DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013

LUIS GERARDO ZAMBRANO GOMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2020

DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013

LUIS GERARDO ZAMBRANO GOMEZ

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

KATERINE MARCELES
Tutora de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pasto, 09 de enero de 2021

DEDICATORIA

El cumplimiento de esta meta la dedico inicialmente a Dios quien me sirve de guía y me llena de sabiduría para tomar las decisiones más acertadas y que me han llevado a tener una vida plena y llena de triunfos, también cabe mencionar a mi madre y mi padre quien con su dedicación y esfuerzo día a día me dieron los mejores consejos, ánimos y ayuda económica para poderme realizarme como profesional, quienes son una fuente constante de inspiración que me motiva cada día dar todo mi esfuerzo y poder retribuir su ayuda.

A mi hermana que dentro del núcleo familiar me brinda su apoyo, su comprensión y su valioso tiempo para apoyarme en las actividades que en su momento fueron obstáculo, pero que gracias a su conocimiento y experiencia se pudieron solucionar de la mejor manera.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACTIVO: elemento físico o lógico que tiene valor para la empresa.

AMENAZA: acción negativa el cual puede alterar o destruir algún activo.

ATAQUE: acción negativa de forma intencionada.

CAUSA: es el origen del riesgo.

CONFIDENCIALIDAD: es un pilar de la información donde esta será segura en cuanto a que no será divulgada sin consentimiento.

IMPACTO: daño que genera una amenaza a un activo de información.

INTEGRIDAD: pilar de la información donde esta estará completa y exacta.

INGENIERÍA SOCIAL: estrategia de un atacante con el fin de engañar a los usuarios para que realicen acciones indebidas.

ISO27001: norma internacional la cual permite gestionar la seguridad de la información.

MAGERIT: metodología que permite el análisis y la gestión de los riesgos de los sistemas informáticos.

RIESGO: probabilidad de que los activos de información reciban algún impacto negativo de una amenaza.

VULNERABILIDAD: debilidad o puntos frágiles que tienen los activos de información.

RESUMEN

Hoy en día, toda organización debe asegurar que los activos de información cuenten con un sistema aceptable de seguridad, con el fin de salvaguardar la información que se procesa y se almacena en estos, dado que, actualmente estos archivos son indispensables a nivel empresarial.

En este sentido, a través de la construcción de un sistema de gestión de seguridad de la información, se aporta a la empresa Cooperativa Multiactiva de Centrales Eléctricas de Nariño con el fin de que sean parte del cambio y que por medio del diseño e implementación de un SGSI puedan asegurar la integridad, confidencialidad y disponibilidad de sus datos.

Para el desarrollo del diseño del SGSI se tomó en cuenta los parámetros de la norma ISO/IEC 27001:2013 y de la metodología MAGERIT, siendo esta última la que permitió identificar los activos de información, valorarlos, identificar sus amenazas y valorar su impacto y sus riesgos, a partir de esta información se realizaron algunas recomendaciones con el fin de que los funcionarios de la empresa implementen políticas frente a su sistema de gestión de seguridad lo que les permitirá tener control sobre sus activos.

PALABRAS CLAVE: Integridad, Disponibilidad, Confidencialidad, ISO 27001, amenazas, riesgos, políticas, vulnerabilidad, controles, activos.

INTRODUCCIÓN

Actualmente la competencia entre empresas es mayor, los nuevos desafíos que se enfrentan son múltiples, motivo por el cual, la empresa que esté más preparada ante estas nuevas circunstancias, tendrá ventajas en el mercado, algunas empresas con el fin de obtener y estar un paso adelante se han valido de las tecnologías de la información y comunicación (TIC) con el propósito de implementar herramientas que les permitan manejar sus operaciones de forma más eficazmente, dichas mejoras empresariales traen grandes beneficios, algunos de estos son: almacenamiento y procesamiento de gran cantidad de información, automatización de procesos, comercio electrónico, relaciones sociales a nivel mundial bajo redes sociales, entre otros.

Estos cambios no solo traen una nueva forma de vida, también traen consigo múltiples problemas y, sobre todo, cuando se refiere a la seguridad de la información que se maneja, procesa y almacena bajo los diferentes medios tecnológicos, de tal manera que las empresas deben estar conscientes de que continuamente están expuestas a múltiples amenazas y riesgos, vulnerando la confidencialidad, integridad y disponibilidad de la información; es por este motivo, que se han estructurado herramientas para gestionar y asegurar la información mediante procesos y pasos definidos, este proceso se conoce como Sistema de Seguridad de la Información SGSI, como afirma Neira [1], un SGSI contiene unas políticas y directrices que junto con el apoyo financiero para ejecutarlas, conllevan a una organización a proteger sus activos de información la , en este caso, cabe resaltar que la presente investigación se basó bajo la norma internacional ISO/IEC 27001, la cual, permite establecer un enfoque integral mejorando la seguridad de la información.

El SGSI es una herramienta fundamental para asegurar y proteger los datos y los activos de información asociados a estos. El desarrollo de este proyecto estará basado en la implementación de un Sistema de Seguridad de la Información bajo la norma ISO 27001:2013 el cual brindará pautas, buenas prácticas y procedimientos adecuados para la empresa Cooperativa Multiactiva De Centrales Eléctricas De Nariño (COOPCEN).

La implementación del SGSI en COOPCEN surgió como una necesidad, dado que, la empresa ha crecido exponencialmente, por lo cual, el volumen de información que se maneja en las diferentes áreas es mayor, de esta manera el SGSI permitió protegerla bajo ciertos controles y políticas, lo que significa la utilización de normas y buenas rutinas con el fin de asegurar el buen manejo de la información.

[1] NEIRA, Agustín y SPOHR, Javier. ISO27000.es. “International Organization For Standardization Iso27000”. [online] [citado abril 2020]. Disponible en internet: http://www.iso27000.es.

Por último, bajo el SGSI en COOPCEN, se dieron los primeros pasos y las primeras evaluaciones que valoraron la importancia de la información y cómo ésta juega un papel fundamental en los diferentes procesos de la empresa; así mismo, se concientizó a través de la divulgación del presente proyecto a las directivas y personal sobre el manejo de las diferentes tecnólogas de información y comunicación con el fin de que los diferentes controles que establece la Norma ISO 27001:2013 sean efectivos a la hora de asegurar la confidencialidad, integridad y disponibilidad de la información.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

Las nuevas tecnologías de la información y comunicación presentes en las instituciones, compañías, organizaciones y cooperativas de cualquier sector económico permiten competir en el mercado actual, apoyando de esta manera al crecimiento empresarial, a partir de la innovación tecnológica.

La implementación de nuevas tecnologías en el ámbito organizacional, conllevan a un reto fundamental, el cual, es estar preparado ante cualquier riesgo o amenaza que comprometa los activos de información y la continuidad del negocio, según Pérez [2]: Los cambios constantes de las tecnologías han llevado a un desafío a las organizaciones, el cual es garantizar la seguridad de los activos de las diferentes amenazas, por esta razón es que un SGSI basado en normas internacionales permite generar políticas, procedimientos y responsabilidades que se ajustan a las necesidades de cada organización.

Ahora bien, proteger la información y los activos de comunicación presentes en la Cooperativa Multiactiva De Centrales Eléctricas De Nariño, se ha convertido en un requisito indispensable, debido a que durante el largo tiempo de actividad económica no se ha realizado ningún estudio que determine la capacidad de la organización para enfrentar situaciones como: perdida de información física y/o digital, amenazas internas o externas que puedan comprometer la continuidad del negocio.

Actualmente, la Cooperativa Multiactiva De Centrales Eléctricas De Nariño, posee una infraestructura tecnológica que no ha sufrido cambios ni adecuaciones periódicas, esto ha conllevado a la empresa a enfrentar fallos en los elementos tecnológicos lo que ha ocasionado que la continuidad del negocio se vea afectada.

La Cooperativa Multiactiva De Centrales Eléctricas De Nariño no posee una política de seguridad de la información que le permita controlar sus activos, políticas donde se involucre tecnologías que procesen, capturen y almacenen información, lo cual les proporcionaría minimizar los riesgos que afecten la disponibilidad, confidencialidad e integridad de la información.

Por otra parte, el desconocimiento del personal, junto con la ausencia de políticas y controles, generan un escenario donde los elementos tecnológicos con que cuenta

[2] PEREZ, Andrés y GONZÁLEZ, Omar. Diseño Del Sistema De Gestión De Seguridad De La Información - Sgsi- Para Los Procesos Críticos De La Cooperativa Febor Basado En La Norma Iso 27001:2013. [online]. Trabajo de grado. Bogotá. UNAD. Facultad De Ingeniería. 2019. 20 p. [citado abril 2020]. Disponible en internet:http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6433/SGSI%20-%20FEBOR%20-20Trabajo%20de%20Grado.pdf?sequence= 2&isAllowed=y.

la organización estén expuestos a las diferentes amenazas conllevando a una parálisis de los procesos que día a día se desarrollan en la Cooperativa.

1.2 FORMULACIÓN DEL PROBLEMA

Hoy en día las organizaciones tienen una relación amplia con las nuevas tecnologías de la información y comunicación, las cuales soportan los procesos misionales; de igual forma, almacenan y procesan información de vital importancia. No obstante, se encontró que la empresa Cooperativa Multiactiva De Centrales Eléctricas De Nariño dentro de sus planes de mejora continua, no tiene en cuenta la protección tanto de la información como de los activos que interactúan con esta.

La Cooperativa en sus procesos de afiliación, crédito financiero, ingreso de fondos, afiliaciones y gestión tecnológica los cuales se soportan bajo el uso de tecnologías tanto hardware y software, no ha generado aun un panorama de amenazas que permita determinar los diferentes controles y los que sean más adecuados que garanticen la eliminación o mitigación del impacto al desarrollo normal de los procesos. En este sentido, al no existir normas, lineamientos y políticas de seguridad de la información, la Cooperativa Multiactiva De Centrales Eléctricas De Nariño se expone constantemente a diferentes amenazas que impliquen perdida de información y retraso del funcionamiento de los procesos, afectando la calidad del servicio.

Teniendo en cuenta lo anterior, el desarrollo del proyecto se basó en dar respuesta al siguiente interrogante, ¿Cómo el diseño de un sistema de gestión de seguridad de la información basado en las normas ISO 27001 versión 2013, permitirá establecer políticas y controles de seguridad adecuados para salvaguardar la integridad, disponibilidad y confidencialidad de la información en la Cooperativa Multiactiva De Centrales Eléctricas De Nariño?

2. JUSTIFICACIÓN

Hoy en día en las empresas y organizaciones se hace necesario contar con un plan o estrategia esquematizado, en el que se especifique cuál es el plan de acción para proteger la información, un plan que incluya políticas y controles especiales, que permita minimizar los riesgos que puedan derivar a una potencial amenaza.

Los riesgos de índole ambiental o los causados por la indebida manipulación de las tecnologías presentes en la cooperativa sea de forma premeditada o sin alguna intensión, son algunas de las fuentes que ponen en riesgo la continuidad del negocio; de tal forma que, un SGSI en el que se especifiquen políticas y controles que logren mantener la confidencialidad, integridad y disponibilidad de la información, permitirá a los agentes empresariales tanto de la gerencia como de los demás miembros les resulte más fácil actuar frente a cualquier evento fortuito que afecte la continuidad de la empresa, dado que, contarán con herramientas para actuar frente a las amenazas.

Igualmente, cabe resaltar que un sistema de gestión de seguridad de la información para la Cooperativa Multiactiva de Centrales Eléctricas de Nariño (COOPCEN) ayuda a reconocer los recursos tecnológicos presentes, los cuales, permiten el continuo movimiento de información teniendo en cuenta, cada uno de los procesos que desarrollen las diferentes áreas empresariales; además de identificar riesgos asociados a cada activo.

En consecuencia, el sistema genera confianza entre sus asociados a la hora de ofrecer los servicios, dado que, cumple con las normas internacionales, por lo tanto, cada cliente tendrá la plena seguridad de que los datos suministrados cuentan con parámetros claros de seguridad y confidencialidad, cumpliendo la legislación colombiana vigente de protección de datos personales.

El diseñar el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013, generará sólidos lineamientos a las exigencias de seguridad, lo que conllevará a COOPCEN a mejorar la imagen, mejorar la competitividad y generar confianza entre sus posibles y futuros clientes.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad (SGSI) de la Información para la Cooperativa Multiactiva de Centrales Eléctricas de Nariño. (COOPCEN), basado en la norma ISO/IEC 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

Identificar los activos de información que están presenten en la Cooperativa Multiactiva de Centrales Eléctricas de Nariño. (COOPCEN), con el fin de determinar los dominios aplicables para el diseño del SGSI.

Identificar las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos de información que afecten la continuidad del negocio.

Establecer controles necesarios, de acuerdo a la norma ISO/IEC 27001:2013 que permita garantizar la disponibilidad, confidencialidad e integridad de la información.

Establecer políticas de seguridad de la información aplicables a COOPCEN que permitan mitigar los riesgos identificados.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

Para el desarrollo de este proyecto fue necesario indagar fuentes bibliográficas, sobre todo proyectos que tienen relación con la implementación de un sistema de gestión de seguridad de la información basados en la norma ISO 27001:2013 y que concuerden con la afinidad del proyecto a ser llevado y aplicado a una cooperativa de ahorro.

Dentro de las referencias que se mencionaran a continuación, todas concuerdan en que la necesidad de crear un SGSI es lograr salvaguardar los activos de información, permitiendo tener confidencialidad, integridad y disponibilidad de la información, bajo políticas y mecanismos propios de la Norma ISO 27001:2013 como lo afirma José Higinio Ruiz Peña en su trabajo investigativo, desarrollado en el año 2018:

"Un eficiente SGSI, conformado por políticas, procedimientos y mecanismos que permitan salvaguardar la información y mantener la confidencialidad, integridad, disponibilidad, autenticidad, autorización y el no repudio de la misma, es lo que necesita una organización con un direccionamiento estratégico como el de COOPSENA, para llevar a cabo sus operaciones de manera continua, a pesar de las anomalías, fallas técnicas o eventos naturales fortuitos que puedan presentarse en un momento dado."[3]

Este proyecto denominado DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTA, brinda una visión y permite obtener criterios del proceso a seguir para la implementación del SGSI con el fin de conocer los riesgos, detectarlos y minimizar las amenazas.

Según el documento anteriormente mencionado la realización de la investigación pretende abordar la situación actual de la cooperativa con relación a la seguridad de la información; mediante la observación y entrevistas se obtendrán información la cual permitirá brindar un panorama del estado actual referente a seguridad informática, de tal manera que el objetivo que se lleva a cabo en este proyecto está muy relacionado con el objetivo de la investigación descrita.

Otro referente que se identificó y que está estrechamente relacionado con los objetivos de este proyecto, es el proyecto de grado denominado: DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA PEÑALOSA CÍA.

[3] PEÑA, Jose. Diseño De Un Sistema De Gestión De Seguridad De La Información (Sgsi) Bajo La Norma Iso/Iec 27001:2013, En La Cooperativa Multiactiva Del Personal Del Sena, En Bogotá. [online]. Trabajo de grado. Bogotá. UNAD. escuela de ciencias básicas, tecnología e ingeniería. 2018. 29 p. [citado abril 2020]. Disponible en internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17300/1/80267 708.pdf

S.A.S. SEDE PRINCIPAL CÚCUTA, realizado por JOHANNA CAROLINA ARARAT MUÑOZ quien se enfoca en un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, con el cual, pretendía mejorar la seguridad de la información mediante controles que mitiguen los riesgos humanos, físicos, lógicos, ambientales; esto lo logró, bajo la utilización de la metodología MAGERIT la cual permitió realizar un análisis de los riesgos y amenazas a los que se exponen los activos de información de la empresa.

También se abordó el proyecto denominado DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA GED (GESTION ESTRATEGIA Y DESARROLLO) DE LA CIUDAD DE BOGOTA, elaborado en el año 2017 por la autora LINA PATRICIA MENDOZA PENAGOS, en el cual especifica que el SGSI permite desarrollar una evaluación inicial, que identifique los riesgos y el impacto que genera, si se produjera; la identificación de los riesgos se realiza bajo la metodología MAGERIT, para finalmente brindar una respectiva retroalimentación y recomendaciones a la gerencia sobre los controles necesarios a implementar para evitar la violación de la integridad, disponibilidad y confidencialidad de la información.

Cabe mencionar también el proyecto denominado DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS ASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013, desarrollada por el autor LUIS CARLOS DIAZ RICARDO en el año 2017, el cual, describe lo siguiente acerca de la implementación del SGSI:

> Para poder llevar a cabo el diseño de un SGSI, es necesario tener pleno conocimiento de los bienes que posee una empresa y los riesgos a los cuales están expuestos, para llevar a cabo este proceso es necesario la implementación de una metodología que establezca las pautas para tal fin, en este caso será utilizada Magerit, la cual se centra en tres fases, la planeación, el análisis de riesgo y el tratamiento del riesgo, con ello se logra obtener una idea clara de los riesgos y además se definen salvaguardas para ser utilizados en caso de presentarse uno de ellos.[4]

La anterior referencia cuenta con una de las características que aborda el presente proyecto y que es la utilización de la metodología MAGERIT, la cual servirá de herramienta para dar un análisis detallado de los activos de información y clasificación de los tipos de amenazas presentes en estos.

[4] DIAZ, Luis. Diseño De Un Sistema De Gestión De La Seguridad De La Información En La Ips Assalud De Corozal Sucre, Mediante La Implementación De La Metodología MAGERIT (V3.0) Y La Norma Iso 27001:2013. [online]. Trabajo de grado. Sucre. UNAD. escuela de ciencias básicas, tecnología e ingeniería. 2017. 12 p. [citado abril 2020]. Disponible en internet:https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14386/5/1066172091.pdf

4.2. MARCO TEORICO

4.2.1 Sistema De Gestión De Seguridad De La Información (SGSI). Como la información es un activo, el cual todas las empresas u organizaciones procesan, transforman y almacenan con el fin de generar un análisis y de ahí extraer reportes que permitan tomar decisiones estratégicas frente al crecimiento de esta, se hace necesario protegerla; por lo tanto, se convierte este activo en un insumo de gran valor, el cual requiere algunos cuidados especiales y aún más, cuando la información pertenece a un tercero, motivo por el cual, dicha protección requiere estar basada bajo la normatividad vigente internacional, que conlleve a la disponibilidad, integridad y confidencialidad de la información.

Es de gran importancia contar con la planificación, diseño y puesta en marcha de un sistema de seguridad de la información; un sistema, que permita identificar amenazas, vulnerabilidades y riesgos en los pueden estar expuestos los activos de información, esto con el fin de generar controles y políticas que permitan garantizar el cumplimiento de diversas actividades que las organizaciones o empresas realicen, sin poner en riesgo los activos de información.

"Por tanto, un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales." [5]

EL sistema de gestión de la seguridad de la información está conformado por normas, en las cuales, se especifican las prácticas que durante el trascurrir de los años han dado buenos resultados en las organizaciones y empresas a la hora de mejorar la seguridad de sus activos de información y que, bajo la implementación de medidas a nivel físico y lógico permitan prevenir y detectar amenazas garantizando la continuidad del negocio.

El sistema de seguridad de información se basa en la gestión de la información, la cual garantiza:

- Confidencialidad: "La confidencialidad se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados" [6]

  Esto quiere decir, que todo tipo de información con la que cuente una empresa u organización no tiene que ser divulgada a un tercero que no cuente con plena autorización, dado que, cierta información puede ser

[5] NEIRA, op. cit, p.12

[6] PMG SSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información [blog]. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? 06 junio de 2017. [citado abril 2020]. Disponible en internet: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion

manipulada y utilizada para causar algún tipo de ataque empresarial que pueda perjudicar la continuidad del negocio.

- Integridad: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización, que la información con la que se cuenta es válida y consistente. Este objetivo es muy importante cuando se está realizando trámites bancarios por Internet, dado que, toda empresa deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito, bajo esta cualidad se garantiza que la información se encuentre exacta, sin modificaciones inapropiadas.

.

- Disponibilidad: cuando se requiera utilizar la información y los elementos que interactúan con esta, se espera que no exista algún problema de acceso, siempre y cuando exista la autorización pertinente, como afirma Fernández [7]; Por ser la información uno de los principales activos de las organizaciones, deberá protegerse mediante la implementación, mejora y mantenimiento constante de controles que brinden seguridad en cuanto a que la información deberá estar disponible a los usuarios que estén autorizados para su uso, permitiendo garantizar el cumplimiento legal y el logro de los objetivos del negocio.

4.2.2 ISO/IEC 27001. Esta norma nace como necesidad de preservar la seguridad de la información, la cual es una entrada y salidas de los diferentes procesos de las organizaciones.

"ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2."[8]

Esta norma abarca los requerimientos necesarios que se deben tener en cuenta en el SGSI, la cual contiene los objetivos de cada dominio que la integra, dichos dominios contendrán controles que serán necesarios para dar cumplimiento a la norma, los dominios que estructuran la norma son:

- Políticas de Seguridad de la Información
- Organización de la Seguridad de la Información
- Seguridad relativa a los recursos humanos
- Gestión de activos

[7] FERNANDEZ, Carlos. La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información. [online]. Garantía de Confidencialidad, Integridad y Disponibilidad de la información. Septiembre 2012. 41 p. [citado abril 2020]. Disponible en internet: https://www.pmg-ssi.com/wp-content/uploads/2013/12/ISO-27001-ISOTools.pdf

[8] ADVISERA EXPERT SOLUTIONS Ltda. ¿Qué es norma ISO27001? [sitio web]. Una introducción a los conceptos básicos. [citado abril 2020]. Disponible en internet: https://advisera.com/27001academy/es/que-es-iso-27001/

- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisiciones desarrollo y mantenimiento de los sistemas de información
- Relación de proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad de negocio
- Cumplimiento

Para Russel [9], como la información es esencial para los procesos y operaciones de las organizaciones se vuelve fundamental contar con un SGSI bien estructurado que permita gestionar los riesgos para que de esta forma la alta gerencia tenga la tranquilidad de que su negocio está actuando bajo lo legal y que una interrupción de las operaciones es muy mínima.

La norma es aplicable para cualquier tipo de organización sin importar el tamaño ni su tipo de actividad comercial, con la aplicabilidad de esta se puede lograr obtener una certificación, lo que permite generar un grado de confianza a los clientes, proveedores, gerencia y recursos humanos en el tratamiento de los datos y los activos que procesan, trasforman y almacena la información en una empresa u organización.

4.2.3 Ciclo Deming En La Norma ISO/IEC 27001:2013. La norma ha establecido que siempre se parte de un estado inicial en la implementación de un SGSI y que bajo este estado se evoluciona y genera una mejora continua, bajo fases que, agrupadas, se denominan el modelo PDCA o conocido como el ciclo Deming.

"El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (Plan-Do-Check-Act, de sus siglas en inglés), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización."[10]

En esta fase inicial se planifica el SGSI, aquí se establecen los objetivos, el inventario de activos de información y también se selecciona la metodología de riesgo que mejor se adapte al plan, con la cual se medirá el nivel de riesgo de los diferentes activos de información.

---

[9] RUSEEl, Julián. ISO 27001:2013 guía de implementación para la seguridad de la información [online]. 5 p. [citado abril 2020]. Disponible en internet: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

[10] ANA, Andrés y Gómez, Luis. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes [online]. 2009. 14 p. [citado abril 2020]. Disponible en internet: http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf

Hacer: Mediante los controles seleccionados, los cuales, servirán para mitigar las amenazas se da inicio a la implementación del SGSI, donde además se relaciona los responsables.

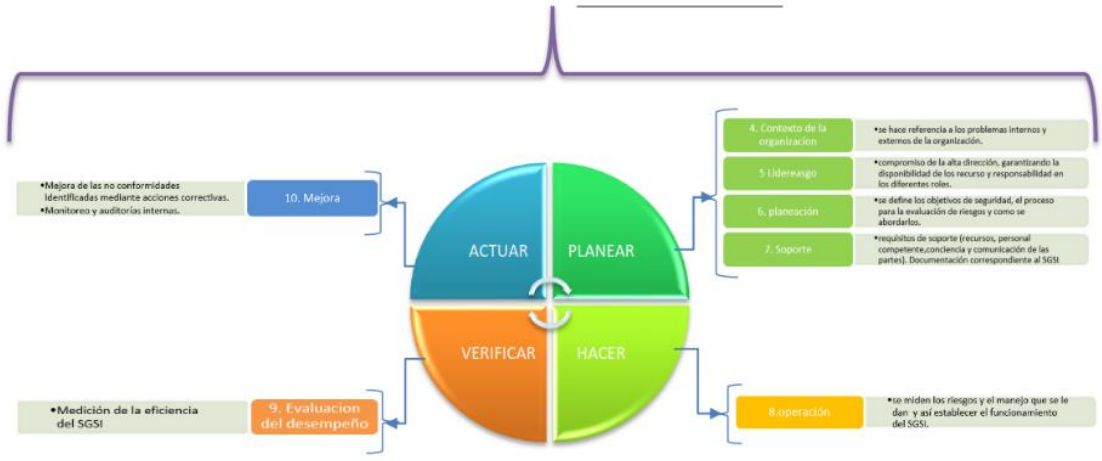
Verificar: Durante este proceso se realizan las revisiones pertinentes para verificar que se cumpla con los objetivos del SGSI, de esta manera, será posible la detección de errores para generar soluciones pertinentes que den continuidad al sistema.

Actuar: En este paso se pretende mejorar cualquier falta de conformidad en la norma ISO 27001 esta tendrá que ser solucionada de inmediato, todas las mejoras en los servicios que ofrece la entidad u organización deben ser revisadas, registradas y autorizadas. Para controlar dicha actividad se dispone de diferentes auditorías internas que permiten detectar la evaluación y gestión de todas las actividades de mejora.

> "En resumen, en la primera fase Planear se establecen las actividades que se van a mejorar y los objetivos a alcanzar. En la segunda etapa Hacer, se ejecuta lo establecido, es decir implementar lo propuesto. En la tercera etapa Verificar, se prueba lo implementado por un plazo de tiempo para verificar su funcionamiento óptimo. Si lo propuesto no cumple lo planteado inicialmente entonces se tiene que variar para ajustarlo a los objetivos establecidos. Por último, en la última etapa Actuar, al finalizar el plazo de prueba se estudia lo obtenido, es decir la situación final, y se compara con la situación inicial de las actividades."[11]

En la figura 1 se relaciona la estructura de la norma ISO/IEC 27001 con el modelo DEMING.

Figura 1. Modelo DEMING



Fuente: El autor

[11] BERNAL, Jorge. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua [online]. Agosto 23 2013. [citado abril 2020]. Disponible en internet: https://www.pdcahome.com/5202/ciclo-pdca/

4.2.4 Metodologías De Gestión De Riesgos. En la actualidad, existen varias metodologías que permiten determinar el nivel de seguridad, calcular los riesgos de los activos identificados, evaluar el impacto cuando existan casos de violación de la seguridad y detallar las vulnerabilidades y amenazas presentes en los procesos donde se involucre información importante para las organizaciones.

La gestión de riesgos permite generar medidas que deben adoptarse con el objetivo de prevenir y reducir los riesgos identificados; de tal manera que, la identificación de estos se logra bajo metodologías que ayudan a realizar el análisis correspondiente, abarcando los activos de información presentes en la organización.

Entre las metodologías de gestión de riesgo se encuentran:

METODOLOGÍA MAGERIT

Actualmente, esta metodología está bien documentada, su característica principal es que divide los activos de información en diferentes grupos, con el fin de abarcar riesgos en cada uno de estos; esta se conforma por las siguientes etapas:

- Planificación.
- Análisis de Riesgos.
- Gestión de los Riesgos.
- Selección de Salvaguardas.

"MAGERIT consiste en un método sistemático para el análisis y gestión de los Riesgos que derivan del uso de la información. Su fin es informar de los riesgos y de la necesidad de gestionarlos a los responsables de la actividad, así como ayudar a encontrar y planificar un plan adecuado para tratarlos. Su herramienta para aplicar esta metodología se llama Pilar "Procedimiento Informático-Lógico para el Análisis de Riesgos."[12]

La utilidad de esta metodología se basa en que es aplicable a empresas que están iniciando con el desarrollo e implementación de un SGSI, ya que permite centrase en los riesgos que puedan ser los causantes de una interrupción del negocio. Otro punto clave de esta metodología, es que está alineado a la norma ISO/IEC 27001 de tal manera que no habrá problemas al querer obtener una certificación internacional.

OCTAVE

"Es una técnica efectiva de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en Carnegie Mellon University. Octave es un conjunto de herramientas, técnicas y métodos para la

[12] BARTOLOME, Iván. Análisis de MAGERIT y Pilar [online]. Julio 2019. 7 p. [citado abril 2020]. Disponible en internet: http://uvadoc.uva.es/bitstream/handle/10324/37736/TFG-I-1213.pdf?sequence=1&isAllowed=y

evaluación del riesgo. Tiene en cuenta también la definición de los activos incluyendo: personas, hardware, software, información y sistemas."[13]

Dentro de las características principales de esta metodología es que involucra al personal en la concientización sobre cuidar los activos relacionados con la información; esta metodología está constituida por 3 atapas:

- Generar perfiles de amenazas basadas en los activos.
- identificar posibles vulnerabilidades de la infraestructura.
- Desarrollar estrategias y planes de seguridad.

MEHARI

La metodología MEHARI se desarrolló por un club Francés dedicado a la seguridad de la información, sus inicios datan del año 1996, esta metodología se basa en crear un análisis de riesgo de forma individual, de tal forma que se genera un panorama de todos los tipos de riesgos dentro de una organización para realizar un análisis en cada escenario y así ejecutar y tomar decisiones para cada situación.

Esta metodología se acopla a los requerimientos de la norma ISO/IEC 27005:2008, la utilización de esta provee un conjunto de herramientas que están diseñadas para gestionar la seguridad a mediano, corto y largo plazo, para GALLARDO, María y JÁCOME, Paúl [14], la metodología es un gran apoyo al personal que está al frente de la responsabilidad de la seguridad informática, mediante el análisis de situaciones de riesgo, la cual, deberá arrojar una evaluación cuantitativa; MEHARI estará articulada al contexto de la organización acoplando los objetivos estratégicos, la metodología permite generar políticas de seguridad y controles para mantener los riesgos a un nivel aceptable.

Para la metodología MEHARI existen unos riesgos que pueden presentarse en una organización por factores como:

- Estructurales u organizativos que depende mucho de las actividades de la organización, su contexto y entrono.
- Factores de reducción del riesgo lo que conllevan a que, si se selecciona unas medidas inadecuadas, el riesgo puede presentarse con más severidad.

Las fases que componen la metodología MEHARI son las siguientes:

- Fase preparatoria: donde se recogen datos de la estructura de la

[13] VANEGAS, Gonzalo y PARDO, Cesar. Hacia un modelo para la gestión de riesgos de TI en Mi Pymes: MOGRIT [online]. Septiembre 16 2014. 38 p. [citado abril 2020]. Disponible en internet: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/view/1860/2398

[14] GALLARDO, María y JÁCOME, Paúl. Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctricas Quito S.A. Quito. 2011. P. 18.

organización, del contexto donde se abordarán los riesgos necesarios para el posterior análisis y tratamiento; aquí se establecen los límites y el alcance técnico.

- Fase operacional: en esta fase se analiza la operatividad de la organización, con el fin de concluir que está funcionando mal en unas u otras actividades para evaluar la gravedad del mal funcionamiento, con esto se puede proseguir a los activos relacionados del análisis anterior.

- Fase de tratamiento del riesgo y planificación: en este punto se determina la forma más adecuada de tratar los riesgos y que sea acorde con la organización.

ISO/IEC 27005

Este estándar internacional se da a conocer en julio del 2008, el cual contiene unas guías que permiten a las organizaciones gestionar los riesgos de seguridad de la información. Esta norma, está alineada a la norma ISO/IEC 27001, según NAVARRO, Judith[15], la norma ISO/IEC 27005 se acomoda a cualquier tipo de organización que esté motivada a generar el panorama de riesgos y poder gestionarlos a tiempo evitando complicaciones futuras en la seguridad de la información; esta norma, permite detectar y categorizar los riesgos con el fin de brindarles el control y manejo respectivo y, como consiguiente, brindar el seguimiento continuo a través de una valoración cuantitativa y cualitativa.

El proceso de gestión de riesgo según ISO/IEC 27005 se basa en los siguientes pasos:

- Establecer el contexto, conocer plenamente la organización y definir el alcance
- Análisis y evaluación de riesgo, donde se identifican los riesgos y se genera acciones para reducirlos.
- Tratamiento del riesgo, se definen controles los cuales estarán basados bajo la norma ISO/IEC 27001.
- Aceptación del riesgo, se clasifican los riesgos residuales los cuales son los que por alguna razón no serán tratados generando su justificación de la aceptación de este riesgo.
- Comunicación del riesgo, se da a conocer a las diferentes áreas la forma de cómo se llevará el tratamiento de los riesgos.
- Seguimiento y análisis, se realiza un mejoramiento continuo dependido de los resultados que se obtengan de la implementación de los diferentes controles.

[15] NAVARRO, Judith. Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI. 2019. P. 16.

4.3. MARCO CONCEPTUAL

4.3.1 Vulnerabilidad: son los puntos débiles que pueda tener un activo de información, que permita el ingreso de amenazas, estas debilidades pueden desarrollarse por una incorrecta configuración, instalación.

4.3.2 Amenaza: en el contexto de la informática, una amenaza es todo aquello que pone en riesgo la integridad, confidencialidad y disponibilidad de la información, dentro de las amenazas se puede mencionar incendios, inundaciones, asonadas, disturbios y delincuencia.

4.3.3 Activo: son aquellos elementos que tienen valor para las empresas, ya que de estos depende el funcionamiento, entre los activos se tiene recursos tecnológicos, humanos y físicos.

4.3.4 Ataque: es el método por el cual se intenta expones o alterar los sistemas de información con el fin de tener el control de estos sin alguna autorización, los ataques aprovechas las falencias o vulnerabilidades de los activos de información.

4.3.5 Política: son normas o lineamientos que proponen las empresas o instituciones con el fin de prevenir las amenazas, estas políticas normalmente son rigurosas y deben ser puestas en práctica por el personal.

"Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes datos, sin importar el origen de estos."[16]

4.3.6 Impacto: nivel de afectación en los activos cuando existe una amenaza aprovechándose de una vulnerabilidad.

4.3.7 Riesgo: es la posibilidad que alguna amenaza se presente en una entidad o empresa y genere un desastre, lo que pueda ocasionar dependerá del nivel de vulnerabilidad.

4.4. MARCO LEGAL

El uso de las tecnologías de la información y comunicación han traído muchos beneficios en las operaciones de las empresas, pero ala ves también han generado problemas de seguridad donde la información es el activo más vulnerado, dichas acciones son generadas por delincuentes informáticos.

---

[16] ARRIETA, Álvaro. Políticas y normas de seguridad Informática [online]. 2011. 6 p. [citado abril 2020]. Disponible en internet: https://www.cvs.gov.co/jupgrade/images/stories/docs/Alertas/Politicas_de_ Seguridad_ Informática _CVS_2011-.pdf

Los delitos informáticos han llevado a implementar en los gobiernos nacionales como internacionales leyes y normas para así brindar a las víctimas soportes jurídicos.

4.4.1 Ley 1273 De 2009. Con la ley 1273 de 2009 se crea unos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos, afirma Párraga [17], en el año 2006 mediante solicitud del presidente Álvaro Uribe Vélez se dio la iniciativa de generar esta normatividad la cual se da a conocer en el año 2009 llamándose ley de la protección de información y de los datos, la cual está dividida en dos capítulos, el primero denominado De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos en los cuales se aborda temas como acceso involuntario a sistemas de información, obstaculizar el funcionamiento normal de sistemas informáticos, el capturar información de forma ilegítima, el que realice daños en datos e infra estructura tecnológica, el que manipule software malicioso distribuyéndolo o vendiéndolo, el que saque provecho de datos personales contenidos en ficheros, archivos o base de datos, suplantar un sitio web con el fin de acceder a datos personales.

Además, que los delitos anteriormente descritos tendrán aumento de penas si la conducta se da con particularidades como:

- Atacar un sistema estatal.
- Ser servidor público.
- Aprovechar la confianza.
- Revelar o divulgar información en perjuicio de otro.
- Obtener beneficios para sí o para un tercero.
- Para fines terroristas o afectar la seguridad o defensa nacional.
- Utilizar a otras personas de buena fe.
- Si el que realiza estas conductas es el administrador del sistema, las tecnologías asocias a este.

El segundo capítulo se refiere a los atentados informáticos y otras infracciones entre ellas el hurto informático y trasferir no consentida de activos valiéndose de alguna manipulación informática.

En la siguiente tabla se especifica los artículos de la ley en mención junto a la pena de prisión y multas que conllevan la violación de esta ley.

[17] PARRAGA, Andrés. Análisis de los delitos Informáticos en el actual sistema penal colombiano [online]. 2017. 43 p. [citado abril 2020]. Disponible en internet: https://repository.unilibre.edu.co/bitstream/handle/10901/11041/AN%C3%81LISIS%20DE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20EL%20ACTUAL%20SISTEMA%20PENAL%20COLOMBIANO%20revisado%20NHJ%20OK.pdf?sequence=3&isAllowed=y

Tabla 1. Ley 1273 de 2009

Capítulo 1	
Artículo 269a. acceso abusivo a un sistema informático.	Condena entre 48 a 96 meses y una multa de 100 a 1000 SMMLV.
Artículo 269b. Obstaculización ilegítima de un sistema informático o red de telecomunicación	Condena entre 48 96 meses y en multa de 100 a 1000 SMMLV.
Artículo 269c. Interceptación de datos informáticos	Condena entre 36 a 72 meses.
Artículo 269d. Daño informático.	condena entre 48 a 96 meses y en multa de 100 a 1000 SMMLV.
Artículo 269e. Uso de software malicioso.	Condena entre cuarenta 48 a 96 meses y en multa de 100 a 1000 SMMLV.
Artículo 269f. Violación de datos personales.	Condena entre 48 a 96 meses y en multa de 100 a 1000 SMMLV.
Artículo 269g. Suplantación de sitios web para capturar datos personales.	Condena entre 48 a 96 meses y en multa de 100 a 1000 SMMLV., siempre que la conducta no constituya delito sancionado con pena más grave.
Artículo 269h. Circunstancias de agravación punitiva	Se otorgará la pena más alta cuando haya sevicia en los procedimientos.
Capítulo 2	
Artículo 269i. Hurto por medios informáticos y semejantes	Incurrirá en las penas señaladas en el artículo 240 de este código que corresponde a hurto calificado.
Artículo 269j: Transferencia no consentida de activos.	Condena entre 48 a 120 meses y en multa de 200 a 1500 SMMLV.

Fuente: El autor

Gracias a este marco jurídico se convierte en un instrumento de gran efectividad para que cualquier entidad de orden público o privado tengan un sustento para adelantar acciones contra las personas que incurran en conductas delictivas.

4.4.2 Ley Estatutaria 1581 De octubre Del 2012

"Artículo 1. Objeto. 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."[18]

Con esta ley se permite que las personas tengan derechos sobre los datos que se registren en las bases de datos o archivos y que sean susceptibles de tratamiento por entidades de naturaleza pública o privada, con lo cual las personas podrán rectificar y actualizar.

4.5. MARCO CONTEXTUAL

"Cooperativa Multiactiva de Centrales Eléctricas de Nariño Ltda., cuya sigla es "COOPCEN LTDA" es una persona jurídica de Derecho Privado, empresa asociativa sin ánimo de lucro, de responsabilidad limitada, de número de asociados y de patrimonio social variable e ilimitado; regida por la ley, los principios universales del cooperativismo y el presente estatuto."[19]

4.5.1 Reseña Histórica. En el año 1965, visitó a la ciudad de Pasto, un funcionario de apellido Rojas proveniente de la seccional Valle del Cauca (Cali), dicho funcionario visitaba a las empresas que se crean competentes y tuvieren el personal suficiente para organizar cooperativas de ahorro y crédito, es así que el catorce (14) de noviembre de 1965, se reunieron treinta y dos (32) trabajadores de las diferentes oficinas de CENTRALES ELÉCTRICAS DE NARIÑO CEDENAR S.A., en el salón de UTRANA, antiguo edificio de SIMANA, con el propósito de constituir una Cooperativa, la que denominaron COOPERATIVA DE AHORRO Y CRÉDITO DE LOS TRABAJADORES DE LAS EMPRESAS ELÉCTRICAS DE NARIÑO, con domicilio principal en la ciudad de Pasto, se eligió una Junta Provisional.

Los miembros del Consejo Provisional acordaron fundar la Cooperativa con un capital inicial de trescientos veinte ($ 320.oo) pesos, el que fue aportado por los socios fundadores, además recaudaron el valor de ciento sesenta ($ 160.oo) por concepto de cuota de admisión, valores que fueron depositados en el Banco de Colombia, sección Ahorros.

Mediante Resolución No. 00601 del 26 de noviembre de 1965, la Superintendencia Nacional de Cooperativas de la ciudad de Bogotá concedió personería Jurídica.

---

[18] CONGRESO DE COLOMBIA. Ley estatutaria 1581 del 17 de octubre de 2012. [online]. 17 de octubre de 2012. [citado abril 2020]. Disponible en internet: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

[19] COOPCEN. Estatutos. [Online]. [citado en mayo de 2020]. Disponible en: http://www.coopcen.coop/index.php/normatividad-aa/category/5-estatutos

Con Escritura No. 2200 del 11 de diciembre de 1965 en la Notaría Segunda del Círculo de Pasto, fue protocolizada como COOPERATIVA DE AHORRO Y CRÉDITO DE TRABAJADORES DE LAS EMPRESAS ELÉCTRICAS DE NARIÑO LTDA.

Con Resolución 0029 del 7 de enero de 1986, fue aprobada la reforma total de los Estatutos de la Cooperativa y que a partir de esta fecha se denominó COOPERATIVA DE AHORRO Y CRÉDITO DE CEDENAR LIMITADA, COOPCEN LTDA., protocolizado bajo Escritura No. 217 del 24 de enero de 1986.

Posteriormente y dadas las necesidades de crecimiento de la Cooperativa se reformó estatutos y se la denominó COOPERATIVA MULTIACTIVA DE TRABAJADORES JUBILADOS Y PENSIONADOS DE CEDENAR LTDA, la que quedó abierta tanto para funcionarios activos, jubilados, pensionados de Pasto y sus Seccionales de CEDENAR S.A. y para particulares que quieran afiliarse.

En noviembre de 2017, el Consejo de Administración en cabeza del señor José Francisco Pérez promovió la reforma de estatutos y gracias al trabajo de dicho consejo con el aporte de los asociados, la Asamblea General aprobó los estatutos por los que la Cooperativa se rige a la fecha y cambió de razón social, como COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO LTDA.

4.5.2 Misión

"Somos una cooperativa del sector de la economía solidaria, comprometidos con el mejoramiento de la calidad de vida de nuestros asociados a través de la gestión del crédito, la capacitación y la cooperación con recursos y proyectos que dinamizan el crecimiento sostenible de COOPCEN."[20]

4.5.3 Visión

"Seremos una cooperativa reconocida en el sector solidario, que propenda por el bienestar de los asociados y sus familias, creceremos de manera sostenida y generaremos valor agregado a los asociados a través de la presentación de servicios con altos niveles de calidad y eficiencia"[21]

4.5.4 Domicilio Y Ámbito Territorial

"El domicilio principal de COOPCEN LTDA será la ciudad de San Juan de Pasto, Departamento de Nariño, Republica de Colombia, tiene como ámbito de operaciones todo el territorio nacional y podrá extenderse al exterior. Podrá establecer oficinas, sucursales y agencias en cualquier parte del país o del exterior que sean necesarias para la prestación de sus servicios según las normas legales vigentes para tales propósitos."[22]

---

[20] Ibíd.

[21] Ibíd.

[22] Ibíd.

Actualmente la dirección física donde realiza las operaciones es Carrera 32 #19ª - 28 Las Cuadras.

Las actividades realizadas para el cumplimiento de su misión son las siguientes:

- COOPCEN LTDA., realizará a través de recursos lícitos, provenientes de los aportes sociales, descuentos de salarios e ingresos de los asociados, recursos del sector financiero y comercial, las siguientes actividades.
- Fomentar el aporte entre sus asociados y prestar el servicio de crédito en sus diferentes modalidades. Para esto realizará operaciones de libranza o descuento directo de acuerdo a los términos establecidos por la Ley.
- Promover programas y servicios de capacitación, seminarios, eventos sociales y culturales tendientes a satisfacer las necesidades de los asociados, familiares y terceros.
- Desarrollar e impulsar la solidaridad y la ayuda mutua entre los asociados estimulando la participación consciente de los mismos alrededor de los servicios y actividades que desarrolla la cooperativa.
- Compra y venta de bienes y servicios, entre otros.
- Arrendamiento de bienes.
- Compra y venta de cartera.

La Cooperativa desarrolla programas de beneficio y actividades que brindan el mejoramiento social, económico de las familias de los asociados, fomentando el aporte entre los asociados y prestando el servicio de créditos en sus diferentes modalidades.

Créditos Ordinarios
Monto. Hasta dos (2) veces el valor de los aportes sociales.
Intereses. 1,5% TNMV. 20.98% TEA

Crédito Ordinario Sin Aportes
Monto. Desde $ 496,870.00 hasta 50,001,656.00
Intereses. 1,5% TNMV. 20.98% TEA

Crédito Navideño
Monto. Desde $ 1,656,232.00 hasta $ 2,484,348.00
Interés. 1,3 % TNMV. 16.77% TEA
Créditos para salud.
Monto. Entre uno (1) y diez (10) Salarios Mínimos Mensuales Legales Vigentes.
Intereses. 1.0% TNMV. 12.68% TEA.

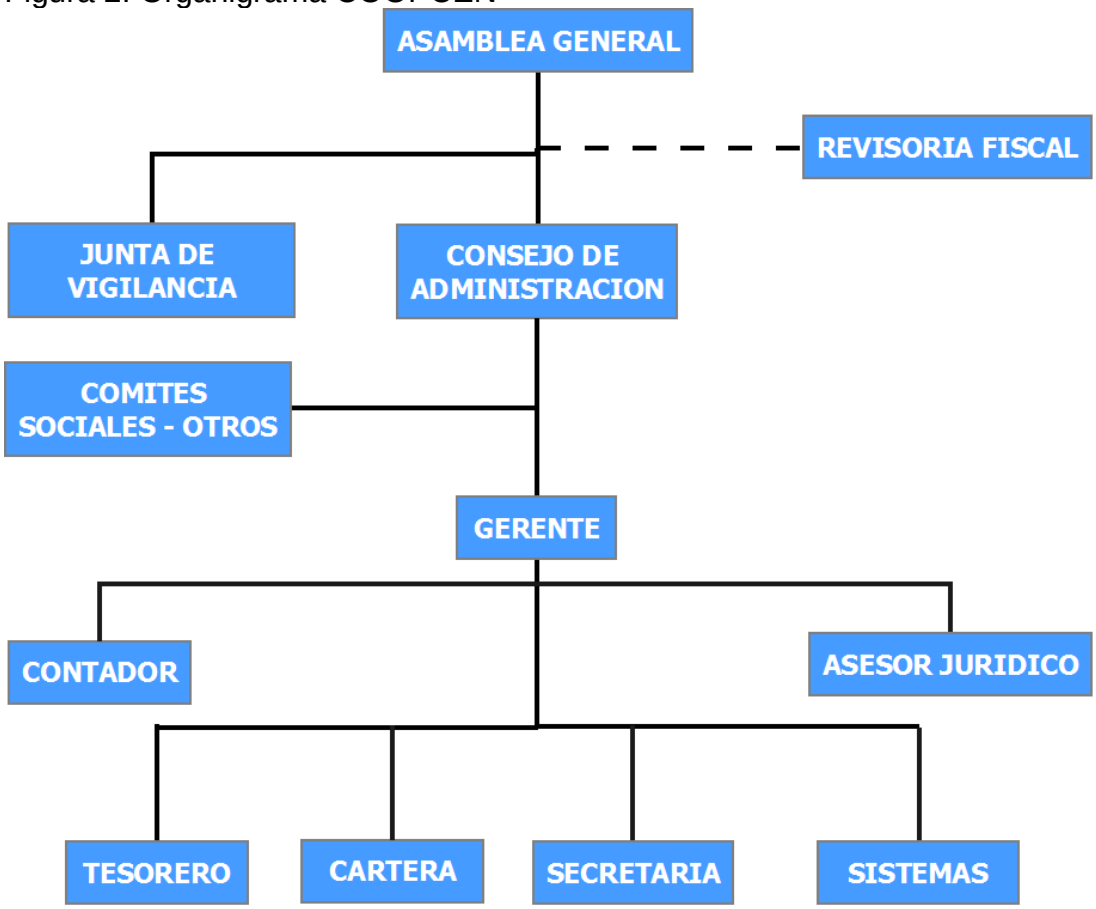
Créditos para educación (básica y pregrado).
Intereses. 1.0% TNMV. 12.68% TEA
Monto. Desde $ 496,870.00 hasta $ 16,562,320.00

Créditos para educación (especializaciones- maestrías - doctorado)
Monto. Desde $ 1,739,044.00 Hasta $ 49,686,960.00
Intereses. 1.3% TNMV. 16,77% TEA

Créditos Para Recreación Y Turismo
Monto Desde $ 496,870.00 hasta 16,562,320.00
Interés. 1,3 % TNMV. 16.77% TEA.

4.5.5 ORGANIGRAMA

Figura 2. Organigrama COOPCEN



Fuente: https://www.coopcedenar.com/index.php/quienes-somos/organigrama

5. DISEÑO METODOLÓGICO

El proyecto se basó en teorías de la investigación aplicada, por lo cual, se utilizaron y aplicaron métodos cuantitativos y cualitativos, donde los diferentes anexos de la norma ISO/IEC 27001:2013 y la metodología de riesgo seleccionada, a través de un análisis de la misma, sirvieron para obtener datos que se cuantificaron y se extrajeron aportes y soluciones de mejora.

A partir de los enfoques cuantitativo y cualitativo se obtuvieron datos que permitieron dar claridad a la importancia de proteger la información para generar en la empresa una dinámica óptima, donde las operaciones realizadas en esta, tengan un grado de confianza a la hora de procesar y almacenar información valiosa.

El proyecto se desarrolló mediante fases que buscaron alcanzar los objetivos específicos planteados, estos son:

En la primera fase se identificaron y clasificaron los activos de información con los cuales cuenta COOPCEN, junto a esta actividad se describirá el estado del activo tanto físico como funcional.

Para la segunda fase se analizó la información recopilada de los activos de información y se determinó los factores que ponen en riesgo la integridad, confidencialidad, y disponibilidad de la información; este análisis se realizó aplicando una metodología de gestión de riesgo, la cual permitió conocer las vulnerabilidades, amenazas y riesgos.

En la tercera fase se establecen los controles de acuerdo a la norma ISO/IEC 27001:2013, que eran necesarios para el diseño del sistema, esto se extrajo a partir del diagnóstico realizado mediante el análisis de riesgo.

Finalmente, en la cuarta fase se diseñó la propuesta de políticas de seguridad, acorde a las necesidades de la empresa para así poder mitigar los riesgos.

Para desarrollar el proyecto se utilizaron fuentes de información que estaban estrechamente relacionadas con las actividades de la empresa; además, bajo el seguimiento y observación directa se verificaron puntos críticos y fundamentales presentes en la infraestructura de la empresa que permitieron tener una idea objetiva del panorama actual de las actividades, activos de información, talento humano, procesos y documentos.

Con todo lo anterior se utilizaron también técnicas para la recopilación de información, entre estas están:

Entrevista: bajo este instrumento se procedió a realizar preguntas abiertas y cerradas que permitieron corroborar información que ya se ha obtenido

previamente. Este instrumento también permitió tener un acercamiento directo con las personas en los mismos puestos de trabajo y de esta forma se verifico situaciones atípicas o posibles problemas en donde puedan existir oportunidades de mejora.

Lista de chequeo: método que permitió verificar la existencia o no de algún control, política o acción con respecto a la seguridad de la información, a través de, preguntas y cuestionarios que se basaron en los dominios y controles de la norma ISO/IEC 27001:2013. Estas preguntas del cuestionario fueron consignadas bajo la información que cada usuario de las diferentes áreas de la COOPERATIVA brindó.

Observación: bajo autorización previa se estuvo presente situaciones o hechos que permitan realizar la recolección de datos y a partir de esto se pudo realizar el análisis de los mismos; la información puede ser evidenciada bajo videos, fotos u observación directa, como afirma KOCH [23], mediante el registro visual se registran momentos, situaciones imprevistas, conducta y actividades las cuales arrojan datos cualitativos como cuantitativos que permiten generar el desarrollo de un estudio.

[23] KOCH, Federico. Metodología proyectual. [online]. 2012. 3 p. [citado abril 2020]. Disponible en internet: https://kochfede.files.wordpress.com/2013/03/metodologia-proyectual-apuntes-1.pdf

6. DESARROLLO DE LOS OBJETIVOS

6.1 FASE 1: IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN QUE ESTÁN PRESENTES EN LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO (COOPCEN), CON EL FIN DE DETERMINAR LOS DOMINIOS APLICABLES PARA EL DISEÑO DEL SGSI.

LA ALTA DIRECCIÓN EN EL DESARROLLO DEL PROYECTO.

En la realización del proyecto es de gran importancia que la gerencia y dirección institucional acompañen el proceso, ya que son estos los que conocen directamente las actividades y objetivos de la Cooperativa; además de comprender como se maneja y gestiona la información. En este sentido, para la implementación del SGSI la gerencia debe estar comprometida en gestionar los riesgos, garantizando la seguridad de los activos de información y por ende la continuidad del negocio.

En cuanto a la realización del presente proyecto se solicitó el apoyo de la gerencia, quien, en conjunto con los diferentes comités y el concejo administrativo, dieron el aval y autorización para el desarrollo efectivo de los objetivos propuestos en la presente investigación.

6.1.1 Alcance Del Proyecto. Para el desarrollo del proyecto se desarrollaron las siguientes actividades:

- Definir los activos de información que están presentes en la Cooperativa y sobre los cuales se plantean medidas para su protección, referenciando estas medidas bajo la norma ISO/IEC 27001:2013.
- Identificar las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos de información que afecten la continuidad del negocio.
- Generar un análisis de los riesgos, calificando estos de forma cuantitativa y cualitativa para poder realizar su tratamiento.
- Establecer los controles necesarios, que permitan garantizar la disponibilidad, confidencialidad y disponibilidad de la información.

6.1.2 Metodología Utilizada Para La Gestión De Riesgos. El desarrollo del proyecto se basó en la metodología MAGERIT, la cual se ha convertido en una de las herramientas principales para evaluar los riesgos y amenazas que vulneren la integridad, disponibilidad y confidencialidad de la información, según la consultora de tecnología española TITHINK [24], para los profesionales que trabajan con las nuevas tecnologías de la información y la comunicación, esta metodología permite conocer el valor de los activos de información y cuanto están ante una eventual

[24] TITHINK. Gestión de Riesgos. Magerit. 2013. P. 3.

situación de riesgo con el fin de poder gestionarlos de manera adecuada bajo unos pasos definidos sin la necesidad de caer en la improvisación.

Esta metodología está diseñada para cualquier empresa independientemente de su actividad económica; partiendo de esta, se desarrollaron las siguientes etapas:

- Identificar los activos, y sus respectivas amenazas, vulnerabilidades y riesgos.
- Determinar los Controles de seguridad.
- Valorar el impacto.
- Valorar el riesgo

Para el desarrollo del proyecto y para poder determinar la metodología se realizó un estudio comparativo entre las más representativas, entre ellas:

- OCTAVE
- MAGERIT
- LA NORMA ISO 27005
- MEHARI

Con las anteriores metodologías y normas se realiza un análisis comparativo de las ventajas y desventajas, lo que permitió seleccionar la que mejor se adapte al contexto y necesidades de la organización; a continuación, en la tabla No 2 se genera el comparativo de las anteriores metodologías y normas mencionadas.

Tabla 2 Comparativo Metodologías y Normas

METODOLOGÍA	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
OCTAVE	Creada en Estados Unidos por la Universidad Carnegie Mellon. Su aplicabilidad puede darse en pequeñas empresas, organizaciones públicas y privadas En esta metodología los activos pueden ser: - sistemas definidos en hardware como en software, y datos	Comprende los procesos de análisis y gestión de riesgos. Permite involucrar a todo el personal de la organización. Es una de las más complejas involucrando en el modelo procesos, recursos, activos.	No tiene en cuenta el no repudio de la información dentro de los objetivos de seguridad. Exige el uso de muchos documentos para el análisis de riesgos. Para su uso externo es

	- personas Constituida por 3 fases: Fase 1 visión organizativa (Activos, Amenazas, Prácticas Actuales, Vulnerabilidades Organizativas, Requerimientos seguridad). Fase 2 Visión Tecnológica (Componentes Clave, Vulnerabilidades Técnicas). Fase 3 Estrategia y Plan de Desarrollo (Riesgos, Estrategia de Protección, Plan de Mitigación).		limitado requiere de una licencia.
MAGERIT	Creada en España por el concejo Superior de Administración Electrónica de España en su primera versión del año 1997. Compuesta por los siguientes pasos: 1.Determinar activos 2.Determinar amenazas de los activos. 3.Determinar salvaguardas. 4. Estimar el impacto. 5. Estimar el riesgo. Esta metodología logra planificar medidas para	La documentación es amplia con respecto a los activos, amenazas y recursos de información. El análisis puede arrojar resultados cuantitativos y cualitativos. Para su utilización no requiere autorización previa.	No se tiene en cuenta los procesos y recursos dentro del análisis. Las políticas de seguridad no están bien relacionadas.

	mantener los riesgos bajo control.		
LA NORMA ISO 27005	Nace en la Organización para la estandarización ISO. Considera análisis cuantitativo y cualitativo. Su función está centrada en la evolución del riesgo y su tratamiento. Compuesta por los anexos que permite el desarrollo de: - valoración de activos - valoración del impacto -ejemplos de amenazas -Lista de vulnerabilidades. El proceso es iterativo, por lo tanto, se compagina con el modelo Deming (planificar, hacer, verificar y actuar).	Se aplica a diferentes tipos de organizaciones y empresas, comerciales, gubernamentales. Por ser un estándar internacional genera su utilización mayor aceptación.	No define una forma de valoración de las amenazas. No es certificable
MEHARI	Desarrollada por el Club De La Seguridad De la Información de Francia en el año 1998. Las fases que la componen son: 1. Análisis o evaluación de riesgos 2. Evaluaciones de seguridad. 3. Análisis de amenazas	Facilidad de uso que permite cuantificar y cualificar el riesgo. Permite la disminución del riesgo en función del tipo de organización. Tiene amplios recursos	No tiene en cuenta el no repudio de la información dentro de los objetivos de seguridad.

		bibliográficos con manuales, guías y humientas para el análisis de riesgo.	

Fuente: El autor

Bajo la anterior comparación, donde se destacan las cualidades de cada metodología el desarrollo del proyecto, finalmente se determinó utilizar la metodología MAGERIT, debido a que esta posee un gran reconocimiento a nivel mundial, acompañada de la documentación pertinente de forma gratuita desde el portal web https://administracionelectronica.gob.es/, el cual no pose restricción alguna para su uso.

Otro de los puntos clave de la elección de la metodología MAGERIT es que dispone de las diferentes tablas de frecuencia para el análisis de forma cuantitativa y cualitativa, además su gran adaptación de uso que no restringe al tipo de organización en cuanto a naturaleza jurídica y tamaño.

La metodología MAGERIT se compagina de manera adecuada a la norma ISO/IEC 27001:2013 lo que garantiza que una vez se finalice el análisis de riesgo, se generen controles en los diferentes activos identificados con un grado alto de riesgo.

6.1.3 Análisis Y Gestión De Riesgos En La Organización. A través de la metodología MAGERIT se realizará las etapas anteriormente descritas y con la cual se dará el cumplimiento de los objetivos propuestos en el proyecto.

6.1.4 Activos De Información. Durante el desarrollo del proyecto se determinaron los activos que están a disposición de la Cooperativa los cuales están estrechamente relacionados con los datos que se procesan, almacenan y presentan salidas. La identificación de los activos se logra bajo la observación directa como datos relacionados en el sistema contable que posee la Cooperativa.

La clasificación de cada activo se realizará de acuerdo a lo propuesto por la metodología MAGERIT, la cual propone mediante una nomenclatura identificar cada activo de información para su análisis posterior, en la tabla No. 3 se tiene la clasificación de los activos de información según la metodología.

Tabla 3. Tipos de activos

NOMENCLATURA	NOMBRE
[D]	DATOS
[S]	SERVICIOS
[SW]	SOFTWARE APLICACIONES
[HW]	HARDWARE

[COM]	REDES Y COMUNICACIONES
[MEDIA]	SOPORTES DE INFORMACION
[K]	CLAVES CRIPTOGRAFICAS
[L]	INSTALACIONES
[AUX]	ELEMENTOS AUXILIARES
[P]	PERSONAL

Fuente: El autor

Los activos de información que harán parte del análisis serán los que interactúen con los considerados procesos de afiliación, crédito financiero, ingreso de fondos, afiliaciones y gestión tecnológica, debido a que estos son dentro de la organización las principales actividades que dan cumplimiento a la misión, además de ser los servicios primordiales para los asociados de COOPCEN; por ende, proteger el buen funcionamiento de los activos de las áreas de secretaría, cartera, contabilidad, tesorería y sistemas donde se ejecutan los anteriores procesos mencionados se hace indispensable para evitar la no continuidad o perdida de información que ponga en tela de juicio la calidad de los servicios.

Por ser los procesos donde el movimiento, procesamiento y almacenamiento de información es constante y de gran valor para la Cooperativa, los activos aquí involucrados entraran a formar parte de la identificación para su posterior valoración, identificación de amenazas y vulnerabilidades.

Cada activo identificado en la Cooperativa estará dentro del grupo correspondiente según su función, de tal manera que cada activo también tenga una nomenclatura la cual es especificada por la metodología MAGERIT, al renombrar los activos se crea la tabla No 4, donde se relacionan los activos disponibles en la empresa.

Tabla 4. Identificación de activos

COD	NOMBRE	NOMENCLATURA ACTIVO	DESCRIPCION	CANTIDAD
		[BD]	Base de datos en la nube	1
[D]	DATOS	[files]	Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.	1
		[int]	Archivo principal de información asociados, proveedores, convenios, comunicados, circulares.	1
[S]	SERVICIOS	[www]	Navegación -Internet	1
		[file]	Almacenamiento en la nube de BD	1

		[servimp]	impresión y scanner en red	1
[SW]	SOFTWARE APLICACIONES	[sub]	Sistema financiero LINIX web - escritorio	1
		[dbms]	Sistema gestión BD en la nube	1
		[office]	OFFICE 2010	11
		[os]	WINDOWS 7 PRO OEM	11
		[browser]	Google Chrome	N/A
[HW]	HARDWARE	[cel]	Celular Smartphone empresarial	2
		[pc]	Equipo de escritorio	9
		[mobile]	Equipo portátil	2
		[print]	Impresoras	6
		[modem]	modem internet	2
		[switch]	SW 24 Puertos	1
		[wap]	Access Point	1
		[cam]	Cámaras de seguridad	6
[COM]	REDES Y COMUNICACIONES	[lan]	red de área local COOPCEN	1
		[Internet]	Internet	2
		[PSTN]	Red telefónica	1
[MEDIA]	SOPORTES DE INFORMACION	[disk]	Disco externo	1
		[san]	Almacenamiento en red	1
		[usb]	almacenamiento externo baja capacidad	3
[L]	INSTALACIONES	[Infra]	Planta física COOPCEN	1
[AUX]	ELEMENTOS AUXILIARES	[UPS]	Sistemas de alimentación interrumpida	1
		[cabling]	Sistema Cableado UTP Cat 5	1
		[can]	canaleta 22 12X5	N/A
		[wire]	Sistema Cableado eléctrico	1
[P]	PERSONAL	[ui]	Personal interno administrativos	9
		[ue]	Personal externo afiliados, concejo y comités	N/A

Fuente: El autor

6.1.5 Valoración De Activos De Información. Para la valoración de los activos de información se utiliza unas medidas cuantitativas que permitirá realizar cálculos matemáticos simples los cuales generar valores que miden la criticidad de los activos en el cumplimiento de los objetivos de la organización.

La escala está expuesta en la metodología MAGERIT, la cual puede se puede estructurar los diferentes rangos a la necesidad de la organización, para el desarrollo del presente proyecto se estructura los siguientes criterios de valoración. Ver tabla No 5.

Tabla 5. Escala de valoración de Activos

DETALLE DEL CRITERIO	VALOR	
Daño o impacto MUY ALTO en los objetivos de la organización	=6	MUY ALTO
Daño o impacto ALTO en los objetivos de la organización	> 4 <6	ALTO
Daño o impacto MEDIO en los objetivos de la organización	>2 y <4	MEDIO
Daño o impacto BAJO en los objetivos de la organización	>0 y <2	BAJO
Daño o impacto IRRELEVANTE en los objetivos de la organización	= 0	IRRELEVANTE

Fuente: El autor

La valoración anteriormente definida en la Tabla 7 se aplicará a las 5 dimensiones asociadas de cada activo de información que son:

[D] disponibilidad
[I] integridad
[C] confidencialidad
[A] autenticidad
[T] trazabilidad

Para valorar cada activo dependiendo de sus diferentes dimensiones se tendrá que realizar algunas preguntas que permitan abordar la dimensión a evaluar como se muestra en la Tabla 6.

Tabla 6. Preguntas para valorar dimensiones

DIMENSIÓN	PREGUNTA	DESCRIPCIÓN
Disponibilidad [D]	¿Qué relevancia tiene el activo si no está disponible?	Tendrá un valor MUY ALTO si el activo al no estar disponible afecta considerablemente la continuidad de la operación.

		Será BAJO si no afectan las operaciones.
Integridad [I]	¿Qué relevancia tiene el activo si este es modificado o alterado?	Tendrá un valor MUY ALTO si el activo al ser modificado o alterado afecte gravemente a la empresa. Será BAJO si al ver cambios en el activo no afecte las operaciones.
Confidencialidad [C]	¿Qué relevancia tiene el activo si este es manipulado o conocido por persona no autorizada?	Tendrá un valor MUY ALTO si al exponer el activo o divulgarlo públicamente ocasionara consecuencias negativas. Será BAJO si no trae consecuencias.
Autenticidad [A]	¿Qué relevancia tiene el activo si no controla el acceso?	Tendrá un valor MUY ALTO si al activo no se le puede controlar el acceso ocasionando afectaciones a la empresa Será BAJO si la afectación es irrelevante.
Trazabilidad [T]	¿Qué relevancia tiene le activo si no existe constancia de su uso?	Será MUY ALTO si el seguimiento de su uso no se puede controlar. Será BAJO si el seguimiento es controlable.

Fuente: El autor

Teniendo las diferentes escalas sobre la cual se trabajará para valorar los activos de información se procede a generar el análisis cuantitativo y cualitativo el cual se expresa en la tabla No. 7.

Tabla 7. Valoración de activos por Dimensión

TIPO DE ACTIVO	NOMENCLATURA ACTIVO	DESCRIPCIÓN	CANTIDAD					VALOR CUALITATIVO	VALOR CUANTITATIVO
			D	I	C	A	T		
DATOS	[BD]	Base de datos en la nube	6	6	6	6	6	6	MUY ALTO

	[files]	Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.	2	6	6	5	4	4,6	ALTO
	[int]	Archivo principal de información asociados, proveedores, convenios, comunicados, circulares.	6	6	6	6	6	6	MUY ALTO
SERVICIOS	[www]	Navegación -Internet	4	3	6	5	6	4,8	ALTO
	[file]	Almacenamiento en la nube de BD	6	6	6	6	6	6	MUY ALTO
	[servimp]	Impresión y scanner en red	3	3	2	3	3	2,8	MEDIO
SOFTWARE APLICACIONES	[sub]	Sistema financiero LINIX web - escritorio	6	6	6	6	6	6	MUY ALTO
	[dbms]	Sistema gestión BD en la nube	6	6	6	6	6	6	MUY ALTO
	[office]	OFFICE 2010	4	4	6	6	5	5	ALTO
	[os]	WINDOWS 7 PRO OEM	6	6	6	6	6	6	MUY ALTO
	[browser]	Google Chrome	4	5	6	6	5	5,2	ALTO
HARDWARE	[cel]	Celular Smartphon	3	2	4	3	4	3,2	MEDIO

		e empresarial							
	[pc]	Equipo de escritorio	5	5	6	6	5	5,4	ALTO
	[mobile]	Equipo portátil	4	5	6	6	5	5,2	ALTO
	[print]	Impresoras	3	3	2	3	3	2,8	MEDIO
	[modem]	Modem internet	6	5	5	5	4	5	ALTO
	[switch]	SW 24 Puertos	6	6	6	6	6	6	MUY ALTO
	[wap]	Access Point	3	2	3	2	2	2,4	MEDIO
	[cam]	Cámaras de seguridad	3	5	6	5	4	4,6	ALTO
REDES Y COMUNICACIONES	[lan]	Red de área local COOPCEN	6	5	6	6	6	5,8	ALTO
	[Internet]	Internet	6	6	6	6	6	6	MUY ALTO
	[PSTN]	Red telefónica	2	3	2	3	2	2,4	MEDIO
SOPORTES DE INFORMACION	[disk]	Disco externo	3	5	6	6	5	5	ALTO
	[san]	Almacenamiento en red	4	5	6	5	5	5	ALTO
	[usb]	Almacenamiento externo baja capacidad USB	2	3	6	5	2	3,6	MEDIO
INSTALACIONES	[Infra]	Planta física COOPCEN	6	6	6	6	6	6	MUY ALTO
ELEMENTOS AUXILIARES	[UPS]	Sistemas de alimentación interrumpida	5	5	3	4	3	4	MEDIO
	[cabling]	Sistema Cableado UTP Cat 5	5	5	4	4	3	4,2	ALTO

	[can]	Canaleta 22 12X5	2	3	2	2	2	2,2	MEDIO
	[wire]	Sistema Cableado eléctrico	6	6	5	4	4	5	ALTO
PERSONAL	[ui]	Personal interno administrativos	5	5	4	4	4	4,4	ALTO

Fuente: El autor

6.2 FASE 2: IDENTIFICACIÓN DE LAS AMENAZAS, VULNERABILIDADES Y RIESGOS A LOS QUE ESTA EXPUESTO LOS ACTIVOS DE INFORMACIÓN QUE AFECTAN LA CONTINUIDAD DEL NEGOCIO.

6.2.1 Identificación Y Valoración De Amenazas. Teniendo la valoración de los activos, se identifican las amenazas con su respectiva valoración a cada uno de los activos anteriormente identificados, para esto se toma como base la clasificación de las diferentes amenazas que plantea la metodología MAGERIT como se describe en la tabla No. 8.

Tabla 8. Amenazas MAGERIT.

TIPO DE AMENAZA	DESCRIPCIÓN
[N] Desastres naturales	Eventos que ocurren por fenómenos de la naturaleza.
[I] De origen industrial	Sucesos que ocurren de forma accidental, producido por las labores que realiza el ser humano.
[E] Errores y fallos no intencionados	Fallos no intencionales a causa del desconocimiento.
[A] Ataques intencionados	Fallos deliberados generados por personas inescrupulosas, que pretenden alterar los procesos para beneficio propio.

Fuente: El autor

Cada amenaza identificada en la tabla No. 8 tiene unas categorías las cuales se relaciona en la tabla No.9 y las cuales afectan a ciertas dimensiones.

Tabla 9. Categorías de amenazas

ETIQUETA	AMENAZAS	DIMENSION AFECTADA
	[N] Desastres Naturales	
[N.1]	Fuego	[D]
[N.2]	Daño por agua	[D]
[N.*]	Otros desastres	[D]
	[I] De origen industrial	
[I.1]	Fuego	[D]
[I.2]	Daños por agua	[D]
[I.*]	Desastres industriales	[D]
[I.3]	Contaminación mecánica	[D]
[I.4]	Contaminación electromagnética	[D]
[I.5]	Avería de origen físico o lógico	[D]
[I.6]	Corte del suministro eléctrico	[D]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
[I.8]	Fallo de servicios de comunicación	[D]
[I.9]	Interrupción de otros servicios o suministros esenciales	[D]
I.10]	Degradación de los soportes de almacenamiento	[D]
[I.11]	Emanaciones electromagnéticas	[C]
	[E] Errores y fallos no intencionados	
[E.1]	Errores de los usuarios	[D][I][C]
[E.2]	Errores del administrador	[D][I][C]
[E.3]	Errores de monitorización	[I]
[E.4]	Errores de configuración	[I]
[E.7]	Deficiencias en la organización	[D]
[E.8]	Difusión de software dañino	[D][I][C]
[E.9]	Errores de re-encaminamiento	[C]
[E.10]	Errores de secuencia	[I]
[E.14]	Escapes de información	[C]
[E.15]	Alteración accidental de la información	[I]
[E.18]	Destrucción de la información	[D]
[E.19]	Fugas de información	[C]
[E.20]	Vulnerabilidades de los programas (software)	[D][I][C]
[E.21]	Errores de mantenimiento o actualización (software)	[D][I]
[E.23]	Errores de mantenimiento o actualización (hardware)	[D]

[E.24]	Caiga del sistema por agotamiento de recursos	[D]
[E.25]	Perdida de equipos	[D][C]
[E.28]	Indisponibilidad del personal	[D]
[A] Ataques intencionados		
[A.3]	Manipulación de los registros de actividad	[I]
[A.4]	Manipulación de la configuración	[D][I][C]
[A.5]	Suplantación de la identidad del usuario	[C][A][I]
[A.6]	Abuso de privilegios de acceso	[D][I][C]
[A.7]	Uso no previsto	[D][I][C]
[A.8]	Difusión de software dañino	[D][I][C]
[A.9]	Re-encaminamiento de mensajes	[C]
[A.10]	Alteración de secuencia	[I]
[A.11]	Acceso no autorizado	[C][I]
[A.12]	Análisis de tráfico	[C]
[A.13]	Repudio	[I]
[A.14]	Interceptación de información	[C]
[A.15]	Modificación deliberada de la información	[I]
[A.18]	Destrucción de la información	[D]
[A.19]	Divulgación de información	[C]
[A.22]	Manipulación de programas	[D][I][C]
[A.23]	Manipulación de los equipos	[C][D]
[A.24]	Denegación de servicio	[D]
[A.25]	Robo	[C][D]
[A.26]	Ataque destructivo	[D]
[A.27]	Ocupación enemiga	[D][C]
[A.28]	Indisponibilidad del personal	[D]
[A.29]	Extorsión	[D][I][C]
[A.30]	Ingeniería social	[D][I][C]

Fuente: El autor

Bajo la anterior clasificación de las amenazas a las cuales se ven expuestos los activos de COOPCEN se procede a realizar el respectivo registro, determinando un valor a las amenazas bajo el parámetro de frecuencia.

La frecuencia será el número de veces que la amenaza reaparece en un periodo de tiempo, esta frecuencia también se la denomina probabilidad y se la suele modelar cualitativamente.

De tal manera para realizar la escala de frecuencia se basará según la metodología MAGERIT la cual se define en la tabla No. 10.

Tabla 10. Frecuencia de la amenaza

Valoración cualitativa	Frecuencia	Valor Cuantitativo
MA	A diario	5
A	mensualmente	4
M	1 ves al año	3
B	Cada varios años	2
MB	Siglos	1

Fuente: El autor

Con la valoración cualitativa y cuantitativa de la frecuencia se realizará el análisis de la frecuencia de cada activo, adjunto a este análisis también se obtendrá el impacto que genera dicha amenaza, el impacto se obtendrá bajo una tabla de doble entrada donde intervendrán los siguientes conceptos:

Degradación: es la valoración de la afectación al activo que resulta de hacerse real la amenaza, la cual puede estar en 1% degradación poco considerable, 50% degradación medianamente y 100% degradación total.

Impacto: es el alcance del daño que puede llegar a producir si una amenaza se materializa, este impacto está basado en la operatividad de los procesos de la Cooperativa.
El impacto está categorizado así:

- Impacto insignificante (1)
- Impacto menor (2)
- Impacto moderado (3)
- Impacto mayor (5)
- Impacto desastroso (8)

Con los anteriores conceptos se obtiene la tabla de estimación de impacto Tabla No. 11.

Tabla 11. Estimación de impacto

	DEGRADACIÓN		
IMPACTO	1%	50%	100%
MUY ALTO	3	5	8
ALTO	2	3	5
MEDIO	1	2	3
BAJO	1	1	2
MUY BAJO	1	1	1

Fuente: El autor

Con la anterior información se genera la tabla No. 12 evaluación amenazas con su frecuencia e impacto, en la cual se valora cualitativamente y cuantitativamente el impacto generado de las amenazas relacionadas en los diferentes activos.

Tabla 12. Evaluación amenazas con su frecuencia e impacto

TIPO DE ACTIVO	Cód. ACTIVO	DESCRIPCION	AMENZAS	FRECUENCIA	DEGRADACION	DAÑO/IMPACTO (VALOR)	DAÑO/IMPACTO CULAITATIVO
DATOS	[BD]	Base de datos en la nube	[E.1] Errores de los usuarios	5	1%	1	BAJO
			[E.21] Errores de mantenimiento / actualización (software)	3	1%	1	BAJO
			[E.15]Alteración accidental de la información	4	1%	1	MEDIO
			[A.6] Abuso de privilegios de acceso	2	1%	2	ALTO
			[I.5]Avería de origen físico o lógico	3	1%	3	MUY ALTO
			[A.24]Denegación de servicio	2	1%	2	ALTO
	[files]	Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.	[N.1]Fuego	1	100%	5	ALTO
			[N.2]Daño por agua	1	100%	3	MEDIO
			[A.11]Acceso no autorizado	2	50%	2	MEDIO
			[A.25]Robo	2	100%	3	MEDIO
	[int]	Archivo principal de información asociados,	[N.1]Fuego	1	100%	8	MUY ALTO
			[N.2]Daño por agua	1	100%	5	ALTO
			[A.11]Acceso no autorizado	2	50%	2	MEDIO
			[A.25]Robo	2	100%	3	MEDIO

		proveedores, convenios, comunicados, circulares.					
SERVICIOS	[www]	Internet	[I.8] Fallo de servicios de comunicación	4	50%	8	MUY ALTO
			[A.11]Acceso no autorizado	2	50%	2	MEDIO
			[A.7]Uso no previsto	4	50%	2	MEDIO
			[I.6]Corte del suministro eléctrico	4	50%	3	ALTO
	[file]	Almacenamiento en la nube de BD	[I.9]Interrupción de otros servicios o suministros esenciales	4	1%	2	ALTO
	[servimp]	Impresión y scanner en red	[A.7]Uso no previsto	4	50%	2	BAJO
			[I.6]Corte del suministro eléctrico	4	50%	2	MEDIO
			[I.9]Interrupción de otros servicios o suministros esenciales	4	1%	1	BAJO
SOFTWARE APLICACIONES	[sub]	Sistema financiero LINIX web - escritorio	[I.8] Fallo de servicios de comunicación	4	50%	5	ALTO
			[I.5]Avería de origen físico o lógico	3	1%	3	MUY ALTO
			[E.1] Errores de los usuarios	5	1%	1	BAJO
			[A.7] Uso no previsto	2	1%	1	BAJO
			[A.24] Denegación de servicio	2	1%	2	ALTO
			[A.11] Acceso no autorizado	2	50%	3	ALTO
			[A.18]Destrucción de la Información	2	100%	5	ALTO

	[office]	OFFICE 2010	[E.21] Errores de mantenimiento / actualización (software)	4	50%	3	ALTO
			[E.20] Vulnerabilidades de los programas (software)	3	50%	3	ALTO
			[A.7] Uso no previsto	4	50%	1	MUY BAJO
			[E.4] Errores de configuración	3	1%	1	MEDIO
			[E.8] Difusión de software dañino	4	100%	5	ALTO
			[A.11] Acceso no autorizado	2	50%	2	MEDIO
			[A.22]Manipulación de programas	3	50%	2	MEDIO
	[os]	WINDOWS 7 PRO OEM	[E.21] Errores de mantenimiento / actualización (software)	4	100%	5	ALTO
			[E.8] Difusión de software dañino	4	100%	5	ALTO
			[A.7] Uso no previsto	4	50%	3	MEDIO
			[A.11]Acceso no autorizado	2	50%	3	ALTO
			[A.15]Modificación deliberada de la información	2	50%	2	BAJO
			[E.4] Errores de configuración	3	1%	2	ALTO
			[A.22]Manipulación de programas	3	50%	3	ALTO
	[browser]	Google Chrome	[E.20] Vulnerabilidades de los programas (software)	3	50%	2	MEDIO
			[A.7] Uso no previsto	4	50%	2	BAJO
			[E.4] Errores de configuración	3	1%	1	MEDIO

			[E.8] Difusión de software dañino	4	100%	3	MEDIO
			[A.11] Acceso no autorizado	2	50%	2	MEDIO
			[A.22]Manipulación de programas	3	50%	2	MEDIO
HARDWARE	[cel]	Celular Smartphone empresarial	[E.25]Perdida de equipos	2	100%	3	MEDIO
			[A.7]Uso no previsto	4	50%	2	BAJO
			[A.25]Robo	2	100%	2	BAJO
	[mobile]	Equipo portátil	[I.6]Corte del suministro eléctrico	4	50%	3	ALTO
			[I.5]Avería de origen físico o lógico	3	50%	3	ALTO
			[E.23] Errores de mantenimiento o actualización (hardware)	3	50%	2	MEDIO
			[I.3]Contaminación mecánica	4	100%	3	MEDIO
			[E.25]Perdida de equipos	2	100%	3	MEDIO
			[A.6] Abuso de privilegios de acceso	2	1%	3	MUY ALTO
			[A.7]Uso no previsto	2	50%	2	BAJO
			[A.23]Manipulación de los equipos	2	50%	2	MEDIO
	[pc]	Equipo de mesa	[I.6]Corte del suministro eléctrico	4	1%	3	MUY ALTO
			[I.5]Avería de origen físico o lógico	3	50%	3	ALTO
			[E.23] Errores de mantenimiento o actualización (hardware)	3	50%	2	MEDIO
			[I.3]Contaminación mecánica	4	100%	3	MEDIO
			[E.25]Perdida de equipos	2	100%	5	ALTO
			[A.6] Abuso de privilegios de acceso	2	1%	3	MUY ALTO

			[A.7]Uso no previsto	4	50%	3	MEDIO
			[A.23]Manipulación de los equipos	2	50%	2	MEDIO
	[print]	Impresoras	[I.5]Avería de origen físico o lógico	3	50%	2	MEDIO
			[E.23] Errores de mantenimiento o actualización (hardware)	3	50%	2	MEDIO
			[I.3]Contaminación mecánica	4	100%	3	MEDIO
			[E.25]Perdida de equipos	2	100%	3	MEDIO
			[A.6] Abuso de privilegios de acceso	2	1%	1	BAJO
			[A.7]Uso no previsto	4	50%	3	MEDIO
			[A.23]Manipulación de los equipos	2	50%	2	MEDIO
	[modem]	Modem internet	[I.7] Condiciones inadecuadas de temperaturas o humedad	5	50%	3	ALTO
			[I.5]Avería de origen físico o lógico	3	50%	3	ALTO
			[E.23] Errores de mantenimiento o actualización (hardware)	3	50%	3	ALTO
			[E.25]Perdida de equipos	2	100%	3	MEDIO
			[A.7]Uso no previsto	2	50%	3	MEDIO
			[I.6]Corte del suministro eléctrico	4	50%	3	ALTO
			[A.23]Manipulación de los equipos	2	50%	3	ALTO
	[switch]	SW 24 Puertos	[I.7] Condiciones inadecuadas de temperaturas o humedad	3	50%	3	ALTO
			[I.5]Avería de origen físico o lógico	3	50%	3	ALTO
			[E.23] Errores de mantenimiento o	2	50%	3	ALTO

			actualización (hardware)				
			[E.25]Perdida de equipos	2	100%	5	ALTO
			[A.7]Uso no previsto	2	50%	3	MEDIO
			[I.6]Corte del suministro eléctrico	4	50%	3	ALTO
			[A.23]Manipulación de los equipos	2	50%	3	ALTO
			[E.2]Errores del administrador	3	1%	2	ALTO
			[A.11]Acceso no autorizado	2	50%	3	ALTO
	[wap]	Access Point	[I.7] Condiciones inadecuadas de temperaturas o humedad	5	50%	2	MEDIO
			[I.5]Avería de origen físico o lógico	3	50%	2	MEDIO
			[E.23] Errores de mantenimiento o actualización (hardware)	3	50%	2	MEDIO
			[E.25]Perdida de equipos	2	100%	3	MEDIO
			[A.7]Uso no previsto	2	50%	2	BAJO
			[I.6]Corte del suministro eléctrico	4	50%	2	MEDIO
			[A.23]Manipulación de los equipos	2	50%	2	MEDIO
			[E.2]Errores del administrador	3	1%	1	BAJO
			[A.11]Acceso no autorizado	2	50%	2	MEDIO
			[E.9]Errores de Re-encaminamiento	2	1%	1	BAJO
	[cam]	Cámaras de seguridad	[I.3]Contaminación mecánica	4	100%	2	BAJO
			[I.5]Avería de origen físico o lógico	3	100%	3	MEDIO
			[E.23] Errores de mantenimiento o actualización (hardware)	3	50%	2	MEDIO

			[A.7]Uso no previsto	2	50%	3	MEDIO
			[A.23]Manipulación de los equipos	2	50%	2	MEDIO
			[A.25]Robo	2	100%	2	BAJO
REDES Y COMUNICACIONES	[lan]	Red de área local COOPCEN	[E.9] Errores de [re-]encaminamiento	4	1%	2	ALTO
			[I.8] Fallo de servicios de comunicación	4	50%	3	MEDIO
			[A.5] Suplantación de la identidad del usuario	2	1%	2	ALTO
			[A.12] Análisis de tráfico	2	1%	2	ALTO
			[A.14] Interceptación de información (escucha)	2	1%	2	ALTO
			[A.24] Denegación de servicio	2	1%	2	ALTO
			[E.2]Errores del administrador	3	1%	2	ALTO
			[A.7]Uso no previsto	2	50%	3	MEDIO
			[A.11]Acceso no autorizado	2	50%	3	ALTO
	[PSTN]	Red telefónica	[I.6]Corte del suministro eléctrico	4	50%	2	MEDIO
			[A.7]Uso no previsto	2	50%	2	BAJO
			[A.9] Re-encaminamiento de mensajes	2	1%	2	ALTO
SOPORTES DE INFORMACION	[disk]	Disco externo	[A.11]Acceso no autorizado	1	50%	2	MEDIO
			[E.15]Alteración accidental de la información	3	1%	3	MUY ALTO
			[E.25]Perdida de equipos	2	100%	5	ALTO
			[I.10]Degradación de los soportes de almacenamiento	2	50%	2	BAJO
			[A.25]Robo	2	100%	5	ALTO
			[A.7]Uso no previsto	4	50%	3	MEDIO

	[san]	Almacenamiento en red	[A.11]Acceso no autorizado	1	50%	3	ALTO
			[E.15]Alteración accidental de la información	4	1%	3	MUY ALTO
			[E.25]Perdida de equipos	2	100%	5	ALTO
			[I.10]Degradación de los soportes de almacenamiento	2	50%	3	MEDIO
	[usb]	almacenamiento externo baja capacidad USB	[A.11]Acceso no autorizado	1	50%	2	MEDIO
			[E.15]Alteración accidental de la información	4	1%	3	MUY ALTO
			[E.25]Perdida de equipos	2	100%	5	ALTO
			[I.10]Degradación de los soportes de almacenamiento	2	50%	2	BAJO
			[A.25]Robo	2	100%	5	ALTO
			[A.7]Uso no previsto	4	50%	3	MEDIO
INSTALACIONES	[Infra]	Planta física COOPCEN	[N.1] Fuego	1	100%	8	MUY ALTO
			[N.2] Daños por agua	4	50%	2	MEDIO
			[N.*] Desastres naturales.	2	100%	3	MEDIO
			[A.27] Ocupación enemiga	2	50%	2	MEDIO
			[A.11]Acceso no autorizado	2	50%	3	ALTO
			[A.26]Ataque destructivo	2	50%	2	MEDIO
ELEMENTOS AUXILIARES	[UPS]	Sistemas de alimentación interrumpida	[I.7]Condiciones inadecuadas de temperatura o humedad	3	50%	2	MEDIO
			[I.9]Interrupción de otros servicios o suministros esenciales	3	50%	2	MEDIO
			[I.5]Avería de origen físico o lógico	3	100%	5	ALTO

	[cabling]	Sistema Cableado UTP Cat 5	[N.1] Fuego	1	100%	5	ALTO
			[N.2]Daño por agua	1	50%	2	MEDIO
			[I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	2	MEDIO
			[E.2] Errores del administrador	2	1%	5	
	[can]	Canaleta 22 12X5	[N.1] Fuego	1	100%	2	BAJO
			[N.2]Daño por agua	1	1%	1	MUY BAJO
			[I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	2	MEDIO
	[wire]	Sistema Cableado eléctrico	[N.1] Fuego	1	100%	3	MEDIO
			[N.2]Daño por agua	1	1%	1	MUY BAJO
			[I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	2	MEDIO
PERSONAL	[ui]	personal interno administrativos	[A.28] Indisponibilidad del personal	3	1%	1	MEDIO
			[E.1] Errores de los usuarios	4	1%	2	ALTO
			[A.30] Ingeniería social (picaresca)	2	1%	2	ALTO

Fuente: El autor

6.2.2 Valoración Del Riesgo. Para la valoración del riesgo se realiza la matriz de riesgo tabla No. 13, la cual especifica la relación entre el impacto y la probabilidad que ya se evaluaron en la tabla No. 12, de tal amanera que para obtener el riesgo se utilizara la ecuación matemática siguiente:

RIESGO= Probabilidad * Impacto

Tabla 13. Matriz de riesgo

PROBABILIDAD	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24

2	2	4	6	10	16
1	1	2	3	5	8
	1	2	3	4	8
	IMPACTO				

Fuente: El autor

El resultado de la operación anterior será acotejado con la matriz de impacto para conocer su valor y así poder relacionarlo cualitativamente con la tabla No. 14 nivel de riesgo.

Tabla 14. Nivel de Riesgo

NIVEL DE RIESGO	
11-40	EXTREMO
8-10	INTOLERANTE
3-7	TOLERANTE
1-2	ACEPTABLE

Fuente: El autor

Este proceso se realiza con los diferentes activos identificados en COOPCEN obteniendo los niveles de riesgos descritos en la tabla No. 15.

Tabla 15. Estimación del riesgo

TIPO DE ACTIVO	Cód. ACTIVO	DESCRIPCION	AMENZAS	FRECUENCIA	DAÑO/IMPACTO (VALOR)	RIESGO Cuantitativo	RIESGO cualitativo
DATOS	[BD]	Base de datos en la nube	[E.1] Errores de los usuarios	5	1	5	TOLERABLE
			[E.21] Errores de mantenimiento / actualización (software)	3	1	3	TOLERABLE
			[E.15]Alteración accidental de la información	4	1	4	TOLERABLE
			[A.6] Abuso de privilegios de acceso	2	2	4	TOLERABLE
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE
			[A.24]Denegación de servicio	2	2	4	TOLERABLE

	[files]	Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.	[N.1]Fuego	1	5	5	TOLERABLE
			[N.2]Daño por agua	1	3	3	TOLERABLE
			[A.11]Acceso no autorizado	2	2	4	TOLERABLE
			[A.25]Robo	2	3	6	TOLERABLE
	[int]	Archivo principal de información asociados, proveedores, convenios, comunicados, circulares.	[N.1]Fuego	1	8	8	INTOLERANTE
			[N.2]Daño por agua	1	5	5	TOLERABLE
			[A.11]Acceso no autorizado	2	2	4	TOLERABLE
			[A.25]Robo	2	3	6	TOLERABLE
SERVICIOS	[www]	Internet	[I.8] Fallo de servicios de comunicación	4	8	32	EXTREMO
			[A.11]Acceso no autorizado	2	2	4	TOLERABLE
			[A.7]Uso no previsto	4	2	8	INTOLERABLE
			[I.6]Corte del suministro eléctrico	4	3	12	INTOLERABLE
	[file]	Almacenamiento en la nube de BD	[I.9]Interrupción de otros servicios o suministros esenciales	4	2	8	INTOLERABLE
	[servimp]	Impresión y scanner en red	[A.7]Uso no previsto	4	2	8	INTOLERANTE
			[I.6]Corte del suministro eléctrico	4	2	8	INTOLERABLE
			[I.9]Interrupción de otros servicios o suministros esenciales	4	1	4	TOLERABLE
SOFTWARE APLICA	[sub]	Sistema financiero LINIX web - escritorio	[I.8] Fallo de servicios de comunicación	4	5	20	EXTREMO
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE
			[E.1] Errores de los usuarios	5	1	5	TOLERABLE

CIONES			[A.7] Uso no previsto	2	1	2	ACEPTABLE
			[A.24] Denegación de servicio	2	2	4	TOLERABLE
			[A.11] Acceso no autorizado	2	3	6	TOLERABLE
			[A.18]Destrucción de la Información	2	5	10	INTOLERABLE
	[office]	OFFICE 2010	[E.21] Errores de mantenimiento / actualización (software)	4	3	12	INTOLERABLE
			[E.20] Vulnerabilidades de los programas (software)	3	3	9	INTOLERABLE
			[A.7] Uso no previsto	4	1	4	TOLERABLE
			[E.4] Errores de configuración	3	1	3	TOLERABLE
			[E.8] Difusión de software dañino	4	5	20	EXTREMO
			[A.11] Acceso no autorizado	2	2	4	TOLERABLE
			[A.22]Manipulación de programas	3	2	6	TOLERABLE
	[os]	WINDOWS 7 PRO OEM	[E.20] Vulnerabilidades de los programas (software)	4	5	20	EXTREMO
			[E.8] Difusión de software dañino	4	5	20	EXTREMO
			[A.7] Uso no previsto	2	3	6	TOLERABLE
			[A.11]Acceso no autorizado	2	3	6	TOLERABLE
			[A.15]Modificación deliberada de la información	2	2	4	TOLERABLE
			[E.4] Errores de configuración	3	2	6	TOLERABLE
			[A.22]Manipulación de programas	3	3	9	INTOLERANTE
	[browser]	Google Chrome	[E.20] Vulnerabilidades de los programas (software)	3	3	9	INTOLERABLE
			[A.7] Uso no previsto	4	2	8	INTOLERANTE

			[E.4] Errores de configuración	3	1	3	TOLERABLE
			[E.8] Difusión de software dañino	4	3	12	INTOLERANTE
			[A.11] Acceso no autorizado	2	2	4	TOLERABLE
			[A.22]Manipulación de programas	3	2	6	TOLERABLE
			[A.22]Manipulación de programas	3	2	6	TOLERABLE
HARDWARE	[cel]	Celular Smartphone empresarial	[E.25]Perdida de equipos	2	3	6	TOLERABLE
			[A.7]Uso no previsto	4	2	8	INTOLERANTE
			[A.25]Robo	2	2	4	TOLERABLE
	[mobile]	Equipo portátil	[I.6]Corte del suministro eléctrico	3	2	12	TOLERABLE
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE
			[E.23] Errores de mantenimiento o actualización (hardware)	3	2	6	TOLERABLE
			[I.3]Contaminación mecánica	4	3	12	INTOLERANTE
			[E.25]Perdida de equipos	2	3	6	TOLERABLE
			[A.6] Abuso de privilegios de acceso	2	3	6	TOLERABLE
			[A.7]Uso no previsto	2	2	4	TOLERABLE
			[A.23]Manipulación de los equipos	2	2	4	TOLERABLE
	[pc]	Equipo de mesa	[I.6]Corte del suministro eléctrico	4	3	12	TOLERABLE
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE
			[E.23] Errores de mantenimiento o actualización (hardware)	3	2	6	TOLERABLE
			[I.3]Contaminación mecánica	4	3	12	INTOLERANTE
			[E.25]Perdida de equipos	2	5	10	INTOLERANTE

			[A.6] Abuso de privilegios de acceso	2	3	6	TOLERABLE
			[A.7]Uso no previsto	4	3	12	INTOLERANTE
			[A.23]Manipulación de los equipos	2	2	4	TOLERABLE
	[print]	Impresoras	[I.5]Avería de origen físico o lógico	3	2	6	TOLERABLE
			[E.23] Errores de mantenimiento o actualización (hardware)	3	2	6	TOLERABLE
			[I.3]Contaminación mecánica	4	3	12	INTOLERANTE
			[E.25]Perdida de equipos	2	3	6	INTOLERABLE
			[A.6] Abuso de privilegios de acceso	2	1	2	ACEPTABLE
			[A.7]Uso no previsto	4	3	12	INTOLERANTE
			[A.23]Manipulación de los equipos	2	2	4	TOLERABLE
	[modem]	Modem internet	[I.7] Condiciones inadecuadas de temperaturas o humedad	5	3	15	EXTREMO
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE
			[E.23] Errores de mantenimiento o actualización (hardware)	2	3	6	TOLERABLE
			[E.25]Perdida de equipos	3	3	9	INTOLERABLE
			[A.7]Uso no previsto	2	3	6	TOLERABLE
			[I.6]Corte del suministro eléctrico	3	2	6	TOLERABLE
			[A.23]Manipulación de los equipos	2	3	6	TOLERABLE
	[switch]	SW 24 Puertos	[I.7] Condiciones inadecuadas de temperaturas o humedad	3	3	9	INTOLERANTE
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE

			[E.23] Errores de mantenimiento o actualización (hardware)	1	5	5	TOLERABLE
			[E.25]Perdida de equipos	2	5	10	INTOLERANTE
			[A.7]Uso no previsto	2	3	6	TOLERABLE
			[I.6]Corte del suministro eléctrico	2	3	6	TOLERABLE
			[A.23]Manipulación de los equipos	2	3	6	TOLERABLE
			[E.2]Errores del administrador	3	2	6	TOLERABLE
			[A.11]Acceso no autorizado	2	3	6	TOLERABLE
	[wap]	Access Point	[I.7] Condiciones inadecuadas de temperaturas o humedad	5	2	10	INTOLERANTE
			[I.5]Avería de origen físico o lógico	3	2	6	TOLERABLE
			[E.23] Errores de mantenimiento o actualización (hardware)	3	2	6	TOLERABLE
			[E.25]Perdida de equipos	2	3	6	TOLERABLE
			[A.7]Uso no previsto	2	2	4	TOLERABLE
			[I.6]Corte del suministro eléctrico	4	2	8	TOLERABLE
			[A.23]Manipulación de los equipos	2	2	4	TOLERABLE
			[E.2]Errores del administrador	3	1	3	TOLERABLE
			[A.11]Acceso no autorizado	2	2	4	TOLERABLE
			[E.9]Errores de Re-encaminamiento	2	1	2	ACEPTABLE
	[cam]	Cámaras de seguridad	[I.3]Contaminación mecánica	4	2	8	INTOLERANTE
			[I.5]Avería de origen físico o lógico	3	3	9	INTOLERANTE
			[E.23] Errores de mantenimiento o actualización (hardware)	3	2	6	TOLERABLE

			[A.7]Uso no previsto	2	3	6	TOLERABLE
			[A.23]Manipulación de los equipos	2	2	4	TOLERABLE
			[A.25]Robo	2	2	4	TOLERABLE
REDES Y COMUNICACIONES	[lan]	Red de área local COOPCEN	[E.9] Errores de [re-]encaminamiento	4	3	12	INTOLERABLE
			[I.8] Fallo de servicios de comunicación	4	3	12	INTOLERANTE
			[A.5] Suplantación de la identidad del usuario	2	2	4	TOLERABLE
			[A.12] Análisis de tráfico	2	2	4	TOLERABLE
			[A.14] Interceptación de información (escucha)	2	2	4	TOLERABLE
			[A.24] Denegación de servicio	2	2	4	TOLERABLE
			[E.2]Errores del administrador	3	2	6	TOLERABLE
			[A.7]Uso no previsto	2	3	6	TOLERABLE
			[A.11]Acceso no autorizado	2	3	6	TOLERABLE
	[PSTN]	Red telefónica	[I.6]Corte del suministro eléctrico	2	2	4	TOLERABLE
			[A.7]Uso no previsto	2	2	4	TOLERABLE
			[A.9] Re-encaminamiento de mensajes	2	2	4	TOLERABLE
SOPORTES DE INFORMACION	[disk]	Disco externo	[A.11]Acceso no autorizado	1	2	2	ACEPTABLE
			[E.15]Alteración accidental de la información	3	3	9	INTOLERANTE
			[E.25]Perdida de equipos	2	5	10	INTOLERANTE
			[I.10]Degradación de los soportes de almacenamiento	2	2	4	TOLERABLE
			[A.25]Robo	2	5	10	INTOLERANTE
			[A.7]Uso no previsto	4	3	12	INTOLERANTE

	[san]	Almacenamiento en red	[A.11]Acceso no autorizado	1	3	3	TOLERABLE
			[E.15]Alteración accidental de la información	4	3	12	INTOLERANTE
			[E.25]Perdida de equipos	2	5	10	INTOLERANTE
			[I.10]Degradación de los soportes de almacenamiento	2	3	6	TOLERABLE
	[usb]	almacenamiento externo baja capacidad USB	[A.11]Acceso no autorizado	1	2	2	ACEPTABLE
			[E.15]Alteración accidental de la información	4	3	12	INTOLERANTE
			[E.25]Perdida de equipos	2	5	10	INTOLERABLE
			[I.10]Degradación de los soportes de almacenamiento	2	2	4	TOLERABLE
			[A.25]Robo	2	5	10	INTOLERANTE
			[A.7]Uso no previsto	4	3	12	INTOLERANTE
INSTALACIONES	[Infra]	Planta física COOPCEN	[N.1] Fuego	1	8	8	INTOLERANTE
			[N.2] Daños por agua	4	2	8	INTOLERANTE
			[N.*] Desastres naturales.	2	3	6	TOLERABLE
			[A.27] Ocupación enemiga	2	2	4	TOLERABLE
			[A.11]Acceso no autorizado	2	3	6	TOLERABLE
			[A.26]Ataque destructivo	2	2	4	TOLERABLE
ELEMENTOS AUXILIARES	[UPS]	Sistemas de alimentación interrumpida	[I.7]Condiciones inadecuadas de temperatura o humedad	3	2	6	TOLERABLE
			[I.9]Interrupción de otros servicios o suministros esenciales	3	2	6	TOLERABLE
			[I.5]Avería de origen físico o lógico	3	5	15	INTOLERANTE
	[cabling]		[N.1] Fuego	1	5	5	TOLERABLE
			[N.2]Daño por agua	1	2	2	ACEPTABLE

	[can]	Sistema Cableado UTP Cat 5	[I.7] Condiciones inadecuadas de temperatura o humedad	3	2	6	TOLERABLE
			[E.2] Errores del administrador	2	5	10	INTOLERABLE
		Canaleta 22 12X5	[N.1] Fuego	1	2	2	ACEPTABLE
			[N.2]Daño por agua	1	1	1	ACEPTABLE
			[I.7] Condiciones inadecuadas de temperatura o humedad	3	2	6	TOLERABLE
	[wire]	Sistema Cableado eléctrico	[N.1] Fuego	1	3	3	TOLERABLE
			[N.2]Daño por agua	1	1	1	ACEPTABLE
			[I.7] Condiciones inadecuadas de temperatura o humedad	3	2	6	TOLERABLE
PERSONAL	[ui]	personal interno administrativos	[A.28] Indisponibilidad del personal	3	1	3	TOLERABLE
			[E.1] Errores de los usuarios	4	2	8	INTOLERANTE
			[A.30] Ingeniería social (picaresca)	2	2	4	TOLERABLE

Fuente: El autor

Con la anterior matriz, que expone la estimación del riesgo, se puede deducir que: de los 29 activos de información que intervienen en el presente proyecto 5 de ellos que corresponde a un 17,24 % están en un nivel de Riesgo extremo, estos 5 son:

- Internet
- Sistema financiero Linix web - escritorio
- Office 2010
- Windows 7 OEM
- Modem internet

Como uno de los objetivos del proyecto es abordar y determinar controles alineados a la norma ISO/IEC 27001:2013 para la gestión de los riesgos de aquellos activos con nivel extremo e intolerable, el análisis del nivel de riesgo también arrojo un total de 24 activos equivalente a un 82,7% frente al total de activos, los cuales presentan un nivel de riesgo intolerable, que son:

- Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.
- Archivo principal de información asociados, proveedores, convenios, comunicados, circulares.

- Internet
- impresión y scanner en red
- Sistema financiero LINIX web - escritorio
- OFFICE 2010
- WINDOWS 7 PRO OEM
- Google Chrome
- Celular Smartphone empresarial
- Equipo portátil
- Equipo de mesa
- Impresoras
- Modem internet
- SW 24 Puertos
- Access Point
- Cámaras de seguridad
- Red de área local COOPCEN
- Disco externo
- Almacenamiento en red
- almacenamiento externo baja capacidad USB
- Planta física COOPCEN
- Sistemas de alimentación interrumpida
- Sistema Cableado UTP Cat 5
- Personal interno administrativos

Cabe mencionar que, dependiendo de la amenaza relacionada con el activo según tabla No. 15 estimación del riesgo, el activo puede tener o no varios niveles de riesgo extremo e intolerable como es el caso del activo sistema operativo Windows 7 Pro OEM que tiene dos amenazas ([E.20] Vulnerabilidades de los programas (software) y [E.8] Difusión de software dañino) en nivel extremo a lo cual se le prestara atención para generar controles adecuados.

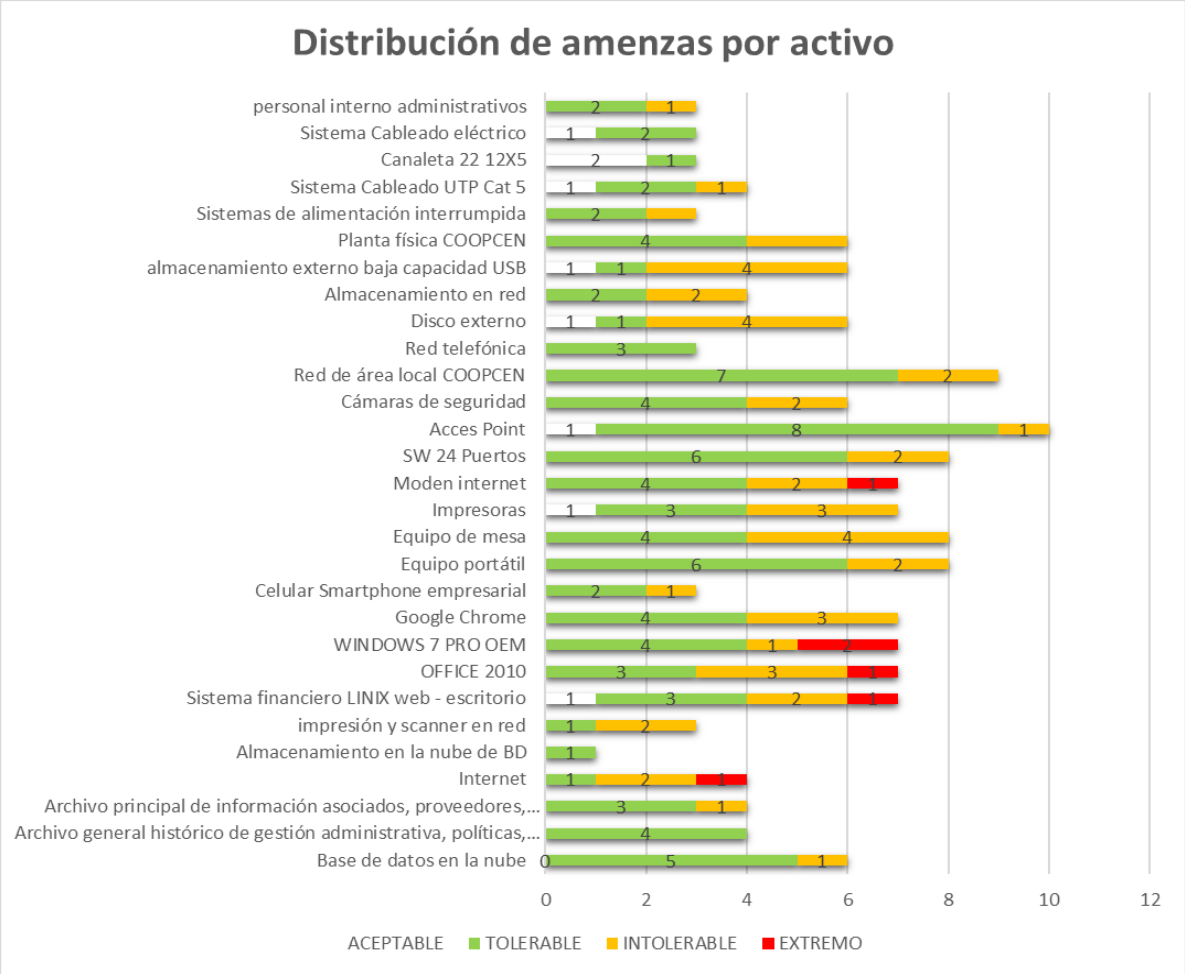
A continuación, se representa gráficamente la distribución de las amenazas con su respectivo nivel de riesgo para los diferentes activos de las áreas de secretaría, cartera, contabilidad, tesorería y sistemas que intervienen en los procesos misionales y están estrechamente relacionados con los datos que se procesan, almacenan y presentan salidas.

En el gráfico están definidos los 29 activos de información organizados de manera vertical, cada uno de estos tiene una barra horizontal en la cual están distribuidas las amenazas identificadas para el activo, cada amenaza genera un nivel de riesgo el cual se calculó bajo la tabla No. 15 estimación del riesgo y que puede ser aceptable, tolerable, intolerable y extremo, por ejemplo:

Para el activo de información Office 2010 se identificaron un total de 7 amenazas las cuales, según cálculo del nivel de riesgo (probabilidad de ocurrencia * impacto)

se tiene, 3 amenazas impactan de forma tolerable, otras 3 de forma intolerable y 1 de manera extrema, para conocer el tipo de amenaza y su nivel de riesgo se describe en la tabla No. 15 estimación del riesgo.

Figura 3. Distribución de amenazas por activo



Fuente: El autor

6.3. FASE 3: ESTABLECIMIENTO DE CONTROLES NECESARIOS, DE ACUERDO A LA NORMA ISO/IEC 27001:2013 QUE PERMITAN GARANTIZAR LA DISPONIBILIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN.

6.3.1 Plan De Tratamiento De Riesgos. Los pasos anteriores permitieron definir, clasificar y evaluar los activos de información sobre los cuales existen amenazas y riesgos realmente potenciales que se identificaron y cuantificaron, bajo la metodología MAGERIT.

Sobre este análisis se generan controles con el fin de poder minimizar el impacto para los activos donde el nivel de riesgo es extremo e intolerable, dichos controles están relacionados con la norma ISO 27001 en su versión 2013 y alineados con la guía de buenas prácticas ISO/IEC 27002:2013, los cuales pueden ser tratados de la siguiente manera según metodología MAGERIT:

Eliminar: bajo este tratamiento se quiere eliminar totalmente el impacto, esto puede darse ya sea eliminando el activo o procesos que generar un alto grado de riesgo.

Reducir: son medidas basadas en actividades técnicas u organizativas que permiten mitigar el riesgo, entre estas actividades se tiene los planes de contingencia, adquisición de elementos para reforzar la protección a los activos.

Asumir: no habrá medidas frente a un riesgo, esto será aplicable teniendo en cuenta que el activo no sufra degradación considerable que pueda afectar la continuidad del negocio.

A continuación, en la tabla No. 16 se genera el plan de tratamiento de riesgos para los activos de mayor riesgo.

Tabla 16. Plan de tratamiento de Riesgos

DESCRIPCIÓN ACTIVO	AMENAZA	VULNERABILIDAD	VALORACIÓN DEL RIESGO	PLAN DE TRATAMIENTO DEL RIESGOS	CONTROL ISO 27002
Base de datos en la nube	[I.5] Avería de origen físico o lógico	Inexistencia de seguimiento al servicio del proveedor	Intolerable	Se debe verificar las políticas de seguridad de la información con el proveedor prestador del servicio de almacenamiento y alojamiento de base de datos del sistema financiero actual, con el fin de conocer y corregir condiciones del contrato.	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores
				Se deberá generar un seguimiento y auditar los servicios del proveedor, que permita minimizar caídas del servicio de almacenamiento remoto de BD	15.2.1 Supervisión y revisión de los servicios prestados por terceros

Archivo Principal	[N.1]Fuego	Inexistencia de elementos que controlen las condiciones inadecuadas de temperatura	Intolerable	Generar medidas para la identificación de posibles indicios de incendio, como alarma detectora de humo. También se debe replantear la distribución de los extintores presentes en la infraestructura, para verificar si su ubicación son las adecuadas.	11.1.4 Protección contra las amenazas externas y ambientales
INTERNET	[I.8] Fallo de servicios de comunicación	Inexistencia de respaldo de proveedor de internet	Extremo	Se debe generar planes de contingencia, recuperación y retorno ante una eventual caída del servicio.	17.1.1 Planificación de la continuidad de la seguridad de la información
				se debe contar con servicio de respaldo de internet para suplir la caída del servicio primario.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
	[A.7] Uso no previsto	Falta de políticas para el uso de los activos	Intolerable	Generar reglas o políticas que regulen el uso de manera eficiente del activo.	8.1.3 Uso aceptable de los activos
	[I.6]Corte del suministro eléctrico	Activo no está dentro de la red de respaldo de energía eléctrica	Intolerable	Adaptar el sistema eléctrico alterno a las necesidades de la organización.	11.2.2 Instalaciones de suministro
Almacenamiento en la nube de BD	[I.9]Interrupción de otros servicios o suministros esenciales	No existe seguimiento y monitorización de los servicios del proveedor	Intolerable	Contar con el proveedor mecanismos de comunicación de peticiones, quejas y reclamos para solventar caída del servicio de tal manera que se hace necesario revisar el nivel de servicio de este.	15.2.1 Supervisión y revisión de los servicios prestados por terceros

Impresión y scanner en red	[A.7] Uso no previsto	Falta de políticas para el uso de los activos	Intolerable	Generar reglas o políticas que regulen el uso de manera eficiente del activo.	8.1.3 Uso aceptable de los activos
Sistema financiero LINIX web - escritorio	[I.8] Fallo de servicios de comunicación	No hay gestión y monitoreo del servicio de software ante vulnerabilidades técnicas.	Extremo	Generar pruebas que permitan identificar las debilidades tanto por parte del servicio como de la organización en el software	12.6.1 Gestión de las vulnerabilidades técnicas
Sistema financiero LINIX web - escritorio	[I.5] Avería de origen físico o lógico	Inexistencia de seguimiento al servicio del proveedor	Intolerable	Se debe verificar las políticas de seguridad de la información con el proveedor prestador del servicio de software financiero actual, con el fin de conocer y corregir condiciones del contrato.	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores
				Se deberá generar un seguimiento y auditar los servicios del proveedor, que permita minimizar caídas del servicio de software financiero.	15.2.1 Supervisión y revisión de los servicios prestados por terceros
	[A.18]Destrucción de la Información	No existe respaldo de la información del sistema del contable	Intolerable	Mediante política debe realizar copias de seguridad y exigir al proveedor la entrega de estos bajo el un plan estructurado.	12.3.1 Copias de seguridad de la información
OFFICE 2010	[E.21] Errores de mantenimiento / actualización (software)	No existe información de los mantenimientos de software	Intolerable	Documentar todo cambio realizado al paquete de software suministrado por un tercero	12.5.1 Instalación del software en sistemas en producción
	[E.20] Vulnerabilidades de los	versión Paquete de software obsoleto	Intolerable	Definir la necesidad y procedimiento para la actualización del	12.5.1 Instalación del software en

	programas (software)			paquete de software.	sistemas en producción
	[E.8] Difusión de software dañino	Inexistencia de procedimiento para instalación de software	Extremo	Controlar las instalaciones de software, mediante herramienta de monitoreo	12.5.1 Instalación del software en sistemas en producción
WINDOWS 7 PRO OEM	[E.20] Vulnerabilidades de los programas (software)	versión Paquete de Sistema operativo obsoleto	Extremo	Definir la necesidad para la actualización del Sistema operativo.	12.5.1 Instalación del software en sistemas en producción
	[E.8] Difusión de software dañino	Inexistencia de procedimiento para instalación de software	Extremo	Controlar las instalaciones de software, mediante herramienta de monitoreo	12.6.2 Restricciones en la instalación de software
	A.22]Manipulación de programas	Inexistencia de políticas y perfiles para el acceso al sistema	Intolerable	Implementar política que permita controlar el acceso al sistema operativo.	9.1.1 Política de control de accesos
Google Chrome	[E.20] Vulnerabilidades de los programas (software)	versión Paquete de software obsoleto	Intolerable	Definir la necesidad y procedimiento para la actualización del paquete de software.	12.5.1 Instalación del software en sistemas en producción
Celular Smartphone empresarial	[A.7]Uso no previsto	Falta de políticas para el uso de los activos	Intolerable	Generar reglas o políticas que regulen el uso de manera eficiente del activo.	8.1.3 Uso aceptable de los activos
Equipo portátil	[I.5]Avería de origen físico o lógico	Avería por el uso y tiempo	Intolerable	definir un plan de mantenimiento bajo una estructura definido tiempos acordes para evitar desgaste físico y lógico del equipo de cómputo	11.2.4 Mantenimiento de los equipos

	[I.3]Contaminación mecánica	No existe definición de puestos de trabajo y ubicación del activo	Intolerable	Análisis de lugar donde se ubica el activo aislándolo del agua, polvo y fuego, implementando sistema de control de temperatura e incendios.	11.1.4 Protección contra las amenazas externas y ambientales
Equipo de mesa	[I.5]Avería de origen físico o lógico	Avería por el uso y tiempo	Intolerable	Definir un plan de mantenimiento bajo una estructura, definido tiempos acordes para evitar desgaste físico y lógico, bajo este plan se identifica la vida útil del activo o su respectivo cambio ya sea por el proveedor del servicio u adquisición de nueva tecnología.	11.2.4 Mantenimiento de los equipos
	[I.3]Contaminación mecánica	No existe definición de puestos de trabajo y ubicación del activo	Intolerable	Se debe generar un plan de respuesta de emergencia y definir mecanismos para identificar las condiciones inadecuadas de temperatura (humedad y calor) del ambiente que puedan generar impacto en los activos presentes. Entre estos a tener en cuenta calefactores y sistemas de aire acondicionado. Teniendo en cuenta que los sistemas deben generar alarmas que pongan en preaviso al personal encargado para	11.1.4 Protección contra las amenazas externas y ambientales

				tomar las medidas necesarias de las condiciones ambientales.	
	[E.25]Perdida de equipos	No existe una identificación de activos de fácil control.	Intolerable	Contar con un inventario de activos permanentemente actualizado, describiendo en este los elementos obsoletos y en uso.	8.1.1 Inventario de activos
		No existe un sistema de monitoreo constante para los equipos de mesa		Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	11.2.1 Ubicación y protección de equipos
	[A.7]Uso no previsto	Falta de políticas para el uso de los activos	Intolerable	Generar reglas o políticas que regulen el uso de manera eficiente del activo.	8.1.3 Uso aceptable de los activos

Modem internet	[I.7] Condiciones inadecuadas de temperaturas o humedad	No existe un sistema de monitoreo constante para los equipos de telecomunicación	Extremo	Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	11.2.1 Ubicación y protección de equipos
	[I.5]Avería de origen físico o lógico	No ha existido cambio de tecnología por parte del proveedor del servicio de internet	Intolerable	Definir un plan de mantenimiento bajo una estructura, definido tiempos acordes para evitar desgaste físico y lógico, bajo este plan se identifica la vida útil del activo o su respectivo cambio ya sea por el proveedor del servicio u adquisición de nueva tecnología.	11.2.4 Mantenimiento de los equipos
	[E.25]Perdida de equipos	Ubicación inadecuada	Intolerable	Se debe definir la ubicación correcta del activo, donde se reduzca los riesgos de acceso no autorizados y peligros ambientales.	11.2.1 Ubicación y protección de equipos

switch 24 puertos	[I.7] Condiciones inadecuadas de temperaturas o humedad	No existe un sistema de monitoreo constante para los equipos de telecomunicación	Intolerable	Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	11.2.1 Ubicación y protección de equipos
	[I.5]Avería de origen físico o lógico	Avería por el uso y tiempo	Intolerable	Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	11.2.1 Ubicación y protección de equipos
	[E.25]Perdida de equipos	Ubicación inadecuada	Intolerable	Se debe definir la ubicación correcta del activo, donde se reduzca los riesgos de acceso no autorizados y	11.2.1 Ubicación y protección de equipos

				peligros ambientales.	
Access Point	[I.7] Condiciones inadecuadas de temperaturas o humedad	No existe un sistema de monitoreo constante para los equipos de telecomunicación	Intolerable	Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	11.2.1 Ubicación y protección de equipos
Cámaras de seguridad	[I.3]Contaminación mecánica	protección física inadecuada	Intolerable	Definir un sistema de protección adecuado, donde las condiciones inadecuadas del medio ambiente (polvo, agua, calor) tengan un impacto menor.	11.1.4 Protección contra las amenazas externas y ambientales
	[I.5]Avería de origen físico o lógico	Avería por el uso y tiempo	Intolerable	Definir un plan de mantenimiento bajo una estructura, definiendo tiempos acordes para evitar desgaste físico y lógico, bajo este plan se identifica la vida útil del activo o su respectivo cambio ya sea por el proveedor del servicio u adquisición de nueva tecnología.	11.2.4 Mantenimiento de los equipos

Red de área local COOPCEN	[E.8] Errores de Re-encaminamiento	No hay control de trasporte de información ni de equipos de las diferentes áreas.	Intolerable	Generar actividades de separación física y lógica de la red de datos, cada segmento estará basado bajo las diferentes tareas y procesos que genera cada área con el fin de definir privilegios en la red de cada segmento. Generar actividades de separación física y lógica de la red de datos, cada segmento estará basado bajo las diferentes tareas y procesos que genera cada área con el fin de definir privilegios en la red de cada segmento.	13.1.3 Segregación de redes
	[I.8] Fallo de servicios de comunicación	No hay seguridad en el cableado de red		Generar revisión del cableado de red para verificar su estado y cumplimiento de las normas actuales, con fin de que esta brinde soporte a los elementos interconectados	11.2.3 Seguridad del cableado
		No hay información de las vulnerabilidades del activo	Intolerable	Se debe obtener un panorama de las vulnerabilidades técnicas del activo, mediante la realización de pruebas y ataques simulados y escaneos de vulnerabilidades.	12.6.1 Gestión de las vulnerabilidades técnicas

Disco externo	[E.15]Alteración accidental de la información	Falta del procedimiento para el trasporte de información en medios extraíbles	Intolerable	Se debe generar un procedimiento para el uso de medios extraíbles donde se informe la forma de trasportar información y quienes serán los directos responsables para dicho proceso.	8.3.1 Gestión de soportes extraíbles
	[E.25]Perdida de equipos	No existe una identificación de activos de fácil control.	Intolerable	Contar con un inventario de activos permanentemente actualizado, describiendo en este los elementos obsoletos y en uso.	8.1.1 Inventario de activos
	[A.7]Uso no previsto	Falta de políticas para el uso de los activos	Intolerable	Generar reglas o políticas que regulen el uso de manera eficiente del activo.	8.1.3 Uso aceptable de los activos
	[A.25]Robo	Ubicación inadecuada del activo	Intolerable	Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	11.2.1 Ubicación y protección de equipos
Almacenamiento en red	[E.15]Alteración accidental de la	No existe configuración de privilegios	Intolerable	Definir y revisar los privilegios de usuario, limitando acciones en los	9.2.5 Revisión de los derechos de acceso

	información			dispositivos de almacenamiento.	de los usuarios.
	[E.25]Perdida de equipos	Ubicación inadecuada	Intolerable	Se debe definir la ubicación correcta del activo, donde se reduzca los riesgos de acceso no autorizados y peligros ambientales.	11.2.1 Emplazamiento y protección de equipos
				Definir límites de acceso a instalaciones de procesamiento de información, asegurando el acceso a usuarios no autorizados.	9.1.1 Política de control de accesos
almacenamiento externo baja capacidad USB	[E.15]Alteración accidental de la información	Falta del procedimiento para el trasporte de información en medios extraíbles	Intolerable	Se debe generar un procedimiento para el uso de medios extraíbles donde se dé a conocer la forma de trasportar información y quienes serán los directos responsables para dicho proceso.	8.3.1 Gestión de soportes extraíbles
	[E.25]Perdida de equipos	No existe una identificación de activos de fácil control.	Intolerable	Contar con un inventario de activos permanentemente actualizado, describiendo en este los elementos obsoletos y en uso.	8.1.1 Inventario de activos
	[A.25]Robo	Ubicación inadecuada del activo	Intolerable	Definir un sistema de protección adecuado en el área específica donde se ubica el activo que permita identificar presencia no deseada, mediante la utilización de sistemas de detección de intrusos o circuito	11.2.1 Ubicación y protección de equipos

				cerrado de televisión, asegurar el perímetro de la Cooperativa, previniendo cualquier intento de acceso indebido.	
	[A.7]Uso no previsto	Falta de políticas para el uso de los activos	Intolerable	Generar reglas o políticas que regulen el uso de manera eficiente del activo.	8.1.3 Uso aceptable de los activos
Planta física COOPCEN	[N.1] Fuego	No hay verificación periódica de los mecanismos de protección de la seguridad física	Intolerable	Se debe identificar y analizar las medidas de protección actuales, plantear un plan de contingencia ante desastres donde se relacione las actividades antes, durante y después de una eventual materialización de la amenaza	11.1.4 Protección contra las amenazas externas y ambientales
	[N.2] Daños por agua	No hay verificación periódica de los mecanismos de protección de la seguridad física	Intolerable		11.1.4 Protección contra las amenazas externas y ambientales
Sistemas de alimentación interrumpida	[I.5]Avería de origen físico o lógico	Avería por el uso y tiempo	Intolerable	Definir un plan de mantenimiento bajo una estructura, definido tiempos acordes para evitar desgaste físico y lógico, bajo este plan se identifica la vida útil del activo.	11.2.4 Mantenimiento de los equipos
Sistema Cableado UTP Cat 5	[E.2] Errores del administrador	No existe etiquetas cables de red para su identificación	Intolerable	Mantenimiento de la red cableada donde se realice la respectiva identificación del cableado de red.	11.2.3 Seguridad del cableado
personal interno administrativo	[E.1] Errores de los usuarios	Desconocimiento sobre las responsabilidades de seguridad de la información.	Intolerable	Es necesario que las políticas que se implemente sean conocidas por el personal y se generen encuentros para	7.2.2 Conciencia ción, educación y capacitació n en

				sensibilizar sobre la seguridad de la información.	Seguridad Informática

Fuente: El autor

6.3.2 Nivel De Cumplimiento Norma ISO/IEC 27001:2013. Bajo el anterior análisis de riesgos se continúa analizando el grado de madurez con respecto a la implementación de la norma ISO/IEC 27001, con que cuentan los procesos de afiliación, crédito, financiero, ingreso de fondos, afiliaciones y gestión tecnológica de las áreas de secretaría, cartera, tesorería y sistemas respectivamente; para obtener dicho análisis se generó la matriz de aplicabilidad mediante el uso del anexo A de la Norma ISO/IEC 27001:2013 donde se especifica si cumple o no con los controles de los diferentes dominios de la norma.

Cada control especificado en la norma es verificado en COOPCEN LTDA bajo entrevistas al personal y observación directa, herramientas que brindaron información, registrada en la matriz de aplicabilidad sobre la cual se calcula el nivel de cumplimiento de cada dominio, con esto se logra identificar el cumplimiento de los dominios y sobre los cuales hay que prestar atención para fortalecer la seguridad de la información.

En la tabla No. 17 se registra el nivel de cumplimiento de los diferentes controles según la norma ISO/IEC 27001:2013, mediante una respuesta que puede ser SI o NO de acuerdo a si la Cooperativa tiene implementado dicho control; Como se observa en la tabla No. 17 tomado como ejemplo, el dominio 6, Aspectos Organizativos, se tiene 7 controles de los cuales se obtiene 1 de respuesta SI, de tal manera que el nivel de cumplimiento sería 1/7= 0,14; el cual se lo multiplica por 100 que equivale al 14% de cumplimiento del dominio 6 Aspectos Organizativos.

Tabla 17. Nivel de cumplimiento

	CONTROLES					**CUMPLE**		**NIVEL DE CUMPLIMIENTO %**
DOMINIO	**OBJETIVO DE CONTROL**	**REFERENCIA**	**CONTROL**	**DESCRIPCIÓN**	**PREGUNTA**	**SI**	**NO**	
5. Políticas Seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1	Políticas para la seguridad de la información	Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección,	¿Existen Políticas para la seguridad de la información?		X	0

				publicado y comunicado a los empleados, así como a todas las partes externas relevantes.				
		5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.	¿Se realiza periódicamente la revisión de las políticas para la seguridad de la información?		X	
6. Aspectos Organizativos SI	6.1 Organización interna	6.1.1	Asignación de responsabilidades para la SI	Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.	¿Hay responsabilidad de los empleados sobre la seguridad de la información?		X	14
		6.1.2	Segregación de tareas	Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada	¿Las funciones de los empleados están definidas, así como la responsabilidad de los activos a cargo?		X	

				o no intencionada, o el de un mal uso de los activos de la organización.				
		6.1.3	Contacto con las autoridades	Se deberían mantener los contactos apropiados con las autoridades pertinentes.	¿Se tiene actualizado el directorio de contactos con autoridades?	X		
		6.1.4	Contacto con grupos de interés especial	Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.	¿Existe contacto con grupos o asociación de seguridad?		X	
		6.1.5	Seguridad de la información en la gestión de proyectos	Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.	¿En los proyectos a ejecutarse en la organización se contempla la seguridad de la información?		X	
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1	Política de uso de dispositivos para movilidad	Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la	¿Se tiene una política para el uso de dispositivos móviles?		X	

				protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.				
		6.2.2	Teletrabajo	Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.	¿Existen políticas para la seguridad de información en la opción de teletrabajo?		X	
7. Seguridad Ligada a los recursos humanos	7.1 Antes de la contratación	7.1.1	Investigación de antecedentes	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y	¿Se realiza verificación de antecedentes para nuevos empleados?	X		67

				los riesgos percibidos.				
		7.1.2	Términos y condiciones de contratación	Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	¿En el contrato de los empleados se determina las obligaciones del trabajo como también de la seguridad de la información?	X		
	7.2 Durante la contratación	7.2.1	Responsabilidades de gestión	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia	¿Se verifica regularmente el cumplimiento de los empleados de las políticas de seguridad de la		X	

				con las políticas y los procedimientos.	información?			
		7.2.2	Concienciación, educación y capacitación en SI	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	¿Se realiza capacitaciones a los empleados en seguridad informática?		X	
		7.2.3	Proceso disciplinario	Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.	¿Existen procesos disciplinarios por incumplimiento del contrato?	X		

	7.3 Cese o cambio de puesto de trabajo	7.3.1	Cese o cambio de puesto de trabajo	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de este deberían estar claramente definidas, comunicadas al empleado o contratista y asignadas efectivamente.	¿Existe proceso para la finalización de un empleado o cambio?	X		
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1	Inventario de activos	Todos los activos deberían estar claramente identificados	¿Se tiene un inventario de los activos claramente identificados y actualizada?		X	0
		8.1.2	Propiedad de los activos	Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.	¿Los activos tienen asignado un responsable?		X	
		8.1.3	Uso aceptable de los activos	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de	¿Se definen norma para el uso de los activos?		X	

				la información y los activos asociados a recursos de tratamiento de la información.				
		8.1.4	Devolución de activos	Todos los empleados y usuarios de terceras partes deberían devolver los activos de la organización que estén en su posesión, una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.	¿Una vez finalizado el contrato del empleado se genera proceso para devolución de activos?		X	
	8.2 Clasificación de la información	8.2.1	Directrices de clasificación	La información debería clasificarse con relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	¿Existe una clasificación de la información en relación a su valor, requisitos legales?		X	
		8.2.2	Etiquetado y manipulado de la información	Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y	¿Existe procedimientos para el etiquetado y tratamiento de la		X	

				tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	información?			
		8.2.3	Manipulación de activos	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.	¿Existe procedimientos para la manipulación de los activos de información dependiendo de su clasificación?		X	
	8.3 Manejo de los soportes de almacenamiento	8.3.1	Gestión de soportes extraíbles	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.	¿Se tiene proceso para el uso y manipulación de medios extraíbles?		X	
		8.3.2	Eliminación de soportes	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando	¿Al terminar su vida útil de los medios extraíbles, estos se desechan de forma adecuada?		X	

				procedimientos formales.				
		8.3.3	Soportes físicos en tránsito	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	¿Se protege la información cuando los soportes son trasladados fuera de la empresa?		X	
9. Control de Accesos	9.1 Requisitos de negocio para el control de accesos	9.1.1	Política de control de accesos	Se debería establecer, documentar y revisar una política de control de accesos con base en las necesidades de seguridad y de negocio de la Organización.	¿Se cuenta con una política donde se especifica las reglas de acceso a los activos de información?		X	29
		9.1.2	Control de acceso a las redes y servicios asociados	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.	¿Se autoriza o restringe el acceso o a las redes y servicios de esta siempre y cuando el tercero o empleado este facultado?	X		

	9.2 Gestión de acceso de usuario	9.2.1	Gestión de altas/bajas en el registro de usuarios	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.	¿Existe un proceso para dar de baja a un empleado con el fin de inhabilitar sus derechos de acceso?		X	
		9.2.2	Gestión de los derechos de acceso asignados a usuarios	Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.	¿Existe un proceso para identificar y modificar la asignación de derechos de acceso a funcionarios como a usuarios?		X	
		9.2.3	Gestión de los derechos de acceso con privilegios especiales	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.	¿Hay control a usuarios o trabajadores con acceso especiales?		X	
		9.2.4	Gestión de información confidencial de autenticación de usuarios	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de	¿Se garantiza que se mantiene la confidencialidad de la información secreta de acceso?		X	

				gestión controlado.				
		9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.	¿Se revisa periódicamente los permisos de acceso?		X	
		9.2.6	Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.	¿Se modifican los derechos de accesos al finalizar o cambio puesto de trabajo?		X	
	9.3 Responsabilidades del usuario	9.3.1	Uso de información confidencial para la autenticación	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información	¿Se exige al empleado que la información de la autenticación sea secreta?		X	

				confidencial para la autenticación.				
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1	Restricción del acceso a la información	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	¿Se restringe el acceso a personal interno como externo al acceso de la información confidencial?		X	
		9.4.2	Procedimientos seguros de inicio de sesión	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on	¿Se verifica y controla el inicio de sesión seguro a los sistemas?		X	
		9.4.3	Gestión de contraseñas de usuario	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.	¿Los sistemas manejan contraseñas fuertes y robustas, bajo una agestión interactiva y adecuada	X		

					para el usuario y empleado?			
		9.4.4	Uso de herramientas de administración de sistemas	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.	¿Se supervisa el uso de software no autorizado?	X		
		9.4.5	Control de acceso al código fuente de los programas	Se debería restringir el acceso al código fuente de las aplicaciones software.	¿Se controla el acceso al código fuente de los sistemas?	X		
10. Cifrado	10.1 Controles criptográficos	10.1.1	Política de uso de los controles criptográficos	Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.	¿Existe una política para la protección de la información mediante controles criptográficos?		X	0
		10.1.2	Gestión de claves	Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas	¿Existe una política para una gestión de claves criptográficas que tengan en cuenta el		X	

				a través de todo su ciclo de vida.	ciclo de vida de estas?			
11. Seguridad física y Ambiental	11.1 Áreas seguras	11.1.1	Perímetro de seguridad física	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.	¿Se restriegue el acceso contra la entrada no autorizada a las instalaciones?	X		40
		11.1.2	Controles físicos de entrada	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.	¿Existen controles de entrada que permitan el acceso a personal autorizado a áreas seguras?	X		
		11.1.3	Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones	¿Las oficinas cuentan con diseño seguro para evitar el acceso no	X		

				de la organización.	autorizado ?			
		11.1.4	Protección contra las amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.	¿Cuentan con protección física contra factores externos y ambientales?		X	
		11.1.5	El trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.	¿Los empleados cuentas con áreas de trabajo seguras?	X		
		11.1.6	Áreas de acceso público, carga y descarga	Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamient	¿Existen controles para las áreas de carga y descarga?	X		

				o de información.				
	11.2 Seguridad de los equipos	11.2.1	Emplazamiento y protección de equipos	Los equipos se deberían ubicar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.	¿Se protege a los equipos de daños ambientales y accesos no autorizados?		X	
		11.2.2	Instalaciones de suministro	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.	¿Todos los quipos cuentas con sistema eléctrico alterno?		X	
		11.2.3	Seguridad del cableado	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la	¿Se protege adecuadamente el cableado eléctrico y de red?		X	

				intercepción, interferencia o posibles daños.				
		11.2.4	Mantenimiento de los equipos	Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.	¿Todos los equipos reciben mantenimiento preventivo de manera constante?		X	
		11.2.5	Salida de activos fuera de las dependencias de la empresa	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.	¿Se controla la retirada de un activo de información fuera de la organización?	X		
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.	¿Se controla el activo retirado de la organización evaluando el riesgo en las instalaciones donde se utilizarán?		X	

		11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.	¿Al eliminar un equipo se realiza actividades para garantizar que la información contenida en este se migre u elimine correctamente?		X	
		11.2.8	Equipo informático de usuario desatendido	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.	¿Los empleados aseguran los equipos desatendidos?		X	
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información	¿Se cuenta con una política de escritorio y pantalla limpia?		X	

				para las instalaciones de procesamiento de información.				
12. Seguridad Operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1	Documentación de procedimientos de operación	Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.	¿Se cuenta con una documentación de procedimientos de actividades que afectan el procesamiento de información?		X	21
		12.1.2	Gestión de cambios	Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.	¿Ante un eventual cambio sobre los activos se genera controles?	X		
		12.1.3	Gestión de capacidades	Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el	¿Se tiene controles para gestionar la capacidad de los activos en uso?		X	

				objetivo de garantizar el rendimiento adecuado en los sistemas.				
		12.1.4	Separación de entornos de desarrollo, prueba y producción	Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.	¿La organización separa pruebas de desarrollo de los entornos de producción?	X		
	12.2 Protección contra código malicioso	12.2.1	Controles contra el código malicioso	Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.	¿Se tiene implementado sistemas de identificación de código malicioso en las terminales?	X		
	12.3 Copias de seguridad	12.3.1	Copias de seguridad de la información	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema con relación a una política de	¿Se realiza un proceso para realizar copias de seguridad de la información?		X	

				respaldo (Backup) convenida.				
	12.4 Registro de actividad y supervisión	12.4.1	Registro y gestión de eventos de actividad	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.	¿Se lleva un registro de eventos bajo log y se realiza una revisión y análisis de estos?		X	
		12.4.2	Protección de los registros de información	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.	¿Se protegen los registros de eventos para evitar pérdidas, corrupción o cambios no autorizados?		X	
		12.4.3	Registros de actividad del administrador y operador del sistema	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados de manera regular.	¿Se protegen los registros de los administradores para evitar manipulación de estos?		X	

		12.4.4	Sincronización de relojes	Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.	¿Los relojes de los sistemas se sincronizan bajo una única fuente de referencia?		X	
	12.5 Control del software en explotación	12.5.1	Instalación del software en sistemas en producción	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.	¿Se tiene algún procedimiento para la instalación de software de acuerdo a las necesidades de la organización?		X	
	12.6 Gestión de la vulnerabilidad técnica	12.6.1	Gestión de las vulnerabilidades técnicas	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias	¿Se realiza una identificación de vulnerabilidades técnicas para su oportuna gestión?		X	

				para abordar los riesgos asociados.				
		12.6.2	Restricciones en la instalación de software	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.	¿Existe control para la instalación de software por parte de usuarios?		X	
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1	Controles de auditoría de los sistemas de información	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.	¿Se realizan auditorías a los sistemas de información?		X	
13. Seguridad en las Telecomunicaciones	13.1 Gestión de la seguridad en las redes	13.1.1	Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.	¿Existe un control y administración de la red?	X		43

		13.1.2	Mecanismos de seguridad asociados a servicios en red	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.	¿Se tiene identificado mecanismos de seguridad dentro los niveles de servicio para los servicios de red?		X	
		13.1.3	Segregación de redes	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.	¿Se tiene segregada la red dependiendo de las áreas y funciones del empleado?		X	
	13.2 Intercambio de información con partes externas	13.2.1	Políticas y procedimientos de intercambio de información	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.	¿Se han definido políticas y procedimientos para el intercambio de información?		X	

		13.2.2	Acuerdos de intercambio	Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.	¿Existen acuerdos para el intercambio de información entre entidades externa?		X	
		13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información referida en la mensajería electrónica.	¿Existe algún mecanismo de protección para la mensajería de correo electrónico?	X		
		13.2.4	Acuerdos de confidencialidad y secreto	se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.	¿Se realizan acuerdos de confidencialidad al personal, para evitar la divulgación de información privada?	X		
14. Adquisición, desarrollo y Mantenimiento de los	14.1 Requisitos de seguridad de los sistemas de	14.1.1	Análisis y especificación de los requisitos de	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos	¿Se identifica los requisitos de seguridad en la fase de		X	38

sistemas de información	información		seguridad	para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.	desarrollo de sistemas de información nuevos o existentes?			
		14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de modificación no autorizada.	¿Existe mecanismos protección para la transmisión de información mediante la red pública?	X		
		14.1.3	Protección de las transacciones por redes telemáticas	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.	¿Existe mecanismos para proteger las transacciones en línea?	X		
	14.2 Seguridad en los procesos de	14.2.1	Política de desarrollo seguro de software	Se deberían establecer y aplicar reglas para el desarrollo de software y	¿Se establecen reglas para la seguridad de la	X		

	desarrollo y soporte			sistemas dentro de la organización.	información en el proceso de desarrollo de software?			
		14.2.2	Procedimientos de control de cambios en los sistemas	En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.	¿Se cuenta con procedimiento sobre los cambios que se realicen en los sistemas?	X		
		14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.	¿Se revisa el funcionamiento correcto de las aplicaciones tras un cambio en el sistema?		X	
		14.2.4	Restricciones a los cambios en los paquetes de software	Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían	¿Existe control sobre las actualizaciones de software?		X	

				controlar estrictamente.				
		14.2.5	Uso de principios de ingeniería en protección de sistemas	Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.	¿Se aplica los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación?		X	
		14.2.6	Seguridad en entornos de desarrollo	Las organización debería establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.	¿Se brinda seguridad a los entornos de desarrollo?		X	
		14.2.7	Externalización del desarrollo de software	La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.	¿Se supervisa la subcontratación de desarrollo de software?	X		

		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.	¿Se realizan las respectivas pruebas de seguridad de un desarrollo de software?		X	
		14.2.9	Pruebas de aceptación	Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.	¿Las nuevas actualización o nuevas versiones de software está sujeto a un proceso de aceptación?		X	
	14.3 Datos de prueba	14.3.1	Protección de los datos utilizados en prueba	Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.	¿Se protegen los datos de prueba en los Desarrollos de software?		X	
15. Relaciones con Suministradores	15.1 Seguridad de la información en las relaciones con suministradores	15.1.1	Política de seguridad de la información para suministradores	Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al	¿Se establecen condiciones para el manejo de la información por parte de terceros y proveedores?	X		60

				acceso por parte de proveedores y terceras personas.				
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.	¿Se tiene establecido y acordado todos los requisitos de seguridad de la información pertinentes a cada proveedor?		X	
		15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y	¿Se tiene en cuenta los requisitos de seguridad de la información para toda la cadena de suministro de los	X		

				productos de tecnología de información y comunicaciones.	proveedores?			
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1	Supervisión y revisión de los servicios prestados por terceros	Las organización debería monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.	¿Se generan mecanismos de monitorización de los servicios proporcionados por terceros?		X	
		15.2.2	Gestión de cambios en los servicios prestados por terceros	Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de	¿Se controla los cambios en los servicios de terceros para evaluar las nuevas necesidades de seguridad?	X		

				reevaluación de riesgos.				
16. Gestión de Incidentes	16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1	Responsabilidades y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	¿Se tiene implementado un procedimiento para la gestión de incidentes de seguridad de la información?		X	0
		16.1.2	Notificación de los eventos de seguridad de la informacion	Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.	¿Ante un evento de seguridad de la información, se realiza las notificaciones correspondientes?		X	

		16.1.3	Notificación de puntos débiles de la seguridad	Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.	¿Se reportan las debilidades sospechosas ante un eventual incidente?		X	
		16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.	¿Se realiza una clasificación de los eventos de seguridad de la información?		X	
		16.1.5	Respuesta a los incidentes de seguridad	Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.	¿Se da solución y seguimiento a los incidentes de seguridad de la información?		X	

		16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.	¿Bajo la solución de los incidentes, se genera un proceso de aprendizaje para la resolución de futuros incidentes o mejora se la seguridad?		X	
		16.1.7	Recopilación de evidencias	La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.	¿Se recopilan evidencia de los incidentes que permitan generar acciones legales o sancionatorias?		X	
17. Aspectos de la SI en la Gestión de la Continuidad de Negocio	17.1 Continuidad de la seguridad de la información	17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.	¿En los planes de continuidad del negocio se tiene integrado la continuidad de seguridad de la información?		X	0

		17.1.2	Implantación de la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.	¿Se dispone de un plan con medidas concretas para gestionar la continuidad de la seguridad de la información?		X	
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.	¿Se verifica, revisa y evalúa periódicamente el plan de continuidad de la información con sus controles definidos?		X	
	17.2 Redundancias	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en	¿Se cuenta con redundancia para los activos que requieran de una disponibilidad alta?		X	

				correspondencia con los requisitos de disponibilidad.				
18. Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.1	Identificación de la legislación aplicable	Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.	¿Se reconoce los requisitos estatutarios, normativos y contractuales legislativos en materia de seguridad informática?		X	25
		18.1.2	Derechos de propiedad intelectual (DPI)	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos	¿Se garanticen el uso del software de acuerdo a los derechos de seguridad intelectual?	X		

				software originales.				
		18.1.3	Protección de los registros de la organización	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.	¿Se aplica los controles necesarios a los registros que se realizan en la organización según los requisitos legales?		X	
		18.1.4	Protección de datos y privacidad de la información personal	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación	¿Se da cumplimiento de la legislación vigente en materia de la protección de datos personales?	X		
		18.1.5	Regulación de los controles criptográficos	Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y	Si la organización cifra la información, ¿se tiene en cuenta la normatividad sobre el uso de estos		X	

				las normativas pertinentes.	controles criptográficos?			
	18.2 Revisiones de la seguridad de la información	18.2.1	Revisión independiente de la seguridad de la información	Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información con base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.	¿Se están realizando revisiones de cumplimiento de la seguridad de la información?		X	
	18.2 Revisiones de la seguridad de la información	18.2.2	Cumplimiento de las políticas y normas de seguridad	Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información	¿La alta gerencia revisa el cumplimiento de las políticas y las normas de seguridad?		X	

				dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.				
		18.2.3	Comprobación del cumplimiento	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.	¿Se evalúan los sistemas de información para que estén acordes a las reglas y políticas de seguridad definidas por la organización?		X	

Fuente: El autor

En el desarrollo de la matriz anterior permitió medir el cumplimiento de los diferentes controles en sus respectivos dominios, este conllevo a generar la tabla No. 18, la cual muestra el grado de madurez para cada dominio de la norma ISO/IEC 27001:2013 donde muestra una comparación del estado actual versus el nivel objetivo que se debería, valoración determinada en porcentaje.

Tabla 18. Cumplimiento de los dominios

	Cumplimiento de los dominios		
	DOMINIO	**Calificación Actual (%)**	**Calificación Objetivo (%)**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100
A.6	ASPECTOS ORGANIZATIVOS SI	14	100
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	67	100
A.8	GESTIÓN DE ACTIVOS	0	100
A.9	CONTROL DE ACCESO	29	100

A.10	CIFRADO	0	100
A.11	SEGURIDAD FÍSICA Y AMBIENTAL	40	100
A.12	SEGURIDAD OPERATIVA	21	100
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES	43	100
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	38	100
A.15	RELACIONES CON SUMINISTRADORES	60	100
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100
A.18	CUMPLIMIENTO	25	100

Fuente: El autor

Para una mejor compresión del nivel de cumplimiento y la brecha que tiene actualmente la organización del nivel de cumplimiento por dominio se genera la figura No. 4 la cual se basa en el instrumento de evaluación del modelo MSPI propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones, donde se muestra los diferentes dominios en su estado.

Los dominios que actualmente no tienen ningún grado de madurez o son inexistente y sobre los cuales se debería tomar en consideración para dar inicio en su implementación se tienen:

- Políticas de seguridad de la información
- Gestión de activos
- Cifrado
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio

Entre estos dominios el de gran importancia las políticas de seguridad de la información que son las normas sobre las culés se deben basar tanto el personal, clientes y proveedores para la reducción del riesgo de pérdida o fuga de información.

Figura 4. Brecha ISO/IEC 27001:2013

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. (2017). Instrumento de medición del MSPI. Bogotá. (Recuperado el 20 de octubre de 2010). disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

6.4 FASE 4: ESTABLECER POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas que se presentan a continuación, están determinadas bajo los resultados obtenidos en el análisis y evaluación de riesgo, el cual, se encuentra articulado con el plan de tratamiento de riesgos relacionado en la tabla No.16, donde se identificaron controles que deberán aplicarse para poder minimizar el impacto en los activos; también se estructuran estas, mediante los datos arrojados del nivel de cumplimiento de los diferentes dominios según tabla No. 18, donde se determina el grado de madurez de cada uno, para así aumentar el nivel de cumplimiento de los dominios para generar medidas a las vulnerabilidades identificadas.

6.4.1 Introducción. Para la Cooperativa Multiactiva De Centrales Eléctricas De Nariño la información, es uno de los mayores activos, dado que, son las diferentes áreas quienes hacen uso de la misma, en este sentido, la transforman, almacenan y comparten con el fin de dar cumplimiento a los objetivos de organizacionales; por esta razón, se hace necesario proteger la información mediante lineamientos de seguridad, garantizando de esta forma, que los riesgos asociados a los diferentes activos que interactúan, sean mínimos.

Las políticas son un instrumento para fortalecer el Sistema de gestión de seguridad de la información, el cual, deberá seguir un proceso de mejora continua, con el objetivo de generar en los empleados y clientes confianza a la hora de utilizar las tecnologías de la información y comunicación; estos lineamientos serán una guía de gran importancia para la protección de la información, por tal motivo el cumplimiento será obligatorio.

6.4.2 Objetivos. Bajo las políticas de seguridad de la información se busca:

- Garantizar la integridad, confidencialidad y disponibilidad de la información; activo de gran valor para la organización.
- El cumplimiento de parámetros y lineamientos del personal de COOPCEN con el fin de mantener un adecuado uso de los activos de información.
- Comprometer a la alta gerencia y brindar las herramientas necesarias para mantener el sistema de gestión de seguridad de la información actualizado.
- Prevenir incidentes de seguridad que afecten los activos de información.
- Definir procedimientos alineados al plan de tratamientos de riesgos para minimizarlos.
- Fortalecer en los empleados la cultura en seguridad de la información.

6.4.3 Alcance. Las políticas de seguridad de la información, aquí definidas, se aplican a los activos de información de los siguientes procesos: afiliación, crédito, financiero, ingreso de fondos y gestión tecnológica para la Cooperativa Multiactiva De Centrales Eléctricas De Nariño sede principal, con el objetivo de garantizar un nivel de seguridad óptimo.

6.4.4 Políticas de Seguridad. Las siguientes políticas de seguridad de la información ayudarán a la gerencia a mejorar sus planes sobre a la hora de tomar decisiones frente a la garantía de la protección de los activos de información bajo las legislaciones vigentes.

6.4.4.1 Organización De La Seguridad De La Información. Para garantizar las diferentes actividades que permitan apoyar la seguridad de la información, es necesario crear un Comité de SGSI, el cual, debe garantizar el cumplimiento de los objetivos del sistema y su mejora continua. Para tal fin, se realizará la actualización y verificación periódica de las políticas, no mayor a 2 meses; los encuentros realizados por el comité serán programados previo aviso, en estos, las decisiones tomadas serán plasmadas en un acta con firma de cada participante dejando constancia de la participación y aceptación de lo acordado.
El comité estará conformado así:

- Líder del SGSI
- Representante del área tesorería

- Representante del área de cartera
- Representante del área contabilidad
- Representante del área de secretaria
- Representante del área jurídica

La creación del anterior comité será oficializada bajo resolución, en la cual se constata la aceptación y cumplimiento de las funciones.

El comité del SGSI tendrá las siguientes funciones:

- Asegurar que exista el apoyo de la gerencia para desarrollar actividades que fortalezcan la seguridad de la información.
- Revisar el estado de la seguridad de la información, generando diagnósticos para de esta manera realizar las acciones o controles necesarios.
- Capacitar al personal sobre seguridad informática.
- Generar planes de acción para mitigar el riesgo.
- Evaluar el nivel de cumplimiento de los dominios según Norma ISO/IEC 27001:2013
- Dar a conocer la documentación generada por el comité.

El líder del comité del SGSI deberá estar al tanto sobre temas de seguridad de la información, por lo cual debe gestionar que COOPCEN esté suscrita a foros especializados en Seguridad de la información o empresas expertas en seguridad de la información, esto con el fin de compartir la información tanto al comité como al personal, fortaleciendo el conocimiento y la protección de los activos de información.

En los nuevos proyectos a ejecutarse en COOPCEN, el comité del SGSI deberá tener en cuenta la seguridad de la información; para esto, en la etapa de planificación del nuevo proyecto se identificarán las amenazas, vulnerabilidades y riesgos, con el fin de abordar controles necesarios que preserven la confidencialidad, integridad y disponibilidad de la información.

6.4.4.2 Gestión de Activos

Inventario de activos: COOPCEN debe garantizar que los activos de información presentes en las instalaciones físicas de la oficina principal estén identificados y registrados bajo un inventario organizado de forma digital; en esta actividad se registraran datos relevantes de la identificación de los activos, para tal fin, se tiene estipulado el formato INAC-SIS en su versión 1.0 bajo hoja de cálculo, adjunto en el anexo A.

El inventario y actualización de activos se realizará anualmente; sin embargo, el tiempo podrá ser menor dependiendo de la necesidad; la responsabilidad del

inventario de activos estará a cargo del funcionario del área de sistemas, quien programará la actividad con los trabajadores de las diferentes áreas quienes son los propietarios de los activos

Clasificación y etiquetado activos: los activos de información serán clasificados dependiendo de la importancia para COOPCEN en cuestión de:

[D] disponibilidad
[I] integridad
[C] confidencialidad

Los activos serán evaluados a partir de cada una de las anteriores variables, asignando un valor cuantitativo, donde 1 es irrelevante, 2 bajo, 3 medio, 4 alto y 5 muy alto, los valores serán registrados en el formato INAC-SIS.

Bajo la clasificación definida se deberá etiquetar cada activo de información de manera física, donde se estipule el nivel e importancia del activo, dicho etiquetado deberá reconocerse fácilmente.

La ejecución de la actividad de clasificación y etiquetado de los activos, la realizará un funcionario del área de sistemas mancomunadamente con las diferentes áreas propietarias de los activos.

Propiedad de los activos: Los activos que hacen parte del inventario deben estar asignados a un funcionario, el cual será el que interactúa con el activo y posee un nivel de acceso alto a este, el cual se llamará usuario. El único propietario del activo de información será la Cooperativa Multiactiva De Centrales Eléctricas De Nariño.

El usuario del activo deberá estar relacionado en el formato INAC-SIS, y el cual debe cumplir con lo siguiente para su cuidado:

- Verificar que, dentro del inventario, los activos asignados hagan parte de este.
- Garantizar que no exista fuga de información, de acuerdo al nivel de importancia del activo.
- Proteger el activo durante su utilización y cuando no se utilice.

Uso de los activos: Durante el desempeño de las labores de los funcionarios de COOPCEN y que involucren activos de información, no deberá participar en actividades que no correspondan a las funciones planteadas en su contrato laboral y que genere una utilización de los activos a cargo.

De tal manera que se plantean las siguientes reglas:

- El uso de internet para fines personales será sancionado, de tal manera que este servicio estará limitado a su uso exclusivamente laboral; el funcionario que utilice el servicio para generar transacciones, compras en línea, chat y redes sociales asumirán el riesgo asociado que implica el uso de internet bajo estas actividades.
- Los documentos impresos por cada área, serán aquellos que hagan parte de los reportes y soportes de las actividades de las funciones asignadas a cada funcionario, de tal manera que se sancionará el uso indebido del servicio de impresión.
- El uso de teléfono fijo como celular corporativo será exclusivamente para comunicación de carácter laboral y no personal
- Los dispositivos de almacenamiento externos serán controlados por el área de sistemas, no obstante, las diferentes áreas podrán hacer uso de estos para transferir información, siempre y cuando el área de sistemas verifique que es de uso exclusivamente laboral y además que autorice y haga el seguimiento oportuno.

Devolución de activos: Al terminar el vínculo laborar o cambio de cargo, todo empleado deberá realizar la devolución de los activos de información que hayan sido asignados en el momento de la vinculación y que se registraron en el acta de entrega y la relación del inventario de activos.

El área de sistemas verificará la entrega de los elementos y deberá generar el respectivo recibido en el acta de devolución, con lo cual se le informará a gerencia de manera escrita la conformidad del recibido; si en dicha entrega alguno de los elementos fuera perdido o dañado intencionalmente, se deberá generar el respectivo cobro al funcionario para la devolución de este.

Teletrabajo: En condiciones donde los funcionarios por situaciones particulares no puedan asistir físicamente a la organización, para desarrollar sus funciones pero les es posible ejecutar estas en modalidad de teletrabajo, el funcionario deberá enviar una petición previa a gerencia, área encargada de aprobar y autorizar el manejo de activo en modalidad de teletrabajo, en este sentido, una vez se cuente con la autorización, el área de sistemas deberá preparar los elementos necesarios en cuanto a elementos de hardware, software y de telecomunicación para que el funcionario pueda realizar normalmente las actividades en modalidad de teletrabajo, según lo contemplado en el artículo 2 del decreto 884 del 2012 y la ley 1221 de 2008, donde se establece la modalidad de teletrabajo con las garantías laborales y de seguridad social para los teletrabajadores, además se especifica las condiciones laborares bajo esta metodología con respeto a las obligaciones del empleado y empleador.

Para el desarrollo de la actividad de teletrabajo, el área de sistemas registrará los datos del empleado como ubicación, teléfono de contacto, la fecha de inicio y fin de la actividad de teletrabajo; así mismo, deberá registrar la salida de los elementos de cómputo que se le sean asignados al funcionario generando la respectiva acta de entrega.

El área de sistemas deberá aplicar los respectivos controles a nivel de hardware y software de los elementos que se asignan al funcionario, con el fin de proteger la información contenida en éstos, para el trasporte de los elementos desde la oficina hacia el lugar donde desarrollará la actividad de teletrabajo, la organización deberá asignarle los recursos y acompañamiento.

El funcionario que esté desarrollando la actividad en la modalidad de teletrabajo no deberá realizar ninguna modificación ni en el hardware ni en el software de los elementos entregados; durante el tiempo que dure esta actividad se establecerán monitoreos con el fin de conocer la efectividad de los controles aplicados a los elementos entregados.

Gestión de medios removibles: La utilización de medios extraíbles como memoria USB, CD-ROM y disco externo estará restringido en todas las áreas de COOPCEN, de tal manera que estos elementos estarán a cargo del área de sistemas quien autorizara su uso una vez se realice el requerimiento del funcionario; en este caso, es el área de sistemas quien estará a cargo del proceso de trasporte de información.

Los dispositivos de almacenamiento externos serán analizados mediante herramienta antivirus antes y después de su uso, así como también una vez se termine el proceso de trasporte de la información se generará la eliminación del contenido de esta.

La utilización de los soportes extraíbles se dará únicamente cuando se agoten las herramientas dispuestas para la trasmisión de información entre las diferentes áreas y terceros, herramientas como correo corporativo y servidor de archivos.

Si la información a trasmitir es crítica y de gran importancia, y que pueda impactar negativamente a la organización ante una eventual perdida, se deberá utilizar herramientas de cifrado.

No se permite el uso de dispositivos extraíbles para trasportar información fuera de las instalaciones de COOPCEN.

Eliminación de soportes: La disposición final de los activos de información se dará previo análisis que realizará el área de sistema, esto con respecto al funcionamiento o pérdida total del activo, una vez se tenga dicho concepto del activo y como resultado sea la eliminación de éste, se tendrá en cuenta lo siguiente:

- Antes de eliminar el activo se debe generar la respectiva copia de la información contenida en los medios magnéticos; seguido a esto se deberá realizar un borrado a bajo nivel donde se asegure que la información ya no puede ser accesible ni recuperada.

Se debe garantizar la destrucción física del activo, donde se constate que es totalmente inutilizable, para la destrucción del activo se puede generar el proceso de incineración o trituración.

6.4.4.3 Seguridad Ligada a los recursos humanos. Todos los funcionarios deben estar en la capacidad de analizar y generar conciencia sobre las amenazas a las que están expuestos ellos, como también las amenazas de los activos que tienen a su cargo, de tal manera que el personal tendrá conocimiento de las diferentes políticas establecidas en este documento, con el fin de que este sea parte del apoyo y de esta forma, garantizar el cumplimiento de estas.

Concienciación y capacitación: Con el fin de que los funcionarios de COOPCEN le den buen uso y aprovechen de forma correcta los activos asignados a su cargo, se deberá generar jornadas de capacitación donde se dé a conocer el SGSI y las presentes políticas; estas jornadas son de asistencia obligatoria, en la cuales se crea un compromiso por parte del funcionario para el buen uso de los recursos informáticos asignados.

Para empleados nuevos dentro de la inducción inicial también se incluirá las temáticas concernientes al SGSI y las políticas en seguridad informática.

En las capacitaciones se informará sobre los riesgos a los que está expuesto COOPCEN en materia de seguridad informática, los deberes, derechos y responsabilidad al cumplimiento de los lineamientos constituidos en el SGSI; en estas capacitaciones se ejecutaran las respectivas evaluaciones con el fin de medir la efectividad de estas.

6.4.4.4 Control de Acceso. Todos los funcionarios deberán acatar la norma con respecto al acceso lógico de los activos de información presentes en COOPCEN; los controles generados para este fin deberán ser conocidos por los funcionarios y estar diseñados teniendo en cuenta el perfil o cargo con la organización.

Políticas de Control de Acceso Lógico: Para el desarrollo de las funciones del personal, estos tendrán acceso a la información necesaria dependiendo del perfil y cargo ejecutado, los cuales se han definido en el manual de procesos de COOPCEN; para el acceso se definen usuarios y contraseñas para cada recurso o servicio asignado al funcionario, estas también serán gestionadas por el área de sistemas.

El área de sistema tendrá la faculta de eliminar y permitir los accesos, por lo cual deberá generar un control para identificar usuarios o situaciones no deseadas que puedan colocar en riesgo la integridad, disponibilidad y confidencialidad de la información.

Las contraseñas iniciales generadas por el área de sistemas para cada usuario, serán únicas, estas se entregan al momento de la contratación.

Todo funcionario una vez tenga el primer acceso al sistema de información o sistema operativo, deberá realizar el cambio de la contraseña de acceso, las cuales, deberán cumplir con un mínimo de 8 caracteres combinando letras, números, caracteres especiales, mayúsculas y minúsculas; para tal fin el área de sistema asistirá al funcionario.

Se deberá generar el cambio de contraseñas de manera regular (cada 4 meses), evitando por parte del funcionario re utilizar la nueva asignación; para el cambio de contraseña se enviará un aviso previo vía correo electrónico.

El uso de las contraseñas será de carácter personal por lo cual no podrán ser trasferibles o compartidas entre los mismos funcionarios o a personas externas; también no se permite que se registren las contraseñas en medios físicos (notas de papel, cuadernos, documentos o archivos).

El área de sistemas realizará un control del acceso para el sistema de información y sistema operativo, con lo cual deberá auditar los eventos de inicio de sesión, de tal manera que recurrentemente se analizarán los registros con el fin de verificar anomalías o acciones de accesos no autorizados.

En caso de terminación de contrato o cambio de cargo, el área de sistemas se encargará de desvincular las contraseñas y usuarios ya sea eliminándolas o generando nuevas, bajo los privilegios del nuevo cargo a ocupar; los privilegios de cada funcionario de COOPCEN serán revisados periódicamente con el fin de controlar cambios o nuevas funcionalidades que se le asignan al personal para poder negarlas o permitirlas.

Para el acceso a redes y servicios de red se tendrá en cuenta las siguientes consideraciones:

- El área de sistemas será la encargada de brindar el servicio a cada funcionario dependiendo de las necesidades y las labores a ejecutar por el funcionario de COOPCEN; además verificará el buen uso y correcto funcionamiento.
- No se permite usar la conexión de internet para ingresar a páginas de pornografía, terrorismo, drogas, juegos y descarga de aplicaciones que

conlleven a violar la seguridad de la información, de tal forma que el área de sistema estará facultada para prohibir el acceso a ciertos sitios.
- No se permite el uso de internet para fines comerciales ajenos a los de COOPCEN.
- Se prohíbe la navegación bajo software no autorizado, por tal razón se controla en cada estación de trabajo la instalación de software distinto a los permitidos y acordados entre COOPCEN y el área de sistemas.

Para el acceso remoto se tendrá en cuenta las siguientes consideraciones:

- Las conexiones remotas realizadas estarán basadas bajo el uso de VPN tanto para el acceso a estaciones de trabajo de COOPCEN como para el acceso del software financiero en la nube, de tal manera que cada funcionario hará uso del software VPN y se le asignará la correspondiente credencial de acceso.
- Si el acceso se realizara desde afuera de las oficinas mediante conexión VPN, el área de sistemas deberá configurar el equipo asignado para tal fin, esto con previa autorización del área gerencial; así como también deberá informar al funcionario las buenas prácticas a la hora de generar un acceso remoto.

6.4.4.5 Seguridad Física y Ambiental.

Áreas seguras: Los funcionarios de COOPCEN y terceros deberán portar el carnet o cédula de ciudadanía respectiva que lo identifique, el cual debe estar situado en una parte visible.

Se debe establecer los perímetros de las áreas con mecanismos de seguridad física.

El acceso a las diferentes oficinas, es exclusivamente para los funcionarios de cada área de tal manera que las puertas de acceso permanecerán cerradas en los momentos de ausencia temporales de estos; el acceso al centro de cableado, data center y lugares críticos de procesamiento de información será explícitamente para el área de sistemas, si por cualquier situación algún funcionario que no haga parte del área de sistemas desea ingresar, lo deberá hacer mediante una autorización aprobada por la gerencia y el administrador del área de sistemas.

El ingreso de personal externo será acompañado y guiado para realizar las actividades que requiera, de tal manera que existirá pleno conocimiento de cada acción realizada, el acceso será controlado en recepción a cargo del funcionario del área de secretaria; lo anterior soportado con los sistemas CCTV que registraran las acciones tanto de los funcionarios como del personal externo.

La organización garantizará la implementación de medidas para asegurar mediante controles, el acceso a las áreas críticas, los cuales serán evaluados por parte del área de sistemas y verificados continuamente, estas áreas deberán estar demarcadas mediante señalización que comuniquen tanto a funcionarios como personal externo del acceso restringido. De igual manera se definirán controles para mitigar amenazas ambientales (temperatura, fuego y humedad) definidos en el plan de tratamiento de riesgos, los cuales deberán ser verificados por el área de sistemas.

No se permite el almacenamiento de productos líquidos o elementos inflamables en los espacios de procesamiento, almacenamiento de información y equipos que soportan la comunicación.

Seguridad en los equipos: Los equipos de procesamiento, almacenamiento y aquellos que soportan la comunicación, se ubicaran de manera adecuada donde se los proteja de manipulación física no autorizada, robo y daños del entorno; la reubicación de estos se basara bajo un estudio de amenazas y riesgos de la nueva ubicación.

Se debe garantizar el suministro de energía a todos los elementos ante una eventual falla del servicio de energía principal, de tal manera que se deberá hacer uso del sistema alterno de energía UPS para suplir el servicio de energía; este respaldo de energía eléctrica se utilizará para equipos de procesamiento, almacenamiento y aquellos que soportan la comunicación, de tal forma que en los puestos de trabajo solo se conectaran bajo este sistema alterno los equipos de cómputo de cada área.

El cableado de red como el de energía eléctrica deben estar protegidos mediante canaletas para evitar su deterioro; es necesario que toda nueva instalación de estas dos redes se regule bajo la normatividad correspondiente, de tal manera que todo cableado deberá estar debidamente etiquetado para que ante un eventual fallo exista una rápida identificación del problema, esto además, permite reducir el riesgo por manipulación indebida.

Para mantener correctamente el funcionamiento e integridad de los equipos de cómputo y elementos de telecomunicación se realizarán jornadas de mantenimiento preventivo, las cuales, estarán soportadas por el área de sistemas, dichas labores se realizarán cada 4 meses y serán programadas en los días donde no exista actividades por parte de los funcionarios; solo el personal del área de sistemas ejecutara dichas labores.

Toda actividad de mantenimiento preventivo se registrará en el formato MAN_COP-01 historial de mantenimiento, equipos de cómputo y telecomunicaciones (Anexo B), el cual está adjunto a la hoja de vida respectiva de los equipos y elementos de telecomunicaciones, donde se registra la descripción de las actividades realizadas de cada elemento y el personal involucrado.

Para los equipos que requieran de mantenimiento o reparación por fuera de las instalaciones de COOPCEN, se deberá solicitar una autorización de salida dirigida a la gerencia y al coordinador del área de sistemas; a estos equipos se les realizará la respectiva copia de seguridad o borrado seguro.

Los equipos de cómputo por ser asignación de COOPCEN a los funcionarios de las diferentes áreas, deberán actuar bajo mecanismos contra la pérdida o robo de información tanto física como digital de tal manera que se establece los siguientes lineamientos para los equipos de cómputo desatendidos y pantalla limpia durante y después de los horarios de trabajo:

- Los documentos físicos que se encuentren en el escritorio de cada funcionario deberán resguardarse en un lugar seguro, en los momentos cuando el empleado se retire del puesto de trabajo, ya sea temporalmente o por fin de la jornada laboral.

- Todos los quipos de cómputo deberán bloquearse automáticamente en un tiempo de 3 minutos, durante el lapso de inactividad, este correcto funcionamiento será monitoreado por el área de sistemas; en los casos que los funcionarios de los equipos computo realicen un momento de ausencia, deberán aplicar dicho bloqueo de pantalla de forma anticipada.

- Todo documento una vez impreso deberá ser retirado de las impresoras.

- Si se utiliza para la impresión hojas recicladas (impresiones fallidas de un lado de la hoja), todo funcionario deberá tener en cuenta que el lado erróneo de impresión no contenga información confidencial, si fuese el caso esta hoja deberá ser destruida a menos que los documentos sean almacenados y utilizados exclusivamente para la organización.

6.4.4.6 Seguridad Operativa. Los procedimientos que se realicen en la infraestructura tecnológica de COOPCEN, deberán ser controlados y estar diseñados bajo una documentación que indique el procedimiento adecuado para mantenimiento, cambio o actualización.

Responsabilidades y procedimientos de operación: Todos los procedimientos que se realicen en los diferentes servicios y recursos tecnológicos deberán estar documentados, entre estos están:

- Realización de Backus.
- Actualización de software.
- Actualización de hardware.
- Administración de servicios.
- Mantenimiento de equipos de cómputo y de elementos de telecomunicación.

Los instructivos serán diseñados y revisados por el Coordinador del área de sistemas quien actualizara cada procedimiento según requerimiento y cambios de tecnología que realice COOPCEN con los activos de información.

Los cambios que se realicen en la infraestructura tecnológica, deberán tener autorización por Gerencia, a quien el comité de SGSI le informara bajo reunión previa sobre las actividades a realizar, esto teniendo en cuenta un estudio y de un análisis previo de riesgo sobre dichas actividades; estas deberán tener un registro donde se relacione lo siguiente:

- Quien autorizo el cambio.
- Persona que realizara el procedimiento del cambio
- Descripción de las labores a ejecutarse.
- Fecha y hora a realizar los cambios
- Conformidad del cambio.

El Coordinador del área de sistemas deberá realizar las respectivas pruebas para garantizar la disponibilidad de los activos de información y telecomunicación, con el fin de evitar pérdidas de disponibilidad o rendimiento por falta de capacidad, de esta manera, las mediciones se ejecutarán periódicamente o cuando se han efectuado cambios en algún servicio o activo de información.

Código malicioso: Se deberá garantizar que los equipos de cómputo estén provistos de software antivirus para la protección y prevención de código malicioso que pueda afectar la confidencialidad, integridad y disponibilidad de la información.

El Coordinador del área de sistemas deberá garantizar que los equipos de cómputo cuenten con software, antivirus, anti spam y antispyware, los cuales deberán tener su respectiva licencia y configuración; en tal caso que las licencias se caduquen se deberá gestionar la adquisición de unas nuevas.

El software antivirus deberá ser actualizado permanentemente; de tal forma que el Coordinador de sistemas administrará el buen funcionamiento de la herramienta, como también se asegura de monitorear bajo la consola de administración los diferentes reportes que conlleven a tomar medidas necesarias ante eventuales ataques o software malicioso.

COOPCEN garantizará que cada año se especifique dentro del presupuesto anual los rubros para la compra de software antivirus, este valor está sujeto a un estudio previo por parte del coordinador de sistemas sobre el software antivirus a adquirir y el que mejor se adapte a las tecnologías con que cuenta COOPEN.
Los funcionarios de COOPCEN ante un eventual mensaje sospechoso o alerta arrojada por el software antivirus deberá reportar al área de sistemas para tomar las medidas necesarias.

Copias de seguridad de la información: Se deberá garantizar que la información generada en las diferentes áreas, sea respaldada mediante copias de seguridad que garanticen la reposición de los datos ante una eventual pérdida de estos.

El Coordinador del área de sistemas deberá generar actividades de respaldo de las copias de seguridad de la información digital de las diferentes áreas de COOPCEN; esta actividad deberá realizarse bajo el procedimiento definido del respaldo y restauración de copias de seguridad, las cuales las ha definido el área de sistemas.

La realización de copias de seguridad se almacenará en medios removibles, dispuestos solo para esta labor, una vez se ejecutan las labores respectivas, estos serán trasportados y almacenados fuera de las instalaciones físicas de COOPCEN; así mismo toda actividad de copia de seguridad deberá ser registrada bajo una bitácora, en la cual se deberá registrar hora, fecha, tipo de copia de seguridad y responsable.

Las labores de copia de seguridad deberán definirse en horarios en que las demás áreas empresariales no estén realizando, para tal fin el Coordinador del área de sistemas deberá definir un cronograma especifico.

Registro de actividad y supervisión: Toda actividad realizada en los sistemas activos de información y elementos de telecomunicación deberá ser monitoreada y registrada; asi como, cada evento que permita generar análisis de la seguridad de la información y sus activos, para tal fin, el área de sistemas se encargara de activar el monitoreo y guardado de registros, los cuales deberán ser salvaguardados para su posterior análisis de fallos y eventos inusuales.

Los registros deberán resguardarse en una unidad extraíble especialmente dedicada para este propósito, el acceso a esta, solo se dará a personal autorizado: Para una correcta recolección de los registros de todo elemento tecnológico que maneje registro de reloj se deberá sincronizar bajo los parámetros de una fuente de referencia, para el caso de COOPCEN se tomara como referencia la hora legal del instituto nacional de metrología disponible en http://horalegal.inm.gov.co/.

Control de instalación de software: La instalación de software estará a cargo del área de sistemas, los funcionarios de esta área serán los únicos que podrán realizar dicha actividad, esta debe ser valorada según necesidad de COOPCEN bajo un estudio previo de los beneficios de la herramienta a instalar o a eliminar; dicho estudio será aprobado por el comité de SGSI quien dará la aprobación de la ejecución de las labores.

Cada cambio realizado por instalación de software, deberá ser registrado en las hojas de vida de cada equipo de cómputo o elemento de telecomunicación que permita evidenciar el historial y seguimiento; así mismo se deberá mantener en los repositorios de software la versión anterior que fue remplazada o eliminada.

Bajo los logs del sistema se monitorea los cambios que han sufrido los equipos de cómputo por motivo de instalación de software, los cuales deben ser resguardados para su análisis y así determinar responsabilidades y controles.

Gestión de Vulnerabilidades técnicas: Se debe obtener un panorama de las vulnerabilidades técnicas del activo, mediante la realización de pruebas, ataques simulados y escaneos de vulnerabilidades, estas actividades deberán estar reguladas por el Coordinador del área de sistemas y se ejecutarán periódicamente.

Las pruebas para identificar vulnerabilidades se deberán documentar para darlas a conocer al Comité de SGSI, así mismo se deberá generar un plan para gestionar y corregir los hallazgos minimizando el nivel de riesgo e impacto.

Auditoria en los sistemas de información: Se ejecutarán auditorías al sistema de información existente en COOPCEN, estas auditorías deben ser programadas por el coordinador del área de sistemas y ejecutadas por un proveedor, con el fin de obtener informes con una percepción objetiva; en estas auditorías se requiere conocer:

- Cumplimiento de la normatividad y políticas del sistema de información que permitan minimizar las amenazas.
- Privilegios de acceso correctos.
- Verificación de procesos y procedimientos.
- Estabilidad del sistema.
- Posibles mejoras.

6.4.4.7 Seguridad En Las Telecomunicaciones. El acceso y trasmisión de información por la red y los activos intermedios que se involucran en este proceso, deberán ser controlados con el fin de asegurar que la información que viaja esté segura.

El coordinador del área de sistemas se encargará de planificar y ejecutar los controles necesarios para asegurar la trasferencia de información mediante la red de datos, para que se mantengan confidenciales y seguros, estos controles también deberán asegurar la disponibilidad de los elementos de interconexión y servicios de red.

Todo servicio deberá ser identificado, asegurando que los protocolos y puertos de comunicación sean los necesarios para su funcionamiento; de tal manera que se deberá inhabilitar todo servicio, puerto y protocolo que no se utilice.
Todas las áreas de COOPCEN estarán segregadas a nivel lógico y físico de la red, donde cada segmento estará basado bajo las diferentes tareas y procesos que genera cada área definiendo privilegios en la red de cada segmento.

Para conexión de dispositivos móviles por parte de visitantes a la red wifi, se tendrá dispuesto una zona ubicada en sala de juntas, donde están la información necesaria para la conexión, la clave de conexión se remplazará periódicamente, así como el nombre del punto de acceso.

Mensajería de correo electrónico: Todas las áreas cuentan con un correo institucional, de tal manera que se prohíbe el uso para el envío y recepción de mensajería por cualquier otro medio que nos sea el correo institucional.

El correo institucional será usado para el cumplimiento de las funciones de cada área por lo cual está prohibido su uso para fines personales.

Cada cuenta de correo electrónico institucional estará limitada en capacidad de almacenamiento, por lo cual cada funcionario de las áreas deberá realizar respaldos y guardado de estos.

El coordinador del área de sistemas monitorea el uso y capacidad del correo electrónico, con el fin de informar anticipadamente a los funcionarios sobre la generación de respaldos para evitar que la capacidad de almacenamiento llegue a su límite.

Acuerdos de Confidencialidad: Para que la información presente en COOPCEN se mantenga confidencial, todo funcionario deberá tener firmado dentro de su contrato laboral los términos y condiciones donde se estipula que la información que utilizara en el cumplimiento de su función no será divulgada o trasferida a miembros externos a la organización.

6.4.4.8 Seguridad En Los Sistemas de Información. El sistema de información actual y los nuevos que se implementen en COOPCEN se deberán analizar, en consecuencia, el proveedor del software deberá especificar las características de seguridad del software, tales como:

- Requisitos de autentificación.
- Privilegios de los usuarios.
- Registro de actividades en el sistema de información.
- Supervisión y monitoreo del sistema de información.
- Controles de seguridad
- Cifrado del sistema de información

Las anteriores características serán puestas a prueba para concluir la efectividad de la seguridad, así mismo se analizará la compatibilidad de los controles implementados en los activos de información y de telecomunicación con la seguridad del sistema de información.

Las nuevas actualizaciones o cambios que se realicen en el sistema de información, ya sea por adquisición de nuevas funcionalidades o actualización de versión por parte del proveedor de software, se generarán previa autorización por parte de COOPCEN, en estos cambios se verificará que no se genere impacto adverso a las aplicaciones, de tal forma que el Coordinador del área de sistemas ejecutara actividades para verificar que las aplicaciones críticas estén funcionales; así mismo que el sistema de información este funcional y cumpla con la ejecución de los procesos de cada área.

6.4.4.9 Proveedores. Los proveedores que presten algún servicio a COOPCEN deberán seguir lineamientos al contrato donde se establecen requisitos legales con respecto a la protección de los datos y confidencialidad de esta.

Mediante el uso del canal de comunicación propuesto por los proveedores. se ejecutarán las respectivas peticiones, quejas y reclamos; también se deberá analizar el nivel de servicios propuesto por estos para contar con el proveedor mecanismos de comunicación de peticiones, quejas y reclamos para solventar caída del servicio, de tal manera que se hace necesario revisar el nivel de servicio con el fin de determinar que el cumplimiento sea el acorde con las necesidades de COOPCEN.

Todo cambio realizado por parte de los proveedores en los servicios prestados, deberá analizarse bajo un escenario de riesgos con el fin de determinar el impacto y así tomar decisiones sobre este, ajustando los controles sobre el servicio y modificando el nivel de servicios para cubrir las nuevas necesidades.

6.4.4.10 Incidentes de Seguridad. Todo incidente de seguridad de la información deberá ser tratado de forma ágil y efectiva por el Coordinador del área de sistemas, siguiendo el procedimiento de incidentes de seguridad de la información PGI_COOP (Anexo C).

Todo incidente de seguridad de la información presente el COOPCEN deberá ser reportado por el funcionario a quien se le presentó el suceso, el incidente deberá ser reportado enviando un correo electrónico al Coordinador del área de sistemas, dicho fallo, debe ser sustentado a través de capturas de pantalla, fotografías y videos.

El coordinador del área de sistemas deberá realizar el registro del incidente, registrando el formulario FI_COOP (Anexo D) reporte de incidentes, el cual, debe estar sustentado con la recolección de evidencias.

A todo incidente presentado se le deberá valorar el impacto que genera según procedimiento de incidentes de seguridad de la información PGI_COOP, sobre esta valoración se genera los respectivos controles para mitigar el impacto; Así como

también se debe detallar las acciones inmediatas que se realizan para mitigar el incidente de seguridad de la información.

Después de todo incidente presentado, se debe generar la respectiva retroalimentación al grupo de trabajo de todas las áreas, con el fin de que se tome conciencia o evitar que los funcionarios recaigan en el mismo suceso; además, esto permite asegurar que a todas las áreas se le realice los respectivos ajustes y soluciones del incidente inicial.

6.4.4.11 Continuidad de Negocio. Para que las actividades ejecutadas en las diferentes áreas que no entren en estado de resección por alguna amenaza, se deberán generar medidas de protección y recuperación.

Se deberá implementar en el plan de continuidad o recuperación ante incidentes o desastres, un apartado donde se estipule la continuidad del negocio enfocado a los aspectos de seguridad de la información, de tal manera que durante y después de eventos que interrumpan el normal funcionamiento de las actividades en las áreas de COOPCEN, se brinde respuesta oportuna y asertiva a la recuperación de los servicios informáticos esenciales.
Bajo los lineamientos definidos en el plan de continuidad del negocio sobre la seguridad de la información, se deberán ejecutar simulacros y pruebas que garanticen la efectividad; así como serán revisadas periódicamente por lo menos una vez al año las estrategias para la recuperación oportuna de los servicios informáticos, dicha actividad estará delegada al comité de SGSI.

El plan de continuidad de seguridad de la información deberá ser comunicado en todas las áreas de COOPCEN; de igual manera los simulacros realizados involucrarán a todo al personal generando con esto la capacidad de afrontar situaciones de amenazas que impliquen la continuidad el negocio en el ámbito de la seguridad de la información.

Bajo las pruebas y simulacros realizados se realizará la retroalimentación necesaria para ajustar o eliminar la estrategia de continuidad del negocio; toda prueba realizada se hará de manera controlada sin afectar las operaciones de COOPCEN, documentándolas y generando los respectivos informes donde se especifique las recomendaciones, lecciones aprendidas y acciones de mejora.

Los servicios críticos que necesiten de respaldo para afrontar fallas para no comprometer la continuidad de negocio, se deberá implementarse opciones de redundancia que generen respaldo de los servicios para suplir la caída del servicio primario.

6.4.4.12 Cumplimiento de los requisitos legales. Con el fin de evitar incumplimiento de políticas, normas y legislaciones con respecto a la seguridad de la información, se deberá generar un análisis donde se documenten todos los

requisitos legales; una vez identificados se mantendrán actualizados, para esta labor el área jurídica deberá asesorar al comité de SGSI con el fin de definir las normas y leyes aplicables, entre las cuales estarán:

- Tratamiento de datos personales
- Protección de la información y de los datos
- Derechos de autor
- Delitos informáticos

Todo software disponible en los equipos de cómputo para su uso por las diferentes áreas deberá cumplir con los derechos de la propiedad intelectual, de tal manera que el área de sistemas estará en constante revisión de las licencias y del software definido para los equipos de cómputo, en ningún caso se usará un software que no cuente con su respectiva licencia.

Los documentos, archivos, libros digitales y artículos que se utilicen como herramientas en las diferentes actividades de las áreas de COOPCEN deberán tener su respectivo permiso o referencia del autor, cuando se utilice ciertas partes del documento; así mismo se debe generar conciencia al personal sobre los derechos de propiedad intelectual.

La información que se genera en las diferentes actividades por los funcionarios de COOPCEN estará monitoreada por el sistema de información; de tal forma que se protege los datos ante una eventual perdida, modificación indebida, o acceso no autorizado.

COOPCEN cuenta con la política de tratamiento de datos personales (Anexo E), la cual, deberá ser integrada en los procesos de capacitación y sensibilización sobre seguridad de la información.

Para verificar el cumplimiento y evolución del sistema de gestión de seguridad de la información en cuanto a controles, políticas, procesos y procedimientos se deberá ejecutar auditorías internas, estas permitirán analizar si el SGSI está alineado a los objetivos misionales de COOPCEN, con el objetivo de ajustar el sistema a las necesidades y cambios organizacionales, esta auditoria será llevada por el comité de SGSI quien generará un informe que será revisado por la gerencia para determinar acciones correctivas.

CONCLUSIONES

Acorde con los resultados obtenidos en la presente investigación se extrajeron algunas conclusiones; en primer lugar, se concluye que para administrar los recursos tecnológicos de una organización es necesario tener en cuenta los controles y políticas estipuladas dentro de un SGSI, este proceso estratégico garantiza la seguridad de la información en los diferentes procesos de la organización.

A través del proceso de implementación del sistema se determinó que el trabajo y el interés que tengan los gerentes, funcionarios de la empresa y comités es indispensable, esto permite implementar adecuadamente los controles y políticas para la protección de los datos, dado que, son los agentes organizacionales los encargados de velar por la seguridad y el cumplimiento de las normas establecidas para darle un uso oportuno a los activos informáticos de la empresa.

Ahora bien, es importante mencionar que las políticas desarrolladas en el proyecto fueron generadas en base a las necesidades y las características de COOPCEN como organización financiera y de cooperativismo, lo cual, fue indispensables para generar una operación eficiente del SGSI; además, surgió la necesidad de incrementar la madures en los diferentes dominios de la norma ISO/IEC 27001:2013, por este motivo, se adaptarán o reformarán las políticas establecidas.

Por otro lado, la metodología MAGERIT, permitió que por medio de unos pasos estratégicos, analizar los activos y dar claridad a los riesgos a los que están expuestos, generando tanto cuantitativamente como cualitativamente resultados del impacto que pueden generar las diferentes amenazas propuestas por la metodología, junto a esto también, se genera la valoración de los activos en cuanto a la necesidad y usabilidad que tienen en el ámbito del almacenamiento, procesamiento y transporte de información.

La valoración de los activos y análisis de riesgos realizada en COOPCEN, determinó aquellos activos que son más críticos y que pueden desatar un impacto alto; con esto se determina bajo un plan de tratamiento de riesgos minimizar este impacto y además, brindarle a la gerencia información de la importancia de los activos de información para el desarrollo de las actividades en las diferentes áreas vitales para el cumplimiento de los objetivos misionales.

Para verificar el cumplimiento de la norma ISO/IEC 27001:2013 se generará un análisis de madurez, esto con el fin de identificar los controles de seguridad de la información, presentes y a mejorar; dichos controles se evaluaron en cada objetivo de control, dando como resultado información sobre el estado en la aplicación de la norma y así poder reforzar los dominios en los cuales se encontraron deficiencias para disminuir la probabilidad o el impacto de los riesgos identificados en cada activo de información.

Para generar un cumplimiento aceptable de la norma ISO/IEC 27001:2013 se definieron políticas de seguridad de la información, con la cuales, se logrará que todos los implicados en las diferentes actividades y procesos que generen el cumplimiento de los objetivos misionales de COOPCEN, se guíen bajo ciertos lineamientos y mejores prácticas de seguridad de la información, con el fin último de mantener la confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

EL SGSI que se diseñó fue un gran paso para la mejora de la seguridad de la información los cual permitió que los procesos de la organización generen un alto grado de confianza al personal como a terceros, pero este paso debe ir aún más allá, ya que se debe realizar las respectivas revisiones y actualizaciones que permita al SGSI mantenerse en el tiempo.

Bajo el análisis de riesgo realizado se recomienda generar medidas de seguridad especialmente a las amenazas que tienen un impacto alto en los procesos de la organización.

Igualmente, se recomienda que en los posteriores análisis de riesgo se involucren los nuevos recursos tecnológicos, los cuales, ya hacen parte de la organización y que sin un uso adecuado pueden afectar la integridad, confidencialidad y disponibilidad de la información.

Se sugiere, además, que se generen procesos de formación a todo el personal de COOPCEN sobre le SGSI, con el fin de que cada funcionario de las diferentes áreas, tome conciencia sobre la importancia de la información y los diferentes activos que la procesan y almacenan. Así mismo, se recomienda establecer procesos de auditoria externa con el fin de obtener puntos de vista alternos sobre la funcionalidad y cumplimiento del SGSI.

Bajo el comité de SGSI se recomienda generar las diferentes actualizaciones y revisiones, con el fin de que esté acorde a las nuevas necesidad y cambios ocurridos, tanto en los activos de información, como en los diferentes cargos y funciones.

Por último, se sugiere que dentro del presupuesto anual se considere que el SGSI necesita de recursos económicos para mantener la efectividad de sus controles a desarrollar y permanezca con un grado de efectividad óptimo, debido a que muchas acciones a ejecutarse generan un gasto.

BIBLIOGRAFÍA

ADVISERA EXPERT SOLUTIONS Ltda. ¿Qué es norma ISO27001? [sitio web]. Una introducción a los conceptos básicos. [citado abril 2020]. Disponible en internet: https://advisera.com/27001academy/es/que-es-iso-27001/.

ANA, Andrés y Gómez, Luis. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes [online]. 2009. 14 p. [citado abril 2020]. Disponible en internet: http://www.varios.cen7dias.es/documentos/documentos/90/.

ARRIETA, Álvaro. Políticas y normas de seguridad Informática [online]. 2011. 6 p. [citado abril 2020]. Disponible en internet: https://www.cvs.gov.co/jupgrade/images/stories/docs/Alertas/Politicas_de_ Seguridad_ Informática _CVS_2011-.pdf.

BARTOLOME, Iván. Análisis de MAGERIT y Pilar [online]. Julio 2019. 7 p. [citado abril 2020]. Disponible en internet: http://uvadoc.uva.es/bitstream/handle/10324/37736/TFG-I-1213.pdf?sequence=1&isAllowed=y.

BERNAL, Jorge. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua [online]. Agosto 23 2013. [citado abril 2020]. Disponible en internet: https://www.pdcahome.com/5202/ciclo-pdca/.

Centro Nacional de Información de Ciencias Médicas.[En linea] Metodología para la Gestión de la seguridad Informática. P. 6. Disponible en World Wide Web: https://instituciones.sld.cu/dnspminsap /files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf.

DIAZ, Luis. Diseño De Un Sistema De Gestión De La Seguridad De La Información En La Ips Assalud De Corozal Sucre, Mediante La Implementación De La Metodología Magerit (V3.0) Y La Norma Iso 27001:2013. [online]. Trabajo de grado. Sucre. UNAD. escuela de ci.

FERNANDEZ, Carlos. La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información. [online]. Garantía de Confidencialidad, Integridad y Disponibilidad de la información. Septiembre 2012. 41 p. [citado abril 2020]. Disponible en internet: https://www.pmg-ssi.com/wp-content/uploads/2013/12/ISO-27001-ISOTools.pdf

GALLARDO, María y JÁCOME, Paúl. Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctricas Quito S.A. [online]. Tesis de grado. Escuela Politécnica Nacional. Quito. 2011. [citado octubre 2020]. Disponible en internet: https://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf

Gestión de Riesgos. Magerit. [online]. TITHINK 2013. [citado octubre 2020]. Disponible en internet: https://www.tithink.com/publicacion/MAGERIT.pdf

NAVARRO, Judith. Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI. [online]. Tesis Master. Universidad Nacional de Ingeniería. Nicaragua. 2019. [citado octubre 2020]. Disponible en internet: https://core.ac.uk/download/pdf/288314661.pdf

NEIRA, Agustín y SPOHR, Javier. ISO27000.es. “International Organization For Standardization Iso27000”. [online] [citado abril 2020]. Disponible en internet: http://www.iso27000.es.

PEÑA, José. Diseño De Un Sistema De Gestión De Seguridad De La Información (Sgsi) Bajo La Norma Iso/Iec 27001:2013, En La Cooperativa Multiactiva Del Personal Del Sena, En Bogotá. [online]. Trabajo de grado. Bogotá. UNAD. escuela de ciencias básicas, tec.

PEREZ, Andrés y GONZÁLEZ, Omar. Diseño Del Sistema De Gestión De Seguridad De La Información - Sgsi- Para Los Procesos Críticos De La Cooperativa Febor Basado En La Norma Iso 27001:2013. [online]. Trabajo de grado. Bogotá. UNAD. Facultad De Ingeniería. 2.

PMG SSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información [blog]. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? 06 junio de 2017. [citado abril 2020]. Disponible en internet:https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion.

RUSEEl, Julián. ISO 27001:2013 guía de implementación para la seguridad de la información [online]. 5 p. [citado abril 2020]. Disponible en internet: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20PDFs/NQA-ISO-27001-Guia-de-imp.

VANEGAS, Gonzalo y PARDO, Cesar. Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT [online]. Septiembre 16 2014. 38 p. [citado abril 2020]. Disponible en internet: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/articl.

ANEXOS

Anexo A Formato INAC-SIS Inventario y clasificación de activos de COOPCEN LTDA

CoopCen Ltda.	INVENTARIO Y CLASIFICACIÓN DE ACTIVOS COOPCEN LTDA						INAC-SIS (VER 1.0)						
	ELABORADO:				FECHA:								
IDENTIFICADOR INTERNO DEL ACTIVO	SERIAL	PROCESO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO (Software,Hardware,Servicios)	LUGAR DE UBICACIÓN	PROPIETARIO DEL ACTIVO	USUARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	ESTADO	IMPORTANCIA			
											disponibilidad	integridad	confidencialidad	Valor de importancia
COM-001	7689gfr54358	CARTERA	computador escritorio		HARDWARE	AREA DE ATENCIÓN AL PUBLICO	COOPCEN	FUNCIONARIO DE CARTERA	OFICINA DE CARTERA	BUENO	4	4	5	4,333333333

Elaborado por: COOPCEN LTDA.

Link: https://drive.google.com/file/d/1acAFQDAs8xiKireGQc3pzLn5hMrmy0tX/view?usp=sharing

Anexo B MAN_COP-01 Historial de mantenimiento equipos de cómputo y telecomunicaciones.

Historial de mantenimiento equipos de cómputo y telecomunicaciones					
EMPRESA	COOPCEN	Fecha de Elab:			
NOMBRE DEL ACTIVO DE		22/09/2020			
CORREO	sistemas@coopcen.coop				MAN_COP-01
HISTORIAL DE MANTENIMIENTOS					
TIPO DE MANTENIMIENTO	PREVENTIVO		FECHA DE MANTENIIENTO		MANTENIMIENTO N°
	CORRECTIVO		HORA DE INICIO		
	REVISION		HORA DE FINALIZACION		
	ACTULIZACIÓN				
DESCRIPCION DEL MANTENIMIENTO					REALIZADO POR
REALIZA MANTENIMIENTO			RECIBE DE CONFORMIDAD		
NOMBRE Y FIRMA			NOMBRE Y FIRMA		

Elaborado por: COOPCEN LTDA.

Link:
https://drive.google.com/file/d/1br0FUvOAE6_bnCRNhCad1XPW8h0xw8-s/view?usp=sharing

Anexo C procedimiento PGI_COOP incidentes de seguridad de la información

CoopCen ltda. COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO **PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	PGI_COOP	20/10/2020
	Versión 1.0	

1. OBJETIVO

Identificar y brindar la atención oportuna a todos los incidentes de seguridad y privacidad de la información, con el fin de mitigar el impacto.

2. ALCANCE

Todo incidente en seguridad de la información deberá ser identificado, clasificado, solucionado y generar aprendizaje a la organización de COOPCEN LTDA.

3. PROCEDIMIENTO:

3.1 Los incidentes de segura serán reportados al correo electrónico sistemas@coopcen.coop , el cual debe estar sustentado con las evidencias correspondientes de lo ocurrido.

3.2 Recibido la notificación vía correo electrónico el coordinador del área de sistemas deberá dirigirse al área donde se presentaron los hechos y recopilar la información bajo el formulario de reporte de incidentes FI_COOP.

Bajo la información recolectada por el coordinador de sistemas se clasificará el incidente bajo lo siguiente:

- Hubo daño o pérdida de información.
- Hubo fuga y/o robo de información.
- Hubo robo de credencias o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presenta un comportamiento anormal del computador y/o sistema de información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, Ransomware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.

Seguidamente se realiza la valoración del impacto según la tabla No.1

IMPACTO	DESCRIPCIÓN	VALORACIÓN
Catastrófico	Si llegara a presentarse: Daños totales a la infraestructura tecnológica de COOPCEN. Mala Reputación a nivel nacional Pérdidas económicas elevadas.	ALTO
Mayor	Si llegara a presentarse: Pérdidas económicas mayores Daños totales a la infraestructura tecnológica de COOPCEN. Mala Reputación a nivel nacional.	
Moderado	Si llegara a presentarse: Pérdidas económicas moderadas Daños parciales a la infraestructura tecnológica de COOPCEN. Llamados de atención a nivel organizacional Mala Reputación al proceso a nivel de organización.	MEDIO
Menor	Si llegara a presentarse: Pérdidas económicas menores Daños pequeños a la infraestructura tecnológica de COOPCEN. Llamados de atención a nivel de procesos. Mala Reputación de las áreas responsables.	BAJA
Insignificante	Si llegara a presentarse: Pérdidas económicas insignificantes Daños pequeños a la infraestructura tecnológica de COOPCEN. Llamados de atención a nivel de grupo Mala Reputación a nivel de grupo.	

Junto a la valoración y en el campo de evidencias del formato reporte de incidentes FI_COOP, se deberá adjuntar las pruebas necesarias que ratifique dicha valoración; estas evidencias serán almacenadas ante posibles usos a nivel judicial.

3.3. Según sea la valoración del incidente se deberá ejecutar la respectiva solución; Ya sea ejecutando tareas de recuperación, restauración, reiniciación, remplazo, reparación de los servicios o activos de información afectados.

3.4. Todo incidente presentado deberá generarse la respectiva retroalimentación al grupo de trabajo de todas las áreas, con el fin de que se tome conciencia o evitar que los funcionarios recaigan en el mismo suceso, además esto permite asegurar que a todas las áreas se le realice los respectivos ajuste y solución del incidente inicial.

3.11 En caso de que se presente un incidente de seguridad de la información el coordinador de sistemas, reportara los incidentes de seguridad a los entes externos de ser necesario.

Se pueden reportar incidentes de seguridad de la información a través de los siguientes canales:

- ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897.
- CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co
- Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/

Elaborado por: COOPCEN LTDA.

Anexo D Formato FI_COOP incidentes de seguridad de la información

CoopCen ltda. COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO	FI_COOP v 1.0
	Fecha:

REPORTE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. **Reportarte**

Nombre y cargo de la persona que reporta:	
Correo electrónico:	
Teléfono:	
Área:	

2.

Información del Incidente	
2.1. Fecha y hora del Incidente:	
2.2. Fecha y hora de detección:	
2.3. Breve descripción del incidente (¿qué pasó?, ¿dónde pasó?, ¿cuándo pasó?, ¿cómo pasó?, ¿Qué servicios y como se afectaron?)	
2.4. Componentes a afectados en el incidente de seguridad de la información.	☐ Zona de red afectada (internet, red interna, red de administración, entre otras): _____
	☐ Tipo de sistema afectado (servidor de archivos, estaciones de trabajo, ya sea de escritorio o móvil, entre otros): _____
	☐ Sistema operativo (especificar versión): _____
	☐ Protocolos o servicios y aplicaciones (especificar versión): _____
	☐ Otro: Especificar_____

CoopCen ltda. COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO	FI_COOP v 1.0
	Fecha:

Información del Incidente	
2.5. Nivel estimado de daño o impacto provocado por el incidente de seguridad de la información:	Crítico ☐ Medio ☐ Bajo ☐ porque:
2.6. evidencias (fotografías, pantallazos, videos.)	Nombre del archivo o documento:
2.8. Detallar las acciones inmediatas que han realizado para mitigar el incidente de seguridad de la información:	

3. Clasificar el incidente de seguridad de la información reportado en el presente anexo con base en las siguientes definiciones:

Clases de Incidente	Aplica	Describir el incidente específico
3.1. Ataques físicos (deliberados o intencionales) tales como: sabotaje, vandalismo, robo de dispositivos, fuga de información en medios físicos, acceso físicos no autorizados, coerción, extorsión, ataque terrorista, entre otros.	☐	
3.2. Daño no intencional o accidental, pérdida de información o pérdida de activos, tales como: información compartida indebidamente, errores u omisiones en sistemas o dispositivos, errores en procedimientos o controles, cambios indebidos a datos, extravío de información o dispositivos, entre otros.	☐	
3.3. Incidentes por desastres naturales o ambientales, tales como: Terremotos, inundaciones, huracanes, incendios, radiación, corrosión, explosiones, entre otros.	☐	
3.4. Incidentes por fallas o mal funcionamiento, tales como: Falla en dispositivos o sistemas, fallas en comunicaciones, en servicios o equipos de	☐	

Clases de Incidente	Aplica	Describir el incidente específico
terceros o en la cadena de suministros, entre otros.		
3.5. Incidentes por la interrupción o falta de insumos, tales como: Ausencia de personal, huelgas, interrupción de servicios de energía, agua, telecomunicaciones, entre otros.	☐	
3.6. Incidentes por intercepción de datos, tales como: espionaje, intercepción de mensajes, wardriving, ataques de hombre en medio, secuestro de sesiones, programas sniffers, robo de mensajería, entre otros.	☐	
3.7. Incidentes por actividad maliciosa (ciber ataques) con el fin de tomar el control, desestabilizar o dañar un sistema informático, tales como: Robo de identidad, Phishing, Negación de servicio (DOS, DDOS), Código malicioso (malware, troyanos, gusanos, inyección de código, virus, ransomware), Ingeniería Social, Vulneración de certificados (suplantación de sitios, certificados falsos), manipulación de hardware (proxies anónimos, skimmers, sniffers), alteración de información (suplantación de direccionamiento y tablas de ruteo, DNS poisoning, alteración de configuraciones), abuso de aplicaciones de auditoría, ataques de fuerza bruta, abuso de autorizaciones, entre otros.	☐	
3.8. Originadas por aspectos legales, tales como: Violación de cláusulas y acuerdos, violación de confidencialidad, decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras), entre otras.	☐	

Elaborado por: COOPCEN LTDA.

Anexo E Política de tratamiento de datos personales.

CoopCen ltda.
Cooperativa Multiactiva de Trabajadores, Jubilados y Pensionados de Cedenar
NIT.891.224.291-1

1. OBJETIVO

Definir los lineamientos necesarios para la protección de datos personales contenidos en las diferentes bases de datos de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., de modo que reciban el tratamiento conforme a los fines previstos.

2. ALCANCE

Esta política es de obligatorio y estricto cumplimiento por parte de todos los empleados de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., los contratistas y terceros que obran en nombre de la cooperativa.

Todos los colaboradores de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., deben observar y respetar estas políticas en el cumplimiento de sus funciones. En los casos en que no exista vínculo laboral se deberá incluir una cláusula contractual para que todos, quienes obren en nombre de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., o lo representen, se obliguen a cumplir estas políticas. El incumplimiento de las mismas originará sanciones de tipo laboral o responsabilidad contractual según el caso. Lo anterior, sin perjuicio del deber de responder patrimonialmente por los daños y perjuicios que cause a los titulares de los datos o a la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., por el incumplimiento de estas políticas o el indebido tratamiento de datos personales.

3. DEFINICIONES Y VOCABULARIO

- **AUTORIZACIÓN:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales
- **AVISO DE PRIVACIDAD:** Comunicación verbal o escrita generada por el Responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **BASE DE DATOS**: Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **DATO PERSONAL:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **DATO PUBLICO:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **DATOS SENSIBLES:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
  El Registro Nacional de Bases de Datos: es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

- **Encargado Del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento
- **Responsable Del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento
- **Transferencia**: La transferencia de datos tiene lugar cuando el Responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

4. DESARROLLO

I. UBICACIÓN

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA" con NIT 891.224.291-1, ubicada en la Carrera 32 No 19 A -28, Pasto, Nariño. Colombia, Teléfono fijo: 7291957, Teléfono Móvil 3155977193, e-mail: secretaria@coopcen.coop

II. NORMATIVIDAD

Estás políticas se rigen y son el resultado de la aplicación del artículo 15 de la Constitución Política de Colombia, de los artículos 1 al 30 de la Ley 1581 de 2012, artículos 1 al 28 del decreto 1377 de 2013, artículos 1 al 16 del Decreto 886 de 2014, contenidos en los capítulos 25 y 26 del Decreto único 1074 de 2015 del sector Comercio, Industria y Turismo.

III. PRINCIPIOS

Con el fin de garantizar la protección de datos personales, la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., se ciñe al cumplimiento de los siguientes principios para efectos del tratamiento (recolección, almacenamiento, uso, circulación o supresión), transferencia y transmisión de datos personales a los cuales tenga acceso.

Principio de legalidad en materia de tratamiento de datos: El tratamiento de datos personales es una actividad reglada que debe sujetarse a las disposiciones vigentes y aplicables que desarrollen el tema.

Principio de finalidad: El tratamiento de datos que lleve a cabo la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., obedecerá a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual será debidamente informada a los titulares de los datos personales.

Principio de libertad: El tratamiento de datos personales que lleve a cabo la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., el personal a su cargo, o cualquier tercero que llegase a tener acceso a las bases de datos de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., en el tratamiento de datos personales garantizará al titular el derecho a obtener en cualquier momento y sin restricción alguna, información acerca de la existencia de datos que le conciernan.

Principio de acceso y circulación restringida: El tratamiento de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la ley.

Principio de seguridad: La información sujeta a tratamiento por parte de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., del personal a su cargo y de cualquier tercero que tenga, llegase a tener acceso a las bases de datos de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., o externos que por algún motivo que intervengan en el tratamiento de datos personales de las bases de datos de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

IV. FINALIDADES ESPECIALES

Además de las finalidades generales, existen finalidades particulares, atendiendo a la relación que tienen las personas con la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., como a continuación se describen:

4.1. Finalidades especiales para el tratamiento de los datos de pacientes:

- Lograr una eficiente comunicación relacionada con nuestros servicios y alianzas, por diferentes medios
- Ofrecer información sobre campañas, programas especiales
- Informar e invitar a campañas de mercadeo, promoción de servicios y educación al asocado.
- Realizar encuesta de satisfacción de servicios y atenciones prestadas
- Contestación, gestión y seguimiento a solicitudes de mejoramiento, peticiones y sugerencias.

4.2. Finalidades especiales para el tratamiento de los datos personales de colaboradores y pensionados

- Realización de publicaciones internas y externas
- Apertura de acceso a plataformas tecnológicas propias de la organización
- Brindar información a empresas que solicitan verificar datos laborales de los empleados para autorización de créditos de dinero o créditos comerciales. (Previa verificación de fuente y uso de datos, se debe centrar en la verificación más no en el suministro de la información).
- Ser contactado directamente en caso de ser requerido, en razón de sus funciones.
- Detectar las necesidades de capacitación e implementar acciones que permitan el desarrollo de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA".,
- Informar y conformar procesos de elección y promoción interna.

4.3. Finalidades especiales para el tratamiento de los datos personales de proveedores y contratistas

- Evaluación de bienes y servicios prestados por proveedores y contratistas
- Seguimiento y gestión de la relación contractual

4.4. Finalidades especiales de los datos personales de visitantes y otros usuarios de la comunidad

- Seguridad de los asociados, visitantes, colaboradores y de la comunidad en general que se encuentran en las instalaciones de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA".

V. TRATAMIENTO AL CUAL PODRÁN SER SOMETIDOS LOS DATOS PERSONALES

- Consulta
- Trámites administrativos
- Envío de información
- Investigación
- Solicitud de diligenciamiento de encuestas
- Realización de llamadas

Nota: frente al tratamiento de los **datos sensibles**, la ley permite que estos sean tratados únicamente cuando:

- El titular de los datos personales haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del titular de los datos personales y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
- El tratamiento se refiere a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

Igualmente, el tratamiento de datos personales de niños, niñas y adolescentes se realizará bajo los parámetros enunciados anteriormente en esta política.

VI. CARTA DE DERECHOS DE LOS TITULARES DE DATOS PERSONALES TRATADOS EN LA COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA".

El titular de los datos personales tratados en la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., tendrá los siguientes derechos:

a. Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
b. Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.
c. Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
d. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley 1581 de 2012, y las demás normas que la modifiquen, adicionen o complementen;

e. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
Nota: La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que, en el tratamiento, el responsable o encargado han incurrido en conductas contrarias a esta ley y a la Constitución;
f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
g. El titular podrá consultar de forma gratuita sus datos personales:
h. Al menos una vez cada mes calendario
i. Cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, el responsable solo podrá cobrar al titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente.

VII. CONSULTAS

Los titulares de los datos personales o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., el cual suministrará a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

La consulta podrá ser formulada a través de los diferentes medios físicos o electrónicos habilitados para ello, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida de conformidad con el término establecido en la ley, contados a partir de la fecha de recibo de la misma en la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., cuando se trate de un medio físico o en el correo electrónico secretaria@coopcen.coop, cuando sea través de un medio electrónico. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

VIII. RECLAMOS

El titular de los datos personales o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., el cual será tramitado bajo las siguientes reglas:

a. El reclamo se formulará mediante solicitud dirigida a la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., ya sea por medio físico o electrónico traumedicalgerencia@gmail.com, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la

recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

b. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

c. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

d. El término máximo para atender el reclamo será de quince (10) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Nota: en el asunto de la solicitud se deberá indicar que se trata de datos personales y especificar si se trata de datos de paciente, colaborador, contratista o proveedor, o usuario en general.

IX. LEGITIMACIÓN PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR

Los derechos de los titulares establecidos en la Ley, podrán ejercerse por las siguientes personas:

- Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro o para otro.

Nota: Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

X. DERECOS DE LOS NIÑOS Y ADOLESCENTES

En el tratamiento de datos personales a cargo de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.

- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente, otorgará la autorización a la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

XI. RESPONSABLES Y CANALES

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., con el fin de garantizar el derecho de acceso a los titulares de los datos personales, para la atención de consultas, reclamos, peticiones de rectificación, actualización y supresión de datos, cuenta mecanismos físicos y electrónicos para la recepción de solicitudes, a través del correo electrónico secretaria@coopcen.coop o físicamente a través de la oficina de la Gerencia de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA".,

XII. AUTORIZACION DEL TITULAR

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., para el tratamiento de datos personales requiere la autorización previa, expresa e informada del titular de los mismos, excepto en los siguientes casos autorizados por la ley 1581 de 2012:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

De la autorización requerida para el tratamiento de datos personales sensibles, cuando dicho tratamiento sea permitido, la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., deberá cumplir con las siguientes obligaciones:

- Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su tratamiento.
- Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.
- Ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles.

12.1. MEDIOS PARA OBTENER Y OTORGAR LA AUTORIZACION:

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., con el fin de dar cumplimiento a lo establecido en la Ley 1581 de 2012, obtendrá de manera previa al tratamiento de los datos personales, la autorización de los titulares o de quienes se encuentren legitimados para ello a través de diferentes mecanismos como: Formato de autorización para la recolección y tratamiento de datos personales, correo electrónico, página web, mensaje de datos, Intranet o cualquier otro mecanismo que permita concluir inequívocamente que la autorización fue otorgada.

En ningún caso, el silencio podrá asimilarse a una conducta inequívoca.

12.2. PRUEBA PARA LA AUTORIZACION:

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., desplegará los medios físicos y electrónicos necesarios para la conservación de la prueba de la autorización otorgada por los titulares de los datos personales para el tratamiento de los mismos sin importar cuál haya sido el medio a través de la cual dicha autorización haya sido obtenida.

12.3. REVOCATORIA DE LA AUTORIZACIÓN Y/O SUPRESIÓN DEL DATO

Los titulares de los datos personales podrán en todo momento solicitar a la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., la supresión de sus datos personales y/o revocar total o parcialmente la autorización otorgada para el tratamiento de los mismos, mediante la presentación de un reclamo.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular de los datos personales tenga un deber legal o contractual de permanecer en la base de datos.

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., pondrá a disposición del titular de los datos personales mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.

XIII. MEDIDAS DE SEGURIDAD

La COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., a través de su Política de Seguridad de la Información y capacitación de personal buscará garantizar el cumplimiento del principio de seguridad de la Ley 1581 de 2012 y demás normas concordantes y complementarias, así como la implementación de la obligación contractual en las relaciones que se adquieran con proveedores y contratistas, que de una u otra forma presten bienes y servicios encaminados a contribuir a la prestación de servicios de la cooperativa.

13.1. PERSONAS A LAS CUALES SE LES PUEDE SUMINISTRAR LA INFORMACION:

La información que reúna las condiciones establecidas en la presente política podrá ser suministrada por la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., a las siguientes personas:

- A los titulares, sus causahabientes o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el titular o por la ley.

13.2. TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES:

Para la transmisión y transferencia de datos personales, se aplicarán las siguientes reglas:

- Las transferencias internacionales de datos personales deberán observar lo previsto en el artículo 26 de la Ley 1581 de 2012; es decir, la prohibición de transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos y los casos excepcionales en los que dicha prohibición no aplica.
- Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al titular ni contar con su consentimiento cuando exista un contrato en los términos del artículo 25 de la Ley 1581 de 2012.
- Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio.
- De manera excepcional, la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., podrá hacer transferencia de datos personales en los siguientes casos:

✓ Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia.
✓ Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública.
✓ Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
✓ Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
✓ Transferencias necesarias para la ejecución de un contrato entre el titular y COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular.
✓ Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

14. DEBERES DE LOS RESPONSABLES Y DE LOS ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

14.1. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO DE DATOS PERSONALES:

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

El Responsable del Tratamiento, al momento de solicitar al titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

- El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- Los derechos que le asisten como titular;
- La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.
- El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en este numeral y, cuando el titular lo solicite, entregarle copia de esta.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el titular;
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento;
- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular;
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
- Informar a solicitud del titular sobre el uso dado a sus datos;
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

- Deber de acreditar puesta a disposición del aviso de privacidad y las políticas de Tratamiento de la información, cuando sea usado este medio.
- Debe conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven.
- Debe conservar prueba de la autorización otorgada por los titulares de datos personales para el tratamiento de los mismos.

14.2. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES:

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento;

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
- Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
- Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente ley;
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares;
- Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;
- Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares;
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Nota 1: en el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

Nota 2: Las políticas de tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

14.3. DEBERES TANTO DE LOS RESPONSABLES COMO DE LOS ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES:

- Deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquellos y ejercer sus derechos sobre los mismos.

- Deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento.

- Deberán designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto 1377 de 2013.

15. TEMPORALIDAD DEL TRATAMIENTO DE DATOS PERSONALES

La permanencia de los datos personales recolectados por la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., estará determinada por la finalidad del tratamiento para los que estos hayan sido recogidos.

Una vez cumplida la finalidad del tratamiento, la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA"., procederá a la supresión de los datos personales recolectados. No obstante, lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

La presente Política de Protección de Datos Personales fue aprobada por la Gerencia y rige a partir del 30 de octubre de 2018 y deja sin efecto alguno cualquier documento anterior que buscara regular el tema en el interior de la COOPERATIVA MULTIACTIVA DE CENTRALES ELECTRICAS DE NARIÑO "COOPCEN LTDA".

Firmado Original
Representante Legal
COOPCEN LTDA.

Anexo F. Resumen Analítica Especializado

Fecha de Realización:	30/11/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de Sistemas
Título:	DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013
Autor(es):	Zambrano Gómez Luis Gerardo
Palabras Claves:	ISO 27001:2013, MAGERIT, activos, riesgos, políticas.
Descripción:	La presente investigación es un proyecto de grado aplicado a la organización COOPCEN LTDA; la cual es una cooperativa del sector de la economía solidaria y que su actividad principal es la de prestar el servicio de crédito en sus diferentes modalidades. El objetivo de proyecto se fundamenta en generar bunas prácticas y procedimientos para minimizar los riesgos y amenazas para así también reducir el impacto que puedan causar; todo esto con el fin de que la información esté íntegra, disponible y confidencial cuando se utilice en los procesos de afiliación, crédito, financiero, ingreso de fondos, afiliaciones y gestión tecnológica, debido a que estos son las principales actividades para dar cumplimiento a la misión de COOPCEN LTDA; por tal razón el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001:2013 y la metodología MAGERIT para el análisis y gestión de riesgos, garantizando la protección de los activos de información.

Fuentes bibliográficas destacadas:

El desarrollo del proyecto se sustenta bajo referentes bibliográficos que hacen énfasis en la implementación de un sistema de gestión de seguridad de la información, así como también el desarrollo del análisis de riesgos bajo la metodología MAGERIT y la norma ISO/IEC 27001:2013.

GALLARDO, María y JÁCOME, Paúl. Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctricas Quito S.A. [online]. Tesis de grado. Escuela Politécnica Nacional. Quito. 2011. [citado octubre 2020]. Disponible en internet: https://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf

Gestión de Riesgos. Magerit. [online]. TITHINK 2013. [citado octubre 2020]. Disponible en internet: https://www.tithink.com/publicacion/MAGERIT.pdf

NEIRA, Agustín y SPOHR, Javier. ISO27000.es. “International Organization For Standardization Iso27000”. [online] [citado abril 2020]. Disponible en internet: http://www.iso27000.es.

Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 2- Catalogo de Elementos. [online] [citado 18 abril 2020] Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

PMG SSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información [blog]. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? 06 junio de 2017. [citado abril 2020]. Disponible en internet: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion.

Contenido del documento:	El desarrollo del proyecto cuenta con 6 capítulos dispuestos así: En el primer capítulo se plantea el problema que da origen a la realización de este proyecto de investigación. El capítulo dos se describe la razón por la cual se requiere tomar medidas para generar el DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013. En el capítulo tres se plantea el objetivo sobre el cual se desarrollan ciertas actividades. Bajo el capítulo cuatro se indaga bajo fuentes bibliográficas externas y que tengan relación con el proyecto desarrollado; también se sustenta el desarrollo del proyecto bajo conceptos en relación con Sistema De Seguridad De La Información. Este capítulo también contiene descripción de las leyes y normas que aplican en la temática del proyecto, igualmente se realiza la descripción de COOPCEN LTDA en la cual se desarrolla la implementación del SGSI.

	En el capítulo 5 se menciona la metodología con la cual se obtendrán datos cualitativos o cuantitativos que permitan abordar el problema de estudio. El capítulo 6 se desarrolla los objetivos propuestos que son: Identificar los activos de información que están presenten en la Cooperativa Multiactiva de Centrales Eléctricas de Nariño. Identificar las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos de información. Establecer controles necesarios, de acuerdo a la norma ISO/IEC 27001:2013. Establecer políticas de seguridad de la información aplicables a COOPCEN que permitan mitigar los riesgos identificados.
Marco Metodológico:	El proyecto se desarrolla bajo el enfoque cuantitativo y cualitativo, se obtendrán datos que permitirá dar claridad a la importancia de proteger la información para generar en la empresa una dinámica óptima donde las operaciones realizadas en esta tengan un grado de confianza a la hora de procesar y almacenar información valiosa. Para desarrollar el proyecto se utilizó fuentes de información que están estrechamente relacionadas con las actividades de la empresa, así también se utiliza las técnicas de recolección de información como la entrevista, lista de chequeo y observación directa.
Conceptos adquiridos:	El desarrollo del proyecto permitió generar Apropiación de la metodología de análisis de riesgo MAGERIT como una herramienta que permite evaluar los riesgos y amenazas que vulneren la integridad, disponibilidad y confidencialidad de la información. También se adquiere conocimiento en la norma ISO/IEC 27001:2013 con sus diferentes objetivos de cada dominio que la integra; igualmente se conoce las diferentes políticas de seguridad de la información que pueden aplicarse y adaptarse según el contexto de cada organización.
Conclusiones:	EL SGSI permite a la organización garantizar la seguridad de la información, bajo controles que protegen los diferentes activos y se establece políticas para ser

	cumplidas por los actores de los procesos que hacen parte del SGSI. Bajo el uso de la metodología MAGERIT se genera la valoración de los activos de información, identificando los más críticos que puedan desencadenar perdida de información, por tal razón se establece un plan de tratamiento de riesgos el cual minimiza el impacto que generan las diferentes amenazas identificadas en cada activo de información. Todos los controles que se implementan bajo la norma ISO/IEC 27001:2013 serán de gran importancia para proteger la información, el cumplimiento de esta llevo a generar políticas de seguridad de la información para que los funcionarios de COOPCEN LTDA se guíen bajo ciertos lineamientos y mejores prácticas de seguridad de la información, con esto el nivel de madurez del cumplimiento de la norma se verá favorecido.

Anexo G. Acuerdo de Confidencialidad

CoopCen Ltda.

Cooperativa Multiactiva de Centrales Eléctricas de Nariño Ltda.

V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE LUIS GERARDO ZAMBRANO GOMEZ Y LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO.

Por la **parte reveladora**
Nombre: **Cooperativa Multiactiva De Centrales Eléctricas De Nariño.**
Dirección: **Carrera 32 # 19A-28 Las Cuadras**
Teléfono: **7291957**
E-mail: **coopcen_cedenar@hotmail.com**

Por la parte **receptora de la información**
Nombre: **Luis Gerardo Zambrano Gómez**
Dirección: Manzana 52 Casa 10 Barrio Chambu II
Teléfono: 3157034818
E-mail: luiszambrano874@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la Cooperativa Multiactiva De Centrales Eléctricas De Nariño, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto aplicado con el título DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013.
   Que la información de propiedad de la Cooperativa Multiactiva De Centrales Eléctricas De Nariño ha sido desarrollada u obtenido legalmente, como resultado de sus procesos,

programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

2. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013, *Luis Gerardo zambrano Gómez* que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de la Cooperativa Multiactiva De Centrales Eléctricas De Nariño.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente a la Cooperativa Multiactiva De Centrales Eléctricas De Nariño, así como también a no utilizar dicha información en beneficio propio ni de terceros, sólo con fines estadisticos y de mejoramiento de la Cooperativa Multiactiva De Centrales Eléctricas De Nariño.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,
3. modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013 lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que

recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Cooperativa Multiactiva De Centrales Eléctricas De Nariño, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de Cooperativa Multiactiva De Centrales Eléctricas De Nariño.

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: información de infraestructura tecnológica, información de procesos, actividades de cada área y activos de información.

10. La información capturada por la **parte receptora** se observará como *cifras para generar información cualitativa y cuantitativa,* no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad de todo el personal de la Cooperativa Multiactiva De Centrales Eléctricas De Nariño no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de la Cooperativa Multiactiva De Centrales Eléctricas De Nariño, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante Luis Gerardo Zambrano Gómez se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa Cooperativa Multiactiva De Centrales

Eléctricas De Nariño para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la emresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcances, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(Luis Gerardo Zambrano Gómez – Cooperativa Multiactiva De Centrales Eléctricas De Nariño)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso

de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las clausulas del presente acuerdo de confidencialidad por parte de *Luis Gerardo Zambrano Gómez.*

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en San Juan de Pasto a los 20 días del mes de marzo de 2020

Como Parte Receptora:

Luis Gerardo Zambrano.
Estudiante UNAD.
C.C. No. 87.069.555 de Pasto

Por la parte reveladora:

Mario Fernando Rodríguez
Gerente COOPCEN.
C.C. No. 79.625.395 de Pasto

Anexo H Autorización para ejecutar proyecto

V0.1

San Juan de Pasto, 20 de marzo de 2020

Señor:
Mario Fernando Rodríguez Chaves
GERENTE COOPCEN.

Asunto: Autorización para la ejecución del proyecto titulado: DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a la Cooperativa Multiactiva De Centrales Eléctricas De Nariño, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA MULTIACTIVA DE CENTRALES ELÉCTRICAS DE NARIÑO BASADO EN LA NORMA ISO 27001:2013.el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: Diseñar un Sistema de Gestión de Seguridad (SGSI) de la Información para la Cooperativa Multiactiva de Centrales Eléctricas de Nariño. (COOPCEN), basado en la norma ISO/IEC 27001:2013.; al mismo

tiempo será apoyado por los objetivos específicos: "Identificar los activos de información que están presenten en la Cooperativa Multiactiva de Centrales Eléctricas de Nariño Ltda. (COOPCEN), con el fin de determinar los dominios aplicables para el diseño del SGSI, Identificar las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos de información que afecten la continuidad del negocio, Establecer controles necesarios, de acuerdo a la norma ISO/IEC 27001:2013 que permita garantizar la disponibilidad, confidencialidad y disponibilidad de la información y establecer políticas de seguridad de la información aplicables a COOPCEN que permitan mitigar los riesgos identificados para obtener como resultado un alto impacto en la seguridad de la empresa Cooperativa Multiactiva De Centrales Eléctricas De Nariño.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por Cooperativa Multiactiva De Centrales Eléctricas De Nariño.
- La empresa Cooperativa Multiactiva De Centrales Eléctricas De Nariño deberá establecer que tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

V0.1

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en San Juan de Pasto, a los 20 días del mes de marzo de 2020

Cordialmente,

Luis Gerardo Zambrano Gómez
Estudiante UNAD.

Mario Fernando Rodríguez Chaves
Gerente COOPCEN.