, ataques cibernéticos de gran escala que comprometan la totalidad del acervo informativo institucional.

Es un error crítico en gestión de riesgos el ignorar la Zona 4 por su baja frecuencia. El análisis debe concentrarse en el impacto acumulado, ya que un solo evento en esta área tiene la capacidad de liquidar la confianza de los socios y generar graves sanciones legales bajo el régimen de la Ley 1581 de 2012, si no se tienen los protocolos de respuesta adecuados.

Riesgo Acumulado

Se debe tener en cuenta en:

- El impacto acumulado que afecta un activo bajo la influencia de una amenaza y la probabilidad de está.
- Debe calcularse para cada activo, en cada dimensión de valoración y por cada amenaza, caracterizándose por ser de valor acumulado, la degradación causada y la probabilidad de la amenaza.

Al enfocarse sobre los activos que soportan el peso del sistema de información, se asegura desarrollar las salvaguardas que hay que crear para los medios de trabajo: copias de respaldo, protección de los equipos, etc.

El riesgo acumulado representa una visión estratégica y sistémica de la vulnerabilidad donde la criticidad de un activo no está determinada por su valor intrínseco o comercial, sino por la relevancia de los servicios y procesos que dependen directamente de su operatividad.

Este concepto, dentro de la metodología MAGERIT, incluye el impacto acumulado, es decir, los daños que se extienden en cadena por toda la dependencia institucional, lo que permite conocer los elementos de infraestructura que, aunque operativamente sean de menor tamaño, son muy importantes para la estabilidad de la organización. En términos matemáticos, esto se expresa como la frecuencia de la amenaza multiplicada por el impacto total heredado de los niveles superiores:

$$Riesgo\ acumulado = Frecuencia\ x\ Impacto\ acumulado$$

Si se trata de una organización del sector solidario, el hecho de priorizar el tratamiento del riesgo bajo esta óptica asegura que las salvaguardas protejan el flujo de información que sostiene el capital social, lo cual garantiza que un fallo técnico en un activo base no se traduzca en una interrupción crítica de los servicios al asociado o en una vulneración de la confianza democrática institucional.

Riesgo Repercutido

Se calcula sobre un activo tomando como referencia:

- Probabilidad de la amenaza y su impacto acumulado sobre un activo.
- Debe calcularse por cada activo, cada dimensión de valoración y cada amenaza, lo que permite establecer el valor del riesgo como el resultado de una función que combina las siguientes tres variables: valor propio, degradación causada y la probabilidad de amenaza.

La evaluación del riesgo repercutido, entendida en función de activos que tienen su propio valor, propicia describir las consecuencias que los incidentes técnicos acarrean para el objetivo del sistema de información. Por ello resulta ser un informe de tipo gerencial muy adecuado para la toma de decisiones críticas en el análisis del riesgo, como puede ser la aceptación de un nivel de riesgo determinado.

El riesgo repercutido se define como la exposición que enfrentan los activos de nivel superior, tales como procesos misionales, servicios al asociado o información estratégica, a raíz de que las amenazas sobre los activos de soporte o infraestructura que los sustentan se materialicen. Mientras que otros indicadores cuantifican la vulnerabilidad técnica, el riesgo repercutido mide los daños desde el punto de vista de la gestión organizacional, estableciendo una relación directa entre la probabilidad de fallo en la base técnica (f) y el valor o impacto propio del activo superior afectado (i):

$$Riesgo\ repercutido = Frecuencia\ x\ Impacto\ Propio$$

Para las organizaciones del sector solidario, este concepto es una herramienta esencial de gobernanza, pues permite convertir incidentes técnicos en impactos que se pueden sentir sobre la prestación de servicios financieros o sociales. Ya que se puede analizar como una amenaza a la infraestructura puede tener repercusiones en los servicios prestados a los asociados permitiendo al encargado de la seguridad informática justificar ante el consejo de administración inversión en seguridad para los activos que componen la parte técnica con el fin de preservar la confianza y el patrimonio de los asociados, más allá del valor comercial de los equipos tecnológicos.

Agregación de Riesgos

Bajos las siguientes condiciones pueden agregarse los riesgos singulares:

- Riesgo repercutido sobre diferentes activos.
- Impacto acumulado sobre activos que no sean dependientes entre sí y que no hereden valor de un activo superior común.
- Sobre activos que no sean independientes no hay que agregar el riesgo acumulado, ya que esto tendería a sobre ponderar el riesgo debido a la inclusión de varias veces el valor acumulado de activos superiores.

- Sobre un mismo activo se puede agregar el riesgo de diferentes amenazas, pero es recomendable considerar en que grado las diferentes amenazas pueden ser recurrentes y son independientes.
- En diferentes dimensiones se puede agregar el riesgo de una amenaza.

Salvaguardas

Las salvaguardas, llamadas controles de la seguridad en la norma ISO/IEC 27001:2022, son fundamentales para el refuerzo y la efectividad de un sistema de gestión de la seguridad de la información, porque se entienden como fundamentos para reducir el impacto de un determinado riesgo según el mismo MINHAP (2012) “Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo” (p. 31).

Las salvaguardas, también conocidas como contramedidas, son disposiciones de seguridad extendidas para que las amenazas provoquen el menor daño posible a una organización. Su función principal es afrontar las amenazas y minimizar o poner bajo control las vulnerabilidades detectadas en un sistema. De la correcta implementación de estas medidas dependerá la protección de la disponibilidad, integridad y confiabilidad de los activos de información (Andrade Talero, 2021).

Existen amenazas que se pueden neutralizar simplemente mediante una organización adecuada de la información, mientras que otras necesitan de recursos técnicos más avanzados como software o hardware, otras más requieren de medidas de seguridad física para proteger los activos de información y, finalmente, se pueden encontrar políticas, procedimientos y capacitaciones que permitirán guiar a la organización en la toma de decisiones con respecto a la seguridad de la información. Según Sales Silva (2023), la formación y la concienciación de los

empleados también son fundamentales para garantizar que el personal comprenda los riesgos potenciales y actúe para minimizarlos.

Selección de Salvaguardas

Aspectos para tener en cuenta para seleccionar salvaguardas relevantes que permitan un adecuado plan de protección:

1. Cada activo se debe proteger de diferente forma, así que es crucial conocer el tipo de activo.
2. Dimensiones de seguridad que requieren protección.
3. Amenazas de las que se requiere proteger los activos.
4. Existencia de salvaguardas alternos.

Adicional se recomienda establecer un principio de proporcionalidad:

1. Centrarse en los activos más valiosos ya sean tipos de valores propios o acumulados.
2. Centrarse en los riesgos más importantes, verificando la mayor probabilidad de que una amenaza ocurra.
3. La protección ante un riesgo que puede llegar a brindar las salvaguardas alternas.

A partir de esta clasificación se pueden obtener dos declaraciones con la cuales se puede excluir o no la aplicación de determinada salvaguarda:

- No aplica: Se afirma que una salvaguarda no es aplicable si técnicamente no se ajusta al tipo de activos que se deben proteger, no resguarda los aspectos requeridos o no es eficaz contra la amenaza específica en cuestión.
- No se justifica: Se indica que una salvaguarda es aplicable, pero resulta excesiva en comparación con el nivel de riesgo que se necesita proteger.

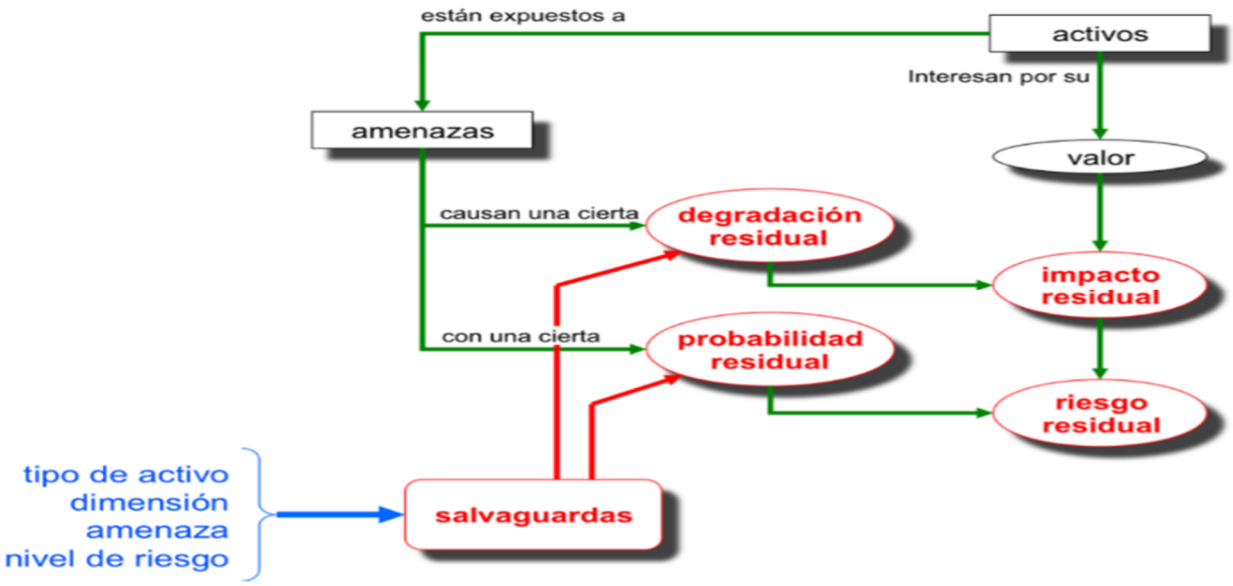
Efecto de las Salvaguardas

Intervienen en el cálculo de los riesgos con:

- Reducción de la probabilidad de las amenazas: ideales para impedir que se materialice la amenaza, estas se pueden identificar como salvaguardas preventivas.
- Limitación del daño causado: existen medidas de protección que restringen directamente el posible deterioro, mientras que otras facilitan la detección inmediata del ataque para prevenir un mayor daño. Hay salvaguardas que incluso se centran en posibilitar una rápida restauración del sistema en caso de que sea destruido por una amenaza. En todas estas situaciones, aunque la amenaza se concreta, sus efectos se minimizan (Calder, 2024).

Figura 5

Elementos de Análisis del Riesgo Residual



Nota. Diagrama sobre los elementos que conforman el análisis de riesgos residuales en activos de información. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones

Públicas. (2012) https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Tipo de Protección

En relación con las salvaguardas se tienen diferentes tipos de protección:

- [PR] prevención: Una salvaguarda se considera preventiva si disminuye la posibilidad de que un incidente suceda. En caso de que esta medida de seguridad no funcione y el incidente se produzca, los daños resultantes serán iguales.
- [DR] disuasión: Una salvaguarda se define como disuasoria cuando impacta en los potenciales atacantes de manera que los desalienta o les hace reconsiderar la idea de atacar. Estas medidas de seguridad operan antes del incidente, disminuyendo las chances de que este se produzca, aunque no afectan el nivel de daño si el atacante decide proceder de todos modos.
- [EL] eliminación: Una salvaguarda se considera eliminadora de un incidente si evita su ocurrencia. Estas medidas de seguridad se aplican antes de que el incidente suceda. Sin embargo, no disminuyen el impacto del daño en caso de que la salvaguarda no sea completamente efectiva y el incidente se produzca de todas formas.
- [IM] minimización del impacto / limitación del impacto: Una salvaguarda se describe como minimizadora o limitadora del impacto cuando restringe o reduce las consecuencias derivadas de un incidente.
- [CR] corrección: Una salvaguarda se clasifica como correctiva cuando, en caso de que ocurra un daño, lo repara. Estas medidas de seguridad intervienen después de que el incidente haya sucedido, y por lo tanto, sirven para disminuir los daños causados.

- [MN] monitorización: Estas salvaguardas funcionan mediante la supervisión de eventos actuales o pasados. Si se identifican situaciones en tiempo real, es posible reaccionar rápidamente para contener el incidente y minimizar su impacto; si se identifican eventos después de que han ocurrido, se puede aprender de ellos para mejorar el sistema de salvaguardas para el futuro.

- [AW] concienciación**:** Son las acciones formativas, dirigidas a las personas intervinientes en el sistema, que pueden influir sobre su funcionamiento: la educación disminuye los errores humanos, operando de esta forma preventivamente. A su vez, potencia la eficacia y la inmediatez de todas las acciones de seguridad, en la medida en que quienes han de conducirlas, lo hacen de forma más eficiente, bien incrementando su efecto o bien evitando, como mínimo, que se debilite por un mal uso.

- [RC] recuperación: Una salvaguarda se considera de recuperación si facilita el retorno al estado previo al incidente. Estas medidas de protección no disminuyen la posibilidad de que ocurra el incidente, pero sí limitan los daños a un lapso temporal específico.

- [DC] detección: Una salvaguarda se considera detectora de ataques cuando notifica de que un ataque se está llevando a cabo. Aunque no puede detenerlo, sí puede activarse y activar otras salvaguardas que intervienen y ayudan a detener el ataque en sí, lo que permitiría disminuir los daños que está causando.

- [AD] administración: Se hace referencia a las medidas de protección que están naturalizadas por los elementos de la seguridad del sistema. Para evitar ataques, se debe tener un inventario estricto de todos los componentes del sistema. Si se olvida que un componente existe, ese componente se quedará sin actualizaciones de seguridad y se convertirá en el punto débil por

donde entrarán los atacantes. Por regla general pueden considerarse como medidas en la línea de las preventivas.

En la Tabla 14 se puede observar la clasificación realizada para el tipo de salvaguardas, en la cual según el efecto de la salvaguarda se le categoriza un tipo determinado.

Tabla 14

Tipos de Salvaguardas

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas
	[DR] disuasorias
	[EL] eliminatorias
Acotan la degradación	[IM] minimizadoras
	[CR] correctivas
	[RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

Nota. Listado de tipos de salvaguardas. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012)

Eficacia de la Protección

Se puede denominar una salvaguarda 100% eficaz si cumple con lo siguiente:

- Aspecto técnico:
    - Al enfrentarse al riesgo que protege se considera técnicamente Idónea;

- siempre se emplea.

- Desde la operación:
  - Se encuentra completamente implementada, ajustada y conservada;
  - Hay protocolos definidos tanto para la operación estándar como para situaciones de incidentes;
  - Los usuarios están capacitados y concienciados;
  - Los posibles fallos son informados a través de controles.

En la Tabla 15 se puede observar que desde una efectividad del 0% para la ausencia de salvaguardas hasta un 100% para las que son ideales y están completamente establecidas, se calculará un nivel de eficacia específico en cada situación particular.

Tabla 15

Eficacia y Madurez de las Salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
20%	L1	Inicial / Ad hoc
40%	L2	Reproducible, pero intuitivo
60%	L3	Proceso definido
80%	L4	Gestionado y medible
100%	L5	Optimizado

Nota. Calificación de eficacia y madurez de las salvaguardas. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012)

La eficacia de la salvaguarda no es un valor fijo, sino una medida de capacidad. Es el tanto por ciento en que una salvaguardia es capaz de reducir el riesgo inicial.

- Si una salvaguarda tiene una eficacia del 0%, el riesgo residual será igual al riesgo potencial (el control no sirve).
- Si tiene una eficacia del 100% (teórico), el riesgo desaparece.

Una salvaguardia puede funcionar de dos maneras diferentes:

- Eficacia sobre la Probabilidad (o Frecuencia): El control actúa antes de que ocurra el incidente. Su propósito es impedir que la amenaza se concrete.

Ejemplo: El Firewall Fortinet ayuda a minimizar las probabilidades de que un atacante externo pueda tener acceso.

- Eficacia del Impacto: El control funciona durante o después del incidente. Su objetivo es que, en caso de que se produzca la amenaza, el daño sea lo menor posible.

Ejemplo: Las copias de respaldo (Backups) no evitan que el servidor falle, pero reducen el impacto de la pérdida de información casi a cero.

Es así como para medir la eficacia total de una salvaguarda se deben tener en cuenta el factor de reducción en el impacto y el factor de reducción de la frecuencia, esta se expresa como un valor entre 0 y 1, por ejemplo si hablamos que una salvaguarda tiene un factor del 20% lo cual nos indica que está en el nivel L1 representaría un valor de 0.2.

Fórmula matemática para combinar ambos factores:

$$E = 1 - [(1 - f_i)\ x\ (1 - \ f_f)]$$

Vulnerabilidades

Según Fernández Climent (2024) se refiere a cualquier fallo o deficiencia que pueda ser explotada por una amenaza, o, de manera más específica, son las debilidades presentes en los activos de información o en sus medidas de seguridad, lo que a futuro significara que exista una mayor probabilidad de materialización de una amenaza potencial.

Impacto Residual

Considerando un grupo de salvaguardas implementadas y el nivel de madurez de su proceso de gestión, el sistema se sitúa en un estado de impacto posible conocido como residual. Esto significa que hemos alterado el impacto, pasando de un valor potencial a uno residual.

Calcular el impacto residual se manifiesta como un proceso sencillo, dado que, como hemos justificado en los epígrafes anteriores, los activos y sus interrelaciones no han variado en nada, solamente la intensidad del deterioro. Entonces, simplemente se vuelven a calcular los impactos para este nuevo nivel de deterioro.

La magnitud de este deterioro, considerando la eficacia de las salvaguardas, es la diferencia que existe entre la eficacia ideal y la eficacia real.

El impacto residual puede estimarse acumulativamente sobre los activos inferiores, o en términos de su efecto sobre los activos superiores.

Riesgo Residual

Con un conjunto específico de salvaguardas implementadas y evaluando la madurez de su proceso de gestión, el sistema se encuentra en una condición de riesgo conocida como residual. Esto implica que hemos transformado el riesgo, de un nivel potencial a uno residual.

El proceso para calcular el riesgo residual es directo. Ya que ni los activos ni sus interrelaciones han cambiado, solo la extensión de la degradación y la probabilidad de amenazas, se vuelven a realizar los cálculos de riesgo utilizando el impacto y la probabilidad residuales de que sucedan.

La extensión de la degradación se considera en la estimación del impacto residual.

La probabilidad residual, teniendo en cuenta la eficacia de las salvaguardas, es la diferencia que existe entre una eficacia ideal y la eficacia real.

El riesgo residual se puede estimar de forma acumulativa en los activos inferiores, o en términos de su repercusión en los activos superiores.

De acuerdo con metodologías estructuradas como MAGERIT, este cálculo se realiza durante la Fase 4 del análisis y gestión de riesgos (Andrade Talero, 2021). Para obtenerlo, se debe seguir la siguiente lógica:

- Combinación de variables: El impacto residual se calcula al combinar el valor estipulado de cada uno de los activos con la valoración inicial de las amenazas, integrando en la ecuación la efectividad de las salvaguardas aplicadas (Suárez González, 2018).
- Estimación de elementos residuales: En la práctica, se debe determinar un nuevo valor para el impacto residual (el daño que aún podría causarse si la defensa falla) y la probabilidad residual (qué tan factible es que el ataque logre superar el control).

Para procesar este cálculo algorítmico, los analistas pueden apoyarse en dos enfoques de modelado:

1. Modelo cuantitativo: Se emplean fórmulas y valores numéricos exactos para cuantificar cuánto riesgo acumulado existía y cuánto riesgo residual queda. Puede implicar cálculos monetarios precisos u horas exactas de inactividad.
2. Modelo cualitativo: Utiliza una escala discreta de valores (por ejemplo, desde "muy bajo" hasta "muy alto" o "crítico") que permite establecer el riesgo remanente sin necesidad de cifras exactas, basándose en la reducción de nivel que aporta el paquete de salvaguardas.

Con la determinación del riesgo residual, se permite visualizar la efectividad real de las medidas de seguridad sobre los activos críticos de la organización. En la metodología MAGERIT, el riesgo residual se define como la magnitud de la amenaza que queda tras la

aplicación de las salvaguardas, y se calcula mediante la degradación sistemática del riesgo potencial (R_P) por la aplicación de la eficacia (E) de los controles derivados del estándar ISO/IEC 27001:2022. El proceso queda expresado mediante la fórmula:

$$R_{r=}R_p\ x\ (1-E)$$

Análisis de Riesgos para Caso Estudio

En la realización de un análisis de riesgos de activos de información del caso de estudio cooperativa de trabajo asociado AGM SALUD CTA, como parámetro inicial retomemos el inventario de activos realizado en la fase anterior registrado en Tabla 16:

Tabla 16

Activos de información de Cooperativa de Trabajo Asociado- AGM SALUD CTA

Ítem	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
1	Servidor Físico - HP Proliant ML110 Gen 10.	Líder Equipo de seguridad	HARDWARE
2	Servidor Físico - HP Proliant ML 350 Gen 10.	Líder Equipo de seguridad	HARDWARE
3	Computadores Corporativos (20)	Líder Equipo de seguridad	HARDWARE
4	Computador portátil (4)	Líder Equipo de seguridad	HARDWARE
5	Switches (3)	Líder Equipo de seguridad	HARDWARE
6	Router Wifi	Líder Equipo de seguridad	HARDWARE
7	Access Point (3)	Líder Equipo de seguridad	HARDWARE
8	Balanceador de Carga	Líder Equipo de seguridad	HARDWARE

Ítem	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
9	Firewall Fortinet 50E	Líder Equipo de seguridad	HARDWARE
10	Documentación de procesos de desarrollo.	Líder Bases de datos	Datos
11	Código Fuente AGM SALUD CTA Nomina.	Líder Bases de datos	DATOS
12	Código Fuente AGM SALUD CTA Financiera.	Líder Bases de datos	DATOS
13	Código Fuente AGM SALUD CTA Gestión talento Humano.	Líder Bases de datos	DATOS
14	Aplicación AGM SALUD CTA Gestión documental.	Líder Bases de datos	DATOS
15	Contratos clientes	Líder Bases de datos	DATOS
16	Políticas de tratamiento de datos personales.	Líder Bases de datos	DATOS
17	Documentación de HelpDesk	Líder Bases de datos	DATOS
18	Expedientes de los empleados	Líder Bases de datos	DATOS
19	Contratos empleados	Líder Bases de datos	DATOS
20	Canal de Internet Dedicado	Ingeniero administración Active Directory	Comunicaciones
21	Canal de Internet Respaldo	Ingeniero administración Active Directory	COMUNICACIONES
22	Cableado de red	Ingeniero administración Active Directory	COMUNICACIONES

Ítem	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
23	Conexiones VPN client to site	Ingeniero administración Active Directory	COMUNICACIONES
24	Red inalámbrica corporativa	Ingeniero administración Active Directory	COMUNICACIONES
25	Red inalámbrica Invitados	Ingeniero administracion Active Directory	COMUNICACIONES
26	Director Área TI	Ingeniero Líder Soporte	PERSONAL
27	Líder Base de datos, administración de red.	Ingeniero Líder Soporte	PERSONAL
28	Líder seguridad informática	Ingeniero Líder Soporte	PERSONAL
29	Líder soporte.	Ingeniero Líder Soporte	PERSONAL
30	Ingeniero administración Active Directory, servicios de red e infraestructura.	Ingeniero Líder Soporte	PERSONAL
31	Ingeniero administración bases de datos.	Ingeniero Líder Soporte	PERSONAL
32	Solución Ofimática	Ingeniero Líder Bases de datos	SOFTWARE
33	Aplicación AGM SALUD CTA Nomina.	Ingeniero Líder Bases de datos	SOFTWARE
34	Aplicación AGM SALUD CTA Financiera	Ingeniero Líder Bases de datos	SOFTWARE
35	Aplicación AGM SALUD CTA Gestión Talento Humano	Ingeniero Líder Bases de datos	SOFTWARE
36	Aplicación AGM SALUD CTA Gestión Documental	Ingeniero Líder Bases de datos	SOFTWARE
37	Bases de Datos	Ingeniero Líder Bases de datos	SOFTWARE

Ítem	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
38	Aplicaciones Móviles	Ingeniero Líder Bases de datos	SOFTWARE
39	Certificados SSL Letsencritp	Ingeniero Líder Bases de datos	SOFTWARE
40	Dominio: agmsaludcta.site, agmsaludcta.com	Ingeniero Líder Bases de datos	SOFTWARE
41	Sitio Corporativo: www.agmsaludcta.com	Ingeniero Líder Bases de datos	SOFTWARE
42	agmsaludctadesk	Ingeniero Líder Bases de datos	SOFTWARE
43	Servidores Virtuales	Ingeniero Líder Bases de datos	SOFTWARE
44	Email office 365	Ingeniero Líder Bases de datos	SOFTWARE
45	OneDrive	Ingeniero Líder Bases de datos	SOFTWARE
46	Sophos	Ingeniero Líder Bases de datos	SOFTWARE
47	Licencia Windows server 2019	Ingeniero Líder Bases de datos	SOFTWARE
48	CentOs 8	Ingeniero Líder Bases de datos	SOFTWARE
49	Suricata	Ingeniero Líder Bases de datos	SOFTWARE

Nota. Listado de activos de información pertenecientes a la cooperativa de trabajo asociado.

Con el inventario de activos de la información definido es recomendable realizar el proceso de valoración cualitativa del inventario identificado el cual se puede visualizar en la Tabla 17:

Tabla 17

Valoración Cualitativa del Inventario de Activos de Información

Datos del activo de información				Dimensión					Atributos									Ubicación	
Ítem	Nombre del activo de información	Proceso propietario del Activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
1	Servidor Físico - HP Proliant ML110 Gen 10.	Líder Equipo de seguridad	HARDWARE	MA	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
2	Servidor Físico - HP Proliant ML 350 Gen 10.	Líder Equipo de seguridad	HARDWARE	MA	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI			X	X	
3	Computadores Corporativos (20).	Líder Equipo de seguridad	HARDWARE	M	M	A	A	A	NO	SI	SI	SI	NO	NO		X		X	
4	Computador portátil (4).	Líder Equipo de seguridad	HARDWARE	M	M	A	A	A	NO	SI	SI	SI	NO	NO		X		X	
5	Switches (3).	Líder Equipo de seguridad	HARDWARE	M	M	A	A	A	NO	SI	SI	NO	SI	SI		X		X	
6	Router Wif.i	Líder Equipo de seguridad	HARDWARE	M	M	A	A	A	NO	SI	SI	NO	NO	NO		X		X	
7	Access Point (3).	Líder Equipo de seguridad	HARDWARE	B	B	M	M	M	NO	SI	SI	NO	NO	NO	X			X	

Datos del activo de información				Dimensión					Atributos								**Ubicación**	
Ítem	Nombre del activo de información	Proceso propietario del Activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
8	Balanceador de Carga.	Líder Equipo de seguridad	HARDWARE	M	M	A	A	A	NO	SI	SI	NO	SI	NO		X		X	
9	Firewall Fortinet 50E.	Líder Equipo de seguridad	HARDWARE	A	MA	MA	MA	MA	NO	SI	SI	NO	SI	SI			X	X	
10	Documentación de procesos de desarrollo.	Líder Bases de datos	DATOS	A	B	MA	MA	M	SI	SI	SI	SI	NO	SI		X		X	
11	Código Fuente AGM SALUD CTA Nomina.	Líder Bases de datos	DATOS	MA	M	MA	MA	A	NO	SI	SI	SI	SI	NO			X		X
12	Código Fuente AGM SALUD CTA Financiera.	Líder Bases de datos	DATOS	MA	M	MA	MA	A	NO	SI	SI	SI	SI	SI			X		X
13	Código Fuente AGM SALUD CTA Gestión talento Humano.	Líder Bases de datos	DATOS	MA	M	MA	MA	A	NO	SI	SI	SI	SI	SI			X		X
14	Aplicación AGM SALUD CTA Gestión documental.	Líder Bases de datos	DATOS	MA	M	MA	MA	A	SI	SI	SI	SI	NO	SI		X			X
15	Contratos clientes.	Líder Bases de datos	DATOS	A	M	A	MA	M	NO	SI	SI	SI	SI	SI		X			X
16	Políticas de tratamiento de datos personales.	Líder Bases de datos	DATOS	A	MA	M	MA	A	NO	NO	SI	NO	SI	SI		X			X

Datos del activo de información				Dimensión					Atributos									Ubicación	
Ítem	Nombre del activo de información	Proceso propietario del Activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
17	Documentación de HelpDesk	Líder Bases de datos	DATOS	M	M	MA	MA	A	NO	SI	SI	SI	SI	NO		X			X
18	Expedientes de los empleados	Líder Bases de datos	DATOS	MA	M	MA	MA	A	NO	SI	SI	SI	NO	NO		X			X
19	Contratos empleados.	Líder Bases de datos	DATOS	MA	M	MA	MA	A	NO	SI	SI	SI	SI	NO		X		X	
20	Canal de Internet Dedicado.	Ingeniero administración Active Directory	COMUNICACIONES	A	MA	M	MA	MA	NO	SI	SI	NO	SI	SI		X			X
21	Canal de Internet Respaldo.	Ingeniero administración Active Directory	COMUNICACIONES	A	MA	M	MA	MA	NO	SI	SI	NO	SI	SI		X			X
22	Cableado de red.	Ingeniero administración Active Directory	COMUNICACIONES	A	MA	M	A	MA	NO	SI	SI	NO	SI	SI		X		X	
23	Conexiones VPN site to site.	Ingeniero administración Active Directory	COMUNICACIONES	A	MA	MA	MA	A	NO	SI	SI	SI	SI	SI		X			X
24	Red inalámbrica corporativa.	Ingeniero administración Active Directory	COMUNICACIONES	A	MA	MA	MA	A	NO	NO	SI	SI	SI	SI		X			X
25	Red inalámbrica Invitados.	Ingeniero administración Active Directory	COMUNICACIONES	M	M	M	M	M	NO	NO	NO	NO	NO	SI	X				X

Datos del activo de información				Dimensión					Atributos									Ubicación	
Ítem	Nombre del activo de información	Proceso propietario del Activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
26	Director Área TI.	Ingeniero Líder Soporte	PERSONAL	A	MA	MA	MA	A	NO	SI	SI	SI	SI	SI			X	X	
27	Líder Base de datos, administración de red.	Ingeniero Líder Soporte	PERSONAL	A	MA	MA	MA	A	NO	SI	SI	SI	SI	SI			X	X	
28	Líder seguridad informática.	Ingeniero Líder Soporte	PERSONAL	A	MA	MA	MA	A	NO	SI	SI	SI	SI	SI			X	X	
29	Líder soporte.	Ingeniero Líder Soporte	PERSONAL	A	MA	MA	MA	A	NO	SI	SI	SI	SI	NO			X	X	
30	Ingeniero administración Active Directory, servicios de red e infraestructura.	Ingeniero Líder Soporte	PERSONAL	A	MA	MA	MA	A	NO	SI	SI	SI	SI	SI			X	X	
31	Ingeniero administración bases de datos.	Ingeniero Líder Soporte	PERSONAL	A	MA	MA	MA	A	NO	SI	SI	SI	SI	SI			X	X	
32	Solución Ofimática.	Ingeniero Líder Bases de datos	SOFTWARE	M	A	A	A	MA	NO	NO	SI	NO	SI	SI		X			X
33	Aplicación AGM SALUD CTA Nomina.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	A	NO	SI	SI	SI	SI	SI			X		X
34	Aplicación AGM SALUD CTA Financiera.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	A	NO	SI	SI	SI	SI	SI			X		X

Datos del activo de información				Dimensión					Atributos								Ubicación	
Ítem	Nombre del activo de información	Proceso propietario del Activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
35	Aplicación AGM SALUD CTA Gestión Talento Humano.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	A	NO	SI	SI	SI	SI	SI			X		X
36	Aplicación AGM SALUD CTA Gestión Documental.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	A	NO	SI	SI	SI	SI	SI			X		X
37	Bases de Datos.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
38	Aplicaciones Móviles.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	A	NO	NO	SI	SI	SI	SI		X			X
39	Certificados SSL Letsencritp.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	MA	NO	SI	SI	NO	SI	SI		X			X
40	Dominio: agmsaludcta.site, agmsaludcta.com .	Ingeniero Líder Bases de datos	SOFTWARE	A	MA	MA	MA	MA	NO	SI	SI	SI	SI	SI		X			X
41	Sitio Corporativo www.agmsaludcta.com	Ingeniero Líder Bases de datos	SOFTWARE	A	MA	MA	A	MA	NO	NO	NO	SI	NO	SI		X			X
42	Agmsaludctadesk.	Ingeniero Líder Bases de datos	SOFTWARE	B	A	MA	MA	A	NO	SI	SI	SI	NO	SI		X			X
43	Servidores Virtuales.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X

Datos del activo de información				Dimensión					Atributos								**Ubicación**	
Ítem	Nombre del activo de información	Proceso propietario del Activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
44	Email office 365.	Ingeniero Líder Bases de datos	SOFTWARE	B	B	A	MA	A	NO	NO	SI	SI	SI	SI		X			X
45	OneDrive.	Ingeniero Líder Bases de datos	SOFTWARE	A	MA	MA	MA	MA	NO	NO	SI	SI	SI	SI		X			X
46	Sophos.	Ingeniero Líder Bases de datos	SOFTWARE	M	A	A	A	MA	NO	SI	SI	SI	SI	SI		X			X
47	Licencia Windows server 2019.	Ingeniero Líder Bases de datos	SOFTWARE	A	M	A	A	M	NO	SI	SI	NO	SI	SI		X			X
48	CentOs 8.	Ingeniero Líder Bases de datos	SOFTWARE	A	M	A	A	M	NO	SI	SI	NO	SI	SI		X			X
49	Suricata.	Ingeniero Líder Bases de datos	SOFTWARE	A	A	A	MA	A	NO	SI	SI	SI	SI	SI		X			X

Nota. Valoración de activos de información registrados.

Cuadro Amenazas Metodológicas Cooperativa

El próximo paso implica identificar las amenazas que podrían impactar en cada activo. Las amenazas se definen como "eventos que suceden". De todas las posibilidades, lo relevante es aquello que puede afectar a nuestros activos y provocarles algún perjuicio.

En el proceso de identificación de amenazas seguimos los parámetros establecidos en la metodología MAGERIT Versión 3, en la cual se sugiere clasificar las amenazas según los siguientes aspectos:

- origen natural,
- del entorno,
- defectos de las aplicaciones;
- causadas por las personas de forma accidental,
- causadas por las personas de forma deliberada.

En la Tabla 18 se realiza mención de las amenazas que pueden llegar a afectar los activos de información presentes en la cooperativa:

Tabla 18

Amenazas que Afectan Activos de Información en Cooperativa AGM SALUD CTA

Tipo amenaza	Amenaza
[N] Desastres naturales	[N1] Fuego
[N] Desastres naturales	[N2] Daños por agua
[N] Desastres naturales	[N*] Desastres naturales
[I] De origen industrial	[I1] Fuego
[I] De origen industrial	[I2] Daños por agua
[I] De origen industrial	[I*] Desastres industriales
[I] De origen industrial	[I3] Contaminación mecánica
[I] De origen industrial	[I4] Contaminación electromagnética
[I] De origen industrial	[I5] Avería de origen físico o lógico

Tipo amenaza	Amenaza
[I] De origen industrial	[I6] Corte del suministro eléctrico
[I] De origen industrial	[I7] Condiciones inadecuadas de temperatura o humedad
[I] De origen industrial	[I8] Fallo de servicios de comunicaciones
[I] De origen industrial	[I9] Interrupción de otros servicios y suministros esenciales
[I] De origen industrial	[I10] Degradación de los soportes de almacenamiento de la información
[I] De origen industrial	[I11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E1] Errores de los usuarios
[E] Errores y fallos no intencionados	[E2] Errores del administrador
[E] Errores y fallos no intencionados	[E3] Errores de monitorización (log)
[E] Errores y fallos no intencionados	[E4] Errores de configuración
[E] Errores y fallos no intencionados	[E7] Deficiencias en la organización
[E] Errores y fallos no intencionados	[E8] Difusión de software dañino
[E] Errores y fallos no intencionados	[E9] Errores de [re-]encaminamiento
[E] Errores y fallos no intencionados	[E10] Errores de secuencia
[E] Errores y fallos no intencionados	[E14] Escapes de información
[E] Errores y fallos no intencionados	[E15] Alteración accidental de la información
[E] Errores y fallos no intencionados	[E18] Destrucción de información
[E] Errores y fallos no intencionados	[E19] Fugas de información
[E] Errores y fallos no intencionados	[E20] Vulnerabilidades de los programas (software)
[E] Errores y fallos no intencionados	[E21] Errores de mantenimiento / actualización de programas (software)
[E] Errores y fallos no intencionados	[E23] Errores de mantenimiento / actualización de equipos (hardware)
[E] Errores y fallos no intencionados	[E24] Caída del sistema por agotamiento de recursos
[E] Errores y fallos no intencionados	[E25] Pérdida de equipos
[E] Errores y fallos no intencionados	[E28] Indisponibilidad del personal
[A] Ataques intencionados	[A3] Manipulación de los registros de actividad (log)
[A] Ataques intencionados	[A4] Manipulación de la configuración
[A] Ataques intencionados	[A5] Suplantación de la identidad del usuario
[A] Ataques intencionados	[A6] Abuso de privilegios de acceso

Tipo amenaza	Amenaza
[A] Ataques intencionados	[A7] Uso no previsto
[A] Ataques intencionados	[A8] Difusión de software dañino
[A] Ataques intencionados	[A9] [Re-]encaminamiento de mensajes
[A] Ataques intencionados	[A10] Alteración de secuencia
[A] Ataques intencionados	[A11] Acceso no autorizado
[A] Ataques intencionados	[A12] Análisis de tráfico
[A] Ataques intencionados	[A13] Repudio
[A] Ataques intencionados	[A14] Interceptación de información (escucha)
[A] Ataques intencionados	[A15] Modificación deliberada de la información
[A] Ataques intencionados	[A18] Destrucción de información
[A] Ataques intencionados	[A19] Divulgación de información
[A] Ataques intencionados	[A22] Manipulación de programas
[A] Ataques intencionados	[A23] Manipulación de los equipos
[A] Ataques intencionados	[A24] Denegación de servicio
[A] Ataques intencionados	[A25] Robo
[A] Ataques intencionados	[A26] Ataque destructivo
[A] Ataques intencionados	[A27] Ocupación enemiga
[A] Ataques intencionados	[A28] Indisponibilidad del personal
[A] Ataques intencionados	[A29] Extorsión
[A] Ataques intencionados	[A30] Ingeniería social (picaresca)

Nota. Amenazas que pueden afectar los activos de información.

Valoración de Amenazas Inventario Activos de Información Caso de Estudio

Conforme avanzamos con el tránsito del SGSI, prosigue la siguiente fase de la valoración de las amenazas, después de la fase de la determinación de las posibles situaciones y/o acciones que se pueden calificar como posibles riesgos que pueden afectar negativamente a la seguridad y funcionamiento de los activos de información de la cooperativa, se continua con la valoración de estos aprovechando como parámetro las recomendaciones realizadas desde la metodología MAGERIT visibles en la Tabla 19.

Tabla 19

Evaluación del Impacto

Triada	Nomenclatura	Cualitativa	Cuantitativo	Descripción
Confidencialidad/ Integridad/ Disponibilidad	MA	Muy alta	5	El daño para la compañía representa el mayor impacto.
	A	Alta	4	El daño para la compañía representa un impacto importante.
	M	Media	3	El daño para la compañía representa un impacto moderado.
	B	Baja	2	El daño para la compañía representa un impacto menor.
	MB	Muy baja	1	El daño para la compañía representa un impacto leve.

Nota. Evaluación del impacto del riesgo sobre la confidencialidad, integridad y disponibilidad. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012) https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Después de obtener la matriz para evaluar el impacto del riesgo hay que enfocarse en realizar la matriz para modelar cualitativamente la probabilidad del riesgo.

En el cálculo del impacto de un riesgo sobre un activo determinado hay que tener como referencia el valor de este activo en sus dimensiones de seguridad para la organización, ya que es determinante para establecer este valor, esto indica que, si el activo no representa un valor alto, su impacto también será menor.

Tabla 20

Evaluación de la Probabilidad

Nomenclatura	Cualitativa	Cuantitativo	Descripción
MA	Muy alta	5	Ocurre una o muchas veces al año.
A	Alta	4	Ocurre una vez cada 2 años.
M	Media	3	Ocurre una vez cada 3 años.
B	Baja	2	Ocurre una vez cada 4 años.
MB	Muy baja	1	Ocurre una vez cada 5 años.

Nota. Evaluación de la probabilidad de que se materialice el riesgo. Adaptado de. Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método, Ministerio de Hacienda y Administraciones Públicas. (2012) https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Con la evaluación estipulada por la Tabla 19 y Tabla 20 es factible continuar con la valoración del riesgo con la cual se quiere cuantificar y priorizar en términos de severidad y probabilidad de ocurrencia los riesgos identificados. Ambos son pasos críticos en el proceso de gestión de riesgos.

Donde por ejemplo si se tiene un riesgo calificado de alto impacto es decir una valoración de impacto en 4, y según el modelado de probabilidad se encuentra dentro de la escala de posible es decir con una valoración de probabilidad de 3, se debe realizar el producto de impacto x probabilidad = valoración del riesgo, es así para el ejemplo planteado se obtendrá una valoración de riesgo en 12.

Figura 6

Valoración del Riesgo Potencial

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoración del riesgo	MA	Crítico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nota. Valoración de los riesgos según su categoría.

Con el modelado para valoración de riesgos se puede realizar el análisis de riesgos de los activos de información, del caso de estudio Tabla 21.

Tabla 21

Valoración de Riesgos de Activos de la Información AGM SALUD CTA

No	Nombre del activo	Evaluación del impacto	Evaluación de la probabilidad	Valoración del riesgo	Amenazas
1	Servidor Físico - HP Proliant ML110 Gen 10.	5	4	20	[E23] Errores de mantenimiento / actualización de equipos (hardware).
2	Servidor Físico - HP Proliant ML 350 Gen 10.	5	3	15	[A11] Acceso no autorizado.
3	Computadores Corporativos (20)	3	4	12	[E2] Errores del administrador.
4	Computador portátil (4)	3	2	6	[A25] Robo
5	Switches (3)	5	2	10	[E23] Errores de

No	Nombre del activo	Evaluación del impacto	Evaluación de la probabilidad	Valoración del riesgo	Amenazas
					mantenimiento / actualización de equipos (hardware).
6	Router Wifi	3	3	9	[A26] Ataque destructivo.
7	Access Point (3)	2	3	6	[A6] Abuso de privilegios de acceso.
8	Balanceador de Carga	4	4	16	[E23] Errores de mantenimiento / actualización de equipos (hardware).
9	Firewall Fortinet 50E	5	4	20	[A11] Acceso no autorizado.
10	Documentación de procesos de desarrollo.	4	3	12	[A11] Acceso no autorizado.
11	Código Fuente AGM SALUD CTA Nomina.	5	2	10	[E2] Errores del administrador.
12	Código Fuente AGM SALUD CTA Financiera.	5	3	15	[A19] Divulgación de información.
13	Código Fuente AGM SALUD CTA Gestión talento Humano.	5	2	10	[A6] Abuso de privilegios de acceso.
14	Aplicación AGM SALUD CTA Gestión documental.	4	3	12	[A19] Divulgación de información.
15	Contratos clientes	5	3	15	[A15] Modificación deliberada de la información.
16	Políticas de tratamiento de datos personales.	3	2	6	[A18] Destrucción de información.

No	Nombre del activo	Evaluación del impacto	Evaluación de la probabilidad	Valoración del riesgo	Amenazas
17	Documentación de HelpDesk	4	2	8	[E18] Destrucción de información.
18	Expedientes de los empleados	4	3	12	[A19] Divulgación de información.
19	Contratos empleados	4	2	8	[A15] Modificación deliberada de la información.
20	Canal de Internet Dedicado	4	2	8	[I8] Fallo de servicios de comunicaciones.
21	Canal de Internet Respaldo	3	2	6	[I8] Fallo de servicios de comunicaciones.
22	Cableado de red	4	1	4	[A12] Análisis de tráfico.
23	Conexiones VPN site to site	4	2	8	[I8] Fallo de servicios de comunicaciones.
24	Red inalámbrica corporativa	4	2	8	[A5] Suplantación de la identidad del usuario.
25	Red inalámbrica Invitados	3	2	6	[A5] Suplantación de la identidad del usuario.
26	Director Área TI	4	2	8	[A28] Indisponibilidad del personal.
27	Líder Base de datos, administración de red.	5	3	15	[E19] Fugas de información.
28	Líder seguridad informática	4	2	8	[E28] Indisponibilidad del personal.
29	Líder soporte.	4	2	8	[E7] Deficiencias en

No	Nombre del activo	Evaluación del impacto	Evaluación de la probabilidad	Valoración del riesgo	Amenazas
					la organización.
30	Ingeniero administración active directory, servicios de red e infraestructura.	5	2	10	[A29] Extorsión.
31	Ingeniero administración bases de datos.	4	2	8	[E28] Indisponibilidad del personal.
32	Solución Ofimática	3	3	9	[E20] Vulnerabilidades de los programas (software).
33	Aplicación AGM SALUD CTA Nomina.	5	2	10	[A11] Acceso no autorizado.
34	Aplicación AGM SALUD CTA Financiera	5	3	15	[A6] Abuso de privilegios de acceso.
35	Aplicación AGM SALUD CTA Gestión Talento Humano	5	3	15	[A15] Modificación deliberada de la información.
36	Aplicación AGM SALUD CTA Gestión Documental	4	3	12	[A22] Manipulación de programas.
37	Bases de Datos	5	3	15	[A18] Destrucción de información.
38	Aplicaciones Móviles	4	2	8	[A22] Manipulación de programas.
39	Certificados SSL Letsencritp	4	2	8	[E2] Errores del administrador.
40	Dominio: agmsaludcta.site, agmsaludcta.com	5	2	10	[E2] Errores del administrador.

No	Nombre del activo	Evaluación del impacto	Evaluación de la probabilidad	Valoración del riesgo	Amenazas
41	Sitio Corporativo: www.agmsaludcta.com	5	3	15	[E8] Difusión de software dañino.
42	agmsaludctadesk	4	2	8	[E9] Errores de [re-]encaminamiento.
43	Servidores Virtuales	5	4	20	[A11] Acceso no autorizado.
44	Email office 365	4	3	12	[E8] Difusión de software dañino.
45	Aplicación OneDrive	4	4	16	[A6] Abuso de privilegios de acceso.
46	Sophos	4	3	12	[E21] Errores de mantenimiento / actualización de programas (software).
47	Licencia Windows server 2019	5	2	10	[I5] Avería de origen físico o lógico.
48	CentOs 8	5	2	10	[A6] Abuso de privilegios de acceso.
49	Suricata	4	2	8	[A18] Destrucción de información.

Nota. Valoración del riesgo para cada activo de información.

En la Tabla 21 se observa la valoración de cada riesgo según la amenaza existente, es así como en la Tabla 22 se listan las vulnerabilidades que pueden ser explotadas por las amenazas mencionadas.

Tabla 22

Listado de Vulnerabilidades que Pueden ser Explotadas por las Amenazas

No.	Nombre de activo	Amenazas metodología Magerit	Vulnerabilidades
1	Servidor Físico - HP Proliant ML110 Gen 10.	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Ausencia de esquemas de remplazo periódico.
2	Servidor Físico - HP Proliant ML 350 Gen 10.	[A11] Acceso no autorizado	Data Center no cuenta con la seguridad suficiente.
3	Computadores Corporativos (20)	[E2] Errores del administrador	Contraseñas débiles, reuso de credenciales, cuentas con contraseñas por defecto, almacenamiento de credenciales en texto plano.
4	Computador portátil (4)	[A25] Robo	Almacenamiento sin protección.
5	Switches (3)	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Configuración insuficiente.
6	Router Wifi	[A26] Ataque destructivo.	Ausencia de esquemas de remplazo periódico.
7	Access Point (3)	[A6] Abuso de privilegios de acceso.	Configuración insuficiente.
8	Balanceador de Carga	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Ausencia de esquemas periódicos para el mantenimiento.
9	Firewall Fortinet 50E.	[A11] Acceso no autorizado.	Denegación de servicio.
10	Documentación de procesos de desarrollo.	[A11] Acceso no autorizado.	Perdida de la información.
11	Código Fuente AGM SALUD CTA Nomina.	[E2] Errores del administrador.	Configuración incorrecta o incompleta.
12	Código Fuente AGM SALUD CTA Financiera.	[A19] Divulgación de información.	Gestión deficiente de accesos y privilegios.
13	Código Fuente AGM SALUD CTA Gestión talento Humano.	[A6] Abuso de privilegios de acceso.	Credenciales y secretos embebidos en el código.
14	Aplicación AGM SALUD CTA Gestión documental.	[A19] Divulgación de información.	Gestión deficiente de accesos y privilegios.
15	Contratos clientes.	[A15] Modificación deliberada de la información.	Control de acceso y autorización deficientes en repositorios y sistemas de gestión documental.

No.	Nombre de activo	Amenazas metodología Magerit	Vulnerabilidades
16	Políticas de tratamiento de datos personales.	[A18] Destrucción de información.	Control de acceso y autorización deficientes en repositorios y sistemas de gestión documental
17	Documentación de HelpDesk	[E18] Destrucción de información.	Almacenamiento y transmisión no cifrados o débiles.
18	Expedientes de los empleados	[A19] Divulgación de información.	Difusión excesiva o distribución no controlada
19	Contratos empleados	[A15] Modificación deliberada de la información.	Almacenamiento y transmisión no cifrados o débiles.
20	Canal de Internet Dedicado.	[I8] Fallo de servicios de comunicaciones	Dependencia exclusiva de un único proveedor de telecomunicaciones.
21	Canal de Internet Respaldo.	[I8] Fallo de servicios de comunicaciones	Ausencia de mecanismos de failover y balanceo.
22	Cableado de red	[A12] Análisis de tráfico	Puertos de red activos y sin control físico.
23	Conexiones VPN site to site.	[I8] Fallo de servicios de comunicaciones	Ausencia de redundancia de túneles / un único túnel activo.
24	Red inalámbrica corporativa	[A5] Suplantación de la identidad del usuario	Uso de protocolos de autenticación débiles o obsoletos.
25	Red inalámbrica Invitados	[A5] Suplantación de la identidad del usuario	Falta de uso de certificados y validación mutua.
26	Director Área TI	[A28] Indisponibilidad del personal	Falta de sucesión formal y planes de reemplazo.
27	Líder Base de datos, administración de red.	[E19] Fugas de información	Accesos privilegiados sin control ni segregación.
28	Líder seguridad informática.	[E28] Indisponibilidad del personal	Conocimientos y documentación concentrados en la persona.
29	Líder soporte.	[E7] Deficiencias en la organización	Roles y responsabilidades mal definidos.
30	Ingeniero administración active directory, servicios de red e infraestructura.	[A29] Extorsión	Ausencia de controles de doble aprobación.
31	Ingeniero administración bases de datos.	[E28] Indisponibilidad del personal	Conocimientos y documentación concentrados en la persona.
32	Solución Ofimática	[E20] Vulnerabilidades de los programas (software)	Macros/VBA habilitadas.
33	Aplicación AGM SALUD CTA Nomina.	[A11] Acceso no autorizado	Control de acceso roto / privilegios excesivos.
34	Aplicación AGM SALUD CTA Financiera	[A6] Abuso de privilegios de acceso	Ausencia de segregación de funciones.

No.	Nombre de activo	Amenazas metodología Magerit	Vulnerabilidades
35	Aplicación AGM SALUD CTA Gestión Talento Humano	[A15] Modificación deliberada de la información	Alteración de la información.
36	Aplicación AGM SALUD CTA Gestión Documental	[A22] Manipulación de programas	Alteración del sistema consiguiendo acceso no autorizado.
37	Bases de Datos	[A18] Destrucción de información	Ausencia de respaldos seguros y verificados.
38	Aplicaciones Móviles	[A22] Manipulación de programas	Secretos embebidos en la app.
39	Certificados SSL Letsencritp	[E2] Errores del administrador	Renovación manual o automatización mal implementada.
40	Dominio: agmsaludcta.site, agmsaludcta.com	[E2] Errores del administrador	Renovación de certificados manual o scripts frágiles que fallan.
41	Sitio Corporativo: www.agmsaludcta.com	[E8] Difusión de software dañino	Subida de archivos sin validación.
42	agmsaludctadesk	[E9] Errores de [re-]encaminamiento	Configuraciones incorrectas de enrutamiento interno del sistema de mesa de ayuda.
43	Servidores Virtuales	[A11] Acceso no autorizado	Credenciales débiles, reutilizadas o por defecto.
44	Email office 365	[E8] Difusión de software dañino	Configuración de anti-malware/antiphishing deshabilitada o insuficiente.
45	OneDrive	[A6] Abuso de privilegios de acceso	Asignación inadecuada de permisos en carpetas y archivos.
46	Sophos	[E21] Errores de mantenimiento / actualización de programas (software)	Definiciones / firmas desactualizadas.
47	Licencia Windows server 2019	[I5] Avería de origen físico o lógico	Ausencia de redundancia o licencias de respaldo.
48	CentOs 8	[A6] Abuso de privilegios de acceso	Acceso SSH con root permitido y sin autenticación fuerte.
49	Suricata	[A18] Destrucción de información	Permisos de archivos y directorios inadecuados.

Nota. Listado de vulnerabilidades que pueden ser explotadas por las amenazas existentes.

Al observar los resultados que nos arroja la Tabla 22 y conforme a la escala de valoración adoptada, se define que todo activo con valoración de riesgo potencial en las categorías Importante (16-20) o Crítico (21-25) requiere de un Plan de Tratamiento de Riesgos inmediato,

en este caso serían los riesgos relacionados en la Tabla 23. Esta decisión se toma porque esos niveles superan el umbral de tolerancia institucional, y suponen una amenaza directa a la continuidad del negocio y a la integridad de la memoria institucional. Si se dejan de realizar controles en estos rangos, la entidad estaría expuesta a consecuencias financieras y legales que son mucho mayores que el costo de implementar las salvaguardas propuestas.

Tabla 23

Listado de Riesgos a Tratar por su Nivel de Categorización

No	Nombre del activo	Valoración del riesgo	Categoría del Riesgo	Amenazas
1	Servidor Físico - HP Proliant ML110 Gen 10.	20	IMPORTANTE	[E23] Errores de mantenimiento / actualización de equipos (hardware).
8	Balanceador de Carga	16	IMPORTANTE	[E23] Errores de mantenimiento / actualización de equipos (hardware).
9	Firewall Fortinet 50E	20	IMPORTANTE	[A11] Acceso no autorizado.
43	Servidores Virtuales	20	IMPORTANTE	[A11] Acceso no autorizado.
45	Aplicación OneDrive	16	IMPORTANTE	[A6] Abuso de privilegios de acceso.

Nota. Listado de riegos categorizados como importantes para su tratamiento.

Posterior a este paso de análisis de los riesgos se procede a postular los controles y salvaguardas como medidas normativas y técnicas con el propósito de reducir los riesgos potenciales, para plantear estas salvaguardas se debe tener como referencia el control que se desea aplicar según la normativa ISO 27001, como ejemplo en la Tabla 24 se registran algunos controles de este estándar que facilitarían tratar los riesgos con criticidad importante.

Tabla 24

Controles Aplicables para Reducción de Riesgos Potenciales

Cod	Activo de Información	Amenaza	Tipo de control	Id Control	Nombre de Control
D01	Servidor Físico - HP Proliant ML110 Gen 10	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Controles Físicos	7.14	Mantenimiento de Equipo
D02	Servidor Físico - HP Proliant ML110 Gen 10	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Controles Tecnológicos	8.32	Gestión del cambio
D03	Servidor Físico - HP Proliant ML110 Gen 10	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Controles Tecnológicos	8.13	Copia de seguridad de la información.
D04	Balanceador de Carga	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Controles Físicos	7.14	Mantenimiento de Equipo
D05	Balanceador de Carga	[E23] Errores de mantenimiento / actualización de equipos (hardware).	Controles Tecnológicos	8.14	Redundancia de las instalaciones de procesamiento de información
D06	Balanceador de Carga	[E23] Errores de mantenimiento /	Controles Tecnológicos	8.9	Gestión de la configuración

Cod	Activo de Información	Amenaza	Tipo de control	Id Control	Nombre de Control
		actualización de equipos (hardware).			
D07	Firewall Fortinet 50E	[A11] Acceso no autorizado.	Controles Tecnológicos	8.5	Autenticación segura
D08	Firewall Fortinet 50E	[A11] Acceso no autorizado.	Controles organizacionales	5.16	Gestión de autenticación
D09	Firewall Fortinet 50E	[A11] Acceso no autorizado.	Controles Tecnológicos	8.16	Actividades de seguimiento
D10	Servidores Virtuales	[A11] Acceso no autorizado.	Controles Tecnológicos	8.5	Autenticación segura
D11	Servidores Virtuales	[A11] Acceso no autorizado.	Controles Tecnológicos	8.22	Segregación en redes
D12	Servidores Virtuales	[A11] Acceso no autorizado.	Controles Tecnológicos	8.9	Gestión de la configuración
D13	Aplicación OneDrive	[A6] Abuso de privilegios de acceso.	Controles Tecnológicos	8.2	Derechos de acceso privilegiado
D14	Aplicación OneDrive	[A6] Abuso de privilegios de acceso.	Controles Tecnológicos	8.16	Actividades de seguimiento
D15	Aplicación OneDrive	[A6] Abuso de privilegios de acceso.	Controles organizacionales	5.15	Control de acceso de Identidad

Nota. Controles tomados de la norma ISO 27001, aplicables para el tratamiento de los riesgos relacionados.

Una vez seleccionados los controles indicados por la norma ISO 27001 con los cuales se busca tratar los riesgos de mayor criticidad para reducir su impacto potencial y obtener el riesgo residual, es necesario definir las salvaguardas y sus respectivas medidas técnicas**,**
es preciso indicar que lo ideal no es tener un gran listado de controles, sino tener identificados los que son viables para aplicar ya que es necesario verificar el presupuesto destinado y la capacidad financiera de la cooperativa para llevar a cabo la implementación de estos controles.

Esto permitirá una implementación correcta para mitigar el riesgo y garantizar la seguridad de los activos más vulnerables. Además, como se observa en la Tabla 25 a estas salvaguardas se les debe asignar un valor de efectividad en relación con frecuencia e impacto ante el riesgo, para así calcular la reducción y determinar el valor del riesgo residual de forma precisa.

Tabla 25

Salvaguardas Seleccionadas para Aplicabilidad Según Controles

No	Activo afectado	Amenazas	Id de Control	Salvaguardas	Acción técnica	Reducción Frecuencia	Reducción de impacto
1	Servidor Físico - HP Proliant ML110 Gen 10.	[E23] Errores de mantenimiento / actualización de equipos (hardware)	7.14	Mantenimiento integral del equipo	Cronograma de limpieza y revisión	0.70	0.10
			8.32	Procedimiento de Reversión	Documentación y prueba del plan de retorno	0.70	0.10
			8.13	Sistema de respaldo y Recuperación	Ejecución de Backup con verificación de integridad	0.10	0.90
2	Balanceador de carga	[E23] Errores de mantenimiento / actualización de equipos (hardware)	7.14	Mantenimiento integral del equipo	Cronograma de limpieza y revisión	0.60	0.10
			8.09	Gestión de la configuración	Exportar el archivo de configuración	0.10	0.50
			8.14	Redundancia de las instalaciones de procesamiento de información	Configurar un clúster Activo-Pasivo o Activo-Activo.	0.30	0.95
3	Firewall Fortinet 50E	[A11] Acceso no autorizado.	8.5	Autenticación Robusta (MFA)	Habilitar FortiToken para todas las cuentas administrativas.	0.95	0.05
			5.16	Gestión de Autenticación	Asegurar Políticas de contraseñas y baja de usuarios	0.60	0.10

No	Activo afectado	Amenazas	Id de Control	Salvaguardas	Acción técnica	Reducción Frecuencia	Reducción de impacto
			8.16	Monitoreo Proactivo de eventos	Configurar el envío de logs de eventos de sistema a un FortiAnalyzer	0.05	0.40
4	Servidores Virtuales	[A11] Acceso no autorizado.	8.5	Autenticación Robusta (MFA)	Vincular herramientas como Microsoft Entra ID (Azure AD), Duo Security o Keycloak.	0.95	0.05
			8.22	Arquitectura de Red Segura	Aislar el tráfico de gestión de los servidores en una VLAN dedicada	0.90	0.6
			8.9	Aplicación de Perfiles de Seguridad (Hardening)	Crear una Plantilla de Servidor Seguro	0.6	0.3
5	Aplicación OneDrive	[A6] Abuso de privilegios de acceso.	8.2	Privilegio de acceso únicamente en el momento necesario	Implementar *Privileged Identity Management (PIM)*	0.85	0
			5.15	Recertificación periódica de accesos	Proceso organizacional trimestral donde los líderes de área validen y firmen que sus colaboradores aún requieren acceso a carpetas sensibles	0.85	0
			8.16	Monitoreo de comportamiento anómalo	Configurar alertas de descarga masiva de archivos y Cambios inusuales de permisos	0	0.60

Nota. Salvaguardas por implementar con sus respetivos valores de factor de frecuencia y factor de impacto.

Al establecer el valor de frecuencia de efectividad y frecuencia de impacto para cada salvaguarda es factible realizar el cálculo de valor de efectividad total para cada una de ellas, en la Tabla 26 se observa el resultado obtenido al aplicar la respectiva fórmula para obtener el valor de eficacia total.

Tabla 26

Cálculo de Eficacia Total de Salvaguardas a Aplicar

No.	Activo	Salvaguardas	Calculo eficacia Total
1	Servidor Físico - HP Proliant ML110 Gen 10	-Mantenimiento integral del equipo -Procedimiento de Reversión -Sistema de respaldo y Recuperación	$f_f = (1 - 0.70)\ x\ (1 - 0.70)\ x\ (1 - 0.10)$ $f_f = 0.30\ x\ 0.30\ x\ 0.90 = 0.081$ $f_i = (1 - 0.10)\ x\ (1 - 0.10)\ x\ (1 - 0.90)$ $f_i = 0.90\ x\ 0.90\ x\ 0.10 = 0.081$ $E = 1 - [0.081\ x\ 0.081]$ $E = 0.9934$
2	Balanceador de carga	-Mantenimiento integral del equipo -Gestión de la configuración -Redundancia de las instalaciones de procesamiento de información	$f_f = (1 - 0.60)\ x\ (1 - 0.10)\ x\ (1 - 0.30)$ $f_f = 0.40\ x\ 0.90\ x\ 0.70 = 0.252$ $f_i = (1 - 0.10)\ x\ (1 - 0.50)\ x\ (1 - 0.95)$ $f_i = 0.90\ x\ 0.50x\ 0.05 = 0.0225$ $E = 1 - [0.252\ x\ 0.0225]$ $E = 0.9943$
3	Firewall Fortinet 50E	-Autenticación Robusta (MFA) -Gestión de Autenticación - Monitoreo Proactivo de eventos	$f_f = (1 - 0.95)\ x\ (1 - 0.60)\ x\ (1 - 0.05)$ $f_f = 0.05\ x\ 0.40\ x\ 0.95 = 0.019$ $f_i = (1 - 0.05)\ x\ (1 - 0.10)\ x\ (1 - 0.40)$ $f_i = 0.95\ x\ 0.90x\ 0.60 = 0.513$ $E = 1 - [0.019\ x\ 0.513]$ $E = 0.9903$
4	Servidores Virtuales	-Autenticación Robusta (MFA) - Arquitectura de Red Segura - Aplicación de Perfiles de Seguridad (Hardening)	$f_f = (1 - 0.95)\ x\ (1 - 0.90)\ x\ (1 - 0.60)$ $f_f = 0.05\ x\ 0.10x\ 0.40 = 0.002$ $f_i = (1 - 0.05)\ x\ (1 - 0.60)\ x\ (1 - 0.30)$ $f_i = 0.95\ x\ 0.40x\ 0.70 = 0.266$ $E = 1 - [0.002\ x\ 0.266]$ $E = 0.9995$
5	Aplicación OneDrive	- Privilegio de acceso únicamente en el momento necesario - Recertificación periódica de accesos - Monitoreo de comportamiento anómalo	$f_f = (1 - 0.85)\ x\ (1 - 0.85)$ $f_f = 0.15\ x\ 0.15\ = 0.0225$ $f_i = \ (1 - 0.60)$ $f_i = 0.95\ x\ 0.40x\ 0.70 = 0.266$ $E = 1 - [0.0225\ x\ 0.4]$ $E = 0.991$

Nota. Salvaguardas y cálculo de efectividad total de las mismas para reducción del riesgo potencial.

Con el valor calculado de la efectividad total para cada salvaguarda es viable proceder con la elaboración de la matriz de riesgos residuales resultantes al implementar las salvaguardas seleccionadas. En la Tabla 27 observamos la matriz obtenida después de implementar las medidas de protección mencionadas y el resultado obtenido al aplicar la fórmula de riesgo residual.

$$R_{Residual} = R_{Potencial}\ x\ (1 - E)$$

Tabla 27

Matriz de Riesgo Residual para Activos en Categorización de Riesgo Importante

No.	Activo afectado	Valoración del riesgo Potencial	Categoría del riesgo	Formula calculo riesgo Residual	Valoración riesgo Residual	Nueva Categorización del riesgo
1	Servidor Físico - HP Proliant ML110 Gen 10.	20	Importante	$R_{Residual} = 20\ x\ (1 - 0.9934)$ $R_{Residual} = 0.132$	0.132	Despreciable
2	Balanceador de Carga	16	Importante	$R_{Residual} = 16\ x\ (1 - 0.9934)$ $R_{Residual} = 0.0912$	0.0912	Despreciable
3	Firewall Fortinet 50E	20	Importante	$R_{Residual} = 20\ x\ (1 - 0.9903)$ $R_{Residual} = 0.194$	0.194	Despreciable
4	Servidores Virtuales	20	Importante	$R_{Residual} = 20\ x\ (1 - 0.9995)$ $R_{Residual} = 0.01$	0.01	Despreciable
5	OneDrive	16	Importante	$R_{Residual} = 16\ x\ (1 - 0.991)$ $R_{Residual} = 0.144$	0.144	Despreciable

Nota. Valorización de riesgos residuales después de implementar Salvaguardas y su respectiva efectividad total.

Al analizar los resultados obtenidos en la Tabla 27 se observa que la disminución en la valoración del riesgo es realmente importante, debido a esto la nueva categorización de estos

riesgos es “ Riesgos Despreciables” esto se debe en gran medida a que el valor de efectividad calculado para las salvaguardas implementadas es un valor lo suficientemente alto para reducir de una forma considerable el valor del riesgo potencial, esto se consigue gracias a que se seleccionaron varios controles de la Norma ISO 27001, para tratar los riesgos seleccionados lo que permite combinar varias capas de seguridad que posee el activo en riesgo. La acción recomendada después de este proceso es aceptar el riesgo y mantener un monitoreo periódico para asegurar que la salvaguarda no pierda efectividad con el tiempo, el resultado final no es solamente una cifra técnica, sino el indicador clave para que los órganos de gobierno de la entidad, como el Consejo de Administración, puedan decidir si el nivel de exposición remanente es aceptable para la sostenibilidad del capital social y la salvaguarda de la confianza de los asociados.

Modelo de Políticas de Seguridad de la Información Estructurado a las Particularidades de las Cooperativas de Trabajo Asociado en Colombia

Características de las Cooperativas de Trabajo Asociado

Es crucial comprender las características únicas de las cooperativas de trabajo asociado al compararlas con las empresas del sector privado. Estas particularidades pueden influir en la forma en que operan, desde su estructura de toma de decisiones hasta sus valores fundamentales. Al entender estas distinciones, se puede comprender como plantear políticas de seguridad de la información que estén acorde a la naturaleza de la economía solidaria.

Propiedad Cooperativa

En el núcleo de una cooperativa de trabajo asociado reside el principio característico de la propiedad de los socios trabajadores. Esto implica que la cooperativa es gestionada y es poseída por los empleados que laboran en ella, uniendo los roles usualmente separados de dueño y trabajador. Así mismo, Presidencia de la República de Colombia (2006), afirma acerca de las cooperativas:

> Son organizaciones sin ánimo de lucro pertenecientes al sector solidario de la economía, que asocian personas naturales que simultáneamente son gestoras, contribuyen económicamente a la cooperativa y son aportantes directos de su capacidad de trabajo para el desarrollo de actividades económicas. (párr.2)

Esta combinación de roles crea un entorno laboral en el que los beneficios y las responsabilidades se comparten, promoviendo el compromiso, la responsabilidad y la igualdad entre todos sus miembros.

La propiedad cooperativa motiva a los socios trabajadores a participar activamente en el éxito de la cooperativa, conscientes de que el resultado de su esfuerzo tiene un efecto directo en el bienestar colectivo y en sus propios beneficios, ya que los dueños y trabajadores son las

mismas personas, eliminando la división entre empleado y patrón existente en la empresa privada tradicional (Arango Jaramillo, 2024) . Esto da lugar a una cultura organizacional singular, caracterizada por la solidaridad, la cooperación y una visión común orientada al crecimiento y la sostenibilidad a largo plazo de la cooperativa.

Además, la estructura de propiedad de los socios trabajadores garantiza que las decisiones reflejen los intereses y necesidades de quienes están directamente involucrados en el funcionamiento diario de la cooperativa.(Horta-Solano, 2018) Esto da lugar a una gestión más democrática y transparente, donde cada socio tiene voz y voto en las decisiones clave que afectan el futuro de la organización.

Este sistema de propiedad cooperativa no solo refuerza el sentido de pertenencia y compromiso entre los socios trabajadores, sino que también promueve una distribución más equitativa de los beneficios económicos generados. Al ser propietarios, los trabajadores se benefician directamente del éxito de la cooperativa, lo que puede resultar en mejores salarios, condiciones laborales y oportunidades de desarrollo profesional.

Capital Variable

El principio de capital variable distingue a las cooperativas de trabajo asociado de otras formas organizativas empresariales. En estas cooperativas, el capital total no permanece estático, sino que varía en función del número de socios que integran la organización. Esto implica que el capital puede aumentar con la incorporación de nuevos socios o disminuir si algunos deciden retirarse.

Además, el capital variable proporciona una base sólida para la adaptación y la innovación dentro de la cooperativa. Al tener la capacidad de aumentar o disminuir el capital según sea necesario, la organización puede financiar nuevas iniciativas, invertir en tecnología y recursos, y responder ágilmente a las oportunidades emergentes en el mercado. Es importante

aclarar que este capital a diferencia de los modelos tradicionales no está orientado a generar una rentabilidad financiera individual o “parasitaria” para el aportante, sino que se concibe como un instrumento subordinado al factor trabajo para el beneficio social y productivo. Bajo esta premisa, y conforme a un modelo de gobernanza democrático y autogestionario, el destino y la inversión de estos recursos no dependen de una dirección jerárquica unilateral, sino que deben contar con la aprobación previa de la Asamblea General de Asociados. Esto garantiza que cualquier inversión de capital responda al interés colectivo, asegurando que los socios, en su doble condición de propietarios y gestores, conserven el control soberano sobre los medios de producción y el futuro de la organización(Arango Jaramillo, 2024).

También refleja el compromiso de cada socio con la cooperativa, ya que generalmente se espera que cada uno contribuya con una cantidad equitativa de capital al unirse. Esta contribución inicial representa la inversión del socio en el proyecto conjunto y su confianza en el éxito compartido de la cooperativa.

El hecho de que cada socio contribuya financieramente al proyecto común desde el principio demuestra su compromiso con el éxito a largo plazo de la cooperativa. Esta inversión inicial no solo representa un respaldo económico, sino también un respaldo emocional y una demostración de confianza en la visión y la misión compartidas de la cooperativa.

Gobernanza Democrática

Una de las características más notables de las cooperativas de trabajo asociado radica en su sistema de gobernanza democrática. En este modelo, las decisiones clave se toman de manera colectiva, siguiendo el principio de "un socio, un voto". Esta regla asegura que cada miembro de la cooperativa, independientemente del tamaño de su inversión, tenga un peso igualitario en la toma de decisiones.

Afirma Arango Jaramillo (2024), el principio de cooperación, inherente al cooperativismo, es el fundamento de las empresas de economía solidaria. Estas entidades, de perfil no capitalista, se distinguen por su adhesión a una gobernación democrática, la cual se ejerce junto a principios como la autogestión y la solidaridad. Este modelo de gestión tiene como fin último mejorar las condiciones socioeconómicas de los asociados a través de la participación y la ayuda mutua.

Este enfoque democrático garantiza que la dirección de la cooperativa refleje fielmente la voluntad y los intereses de todos sus miembros. Facilita una participación de los socios en la definición de estrategias, metas y políticas, fortaleciendo así el sentido de pertenencia y compromiso con la organización. A diferencia de los modelos empresariales convencionales, donde las decisiones pueden ser influenciadas por quienes poseen una mayor participación accionaria, en las cooperativas, la igualdad en el derecho a voto fomenta un ambiente de equidad y solidaridad.

Este modelo democrático no solo contribuye a una gestión más inclusiva y representativa, sino que también fortalece la cohesión interna, ya que las decisiones se alcanzan mediante un proceso de diálogo y consenso. Ante desafíos o nuevas oportunidades, la cooperativa actúa como un frente unificado, donde cada socio se siente valorado y parte esencial del proyecto conjunto. Esta dinámica impulsa la innovación y la adaptabilidad al aprovechar la diversidad de perspectivas y habilidades de sus miembros, en beneficio mutuo y para el desarrollo sostenible de la cooperativa.

Asamblea General

La Asamblea General de socios se erige como el órgano supremo de autoridad dentro de las cooperativas de trabajo asociado, desempeñando un papel crucial en la toma de decisiones sobre la dirección y gestión de la cooperativa. Estas reuniones, celebradas regularmente,

congregan a todos los socios con el propósito de deliberar y decidir sobre asuntos críticos que afectan el curso y la administración de la cooperativa. Este foro democrático es el espacio por excelencia para la participación de los socios en la vida y futuro de la cooperativa, asegurando que todos tengan la oportunidad de expresar sus opiniones, inquietudes y sugerencias (Horta-Solano, 2018).

Durante la Asamblea General se abordan y resuelven asuntos de importancia, como la aprobación de los estados financieros anuales, la elección de los miembros del consejo de administración, la definición de estrategias a largo plazo y la toma de decisiones sobre inversiones significativas o cambios estructurales en la cooperativa. Este proceso garantiza que las decisiones fundamentales se tomen con base en un amplio consenso entre los socios, reflejando el compromiso de la cooperativa con los principios democráticos y la gestión participativa.

La participación de todos los socios en la Asamblea General fortalece el tejido social de la cooperativa, promoviendo una cultura de transparencia, responsabilidad y compromiso colectivo. Al confiar a los socios la responsabilidad de dirigir la cooperativa, se fomentan la igualdad, la solidaridad y una visión compartida, aspectos cruciales para el éxito y la sostenibilidad a largo plazo de la cooperativa. Este enfoque resalta el valor de cada socio como un elemento fundamental en la construcción y desarrollo del proyecto cooperativo.

Autonomía Administrativa

Las cooperativas de trabajo asociado se distinguen por su capacidad de tomar decisiones y gestionarse de manera autónoma e independiente. “Las CTA adelantan su actividad de trabajo con plena autonomía, administrativa y financiera” (Corporación CEPA, 2019). Esta característica resalta que son organizaciones que se autogobiernan y autogestionan completamente por sus socios, quienes desempeñan un papel activo no solo en las actividades diarias, sino también en la

dirección estratégica de la cooperativa. Según (Horta-Solano, 2018), debido a su objeto social las cooperativas necesitan propender su desarrollo de forma autogestionada ya sea que sean creadas para prestar servicios a terceros deben contar con total autonomía administrativa.

Esta estructura garantiza que las decisiones se tomen sin intervención externa, lo que permite que la cooperativa se alinee estrechamente con los intereses y metas de sus miembros, acerca de esto indica Arango Jaramillo (2024), el ámbito de la organización laboral, la autogestión propone sustituir la estructura piramidal de la empresa, donde la dirección se concentra en la cúspide, por un modelo donde la autoridad reside en la comunidad trabajadora. Esta transición elimina el carácter alienante del trabajo, dotándolo de un sentido libertario y creativo.

La autonomía de las cooperativas de trabajo asociado representa un firme compromiso con la independencia y la democracia empresarial. Los socios, al tener el control total sobre la gestión de su cooperativa, tienen la capacidad de adaptarse rápidamente a los cambios en el entorno y las necesidades del grupo, al tiempo que mantienen firmes sus valores y principios fundamentales. Esta autogestión promueve un sentido de responsabilidad y empoderamiento entre los socios, ya que son directamente responsables del éxito y la sostenibilidad de su cooperativa.

Esta independencia no solo fortalece la cohesión y solidaridad internas, sino que también permite que la cooperativa trace su propio rumbo, libre de influencias externas que puedan ser restrictivas o no alineadas con sus objetivos. Al ser las responsables de su propio destino, las cooperativas de trabajo asociado están mejor equipadas para implementar prácticas comerciales éticas y sostenibles que beneficien tanto a los miembros como a la comunidad en general. Definitivamente, la autonomía y autogestión son fundamentales para mantener la integridad, eficacia e innovación dentro de las cooperativas de trabajo asociado.

Autonomía Financiera

Aunque las cooperativas de trabajo asociado pueden recibir apoyo externo, como orientación financiera, subvenciones, créditos o colaboraciones con otras entidades, es esencial destacar que todas las decisiones operativas y financieras se toman internamente, por el conjunto de socios. Esta autonomía en la toma de decisiones garantiza que cualquier influencia o asistencia externa esté alineada con los objetivos, necesidades y valores de la cooperativa sin comprometer su independencia o principios democráticos.

La participación directa de los socios en estas decisiones clave fortalece no solo el sentido de pertenencia y compromiso hacia la cooperativa, sino que también garantiza que las acciones tomadas promuevan el bienestar colectivo y se ajusten a la visión a largo plazo de la entidad. Este control interno permite que la cooperativa mantenga su rumbo y propósito, incluso cuando interactúa o se beneficia de recursos externos.

Esta estructura interna de toma de decisiones no solo refleja el espíritu de autogestión y autonomía de las cooperativas, sino que también proporciona una base sólida para la innovación sostenible y el crecimiento inclusivo. Al mantener el control sobre las decisiones financieras y operativas dentro del grupo de socios, las cooperativas de trabajo asociado aseguran que su desarrollo se lleve a cabo de manera coherente con sus principios fundamentales, fomentando así un modelo empresarial que es tanto resistente como adaptable (Arango Jaramillo, 2024).

Formación Permanente

Las cooperativas de trabajo asociado se destacan por su compromiso con el principio de educación y formación continua de sus socios, reconociendo que el crecimiento personal y profesional de cada miembro contribuye directamente al éxito conjunto de la organización. Este enfoque busca no solo mejorar las habilidades de gestión y las competencias técnicas necesarias

para la operación eficaz de la cooperativa, sino también fomentar un entorno de aprendizaje constante y mejora continua.

A través de programas de capacitación, talleres, seminarios y otras actividades educativas, las cooperativas invierten en el desarrollo humano, asegurando que sus socios estén debidamente preparados para enfrentar los desafíos del mercado y las dinámicas cambiantes del sector en el que operan, incluyendo fortalezas en temas relacionados como seguridad informática, prevención de ataques de ingeniería social y manejo de contraseñas. Esta educación y formación no se limitan únicamente a aspectos técnicos o de gestión, sino que también abordan temas relacionados con los valores cooperativos, la ética empresarial y el desarrollo sostenible, promoviendo así una cultura organizacional diversa y enriquecedora.

Esta inversión en educación y formación refleja la convicción de que el conocimiento y el desarrollo de habilidades son fundamentales para el empoderamiento de los socios y el fortalecimiento de la cooperativa. Al fomentar la participación en procesos educativos, no solo se mejora la competitividad y la eficiencia de la cooperativa, sino que también se contribuye a formar socios más comprometidos, responsables y preparados para tomar decisiones informadas y participar de manera efectiva en la gestión colectiva.

Empoderamiento de los Socios

El énfasis en la formación y educación continua dentro de las cooperativas de trabajo asociado no solo busca mejorar las habilidades y competencias técnicas y de gestión de sus socios, sino que también está profundamente orientado hacia el empoderamiento de estos. Este empoderamiento es esencial para fortalecer la capacidad de cada socio de participar de manera activa y efectiva en la toma de decisiones colectivas, reforzando así el funcionamiento

democrático y participativo que es fundamental para el modelo de negocio cooperativo (Horta-Solano, 2018).

La capacitación en áreas como liderazgo, comunicación, resolución de conflictos y toma de decisiones permite que los socios adquieran herramientas esenciales para contribuir de manera significativa en las discusiones y deliberaciones que configuran el futuro de la cooperativa. Esto garantiza una gobernanza más inclusiva y representativa, donde las opiniones de todos los miembros son escuchadas y valoradas por igual, y donde las decisiones se toman de manera más informada y consensuada.

Además, estas iniciativas formativas buscan proporcionar a los socios una comprensión más profunda de los principios cooperativos y los desafíos económicos, sociales y ambientales actuales, enriqueciendo así el análisis y el debate dentro de la cooperativa. Por lo tanto, la formación no solo mejora las competencias individuales, sino que también construye una sólida base de conocimiento colectivo y fomenta una cultura de aprendizaje mutuo y apoyo compartido.

Al promover el empoderamiento de los socios a través de la formación, las cooperativas de trabajo asociado fortalecen su estructura organizativa, fomentan un mayor compromiso y responsabilidad compartida en la gestión de la cooperativa, y garantizan un desarrollo sostenible y equitativo. Este compromiso con la educación y el empoderamiento refleja una visión a largo plazo donde cada socio no solo contribuye al éxito de la cooperativa, sino que también crece personal y profesionalmente dentro de ella, esto es una gran ventaja ya que no solo los procesos de formación pueden ser enfocados a la naturaleza de gestión de la cooperativa también se puede aprovechar para capacitar en materia de seguridad informática a los responsables de los diferentes activos de información incluso capacitando a los demás asociados en principios de seguridad informática, ingeniería social, prevención de ataques por medio de correo electrónico y gestión de contraseñas.

Innovación

Las cooperativas de trabajo asociado sobresalen por fomentar un ambiente donde la innovación y la creatividad de sus socios son elementos fundamentales para el avance y crecimiento de la organización. Este enfoque proactivo hacia la mejora continua y la diversificación de actividades y servicios es esencial para ajustarse a los entornos de mercado cambiantes y para satisfacer de manera más efectiva las necesidades y expectativas de sus miembros y de la comunidad a la que sirven.

La participación de los socios en procesos creativos y de innovación no solo permite explorar nuevas ideas y conceptos que pueden convertirse en oportunidades de negocio, sino que también promueve una cultura de colaboración y experimentación. Al alentar a sus miembros a compartir sus visiones y propuestas, las cooperativas potencian su capacidad para identificar soluciones originales a problemas complejos, así como para desarrollar productos, servicios o metodologías que las diferencien de sus competidores.

Esta búsqueda constante de innovación se ve favorecida por la estructura democrática y participativa de las cooperativas, donde las decisiones relacionadas con la adopción de nuevas tecnologías, procesos o enfoques de negocio se toman de manera colectiva. Esta apertura al cambio motiva a todos los socios a mantener una actitud activa y comprometida hacia la evolución de la cooperativa, garantizando que las ideas innovadoras sean debidamente consideradas y, cuando sea apropiado, implementadas.

Por lo tanto, el impulso hacia la innovación y la creatividad no solo impulsa el crecimiento y la competitividad de la cooperativa, sino que también contribuye al desarrollo profesional y personal de sus socios, quienes tienen la oportunidad de ver sus ideas y esfuerzos materializarse en proyectos concretos que beneficien al colectivo. En conclusión, las cooperativas

de trabajo asociado se presentan como entornos dinámicos y resistentes, capaces de adaptarse y prosperar en un mundo en constante cambio gracias al poder de la innovación colectiva.

Políticas de Seguridad de la Información Acordes a las Características Distintivas de las Cooperativas de Trabajo Asociado

En la identificación de las particularidades de las cooperativas de trabajo asociado, se plantearon las políticas de seguridad de la información acordes al ámbito organizacional de estas agrupaciones, teniendo en cuenta la norma ISO 27000, de acuerdo con Cárdenas-Solano et al. (2016) los resultados del análisis y evaluación de riesgos deben guiar la creación de la política de seguridad. Esta política es un documento que refleja el compromiso y respaldo de la dirección, además de definir el rol que debe desempeñar en la realización de la misión y visión de la organización. En esencia, se documenta para comunicar la importancia de la seguridad de la información, junto con sus principios, a todos los usuarios de los recursos de información.

La estructura de una política de seguridad de la información debe contener los siguientes ítems con el propósito de asegurar que está cumpla con las necesidades acordes de las características particulares de las cooperativas de trabajo asociado.

Objetivo de Las Políticas de Seguridad de la Información

El objetivo de una política de seguridad de la información debe plantearse como un compromiso claro y conciso por parte de la organización para proteger y asegurar la confidencialidad, integridad y disponibilidad de toda su información, tanto digital como física, contra todo tipo de amenazas, según Fernández Climent (2024), estos objetivos se deben definir de forma que permitan identificar los resultados en materia de seguridad de la información esperados por la organización, así mismo deben contar con características que los permitan ser específicos, medibles, alcanzables, relevantes y con un tiempo definido.

En relación con las particularidades de las cooperativas de trabajo asociado, estos objetivos deben estar acordes a la capacidad de gestión y cumplimiento de estas organizaciones solidarias.

Alcance de la Política

El alcance de la política de seguridad de información debe definirse de manera exhaustiva para abarcar todos los aspectos relacionados con el manejo, acceso, clasificación, almacenamiento y eliminación de activos de información dentro de una cooperativa de trabajo asociado. Esto incluye tanto la información en formato digital como la física, y se extiende a cualquier medio donde esta se almacene, procese o transmita, ya sea en infraestructura propia de la organización, en la nube o en dispositivos móviles.

Normatividad

Se debe establecer el marco legal y regulatorio que guiara las acciones y prácticas de seguridad de la información, identificando las leyes regulaciones, normas y estándares relevantes que se apliquen a la cooperativa de trabajo asociado, proporcionando una descripción detallada de cada norma identificada, mencionando su alcance, objetivos y requisitos claves, enfocándose en las regulaciones destinadas para seguridad de la información y las aplicables a las cooperativas de trabajo asociado.

Lineamientos Generales

Los lineamientos generales de una política de seguridad de la información deben ser definidos por la asamblea general estableciendo como la organización abordara de manera integral y sistemática la protección de la información. Según Wadhwani et al. (2024) la política de seguridad de información debe tener en cuenta aspectos como: estrategia del negocio, requisitos externos de cumplimiento normativo, riesgos y amenazas que puedan afectar la seguridad de la información en el presente y en el futuro. También debe mencionar descripciones

sobre: Definición de seguridad de la información, objetivos específicos o el sistema que garantice que se establecerán dichos objetivos, principios para dirigir todas las actividades necesarias para cumplir con la política, el compromiso para cumplir con los requisitos necesarios para asegurar la seguridad de la información, compromiso para buscar la mejora continua del sistema de seguridad de información, asignación de responsabilidades y roles definidos para gestión de la seguridad de la información.

La política de seguridad de la información debe estar respaldada por políticas específicas por tema, a necesidad de la organización como: Control de acceso, gestión de activos, transferencia de información, etc. El propósito de estas es permitir gestionar las necesidades en materia de seguridad de ciertos grupos específicos, siendo complementarias a la política general de seguridad de la información.

En las cooperativas, la gestión de la seguridad de la información no parte de un modelo jerárquico-piramidal de control, sino que emana del principio de identidad donde los asociados, al mismo tiempo, son aportantes, propietarios y gestores de los activos de información (Horta-Solano, 2018). Con este enfoque la protección de datos e infraestructura tecnológica se rige por la autogestión, donde la decisión sobre el destino de los recursos y el establecimiento de salvaguardas depende de la base asociativa y requiere la legitimación de la Asamblea General, evitando que la seguridad se convierta en un instrumento de subordinación unilateral. Como lineamiento operativo particular, el Factor C (Comunidad) es adoptado como el principal control social de seguridad, potenciando el sentido de pertenencia y la responsabilidad ética del socio frente al patrimonio informativo colectivo, lo cual reduce la necesidad de mecanismos coercitivos de vigilancia típicos de la empresa capitalista (Arango Jaramillo, 2024). Finalmente, todo control técnico o administrativo deberá ser diseñado para mitigar el riesgo de desnaturalización, asegurando que la supervisión de los activos de información no genere relaciones de

dependencia o subordinación que contravengan la normativa laboral vigente y la esencia solidaria de la organización.

Compromisos

Los compromisos en las políticas de seguridad de la información representan expresiones de intención que reflejan la responsabilidad y la dedicación de las cooperativas de trabajo asociado para salvaguardar sus activos de información. Estos compromisos son esenciales para establecer una cultura de seguridad sólida y deben ser claros, cuantificables y alineados con los objetivos estratégicos de la organización. Se debe resaltar para la situación particular de las cooperativas de trabajo asociado, el compromiso entre los asociados, colaboradores, stakeholders en la implementación de las políticas, se deben cubrir mediante los siguientes aspectos:

- Protección de datos.
- Cumplimiento de legislación y normatividad.
- Educación y formación en seguridad informática.
- Concientización.
- Innovación y adaptabilidad.

Responsabilidad Sobre los Activos de Información

La responsabilidad sobre los activos de información es un componente crucial en la gestión efectiva de la seguridad de la información dentro de cualquier organización de economía solidaria y sobre todo en el caso especial de las cooperativas de trabajo asociado. Según Cárdenas-Solano et al. (2016) es indispensable plasmar las responsabilidades y funciones de los empleados y de los demás actores que intervienen en situaciones explicitas de seguridad.

Esta responsabilidad debe ser asignada en todos los niveles, desde consejo de administración hasta el personal operativo, teniendo en cuenta las disposiciones establecidas por

la asamblea de socios y los designados por ella, para asumir las responsabilidades sobre los activos de información, esto implica asignar obligaciones y roles específicos para la protección y el uso adecuado de los activos informativos.

Está asignación de responsabilidades debe ser acorde a la clasificación de los activos de información, siendo primordial realizar los procesos de asegurabilidad ya que es un principio fundamental para determinar su valor, sensibilidad y el riesgo asociado con la pérdida o divulgación no autorizada, Al clasificar adecuadamente los activos de información, las cooperativas de trabajo asociado pueden aplicar los niveles apropiados de protección y cumplir con los requerimientos legales y normativos relacionados con la retención de información.

Es importante especificar que los responsables de cada uno de los activos de información deben estar comprometidos para aplicar cada uno de los controles sobre los mismos, esto se debe aplicar a partir de su generación, administración y destrucción final.

Responsabilidad en el Cumplimiento de las Políticas

La responsabilidad de garantizar el cumplimiento de las políticas de seguridad de la información debe ser compartida y entendida en todos los niveles de las cooperativas de trabajo asociado, desde el consejo de administración hasta los asociados que realizan su contribución laboral. Una estructura de responsabilidad bien definida garantiza que cada persona conozca su función y las expectativas en lo que respecta a la protección de los activos de información.

Consejo de Administración. Debe promover una cultura de seguridad y administrar los recursos necesarios para implementar y mantener las políticas, adicional debe realizar aprobación de las políticas de seguridad de la información y asegurar que estén alineadas con los objetivos estratégicos de la organización.

Departamento de TI. Implementar y gestionar soluciones tecnológicas y controles de acceso para proteger los activos de información, con relación a incidentes de seguridad de la información debe responder y gestionar conforme a las políticas y procedimientos establecidos.

Gerentes y supervisores. Identificar y reportar los riesgos de seguridad de la información específicos de sus áreas, adicional deben garantizar que los asociados que sean sus subalternos cumplan con las políticas y controles establecidos.

Asociados generales. Asumir las políticas y procedimientos de seguridad de la información en su trabajo contributivo.

Proveedores y terceros. Cooperar con auditorías y revisiones de seguridad conducidas por la organización o terceros designados.

Auditoría Interna. Realizar auditorías periódicas para verificar el cumplimiento de las políticas de seguridad de la información, sugiriendo de ser necesario mejoras basadas en los hallazgos de las auditorías. En relación con los activos de información es importante realizar auditorías periódicas sobre los derechos de acceso a los sistemas físicos y lógicos, según Wadhwani et al. (2024) estas revisiones deben realizarse una vez al año o cuando se produzcan cambios importantes en la organización de la compañía, también es indispensable prestar atención a los cambios en los roles de los usuarios, ya sea por ascensos, descensos de cargos o cambios significativos en el trabajo.

Componentes del Modelo

Alcance y Definiciones. El alcance y las definiciones tienen que quedar claramente fijadas para definir los activos, procesos, áreas y partes interesadas que cubre la política, incluyendo los asociados, contratistas y terceros. Debe incorporar un glosario de términos importantes (activo de información, propietario, clasificación del activo de información, uso aceptable, etc.) alineados con la de ISO/IEC 27001 e ISO/IEC 27002. También se sugiere definir

cuáles pueden ser las excepciones y el medio por el que pueden aprobarse, así como definir la relación de la política con el SGSI y otras normas de seguridad internas. Según Fernández Climent (2024) una extensión innecesaria del alcance puede generar inconvenientes en la puesta en marcha y estabilidad del sistema.

Principios, Objetivos y Compromisos. La política de gestión de activos de información se debe basar en los principios de confidencialidad, integridad y disponibilidad de los activos. Estos principios guiarán la adopción de controles acordes con el nivel de riesgo, promoviendo la responsabilidad compartida y el compromiso por la mejora continua de la seguridad de la información.

Los objetivos de la política deben estar enfocados a garantizar la protección integral de todos los activos de información, manteniendo un inventario actualizado, y minimizando los incidentes asociados a los usos indebidos, también es importante asegurar el cumplimiento de los requisitos legales, contractuales y regulatorios a los que pueda verse sometida la organización.

La organización se debe comprometer a proporcionar los recursos necesarios mediante los cuales se ha de implementar la política, también es prioritario asegurar la garantía del cumplimiento normativo de la misma y el fomento de la concienciación en seguridad de la información. Según Fernández Climent (2024), uno de los elementos claves del estándar ISO/IEC 27001:2022 es el liderazgo de la dirección el cual se debe estar reflejado en el compromiso adquirido al definir las políticas de seguridad de la información resaltando que al momento de definir las políticas estas deben ser claras, concisas, comprensibles, también deben ser acorde a los objetivos estratégicos de la compañía y deben ser socializadas a todo el personal, ya sea por medio de capacitaciones con las cuales también se puede formar y concientizar a los empleados en temas relacionados con seguridad de la información, responsabilidades y procedimientos de seguridad.

Normatividad. El proceso de elaboración de la Política para la Gestión de los Activos de la Información debe sustentarse en una base de gran solidez en cuanto al marco normativo, de tal forma que le permita garantizar la efectividad, cumplimiento normativo y alineamiento con las mejores prácticas. Los lineamientos por considerar se estructuran en tres niveles jerárquicos: marco legal externo, normas internacionales y normativa interna.

Marco Legal y Regulatorio Externo (Cumplimiento Obligatorio). El primer nivel de lineamientos viene dado por el marco legal colombiano. Lo anterior implica que el incumplimiento de estas disposiciones puede llevar a sanciones económicas, constitucionales y reputacionales graves.

La política debe traducir dicha necesidad legal en compromisos de acción. Por ejemplo, el criterio de clasificación de la información "deben ser consistentes con los esquemas de clasificación de información adoptados por la organización".

Normas Internacionales y Buenas Prácticas (Cumplimiento Voluntario Pero Estratégico). El segundo nivel de lineamientos viene dado por normas internacionales como la familia de normas ISO/IEC 27000, las cuales ofrecen la metodología de un manejo eficaz. La política debe manifestar explícitamente su correspondencia al marco propuesto.

Normatividad Interna (Cumplimiento Obligatorio Interno). Finalmente, la política de gestión de los activos debe corresponder al ecosistema interno de la organización. Esto implica una horizontalidad con otras políticas corporativas, como la Política de Seguridad de la Información, la Política de control de Accesos y el Código de Conducta. Asimismo, la política deberá encontrar apropiadamente que la gestión de los activos es con arreglo a lo pactado contractualmente para los clientes y los proveedores.

Inventario de Información y Otros Activos. La organización mantendrá un inventario exhaustivo y actualizado de todos los activos relacionados con la información, incluyendo

hardware, software, datos, servicios, documentación y otros elementos esenciales para la operación. Según (Calder, 2024), este inventario deberá reflejar con precisión la ubicación, estado, función y relación de cada activo con otros recursos críticos, garantizando la trazabilidad y control durante todo su ciclo de vida.

Roles y Responsabilidades. En el momento de crear una política para la gestión de activos de la información, es deber de la alta dirección que cada activo de información cuente con un responsable asignado y que a su vez dentro de la organización haya una comunicación clara de esto.

Es importante establecer, documentar y dar a conocer los roles y las responsabilidades relacionadas con la gestión de los activos de información. Deberá ser responsable toda persona y/o parte interesada que tenga acceso, use o gestione activos de información de cumplir con las políticas y procedimientos de seguridad aplicables, incluso la clasificación, etiquetado, uso permitido y devolución de estos activos.

La alta dirección será responsable de la dotación de recursos adecuados así mismo de su seguimiento para poder verificar que estas responsabilidades sean efectivamente implementadas. Los propietarios de los activos serán responsables de la protección y el uso adecuado de los activos que están bajo su custodia y los usuarios de su utilización de acuerdo con lo dispuesto (Wadhwani et al., 2024).

De acuerdo con el principio de autogestión y gestión democrática, estos roles se ejercen de forma transversal entre los órganos de gobierno y los socios. Como órgano máximo, la Asamblea General de Asociados tiene la soberana responsabilidad de aprobar las políticas de inversión y dotación de recursos para la protección del patrimonio informativo, asegurando que estos no sean destinados a la rentabilidad individual sino al beneficio social colectivo. La Junta de Vigilancia, por su parte, opera como el cuerpo técnico-social que vigila que los activos de

información sean administrados correctamente, efectuando visitas de inspección y examinando archivos para comprobar que el uso de la tecnología no cambie el objeto social ni afecte los derechos de los asociados. Con el Principio de Identidad, desaparece la figura del usuario pasivo y nace la del Socio Gestor, quien asume la custodia directa de los activos que utiliza no por una relación subordinada de trabajo, sino en su calidad de copropietario de los medios de producción. En este modelo, el Factor C (Comunidad) pasa a ser el motor de ejecución, donde la vigilancia mutua y el compañerismo operan como controles preventivos contra los usos indebidos de la información. Por último, la coordinación técnica frecuentemente delegada en un Coordinador o comité especializado en lugar de en una dirección jerárquica, ha de asegurar que las medidas de seguridad no se conviertan en instrumentos de mando con riesgo de desnaturalización, manteniendo siempre la distinción entre el control societario de los activos y la subordinación patronal ilegal.

Clasificación y Etiquetado de la Información. La organización habrá de establecer un sistema formal de clasificación de la información, atendiendo a su valor para la organización, a los requisitos legales y contractuales aplicables, y a su sensibilidad y criticidad. La clasificación constitutiva de la información permitirá establecer los controles de seguridad que se aplicarán y garantizar que el nivel de protección proporcionado es el adecuado, de la misma forma que se asocie al riesgo existente para cada activo.

Categorías específicas de clasificación (ej.: Pública, Uso Interno, Confidencial y Restringida) estarán documentadas en detalle y explicadas para que todo el personal sea capaz de aplicarlas. Wadhwani et al. (2024) explican que la categorización de la información establece sus niveles de criticidad (confidencialidad, integridad y disponibilidad) sobre la base de los requerimientos propuestos por las partes interesadas, con el objetivo de atender las exigencias de seguridad de la organización.

También se deben establecer procedimientos de etiquetado de la información, a fin de que cada activo refleje claramente su nivel de clasificación. El etiquetado debe aplicarse a documentos impresos, archivos digitales y medios de almacenamiento, siguiendo convenciones comunes que sean comprensibles para todo el personal. Además, este proceso debe desarrollarse a lo largo del ciclo de vida de la información y los controles de seguridad a aplicar deben estar acordes con el nivel de clasificación de la información, según (Wadhwani et al., 2024), una vez clasificada correctamente la información, será responsabilidad del propietario de dicho activo establecer un sistema de etiquetado con el que se puedan identificar los tipos de información. Aunque el etiquetado de información en los distintos tipos de formato, tanto digital como físico, establece procedimientos diferenciados, estos deben ser los mismos y fáciles de interpretar.

Uso Aceptable, Devolución y Protección de Activos. La compañía tendrá que definir y comunicar lineamientos claros sobre el uso aceptable de los activos de información; esto incluye hardware, software, redes, servicios en la nube y datos corporativos. Wadhwani et al. (2024) explica que estas normas van orientadas a evitar usos inadecuados de los activos de información y a asegurar que estos sólo son utilizados con fines autorizados y en las funciones asignadas. En caso de que estas normas no fuesen seguidas, se considerará que surge incidente de seguridad y se llevará a cabo el tratamiento previsto de acuerdo con los procedimientos disciplinarios.

Al realizar la redacción de la política de gestión de los activos de la información, se deben tener en cuenta los siguientes aspectos asociados a la devolución de los activos:

Definir el alcance: identificar cómo se especifican los tipos de activos que se someten a devolución cuando se pone fin al vinculo del asociado (ejemplo: equipos, terminales móviles, soportes de datos, credenciales de acceso, licencias de uso de software, documentación física o digital).

Establecer un procedimiento formal: señalar cómo se llevará a cabo el proceso de devolución de activos, quién recibirá los activos devueltos y cómo se documentará la trazabilidad de la devolución del activo.

Utilizar la seguridad de la información: establecer controles de seguridad que eviten, durante el proceso de devolución, la pérdida de datos o accesos no autorizados.

Definir las responsabilidades: especificar las obligaciones de los asociados, contratistas o proveedores, respecto a la devolución de los activos, y los roles de las áreas de TI, de seguridad y de recursos humanos como responsables de la actividad subsidiaria de la devolución.

Definir las consecuencias derivadas de la falta de devolución de los activos: concretar que, no devolver los activos, constituye una no conformidad que se deberá gestionar en conformidad a la disciplina o a la seguridad pertinentes.

Asimismo, hay que definir unas medidas de protección razonables contra los accesos no autorizados, la pérdida, la modificación o la destrucción de la información. Según Fernández Climent (2024), los usuarios asumen la responsabilidad de la utilización y la protección correctas de los activos bajo su base de custodia, y la organización garantiza actividades de formación y concienciación orientadas al cumplimiento de tales normas, deben existir controles técnicos y administrativos que apoyen la aplicación de las disposiciones que recoge la política.

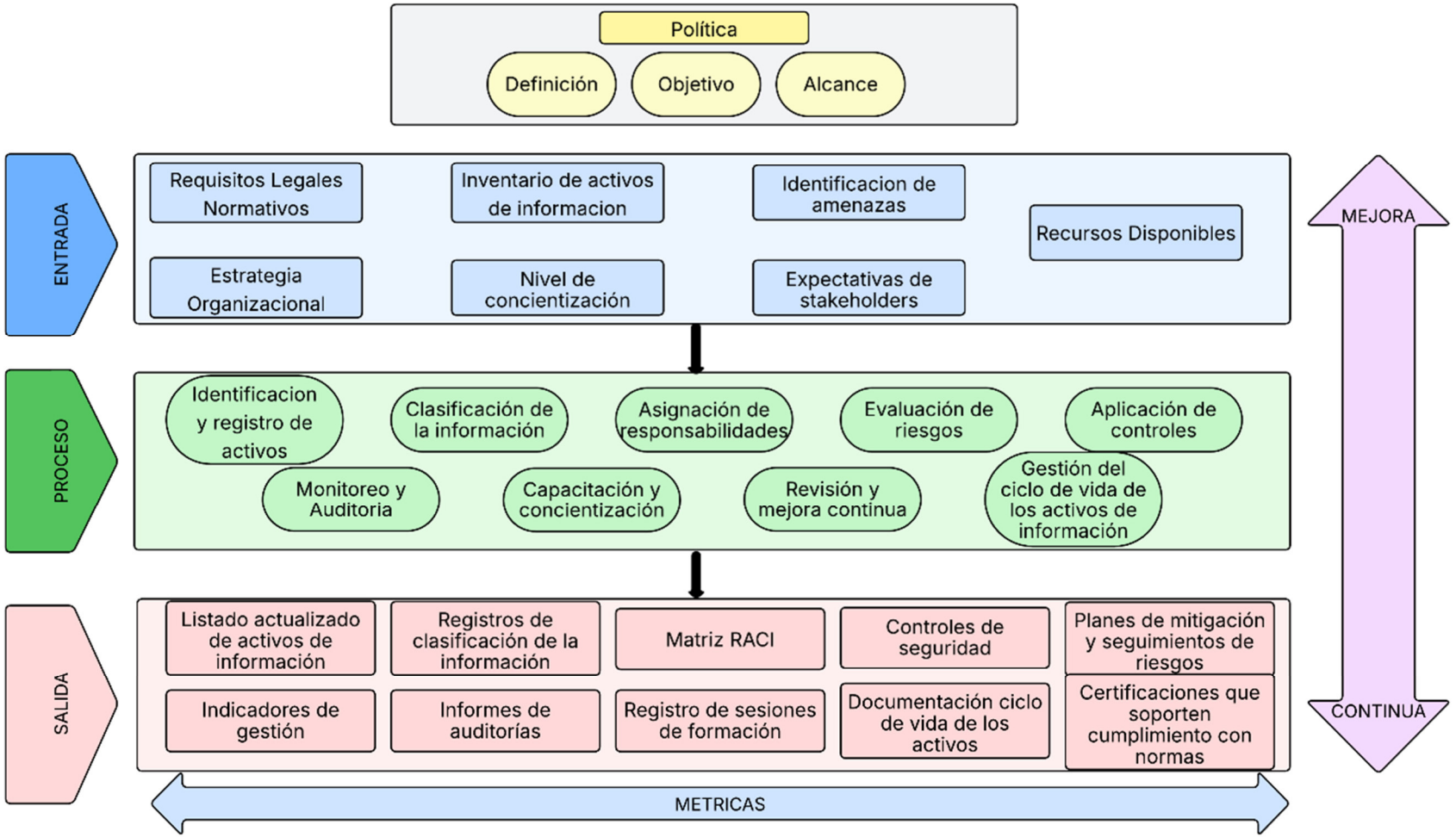
En el caso particular de las Cooperativas de Trabajo Asociado, los controles de uso y protección de activos deben ir más allá de un enfoque restrictivo tradicional, para integrarse en el principio de identidad, donde el asociado asume la custodia del activo de información no como un empleado subordinado, sino como copropietario de los medios de producción. Según este razonamiento, el control esencial es el Factor C (Comunidad), que impulsa una vigilancia social y ética cimentada en la asistencia mutua y la responsabilidad democrática, disminuyendo de manera espontánea la probabilidad de conflictos internos derivados del uso indebido de la

información. Desde el punto de vista operativo las medidas de monitoreo técnico y administrativo deben ser diseñadas y aplicadas bajo criterios de autogestión, asegurando que el seguimiento de los activos de información sea percibido como una salvaguarda del patrimonio colectivo y no como una herramienta de mando jerárquico que desnaturalice la relación societaria, convirtiéndola en una relación laboral encubierta ante la justicia ordinaria. La Junta de Vigilancia es el órgano equivalente de control socia, la cual asumirá el rol de supervisión técnica y administrativa en el proceso de devolución de activos por retiro del asociado, garantizando la trazabilidad de la devolución y la protección del capital intelectual socializado, evitando que el conocimiento crítico de la organización se pierda o sea vulnerado durante la transición de salida del socio.

Gráfica de Abstracción del Modelo

Figura 7

Grafica de Abstracción Modelo de Política de Gestión de Activos de Información



Nota. Grafica del modelo de política de gestión de activos de información.

La grafica del modelo plantea una estructura dividida en tres secciones principales entrada, proceso y salida; esto refleja la existencia de un proceso continuo y sistemático que describe un sistema de gestión que transforme elementos de entrada en resultados concretos.

Entradas del Modelo. Insumos críticos que se convierten en la base del modelo:

- Inventario de activos de información: Listado inicial de activos de información existentes que se requieren proteger.
- Identificación de amenazas: Conocer que es lo que puede afectar a los activos de información.
- Recursos disponibles: Establecer el presupuesto disponible, el personal y la tecnología con la que se cuenta para desarrollar la política.
- Estructura organizacional: Establecer roles, responsabilidades y autoridades de cada elemento que hace parte de la política.
- Nivel de concientización: Su objetivo es evaluar el conocimiento actual del personal en lo relacionado con gestión y protección de los activos de información.
- Expectativas de los stakeholders: Alinear los objetivos de la política con las necesidades de las partes interesadas.

Proceso Central. En esta se encuentran las actividades claves del modelo:

Identificación y Registro de Activos. Detectar todos los activos de información existente, determinando los atributos principales como propietario, ubicación y clasificación, esta actividad debe contener información general que permita conocer a los interesados el propósito de esta y los aspectos que la componen.

- Guia Operativa general:

- Objetivo: Establecer un inventario exhaustivo y actualizado de los activos de información (físicos, digitales e intelectuales) que posee la cooperativa para garantizar su protección como patrimonio social.
- Frecuencia: Semestral o ante cambios significativos en el modelo de trabajo.
- Responsable Primario (R): Comité de Seguridad de la Información / asociados gestores de cada proceso.
- Autoridad / Aprobador (A): Consejo de Administración.

- Procedimiento por realizar:
  - Paso 1. Sensibilizar a los asociados sobre el Principio de Identidad, estos deben entender que los activos con mas que elementos físicos, puede ser a través de acciones como sesiones de trabajo donde se explique que la actividad no debe verse como un simple conteo técnico de computadores (hardware), sino como una estrategia para blindar el patrimonio intelectual de la cooperativa.
  - Paso 2. Los asociados deben ser gestores y liderar la identificación de los activos en sus dependencias y áreas de trabajo, cada área debe realizar en esta actividad una ficha de recolección de datos que incluya los siguientes tipos de activos:
    - Los activos esenciales.
    - Arquitectura del sistema.
    - [D] Datos o información.
    - [S] Servicios.
    - [K] Claves Criptográficas.
    - [SW] Software o aplicaciones informáticas.
    - [HW] Equipamiento informático (hardware).

- [COM] Redes de comunicaciones.
- [Media] Soportes de Información.
- [AUX] Equipamiento auxiliar.
- [L] Instalaciones.
- [P] Personal.

- Paso 3. cada activo requiere un custodio. En el caso de las cooperativas aplicaría al asociado que utiliza el recurso para su labor autogestionada, la acción a realizar es registrar el nombre del asociado responsable y el área a la que pertenece el activo.
- Paso 4. Toda la información que se ha recolectado se centraliza para garantizar la trazabilidad y la replicabilidad, la acción a realizar es ingresar los datos en la matriz de inventarios siguiendo los estándares de la norma ISO 27001.
- Paso 5. la junta de vigilancia debe revisar el inventario con el fin de asegurar que todos los activos registrados están destinados al cumplimiento del objeto social de la cooperativa y que a su vez la asignación de responsabilidades no vulnera la autonomía del asociado.
- Herramientas sugeridas: Se sugiere utilizar herramientas de libre acceso o bajo costo y que permitan facilitar la autogestión por parte de la cooperativa:
  - Software GLPI: Software De código abierto que permite llevar un control detallado de hardware y software sin costos de licencia elevados, ideal para el presupuesto cooperativo.
  - Matriz de inventario parametrizada: Documento en formato colaborativo (Google Sheets o Excel en red local) con campos obligatorios según Magerit v3.0 (Nombre, Tipo, Ubicación, Custodio, Valor Social).

- Etiquetado físico y digital: Uso de códigos QR vinculados al inventario para que cualquier socio pueda verificar la información del activo en tiempo real.

Clasificación de la Información. Elaboración de registros en los cuales se establece la clasificación de la información asignación de valores según su confiabilidad, integridad y disponibilidad teniendo como referencia su sensibilidad para la organización.

- Guia Operativa general:
  - Objetivo: Categorizar los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la cooperativa, asegurando que reciban el nivel de protección adecuado.
  - Frecuencia: Anual o cada vez que se cree un nuevo proceso o servicio.
  - Responsable Primario (R): Asociados dueños del proceso y Comité de Seguridad.
  - Autoridad / Aprobador (A): Consejo de Administración (basado en los lineamientos de la Asamblea).
- Procedimiento por realizar:
  - Paso 1. Definir tres niveles básicos adaptados al sector:
    - Pública/Social: Información de interés para la comunidad y entes de control (ej. Balances sociales, estatutos).
    - Interna/Asociativa: Información necesaria para la ejecución del trabajo diario (ej. Manuales de procedimientos, guías técnicas).
    - Confidencial/Privada: Datos personales de socios (Ley 1581) o secretos técnicos que dan ventaja competitiva a la cooperativa.

- Paso 2. Valoración del activo evaluar el impacto de la perdida de la información en tres niveles:
  - Legal, ¿Posible sanción de la SuperSolidaria?
  - Operativo: ¿Se puede seguir prestando el servicio?
  - Reputacional: ¿Afecta la confianza de los asociados o clientes?
- Paso 3. Etiquetado y registro técnico: Desarrollar acciones para marcar el archivo físico o digitalmente, en el caso de archivo digital usar metadatos o marcas de agua, en el caso de archivo físico por medio de sellos o carpetas.
- Paso 4. Socialización de manejo, se deben establecer acciones para determinar reglas de manejo.
- Paso 5. La Junta de Vigilancia realiza muestreos aleatorios para verificar que la información confidencial de los socios (ej. aportes, salud, datos familiares) esté correctamente protegida y no sea accesible para quienes no la necesitan.
- Herramientas sugeridas:
  - Matriz de Clasificación de Información, Documento guía que defina qué tipo de datos caen en cada categoría.
  - Software de Clasificación Automática: Herramientas que permiten etiquetar correos electrónicos y documentos de Office de forma sencilla.
  - Manuales o guías rápida para que el socio sepa cómo archivar y compartir archivos según su etiqueta.

Asignación de Responsabilidades. Registro de los propietarios y custodios de los activos de información.

- Objetivo: Este consiste en establecer un vínculo formal y técnico entre los activos de información identificados y los actores encargados de su custodia, operación y supervisión. En

el entorno de una CTA, este proceso se fundamenta en el Principio de Identidad, donde la responsabilidad emana de la calidad del asociado como copropietario y gestor, y no de una relación de subordinación laboral. Se busca, por tanto, operativizar la seguridad de la información mediante la delegación democrática de funciones.

- Procedimiento por realizar:
    - Paso 1. El propósito principal en este paso es proceder a la identificación de los niveles de actuación dentro de la estructura de la cooperativa. Es primordial distinguir entre los órganos de dirección (Consejo de Administración), de control social (Junta de Vigilancia) y de ejecución (asociados). Esta diferenciación técnica garantiza que el modelo sea replicable y respete el marco legal de la economía solidaria.
    - Paso 2. Se aplica la metodología RACI para definir el grado de involucramiento de cada actor en relación con los activos de información. La asignación se realiza bajo los criterios técnicos necesarios para la elaboración de la matriz, los cuales son plantear las actividades más relevantes y por cada actividad asignar un responsable, aprobador, informado y consultado.
    - Paso 3. Una vez definidos los roles, se procede a la vinculación de estos con el Régimen de Trabajo Asociado. Cada asociado debe suscribir un documento técnico donde se especifiquen las responsabilidades de custodia, uso aceptable y protección de los activos bajo su cargo. Este paso es fundamental para dotar al modelo de operatividad jurídica y técnica.
    - Paso 4. Se realiza una revisión crítica de las responsabilidades asignadas para asegurar que los mecanismos de control no constituyan indicadores de subordinación laboral. La Junta de Vigilancia debe verificar que las responsabilidades de seguridad se enmarquen en el cumplimiento del objeto social y la protección del patrimonio común, y no en una supervisión jerárquica que desvirtúe la naturaleza asociativa.

- Paso 5. Se crea un protocolo de vigilancia mutua donde la responsabilidad no es solo individual sino colectiva. Estos controles sociales permiten que los grupos de asociados funcionen como una salvaguarda natural, reportando anomalías o riesgos de seguridad basados en la confianza y el compromiso ético con la organización.

Evaluación de Riesgos. Según el análisis de amenazas y vulnerabilidades que afectan los activos de información se debe determinar el riesgo y los controles adecuados para mitigarlo. El modelo propone gestionar los riesgos de manera distinta a las organizaciones tradicionales, priorizando la mitigación del riesgo técnico-legal de desnaturalización de la cooperativa, ya que el uso excesivo de controles de monitoreo o supervisión de los activos podría ser interpretado como prueba de subordinación jerárquica, lo cual acarrea sanciones por intermediación laboral ilegal. Ante ello, el modelo propone desplegar el Factor C (Comunidad) con el cual se aumenta el sentido de pertenencia, convirtiéndose en una salvaguarda natural, técnica y social, donde la protección de los activos de información no se basa en la coacción, sino en el Principio de Identidad, el cual incentiva al socio a proteger la infraestructura tecnológica al reconocerla como una propiedad social y un medio de producción propio. También se trata con seriedad el riesgo de que se pierda capital intelectual cuando se retiran los asociados, ya que en una CTA el recurso humano prima por encima de todo sobre el capital, por eso el modelo contempla controles de 'tecnología socializada' para garantizar que el conocimiento crítico sea un bien compartido por el colectivo autogestionado y no una información individual.

- Procedimiento por realizar:
  - Paso 1. Se utiliza la metodología Magerit v3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) por su ajuste a los estándares internacionales ISO 27001. En esta etapa se define el alcance del análisis que debe comprender tanto la

infraestructura tecnológica como los procesos de “saber hacer” y el capital intelectual socializado de la cooperativa.

- Paso 2. Identificación de amenazas y vulnerabilidades específicas, se procede a la catalogación de amenazas, clasificándolas en origen natural, industrial o humano. Para una cooperativa de trabajo asociado, se otorga especial relevancia a las amenazas de origen humano-organizativo, tales como:
  - Fuga de Conocimiento: Riesgo asociado a la desvinculación de asociados que poseen información crítica no documentada.
  - Errores de Mantenimiento [E23] y Accesos No Autorizados [A11]: Identificados como críticos en la gestión de infraestructura física.
- Paso 3. Se calcula el daño potencial que sufrirá la cooperativa si una amenaza se materializa. La evaluación se hace en términos de impacto social y operativo. El Riesgo inherente es el que resulta de la combinación de la probabilidad de ocurrencia de la amenaza y la magnitud del impacto sobre el activo de información, sin considerar aún la existencia de salvaguardas.
- Paso 4. Se identifican y valoran las medidas de seguridad existentes. En el modelo solidario, es importante determinar controles acordes a las necesidades de la cooperativa y que sean cogerentes con el presupuesto asignado por parte de la asamblea general ya que el dinero destinado para estas medidas puede ser mucho menor al asignado por otras compañías del sector privado, los controles sociales toman gran relevancia ya que demuestran el nivel de compromiso, la vigilancia mutua y la autogestión como barreras preventivas ante incidentes de seguridad internos.
- Paso 5. Después de aplicar las salvaguardas, se calcula el Riesgo Residual. Se elabora un plan de tratamiento si este nivel supera el umbral de aceptación definido por el

Consejo de Administración. Las opciones son evitar, reducir, compartir o asumir el riesgo, siempre priorizando la estabilidad del empleo y el cumplimiento de la normativa de la Superintendencia de la Economía Solidaria.

Aplicación de Controles de Seguridad. Implementar medidas técnicas y organizativas con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

Los controles de seguridad se aplican durante la fase operativa del modelo, cuando se seleccionan y despliegan las salvaguardas necesarias para mitigar los riesgos identificados en las etapas anteriores. Lo que se pretende es crear un entorno técnico y administrativo que proteja la información de la que dispone la empresa. En el campo del desarrollo solidario, esta actividad debe conjugar el rigor técnico con la lógica autogestionaria de la cooperativa, de manera que los controles refuercen la confianza y la ayuda mutua entre los asociados.

- Procedimiento por realizar:
    - Paso 1. Proceder a la selección de controles basados en el Anexo A de la norma ISO/IEC 27001 y los requerimientos específicos de la Resolución 500 de 2021 para el sector solidario. La selección debe ser proporcional al nivel de riesgo residual aceptable definido por el Consejo de Administración. Se priorizan los controles de acceso, cifrado de datos críticos y gestión de vulnerabilidades tecnológicas.
    - Paso 2. Desplegar salvaguardas técnicas y lógicas, se realiza la configuración e implementación de herramientas tecnológicas para la protección de la infraestructura. Este paso incluye;
        - Configuración de reglas en Firewalls (ej. Fortinet) y sistemas de detección de intrusos, lo que también se puede llamar como seguridad perimetral.

- Protección de datos con la implementación de protocolos de cifrado para el almacenamiento y tránsito de información sensible, especialmente bases de datos de asociados y registros financieros.
- Configuración de sistemas de autenticación robustos, alineados con la asignación de responsabilidades de la Matriz RACI, para asegurar la gestión de identidades.

  - Paso 3. A diferencia de lo que ocurre en los entornos corporativos convencionales, este enfoque integra controles fundamentados en la doctrina cooperativa. Aquí es donde cobra relevancia el llamado 'Factor C' (Comunidad), el cual funciona como un mecanismo de protección administrativa donde la defensa contra amenazas internas no depende solo de reglas, sino de la vigilancia mutua y un compromiso ético compartido. De este modo, al socializar y validar los acuerdos de uso aceptable mediante procesos democráticos, se logra transitar hacia una cultura real de autogestión de la seguridad.
  - Paso 4. Para asegurar la sostenibilidad del modelo y mitigar el riesgo inherente a la dependencia individual, resulta estratégico formalizar cada control aplicado mediante protocolos documentados. Este proceso de sistematización transforma el conocimiento tácito —el 'saber hacer'— en memoria institucional. Al hacerlo, la cooperativa no solo garantiza la accesibilidad operativa, sino que construye un robusto capital social que asegura la replicabilidad del sistema ante cualquier eventualidad administrativa.
  - Paso 5. Evaluar la eficacia y validación del control social, esta evaluación debe ser realizada por La Junta de Vigilancia la cual realiza una verificación técnica y social de los controles implementados. Aquí se mide si la salvaguarda cumple con su objetivo de protección sin obstaculizar la operatividad autogestionaria. En esta parte, se verifica que el control no actúe como un mecanismo de subordinación laboral, procurando la integridad del vínculo asociativo.

- Herramientas sugeridas:
  - Repositorio de Configuración Técnica: Documentación estandarizada de las reglas de seguridad aplicadas en dispositivos de red y servidores.
  - Manual de Buenas Prácticas Asociativas: Guía operativa para los socios sobre la aplicación diaria de controles (uso de contraseñas, manejo de copias de seguridad).
  - Tablero de Indicadores de Control: Herramienta para medir la eficacia de los controles (ej. número de incidentes mitigados, nivel de cumplimiento de parches).

Monitoreo y Auditoria. Realizar auditorías periódicas con el propósito de verificar el cumplimiento de la política y los controles establecidos.

La supervisión y la auditoría se caracterizan como procesos de vigilancia sistemática y valoración objetiva orientados a comprobar la eficacia de los controles de seguridad puestos en marcha y el cumplimiento de las normativas institucionales. Dentro del ecosistema de una CTA, esta actividad va más allá de la mera inspección técnica, convirtiéndose en un mecanismo de Control Social donde se garantiza que los activos de información sirvan exclusivamente el objeto social y se cuide el patrimonio común. Lo que se pretende es conseguir que el sistema mejore de forma continuada detectando desviaciones y corroborando que los controles son de naturaleza no subordinada.

- Procedimiento por realizar:
  - Paso 1. Proceder a la definición de las métricas de cumplimiento basadas en el estándar ISO/IEC 27001. Se establecen indicadores técnicos (ej. frecuencia de respaldos exitosos, intentos de acceso no autorizados bloqueados por el Firewall) e indicadores sociales (ej. nivel de participación de los asociados en jornadas de capacitación). Esta fase asegura que la auditoría tenga una base cuantitativa y cualitativa replicable.

- Paso 2. Recolectar y analizan los registros de actividad (logs) de los activos críticos identificados en el inventario. Se controla el comportamiento de la infraestructura tecnológica (servidores, redes, bases de datos) con herramientas de gestión de eventos. El monitoreo debe configurarse para que detecte anomalías de seguridad, pero sin que implique la vigilancia del comportamiento individual del asociado, preservando así la autonomía técnica y evitando el riesgo de desnaturalización.
- Paso 3. Realizar de auditorías de control social a través de la Junta de Vigilancia, ejecutar inspecciones periódicas sobre la gestión de los activos. En este paso, se verifica que el uso de la información sea coherente con los acuerdos cooperativos y los estatutos. Se entrevista a los asociados para evaluar su percepción sobre la efectividad de las salvaguardas y se constata la correcta custodia física y lógica de los activos asignados bajo el principio de Identidad.
- Paso 4. Evaluar hallazgos y detectar las no conformidades, se deben contrastar los resultados del monitoreo y la auditoría con los requisitos definidos en la política de seguridad. Se procede a la clasificación de los hallazgos en:
  - Observaciones: Oportunidades de mejora en el proceso.
  - No Conformidades Menores: Desviaciones puntuales que no comprometen la integridad global.
  - No Conformidades Mayores: Brechas de seguridad que exponen el patrimonio social o la privacidad de los asociados.
- Paso 5. Elaborar informe técnico-social con el que se resume el estado de la seguridad de la información. Este documento se debe presentar ante el Consejo de Administración y socializar en la Asamblea General, lo que asegura la transparencia democrática.

El informe debe incluir un plan de acciones correctivas con responsables y tiempos de ejecución, dando así, cierre al ciclo de retroalimentación del modelo.

- Herramientas Sugeridas:
  - Listas de Verificación (Checklists) de Control Social: Cuestionarios estandarizados para que la Junta de Vigilancia realice auditorías sin requerir un perfil estrictamente informático.
  - Sistemas de Gestión de Eventos (SIEM) de Código Abierto: Herramientas para la centralización de logs que permiten un monitoreo técnico eficiente y de bajo costo.
  - Matriz de Seguimiento de Hallazgos: Documento colaborativo para el registro y cierre de acciones correctivas, asegurando que el modelo sea dinámico y no estático.

Capacitación y Concientización. Educar al personal sobre el manejo adecuado de los activos, a través de promoción de buenas prácticas en seguridad y de medidas necesarias para proteger la información.

Se define la capacitación y concientización como el proceso estratégico mediante el cual se transfieren conocimientos y se forma cultura organizacional, con el fin de fortalecer las capacidades de los asociados para la protección de los activos de información. En el modelo de economía solidaria, esta actividad no es una obligación legal, sino el ejercicio del derecho a la educación cooperativa. La meta esencial consiste en cambiar la visión sobre la seguridad, desde una obligación técnica hacia una obligación ética que surge del principio de identidad, en donde el asociado salvaguarda la información al entenderla como parte del patrimonio común y fundamento de su empleo.

- Procedimiento por realizar:

- Paso 1. Diagnosticar necesidades de formación o capacitación; en cada área de trabajo o dependencia se hace un diagnóstico de los requerimientos de conocimiento técnico y administrativo. Se identifican las brechas entre las competencias actuales de los asociados, con los estándares requeridos por la norma ISO/IEC 27001 y la Resolución 500 de 2021. Este diagnóstico debe incluir la identificación del conocimiento especializado que requiere ser documentado y socializado para evitar la fuga de capital intelectual ante la desvinculación de socios.
- Paso 2. Diseñar del plan de formación con enfoque solidario, se debe proceder al diseño de los contenidos curriculares, los cuales deben integrarse en el plan de trabajo del comité de educación. A diferencia de los modelos tradicionales, el diseño debe incluir módulos sobre:
  - Gobernanza y Autogestión: Explicación de cómo la seguridad protege la propiedad colectiva.
  - Riesgos Jurídicos Propios: Concientización sobre el riesgo de desnaturalización y la importancia de que el control de activos no se convierta en subordinación laboral.
  - Uso Ético de la Información: Fomento del Factor C (Comunidad) como base de la vigilancia mutua y la confianza.
- Paso 3. Ejecutar jornadas de capacitación participativa; se deben llevar a cabo las actividades de formación con metodologías que fomenten la autogestión. Se evita el enfoque magistral y se priorizan los talleres prácticos sobre el uso de herramientas técnicas (ej. gestión de contraseñas, cifrado, copias de seguridad). La ejecución debe ser descentralizada, permitiendo que los asociados con mayor pericia técnica actúen como multiplicadores del conocimiento, reforzando la horizontalidad del modelo.

- Paso 4. Realizar campañas de concientización y sensibilización continua a través del desarrollo de estrategias de comunicación interna (boletines, cápsulas informativas, señalética digital) destinadas a mantener la alerta sobre amenazas recurrentes como la ingeniería social o el acceso no autorizado. La concientización se debe enfocar en el valor social de la información, vinculando la protección de los activos con la sostenibilidad económica y el bienestar de todos los asociados.
- Paso 5. Evaluar la efectividad y la transferencia del conocimiento, se debe realizar medición del impacto de la capacitación a través de instrumentos de evaluación de aprendizaje y de la observación directa en los puestos de trabajo. La Junta de Vigilancia debe dar seguimiento a este proceso para comprobar que los asociados hayan entendido su rol de custodios bajo el esquema de la Matriz RACI. Se debe medir si el conocimiento adquirido se traduce en una disminución de incidentes por error humano y en una mejora en el reporte voluntario de vulnerabilidades.

Revisión y Mejora Continua. Evaluar la efectividad del modelo y actualizar procesos y políticas según cambios tecnológicos, normativos o de negocio.

La revisión y mejora continua es el proceso cíclico y sistemático para evaluar el desempeño del modelo de gestión de activos de información, a fin de garantizar que sea conveniente, adecuado y eficaz. En el contexto de las cooperativas de trabajo asociado, esta fase representa la conclusión del ciclo PHVA (Planear-Hacer-Verificar-Actuar) y se basa en la capacidad de autogestión de la organización. Se trata de encontrar posibilidades de optimización para cerrar las brechas detectadas en las auditorías, a la vez que se adapta el sistema a las nuevas amenazas y se asegura que el patrimonio informativo evolucione junto con las necesidades sociales y productivas de los asociados.

- Procedimiento por realizar:

- Paso 1. Consolidar insumos para la revisión, se debe proceder a la recolección de toda la evidencia generadas en las fases previas del proceso, estos insumos deben incluir:
  - Resultados de las auditorías internas y del monitoreo de los controles.
  - Estado de cumplimiento de los objetivos de seguridad y métricas de desempeño (KPIs).
  - Retroalimentación de los asociados y de los interesados.
  - Cambio en el entorno legal o tecnológico que afecten los activos.
  - Estado de las acciones correctivas y preventivas iniciadas en periodos anteriores.
- Paso 2. Realizar análisis crítico por partes de la alta dirección, se debe convocar a sesión formal por parte del consejo de administración con el propósito de analizar si la estrategia de seguridad sigue siendo coherente con el objeto social de la cooperativa, en este momento se debe evaluar si el uso de los recursos ha sido eficiente y si las salvaguardas implementadas han logrado proteger efectivamente los activos físicos, digitales y documentales sin generar riesgos de desnaturalización laboral.
- Paso 3. Identificar oportunidades de mejora y de toma de decisiones, basarse en el análisis del paso numero 2 con el fin de determinar si es necesario realizar modificaciones en el sistema en los siguientes aspectos:
  - Actualización de políticas de seguridad de la información.
  - Ante cambios en la estructura organizativa reasignar responsabilidades en la matriz RACI.

- Invertir en nuevas herramientas tecnológicas o programas de capacitación según lo determine la asamblea general.
- Ajustar los niveles de aceptación de riesgo ante nuevas vulnerabilidades detectadas.

- Paso 4. Desarrollar la formulación y seguimiento del plan de mejora continua, se deben documentar las decisiones en un plan de mejora que especifique objetivos, metas, responsables y cronogramas de implementación. Cada mejora debe ser tratada como un proyecto de auto gestión, asignándole a un asociado para que lidere el cambio. Se debe establecer un mecanismo de seguimiento técnico con el propósito de verificar que las mejoras sean incorporadas efectivamente a la operación diaria de la cooperativa.
- Paso 5. Aplicar principio de socialización y transparencia administrativa, los resultados de la revisión y los planes de mejora de deben comunicar a los demás asociados. Se deben presentar los avances ante la junta de vigilancia con el fin de validar que las actualizaciones del modelo sigan respetando la autonomía del asociado y la protección del patrimonio común. Este paso debe asegurar que la mejora continua en un proceso aislado sino un compromiso colectivo de todos los asociados de la cooperativa.
- Herramientas sugeridas:
  - Matriz de acciones correctivas y preventivas (CAPA): Herramienta técnica para el registro, análisis de causa raíz y seguimiento de las soluciones implementadas.
  - Tablero de control de mejora continua: Sistema de indicadores visuales que permite monitorear el progreso de los objetivos de seguridad en tiempo real.
  - Actas de revisión por parte del consejo de administración: Formatos estandarizados que garantizan la trazabilidad de las decisiones tomadas por el Consejo de administración.

Gestión del Ciclo de Vida. La gestión del ciclo de vida se entiende como la totalidad de los procesos transversales creados para administrar un activo de información desde su concepción o adquisición hasta su disposición final. En el ecosistema de las cooperativas de trabajo asociado esta tarea no es una gestión técnica de inventarios, sino la custodia del patrimonio social y la garantía de la sostenibilidad del empleo. Lo más importante es garantizar que en cada paso el bien mantenga su integridad y su valor para la comunidad, reduciendo los riesgos de que se pierda el conocimiento y asegurando que la tecnología siempre esté al servicio del objetivo de ayuda mutua.

- Procedimiento por realizar:
    - Paso 1. Planificar y adquirir determinado activo cuando surge la necesidad productiva o social. A diferencia del modelo corporativo tradicional, la adquisición de un activo crítico (software, servidores o metodologías) debe estar alineada con el Plan de Desarrollo de la Cooperativa, se debe realizar evaluación de la inversión a realizar la cual debe ser legitimada por los órganos de dirección (Consejo de Administración) o la Asamblea General de Asociados. Se prioriza la adquisición de herramientas que fomenten la seguridad informática y el control democrático.
    - Paso 2. Crear, identificar y clasificar los nuevos activos, para esto se debe realizar registros en el inventario maestro y asignarle un nivel de criticidad. En este punto, se debe identificar el "saber hacer" asociado al activo, asegurando que el conocimiento técnico no quede aislado en un solo individuo, sino que se prepare para ser compartido a los demás asociados interesados
    - Paso 3. Implementar controles de acceso y sus aceptable previamente definidos en el manual de responsabilidades. Se debe fomentar el Factor C (Comunidad) como mecanismo de vigilancia mutua, donde el cuidado del activo nace de la conciencia de copropiedad.

Es vital asegurar que el monitoreo en esta etapa no derive en conductas de subordinación que puedan desnaturalizar el vínculo asociativo.

- Paso 4. Ejecutar protocolos de mantenimiento preventivo y actualización de seguridad (parches) en los activos que lo requieran. Esta labor de debe realizar bajo principios de autogestión, donde el asociado responsable vela por la salud técnica de su herramienta de trabajo, reportando proactivamente cualquier anomalía al Comité de Seguridad.
- Paso 5. Disponer del activo cuando pierde utilidad o el asociado que lo custodia se desvincula, se procede al cierre seguro de proceso. En el caso de activos con información sensible de debe garantizar el borrado seguro de datos y la recuperación del capital intelectual documentado. Si se trata de un retiro de asociado y el activo era exclusivo para sus realizar sus funciones de contribución laboral, la Junta de Vigilancia supervisa que el activo regrese al inventario general de la cooperativa en condiciones óptimas, evitando la pérdida de información crítica que comprometa la continuidad del servicio.

Salida del Modelo. Componentes que conforman los resultados del modelo:

- Inventario de activos de información: Listado actualizado de los activos de información con su respectivo registro de propietario, ubicación, clasificación, estado y uso.
- Registro de clasificación de la información: Documentos que reflejan como se ha clasificado la información, y como se han etiquetado cada uno de los activos de información.
- Matriz RACI: Documento con información sobre los responsables de cada una de las actividades relacionadas con los activos de información que facilita la gestión de roles y responsabilidades de los activos.

Esta sirve para aportar claridad en proyectos complejos asignando de forma explícita los roles y responsabilidades de cada tarea, decisión y entregable. Su función primordial es trazar un

cuadro donde se representen las actividades en filas y los papeles o roles en columnas, y en cada casilla resultante de la intersección de ambas, se indicará una designación: Ejecutor (Responsable), Responsable Final (Accountable), Consultado (Consulted) e Informado (Informed). Los principales beneficios que ofrece son: reducir los conflictos sobre la autoridad, prevenir la duplicidad de trabajo y aumentar la probabilidad de cumplir con los objetivos del proyecto (Cahyadi & Arviansyah, 2021).

En las organizaciones como las cooperativas de trabajo asociado es necesario redefinir el concepto de autoridad utilizado en la empresa del sector privado por el termino de gobernanza democrática ya que el control es ejercido por la vigilancia social y el compromiso de los socios-propietarios.

- Roles RACI para el contexto de las organizaciones del sector solidario. Al conocer las particularidades en materia de gobernanza de las organizaciones pertenecientes al sector solidario y en especial las cooperativas de trabajo asociado, es necesario plantear una nueva definición para las siglas del modelo RACI:
  - R (responsable): El socio que ejecuta la actividad.
  - A (Aprobador): La responsabilidad superior está a cargo del consejo de administración o Asamblea general, pero en algunas ocasiones esta se designa al representante legal de la cooperativa.
  - C(Consultado): Comités especializados o asesores externos técnicos, cuya opinión es necesaria.
  - I(Informado): Personas que deben conocer los resultados, socios de la cooperativa, a los cuales se les puede informar por canales de comunicación interna.
- Pasos necesarios para la elaboración de la Matriz.

- Paso 1. Identificación de tareas y entregables del modelo: Es importante listar las actividades operativas del ciclo de vida del activo de información, sin enfocarse en las tareas genéricas, a través del uso de herramientas como el mapa de procesos de la cooperativa se puede obtener información para el desglose de actividades como: Levantar inventario de activos, clasificación de la información según el acuerdo cooperativo, mantenimiento de los dispositivos que hacen parte de la infraestructura informática etc.
Es importante utilizar verbos específicos como “Documentar Vulnerabilidades del servidor o “Levantar inventario de activos”, en lugar de términos generales como “Seguridad”
- Paso 2. Identificación de los interesados (Stakeholders): En función a la particularidad de las cooperativas de trabajo asociado los interesados son:
    1. Asamblea General de Asociados: Maxima autoridad.
    2. Consejo de administración o Gerencia: Dirección Ejecutiva.
    3. Junta de Vigilancia: Organismo quien realiza tareas de control interno.
    4. Comité de educación: Encargado de la concientización.
    5. Asociado, Trabajador: Responsable directo de la custodia del activo.
- Paso 3. Asignación de valores en la matriz RACI: La tarea en este paso es cruzar las actividades a realizar con los responsables de cada tarea, cada responsable va en una columna y cada actividad va en una fila, es importante preguntar se aspectos como ¿Quién realiza determinado trabajo? ¿Quién firma el visto bueno? ¿A quién se debe consultar? ¿Quién depende del resultado? etc.

Según el rol de la junta de vigilancia es importante que ella se encuentre con la designación de consultado o informado con el fin de asegurar la transparencia sin efectos adversos en la ejecución de su labor.

- Paso 4. Revisión y validación, Se debe analizar las siguientes situaciones ya que permiten detectar problemas comunes en el diligenciamiento de la matriz:

    1. Filas sin A (aprobador) o al contrario filas con múltiples A, la matriz debe tener solo un aprobador por fila.
    2. Si una persona es A en el 80% o más de las tareas puede surgir un cuello de botella en el proceso.
    3. Mas de 5 C (Consultados) es algo que retrasara el proceso drásticamente.

La matriz debe ser presentada y validada en una sesión de trabajo con los socios de la cooperativa, con el fin de asegurar sentido de pertenencia y responsabilidad de los activos que utilizan.

- Paso 5. Comunicación y mantenimiento, la matriz debe ser un documento de revisión semestral, con el fin de ajustar roles según la rotación de los cargos en los comités a realizarse, igualmente debe ser accesible para todos los socios es por esto que debe publicarse en el repositorio destinado para la socialización a todos los miembros de la cooperativa.

A continuación, en la Tabla 28 se plasma un ejemplo de matriz RACI ajustada a las particularidades se las cooperativas de trabajo asociado:

Tabla 28

Ejemplo Matriz RACI

Tarea/Rol	Ing. Infraestructura (Asociado-Contribución laboral)	Ing. Experto en seguridad (Asociado-Contribución laboral)	Junda de Vigilancia	Consejo de Administración	Asamblea General
Levantar Inventario activos (Infraestructura Informática)	R	R	C	A	I
Realizar Mantenimiento de Servidores	R	C	I	A	I
Realizar Auditorías de seguridad	I	C	R	I	A
Aprobar Inversión en tecnología	C	C	A	I	R

Nota. Valorización de riesgos residuales después de implementar Salvaguardas y su respectiva efectividad total.

La matriz RACI que se muestra en la Tabla 28 no sólo asigna tareas técnicas, sino que pone en marcha la gobernanza democrática de la cooperativa en materia de seguridad de la información. A diferencia de un entorno corporativo tradicional donde la rendición de cuentas "Quien aprueba" es individual y jerárquica, en el caso de la primera actividad este modelo le asigna al Consejo de Administración la tarea de aprobar la información obtenida al realizar el inventario de activos relacionados con la infraestructura informática, mientras que a la junta de vigilancia es la que recibe consulta sobre esta actividad, esto permite asegurar que la gestión de activos esté alineada con el objeto social, mientras que los ingenieros encargados de la parte tecnológica son los responsables de realizar la actividad (R), la asamblea general será informada sobre los resultados arrojen la realización de esta tarea.

- Evaluación de riesgos: Informes de análisis de riesgos asociados a los activos de información, con sus respectivos planes de mitigación y de seguimiento.
- Controles de seguridad: Evidencia de los controles de seguridad aplicados, documentados en políticas y procedimientos operativos.
- Planes de mitigación y seguimiento de riesgos: Informes de análisis de riesgos asociados a los activos de información con sus respectivos planes de contención.
- Indicadores de gestión: Indicadores claves de desempeño con el fin de medir la eficacia de la política.
- Informes de auditorías: Informes de auditorías internas o externas y resultados de revisiones periódicas del inventario y cumplimiento de la política.
- Registro de sesiones de formación: Evidencia de los programas de capacitación y concientización realizados, con muestra del material educativo relacionado con seguridad de la información socializado a los empleados.
- Documentación del ciclo de vida de los activos: Registro de las etapas del ciclo de vida de cada activo de información.
- Certificaciones relacionadas con el cumplimiento de las normas: Informes o evidencias que demuestran el cumplimiento de la norma ISO/IEC 27001.

El modelo establecido se plantea como un proceso cíclico en búsqueda de la mejora continua y que se adapte para la protección de nuevas amenazas y cambios que puedan surgir en la organización.

Métricas para Aplicar. La utilización de métricas es importante para medir el desempeño y eficacia del modelo a seguir, a través de la información que se obtiene de ellas es

posible tomar decisiones que realmente beneficien a la compañía y permitan establecer un proceso de mejora continua en la gestión de activos de información.

A continuación, se indican algunas métricas que se pueden aplicar en base al modelo planteado:

- Métrica porcentaje de actualización del inventario de activos de información:
    - Propósito: Garantizar que el inventario de activos de información se mantiene actualizado.
    - Formula:

$$\frac{Numero\ de\ activos\ actualizados}{Total\ de\ activos\ en\ inventario} * 100 = Porcentaje\ de\ Actualizacion\ de\ Inventario$$

    - Frecuencia: Semestral.
    - Responsable: Responsables de inventario de activos.
    - Umbral de Alerta: < 85%
- Tasa de cumplimiento de formación en concientización de seguridad de la información:
    - Propósito: Medir el grado de participación del personal en los programas de concientización de seguridad de la información.
    - Formula:

$$\frac{Numero\ de\ asociados\ que\ finalizan\ la\ formacion}{Total\ de\ asociados\ citados} * 100 = Tasa\ de\ Cumplimiento$$

    - Frecuencia de medición: Trimestral.
    - Responsable: Responsable de seguridad de la información.
    - Metas y Umbrales: En la Tabla 23 se puede visualizar los rangos propuestos.

Tabla 29

Umbrales para la Métrica Tasa de Cumplimiento de Formación

Nivel de cumplimiento	Clasificación	Acción requerida
95-100 %	Excelente	Mantener buenas prácticas.
85-94%	Aceptable	Plan de mejora para áreas específicas.
75-84%	Mejorable	Notificación a jefes de dependencias.
< 75%	Critico	Intervención inmediata.

Nota. Niveles de estimados para el cumplimiento en la métrica de formación.

- Porcentaje de Riesgos tratados según el plan:
- Propósito: Validar que los tratamientos de riesgo son ejecutado acorde a lo planificado.
- Formula:

$$\frac{Numero\ de\ riesgos\ tratados}{Total\ de\ riesgos} * 100 = Porcentaje\ de\ riesgos\ tratados$$

- Frecuencia: Anual.
- Responsables: Responsable de gestión de riesgos.
- Umbral de Alerta: <85 %

Conclusiones

Se categorizaron los activos de información de la organización, mediante la norma ISO 27001. En este proceso se identificaron, evaluaron y se clasificaron dichos activos relacionados con la seguridad informática, para un adecuado proceso de análisis y gestión de riesgos informáticos que puedan afectar la seguridad de los activos, para lo cual se establecieron controles y salvaguardas para su protección.

La categorización de activos de información proporciona una base sólida para la implementación de medidas de seguridad apropiadas, junto con la asignación de recursos de manera eficiente y la asignación de responsabilidades permite determinar el valor real de la información, así como su adecuada clasificación. Además, facilita una comprensión clara de los riesgos y amenazas potenciales que pueden afectar los activos de información, facilitando la toma de decisiones informadas y estratégicas en la protección de la información y sistemas.

En el análisis y gestión de riesgos asociados a los activos de información de la organización se aplicó la metodología MAGERIT. En esta etapa se determinó el riesgo potencial y la identificación y valoración de amenazas, se logró un mapeo detallado de los posibles eventos que podrían afectar negativamente a las cooperativas de trabajo asociado a través de las vulnerabilidades que puedan llegar a ser explotadas por las amenazas existentes, para reducir el impacto de estos riesgos potenciales se listaron las diferentes salvaguardas aplicables a los activos de información así mismo como los controles aplicables para reducir el valor de impacto de los riesgos mencionados.

Identificar las características particulares en materia de estructura organizacional de las cooperativas de trabajo asociado en materia de funcionamiento administrativo y financiero, permitió realizar la estructuración de un modelo de política de gestión de activos de información que abarque los elementos necesarios para cumplir con la protección adecuada de cada uno de

estos activos de información existentes en estas organizaciones solidarias, en el mencionado modelo se realiza una estructuración de los elementos necesarios para realizar una adecuada gestión de los activos de información a través de una cadena de procesos que inicia con la consolidación de la información existente con el fin de identificar elementos faltantes para complementar y cumplir con los requisitos necesarios para obtener un sistema de gestión de activos de información adecuado a las necesidades de estas organizaciones solidarias.

Recomendaciones

La categorización de activos de información es un paso esencial en la gestión de la seguridad de la información, ya que permite identificar y proteger de una forma adecuada los recursos de información que cuentan con gran valor para compañía u organización adicional a esto facilitar cumplir con los requerimientos normativos gubernamentales establecidos por los entes regulatorios existentes para la protección de datos e información de personas naturales y compañías, esta debe de trabajar en conjunto con una implementación efectiva de controles de seguridad y de una cultura de seguridad sólida en toda la organización.

Se deben crear políticas y procedimientos específicos de seguridad de la información, estas deben abordar aspectos como integridad, disponibilidad, autenticidad mediante controles de acceso, autenticación, gestión de contraseñas, auditoría y control de cambios.

Se deben definir actores responsables de la gestión y protección de cada categoría de activos de información. Esto incluye propietarios, custodios, usuarios, proveedores y stakeholders.

Realizar el análisis y evaluación de riesgos siguiendo la metodología MAGERIT 3, que puedan llegar a afectar a los activos fijos de la organización, permite mantener la información actualizada acerca de las amenazas existentes y de las medidas necesarias para reducir las vulnerabilidades presentes con el propósito de reducir el impacto potencial de los riesgos sobre los activos de información en las cooperativas de trabajo asociado ya que a través de una adecuada gestión de estos riesgos se pueden obtener resultados favorables en la efectividad de los procesos internos y procedimientos puntuales en estas organizaciones.

Tener presente que, al implementar las políticas de seguridad de la información para el manejo y administración de los activos de información en las cooperativas de trabajo asociado, es indispensable tener conocimiento de las particularidades que estas organizaciones poseen, dado

que pertenecen a un sector económico con estructura organizacional especial, que la diferencia de organizaciones del sector público y privado.

Referencias Bibliográficas

Acosta, F. (2024). *Managing the ServiceNow Platform: A comprehensive guide to ServiceNow administration*. BPB Publications. https://perlego.com/book/4308024/managing-the-servicenow-platform-a-comprehensive-guide-to-servicenow-administration-english-edition-pdf

Andrade Talero, D. L. (2021). *Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en MAGERIT v3 [Tesis de Especialización, Universidad Nacional Abierta y a Distancia].* Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/43373

Arango Jaramillo, M. (2024). *Manual de cooperativismo y economía solidaria*. Fondo Editorial – Ediciones Universidad Cooperativa *de Colombia.* https://www.perlego.com/es/book/4407511/manual-de-cooperativismo-y-economa-solidaria

Argüezo Ramírez, E. D. (2019). *Propuesta de un sistema de gestión de seguridad de información para la protección de activos de Información basado en la norma ISO 27001 en el área de informática de la Municipalidad Provincial De Huánuco* [Trabajo de suficiencia profesional, Universidad de Huánuco]. Repositorio Institucional UDH. http://repositorio.udh.edu.pe/handle/123456789/2084?show=full

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos. (2020). *Reporte de Ciberseguridad 2020 riesgos, avances y el camino a seguir en America Latina y el Caribe*. http://dx.doi.org/10.18235/0002513

Barquero Pastor, A. (2024). *Estudio comparativo entre OpenVas y Wazuh* [Trabajo de Fin de Grado, Universidad Politécnica de Cartagena]. Repositorio Digital UPCT. https://repositorio.upct.es/entities/publication/e9d5bb99-f1d1-49f4-833f-6c6aaf181335

Borrero Ochoa, P. C. (2018). *Identificación de Activos de Información, Riesgos y Controles Asociados Para la Empresa Estrategias Empresariales de Colombia Bajo la Norma ISO 27001 e ISO 31000* [Tesis de Especialización, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35641

Calder, A. (2017). *ISO27001/ISO27002: Una guía de bolsillo*. IT Governance Publishing. https://doi.org/10.2307/j.ctt1pwt92r

Calder, A. (2024). Nine steps to success: An ISO 27001:2022 implementation overview. IT Governance Publishing. https://perlego.com/book/4524898/nine-steps-to-success-an-iso-270012022-implementation-overview-pdf/?utm_medium=share&utm_source=perlego&utm_campaign=share-book

Cahyadi, A., & Arviansyah, A. (2021). RACI Matrix Design for Managing Stakeholders in Project (Case Study of PT XYZ). *International Journal of Science, Technology & Management*, *2*(5), 1475-1481. https://doi.org/10.46729/ijstm.v2i5.313

Cárdenas-Solano, L. J., Martínez-Ardila, H., & Becerra-Ardila, L. E. (2016). Gestión de seguridad de la información: revisión bibliográfica. *Profesional de la información*, *25*(6), 931-948. https://doi.org/10.3145/epi.2016.nov.10

Congreso de la República de Colombia. (2000, 14 de julio). *Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4275

Congreso de la República de Colombia. (2008, 31 de diciembre). *Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*.

Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2009, 5 de enero). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado «de la protección de la información y de los datos»- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Corporación CEPA. (2019). *Programa de educación solidaria con énfasis en trabajo asociado (Versión III).* AGM Salud c.t.a. https://agmsalud.com/Comunicados/T_Humano/2023/Cartilla_Educacion_Solidaria.pdf

Cortés, J. (2025). *Sistemas de gestión de seguridad de la información (ISO 27001:2022)*. Ediciones de la U. https://www.perlego.com/es/book/5169492/sistemas-de-gestin-de-seguridad-de-la-informacin-iso-270012022

Cuervo Álvarez, S. (2017). *Implementación ISO 27001* [Trabajo Fin Máster, Universitat Oberta de Catalunya]. O2 Repositori UOC. https://hdl.handle.net/10609/64827

Fernandez Climent, E. (2024). *ISO/IEC 27001:2022 paso a paso: Implementación, auditoría y mejora continua*. Amazon Digital Services. https://www.amazon.com/dp/B0CW1L78BB

Horta-Solano, A. (2018). *Las cooperativas de trabajo asociado como herramienta de subcontratación laboral* [Trabajo de grado de pregrado, Universidad Católica de Colombia].

Repositorio Institucional Universidad Católica de Colombia - RIUCaC. http://hdl.handle.net/10983/15913

International Organization for Standardization. (2017). Information technology — Security techniques — Information security management systems — Guidance (ISO/IEC Standard No. 27003:2017). https://www.iso.org/standard/63417.html

Kosutic, D. (2016). *ISO 27001 Annex A controls in plain English: A step-by-step handbook for information security practitioners in small businesses*. Advisera Expert Solutions Ltd. https://es.everand.com/book/367608539

Ministerio de Hacienda y Administraciones Públicas. (2012, octubre). *Magerit – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I - Método*. Gobierno de España. https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021, 10 de marzo). *Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*. MinTIC. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016). *Guía para la gestión y clasificación de activos de información (GUIA No. 5)*. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. https://gobiernodigital.mintic.gov.co/portal/715/articles-172093_recurso_1.pdf

Newmeyer, K. (2015). Ciberespacio, ciberseguridad y ciberguerra. *II Simposio Internacional de Seguridad y Defensa Perú 2015* (pp. 76-95). Publicaciones ESUP. https://repositorio.esup.edu.pe/bitstream/20.500.12927/113/1/pp.76-95.pdf

Organización Internacional de Normalización & Comisión Electrotécnica Internacional. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información (ISO/IEC 27002:2022)*. https://www.iso.org/standard/75652.html

Organización Internacional de Normalización & Comisión Electrotécnica Internacional. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos (ISO/IEC 27001:2022)*. https://www.iso.org/standard/75652.html

Presidencia de la República de Colombia. (1990, 23 de febrero). *Decreto 468 de 1990. Por el cual se reglamentan las normas correspondientes a las cooperativas de trabajo asociado contenidas en la Ley 79 de 1988 y se dictan otras disposiciones sobre el trabajo cooperativo asociado*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1328

Presidencia de la República de Colombia. (2004, 26 de enero). *Decreto 186 de 2004. (2004, 26 de enero). Por el cual se modifica la estructura la estructura de la Superintendencia de la Economía Solidaria*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49121

Presidencia de la República de Colombia. (2006, 27 de diciembre). *Decreto 4588 de 2006. Por el cual se reglamenta la organización y funcionamiento de las Cooperativas y Precooperativas de Trabajo Asociado*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=22659

Presidencia de la República de Colombia. (2018, 14 de junio). *Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902

Rea-Guaman, M., Calvo-Manzano, J. A., & Feliu, T. S. (2018, 13-16 de junio). A prototype to manage cybersecurity in small companies. *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-6. https://doi.org/10.23919/CISTI.2018.8399252

Sales Silva, F. (2023). *ISO 27001: Directrices para la aplicación independiente (Edición Kindle)*. Fabricio Sales Silva. https://www.amazon.com/-/es/Fabricio-Silva-ebook/dp/B0CNCZRVXH

Sevillano Jaén, F., & Beltrán Pardo, M. (2021). *Dirección de seguridad y gestión del ciberriesgo*. Ediciones de la U. https://es.everand.com/book/556060423/Direccion-de-seguridad-y-gestion-del-ciberriesgo

Soriano Cortés, D. (2021). Las cooperativas de trabajo asociado: una alternativa de trabajo digno, sostenible e inclusivo. *CIRIEC - España. Revista jurídica de economía social y cooperativa,* (38), 11-54. https://dialnet.unirioja.es/servlet/articulo?codigo=8009940

Suárez González, R. (2018). *Análisis de activos de información para un sistema misional basados en la metodología Magerit v3 y la norma ISO 27001:2013.* [[Tesis de especialización, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. http://repository.unad.edu.co/handle/10596/19571

Valencia Valderrama, A. (2019). *Diseño de políticas de seguridad informática basadas en la norma ISO 27001:2013 para instituciones prestadoras de servicios de salud – IPS del departamento del Chocó* [Monografía de especialización, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/36625

Wadhwani, R. R., K-Breukel, E., & Kamalanathan, S. (2024). *ISO/IEC 27001:2022 Control A Ologies*. One Point Six Technologies Pvt. Ltd. https://www.amazon.com/-/es/Rakhi-R-Wadhwani-ebook/dp/B0DH21X7XH#

Watkins, S. (2022). *ISO/IEC 27001:2022: An introduction to information security and the ISMS standard*. IT Governance Publishing. https://www.everand.com/book/607757959/ISO-IEC-27001-2022-An-introduction-to-information-security-and-the-ISMS-standard

Apéndices

Apéndice A

Inventarios Activos de Información - Tipo de Activo Hardware

Tipo de activo	Código del activo	Activo de información	Descripción del activo (Características)	Funciones principales	Cantidad
Hardware	HW-1	Servidor Físico - HP Proliant ML110 Gen 10.	Servidor Hewlet Packard Proliant ML110 Gen 10, ubicado encentro de datos.	Sistema de administración de Active Directory.	1
	HW-2	Servidor Físico - HP Proliant ML 350 Gen 10.	Servidor Hewlet Packard Proliant ML 350 Gen 10, ubicado en centro de datos.	Sistema de administración Bases de Datos Plataformas virtuales, sistema Novasoft.	1
	HW-3	Computadores Corporativos (20)	Marca Lenovo Think Centre M80s Windows 10 pro SSD 240 GB.	Equipos de escritorio de los funcionarios.	40
	HW-4	Computadores Corporativos (20)	Marca Dell Precision 3640 Windows 10 pro, SSD 240 GB.	Equipos de escritorio de los funcionarios.	20
	HW-5	Computador portátil (4)	Marca Lenovo Think Pad L 14 Windows 10 pro SSD 240 GB	Equipos portátiles para gerencias y sala de juntas.	4
	HW-6	Switches (3)	Marca Cisco Catalyst, 24 puertos, conector RJ45, 10/100/1000 Mbps Gigabit Ethernet	Equipo de interconexión de redes.	3

Tipo de activo	Código del activo	Activo de información	Descripción del activo (Características)	Funciones principales	Cantidad
Hardware	HW-7	Router Wifi	Marca TP-Link Archer C9 (AC19000).	Equipo de administración de red Wifi.	1
	HW-8	Access Point (2)	Marca TP-Link EAP 225.	Equipo para acceso a red Wifi.	2
	HW-9	Balanceador de Carga	Marca Fortinet – Forti ADC.	Distribución de trafico entrante de la red (CLARO-ETB)	1
	HW-10	Firewall Fortinet 50E.	Equipo de seguridad perimetral, seguridad Firewall, VPN. IPS, Antivirus, Anti-Spam, Filtrado web.	Realizar enrutamiento de la red, DHCP, seguridad perimetral, VPN acceso remoto).	1

Nota. Tipificación de activos de información de cooperativa de trabajo asociado tipo hardware.

Apéndice B

Inventarios Activos de Información - Tipo de Activo Información

Tipo de activo	Código del activo	Activo de información	Descripción del activo (Características)	Funciones principales	Cantidad
Información	INF-1	Documentación de procesos de desarrollo.	Instructivos, Manuales de procesos, Procedimientos, manuales de funciones.	Información sobre instructivos, procedimientos y manuales.	60
	INF-2	Código Fuente Novasoft Nomina.	Conjunto de sentencias y líneas de texto que constituyen la aplicación.	Conjunto de instrucciones para el funcionamiento del software de nómina.	1
	INF-3	Código Fuente Novasoft Contabilidad.	Conjunto de sentencias y líneas de texto que constituyen la aplicación.	Conjunto de instrucciones para el funcionamiento del software Financiero (contable, tesorería, presupuesto).	1
	INF- 4	Código Fuente Novasoft Tesorería.	Conjunto de sentencias y líneas de texto queconstituyen la aplicación.	Conjunto de instrucciones para el funcionamiento del software Financiero (contable, tesorería, presupuesto).	**1**
	INF-5	Código Fuente Software SARA Software De Nomina y gestión de recursos Humanos.	Conjunto de sentencias y líneas de texto queconstituyen la aplicación.	Conjunto de instrucciones para el funcionamiento del software SARA.	1
	INF-6	Código Fuente Software SOFIA Software gestión Administrativa y Financiera.	Conjunto de sentencias y líneas de texto queconstituyen la aplicación.	Conjunto de instrucciones para el funcionamiento del software SOFIA.	1
	INF-7	Aplicación AGMCTA Gestión documental.	Conjunto de sentencias y líneas de texto queconstituyen la aplicación	Conjunto de instrucciones para el funcionamiento del software gestión documental.	1

Tipo de activo	Código del activo	Activo de información	Descripción del activo (Características)	Funciones principales	Cantidad
Información	INF-8	Expedientes afiliación asociados.	Archivos en formato Word o PDF que incluyen detalles sobre documentos de vinculación y asociación a la cooperativa.	Conjunto documentos legales establecidos con asociados.	1500
	INF-9	Políticas de tratamiento de datos personales.	Archivo en formato Word o PDF que establece las directrices de la compañía para el manejo de información personal.	Conjunto de normas y directrices para la manipulación uso de los datos personales de los clientes.	1
	INF-10	Expedientes financieros.	Documentos formato Físico/Digital, carpetas con documentos financieros de la organización soportes de pago, facturas emitidas.	Documentos digitales y físicos donde se resguardan los documentos financieros que hacen parte de la historia contable de la organización.	20
	INF-11	Contratos Empresas clientes	Documentos contractuales en Word o PDF, legales con los cuales se soporta el vínculo empresarial con las empresas cliente.	Conjunto documentos legales establecidos como contrato de vinculo comercial con las empresas clientes.	10

Nota. Tipificación de activos de información de cooperativa de trabajo asociado tipo de activo información.

Apéndice C

Inventarios Activos de Información - Tipo de Infraestructura de Red

Tipo de activo	Código del activo	Activo de información	Descripción del activo (características)	Funciones principales	Cantidad
Infraestructura de red	RED-1	Canal de Internet Dedicado.	Canal internet, proveedor Claro, fibra óptica, 400 MB, ubicado en la sede.	Proporcionar a la red interna de la compañía conexión a Internet.	**1**
	RED-2	Canal de Internet Respaldo.	Canal internet fibra óptica, proveedor ETB, fibra óptica, 300 MB, ubicado en la sede.	Proporcionar a la red interna de la compañía conexión a Internet (conexión de respaldo).	**1**
	RED-3	Cableado de red.	Cableado de red Local conexiones físicas internas Categoría 6A.	Medio para establecer conexión física entre los nodos de red de la cooperativa.	**1**
	RED-4	Conexiones VPN client to site.	Conexiones para trabajo remoto OpenVPN, FortiClient.	Brindar acceso seguro remoto externo a la red local de la cooperativa.	**1**
	RED-5	Red inalámbrica corporativa.	Conexión Inalámbrica corporativa wifi	Brindar acceso inalámbrico a segmento de red local de la cooperativa.	1
	RED-6	Red inalámbrica Invitados.	Conexión Inalámbrica invitados wifi.	Brindar acceso inalámbrico a Internet externo a la red local a personas no hacen parte de la Cooperativa.	1

Nota. Tipificación de activos de información de cooperativa de trabajo asociado tipo de activo Infraestructura de red – Medios para transmisión de Datos.

Apéndice D

Inventarios Activos de Información - Tipo Recurso Humano

Tipo de activo	Código del activo	Activo de información	Descripción del activo (características)	Funciones principales	Cantidad
Recurso Humano	RH-1	Director Área TI.	Profesional ingeniero de sistemas, especializado en desarrollo gerencia TI.	Gerenciar el área de TI.	1
Recurso Humano	RH-2	Líder Base de datos, administración de red.	Ingeniero de Sistemas, con especialización en base de datos o seguridad informática.	Liderar los sistemas involucrados en las bases de datos de la organización.	1
Recurso Humano	RH-3	Líder soporte	Profesional, Ingeniero de sistemas.	Liderar el grupo de soporte técnico de la compañía.	1

Nota. Personal que, debido a su importancia en el proceso de gestión de activos de información, debe tipificarse como recurso humano.

Apéndice E

Inventarios Activos de Información - Tipo Software

Tipo de activo	Código del activo	Activo de información	Descripción del activo (Características)	Funciones principales	Cantidad
Software	SW-1	Solución Ofimática	Licencia Microsoft Office 365, Outlook, Word, Excel y PowerPoint.	Brindar acceso a Hojas de Cálculo, editor de Texto.	60
	SW-2	Aplicación Novasoft Nomina.	Aplicación gestión calculo nómina de empleados o funcionarios.	Brindar acceso a software e Nomina empleados.	1
	SW-3	Aplicación Novasoft contabilidad.	Aplicación servicios financieros internos, contabilidad, tesorería, presupuesto.	Software para procesos contables y financieros.	1
	SW-4	Aplicación Novasoft Nomina.	Aplicación servicios financieros internos, Nomina.	Software para procesos de Nomina.	1
	SW-5	Aplicación Novasoft Tesorería.	Aplicación servicios financieros Tesorería.	Software para procesos tesorería.	1
	SW-6	Aplicación SOFIA Gestión Financiera.	Aplicación gestión Financiera (contabilidad y tesorería).	Software para procesos gestión Financiera.	1
	SW-7	Aplicación SARA Gestión Talento Humano y Nomina.	Aplicación gestión Talento Humano y Nomina.	Software para procesos gestión Talento Humano.	1
	SW-8	Aplicación AGMCTA Gestión documental	Aplicación gestión documental carpetas de afiliación de asociados, empresas clientes y proveedores.	Software para procesos administración gestión documental.	1
	SW-9	Bases de Datos	MariaDB, Postgres.	Motor bases de datos software nomina, financiera, gestión talento humano, gestión documental.	1
	SW-10	Aplicaciones Móviles	Aplicaciones disponibles en la PlayStore (Android) y AppStore (iOS).	Acceso a clientes a plataforma organización.	1

Tipo de activo	Código del activo	Activo de información	Descripción del activo (Características)	Funciones principales	Cantidad
Software	SW-11	Certificados SSL Letsencritp	Certificados SSL Web para los diferentes portales corporativos y de servicios.	Protocolo de seguridad para establecer conexión con servidores WEB.	2
	SW-12	Dominio: agmsaludcta.com	Dominios de internet para las aplicaciones.	Dominios para portales de la compañía.	1
	SW-13	Sitio Corporativo: www.agmsaludcta.com	Sitio web corporativo	Página web para socialización de servicios de la cooperativa.	1
	SW-14	Servidores Virtuales	Servidores virtualizados por medio de VMware.	Hosting portales compañía.	2
	SW-15	Email office 365	Servicio de Correo electrónico corporativo, servicio SaaS.	Servicio correo electrónico funcionarios de la compañía.	100
	SW-16	OneDrive	Software de almacenamiento de archivos, utilizado como repositorio de información.	Servicio almacenamiento en la nube.	100
	SW-17	Kaspersky End Point	Antivirus instalado en terminales Windows.	Antivirus protección local terminales.	100
	SW-18	Servidores	Licencia Windows server 2012.	Licencias Servidores Active Directory.	2
	SW-19	Servidores	CentOs 8.	Licencias servidores bases de datos, hosting plataformas.	2

Nota. Activos de información que debido a su funcionalidad son tipificados como software.

Apéndice F

Asignación Criterios a Activos de Información Registrados

Código del Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Color
HW-1	3	3	3	9	Rojo
HW-2	3	3	3	9	Rojo
HW-3	3	3	2	8	Rojo
HW-4	3	3	2	8	Rojo
HW-5	3	3	3	9	Rojo
HW-6	3	3	3	9	Rojo
HW-7	3	3	2	8	Rojo
HW-8	3	3	3	9	Rojo
HW-9	3	3	3	9	Rojo
HW-10	3	3	3	9	Rojo
INF-1	3	3	3	9	Rojo
INF-2	3	3	2	8	Rojo
INF-3	3	3	3	9	Rojo
INF-4	3	3	3	9	Rojo
INF-5	3	3	3	9	Rojo
INF-6	3	3	3	9	Rojo
INF-7	1	3	3	7	Naranja
INF-8	2	3	2	7	Naranja
INF-9	3	3	2	8	Rojo
INF-10	3	3	3	9	Rojo
RED-1	3	3	3	9	Rojo
RED-2	3	3	1	7	Naranja
RED-3	3	3	3	9	Rojo
RED-4	1	3	3	9	Rojo
RED-5	3	3	2	8	Rojo
RED-6	3	3	1	7	Naranja
RH-1	3	3	3	9	Rojo
RH-2	3	3	9	9	Rojo
RH-3	3	3	3	9	Rojo
RH-4	3	3	3	9	Rojo
RH-5	3	3	3	9	Rojo
RH-6	3	3	3	9	Rojo
SW-1	3	3	3	9	Rojo
SW-2	3	3	3	9	Rojo
SW-3	3	3	3	9	Rojo
SW-4	3	3	3	9	Rojo
SW-5	3	3	3	9	Rojo
SW-6	3	3	3	9	Rojo
SW-7	3	3	3	9	Rojo
SW-8	3	3	3	9	Rojo
SW-9	3	3	3	9	Rojo
SW-10	3	3	3	9	Rojo
SW-11	3	3	3	9	Rojo
SW-12	3	3	3	9	Rojo

Código del Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Color
SW-13	3	3	3	9	Rojo
SW-14	3	3	3	9	Rojo
SW-15	3	3	3	9	Rojo
SW-16	3	3	3	9	Rojo
SW-17	3	3	3	9	Rojo
SW-18	3	3	3	9	Rojo
SW-19	3	3	3	9	Rojo

Nota. Calificación de criterios de confidencialidad, integridad y disponibilidad.