DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMFENALCO QUINDÍO

MAGDA MAYERY BAQUERO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ARMENIA
2019

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMFENALCO QUINDÍO

MAGDA MAYERY BAQUERO CARDONA

Trabajo de Grado para optar al título de Especialista en Seguridad Informática.

Director
ING. LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ARMENIA
2019

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Armenia, diciembre de 2019

DEDICATORIA

A mis seres queridos, por todo su apoyo y amor, el cual me impulsa a seguir creciendo como persona y como profesional, para brindarles bienestar y tranquilidad.

AGRADECIMIENTOS

Agradezco a la UNAD y a todos los docentes que durante el proceso de formación, me acompañaron y compartieron sus conocimientos, para ayudarme a ser una mejor profesional, a pesar de la distancia y del tiempo.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

La Caja de Compensación Familiar del Quindío, Comfenalco Quindío, es la única Caja de Compensación Familiar y una de las empresas más grandes y de las mayores generadoras de empleo en el departamento del Quindío, Colombia.

El objeto misional de la organización es el pago de subsidio familiar a los trabajadores afiliados a la Caja con categorías A y B, proceso a través del cual recoge gran parte de información confidencial tanto de las empresas afiliadas como de sus trabajadores y beneficiarios, información que se recibe y procesa tanto de manera física como digital, la cual reviste vital importancia para la organización, dado que dicha información se constituye como soporte principal para las gestiones de la misma y su manejo y custodia es responsabilidad de la entidad.

En este trabajo se describen los objetivos, el alcance y el diseño de un Sistema de Seguridad de la Información para Comfenalco Quindío fundamentado en la norma NTC/ISO 27001:2013 dirigido hacia los procesos considerados críticos para la empresa desde la perspectiva de su Misión y Visión. En este orden de ideas, se realiza un diagnóstico de la situación mediante la aplicación de un análisis diferencial respecto a la norma seguido de la identificación de amenazas y vulnerabilidades en el contexto de la metodología de análisis y gestión de riesgos MAGERIT y finalmente se diseñan los documentos base que puedan servir a la Caja para llevar a cabo los planes de tratamiento de riesgos.

En razón a lo anterior y dado que la empresa cuenta con la certificación en la NTC ISO 9001:2008, se definió elaborar para dicha organización un DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMFENALCO QUINDÍO.

Para la elaboración de dicho modelo se tuvo en cuenta:

I. La NTC/ISO 27001:2013.

La cual proporciona las herramientas necesarias para el establecimiento de un Sistema de Gestión de la Seguridad Informática, además de que cuenta con el anexo A, el cual recoge los objetivos de control y controles que las empresas deben implementar a fin de minimizar el impacto ante la eventual materialización de una amenaza informática, dando como resultado la Política General de Seguridad de la Información, teniendo en cuenta los objetivos de control y controles seleccionados para la organización.

II. La metodología de análisis y gestión de riesgos MAGERIT.

MAGERIT proporciona una metodología para la elaboración del análisis y gestión de riesgos de la organización. Dicha metodología resulta ser de fácil entendimiento y aplicación, además de que se adapta fácilmente a organizaciones pequeñas, medianas y grandes. Resultado de este análisis se proporcionan las salvaguardas necesarias para minimizar el impacto ante la eventual materialización de una amenaza informática.

Palabras Claves: Sistemas de Gestión de la Seguridad de la Información (SGSI), Estándar ISO/IEC 27001:2013, Metodología de Riesgos Informáticos, MAGERIT.

ABSTRACT

The Quindío Family Compensation Fund, Comfenalco Quindío, is the only Family Compensation Fund and one of the largest and largest employment generating companies in the department of Quindío, Colombia.

The missionary purpose of the organization is the payment of family subsidy to workers affiliated to the Fund with categories A and B, a process through which it collects a large part of confidential information from both affiliated companies and their workers and beneficiaries, information that it is received and processed both physically and digitally, which is of vital importance to the organization, given that this information is constituted as the main support for the management of the same and its management and custody is the responsibility of the entity.

This paper describes the objectives, scope and design of an Information Security System for Comfenalco Quindío based on the norm NTC / ISO 27001: 2013 directed towards the processes considered critical for the company from the perspective of its Mission and View. In this order of ideas, a diagnosis of the situation is made through the application of a differential analysis with respect to the standard followed by the identification of threats and vulnerabilities in the context of the MAGERIT risk analysis and management methodology and finally the base documents that can be used by the Fund to carry out the risk treatment plans.

Due to the above and given that the company has the certification in the NTC ISO 9001: 2008, it was defined to prepare for this organization an DESIGN OF THE INFORMATION SECURITY MANAGEMENT SYSTEM FOR COMFENALCO QUINDIO COMPANY.

For the elaboration of said model, the following was taken into account:

I. The NTC / ISO 27001: 2013.

Which provides the necessary tools for the establishment of a Informatic Security Management System, in addition to having the Annex A, which includes the control and control objectives that companies must implement in order to minimize the impact to the eventual materialization of a computer threat, resulting in the General Information Security Policy, taking into account the control objectives and controls selected for the organization.

II. The methodology of risk analysis and management MAGERIT.

MAGERIT provides a methodology for the organization's analysis and risk management. This methodology turns out to be easy to understand and apply, as well as being easily adapted to small, medium and large organizations. The result

of this analysis is to provide the necessary safeguards to minimize the impact of the possible materialization of a computer threat.

Key Words: Information Security Management Systems (ISMS, ISMS), ISO / IEC 27001: 2013 Standard, IT Risk Methodology, MAGERIT

1. INTRODUCCION

La información desde todas sus formas de presentación, se constituye en uno de los principales activos de cualquier organización, la cual es necesaria para el normal funcionamiento y alcance de los objetivos misionales de la entidad a la que pertenece, con el agravante que a medida que crecen las empresas crece también el volumen de información que genera e igualmente los riesgos asociados de tal manera que los delitos informáticos y otros riesgos de los sistemas de información inciden en el crecimiento de la búsqueda de seguridad por parte de las organizaciones y empresas. Es por ello que, hoy por hoy, más empresas se están ocupando de su protección desde dimensiones que implican la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la misma.

Atendiendo a la premisa anterior, actualmente existen en el medio, una serie de normas que brindan modelos para la Gestión de la Seguridad Informática, las cuales se encargan de definir, alcanzar y mantener unos niveles apropiados de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad para la información que necesita para operar, niveles que se habían definido anteriormente como dimensiones. Un ejemplo claro de tales normas es la NTC/ISO 27001:2013, “Sistemas de Gestión de la Seguridad de la Información”.

La necesidad de establecer políticas y protocolos para atender de manera eficaz y efectiva, no sólo las debilidades conocidas sino también las desconocidas, ha derivado en un cambio de enfoque en materia de seguridad informática pasando de ser netamente basado en la tecnología a ámbitos más amplios como lo son la organización en sí, la cultura corporativa, aspectos legales y obviamente la tecnología.

La Caja de Compensación Familiar del Quindío, Comfenalco Quindío, es la responsable de llevar a cabo el pago del subsidio familiar a los trabajadores afiliados; de brindarles a sus familias espacios para atención en salud, esparcimiento, deporte y recreación así como también ofrecerles a los trabajadores la posibilidad de adquirir vivienda. Las anteriores son tareas que revisten una gran importancia para el desarrollo del departamento del Quindío. Es por ello que la protección de su información y de sus activos informáticos cobran una importancia muy especial por su contenido social y económico.

Mediante el presente proyecto se pretende diseñar un Sistema de Gestión de Seguridad de la Información para Comfenalco, Quindío, que sirva como base para su posterior implementación bajo la orientación y apoyo de la Dirección de la Caja para lo cual se ha tomado como guía orientadora la norma NTC/ISO 27001:2013 para adelantar las fases de diagnóstico de la situación actual de la Caja y el análisis diferencial respecto a los controles y objetivos de control señalados por la

norma; acorde con este objetivo se ha seleccionado la metodología MAGERIT para el de análisis y gestión de riesgos y amenazas.

TERMINOS Y DEFINICIONES

Para los propósitos de este trabajo se utilizan los siguientes términos y definiciones:

ACTIVO INFORMÁTICO: Es todo aquello que pueda generar valor para la empresa u organización y que éstas sientan la necesidad de proteger. Están representados por los objetos físicos (toda clase de hardware), objetos abstractos (software, bases de datos, sistemas operativos, archivos ofimáticos) incluye el personal de trabajo y las oficinas.

AMENAZA: Es la posibilidad de que un intruso o evento explote una vulnerabilidad presente en el sistema generando un resultado no deseado para la organización

ATAQUE: Es el intento no autorizado de acceso, alteración, uso, divulgación, robo o destrucción de un activo.

CONFIDENCIALIDAD: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

IMPACTO: Es el grado de afectación de un incidente o concreción de una amenaza sobre los procesos de la organización.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

POLÍTICAS DE SEGURIDAD DE LA INFORMACION: Es un documento donde se establecen con la mayor claridad posible el compromiso de la dirección con el SGSI y el conjunto de reglas y medidas a seguir por todos los empleados de la empresa para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información.

RIESGO INFORMÁTICO: Es la probabilidad de que se produzca un impacto sobre un activo específico, en un dominio o sobre toda la organización.

RIESGO RESIDUAL: Riesgo que subsiste después de aplicar las medidas adecuadas para mitigar el riesgo inicial.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Es un marco administrativo donde las organizaciones definen y analizan los riesgos y trazan los lineamientos y procedimientos que permitan preservar la seguridad de la información.

VULNERABILIDAD: Indica la potencialidad de que se concrete una amenaza sobre un activo.

2. OBJETIVOS

2.1. General

Realizar el diagnóstico de la seguridad de información en la red de datos, de la empresa Comfenalco Quindío, aplicando metodologías de análisis y gestión de riesgos.

2.2. Específicos

- Realizar un análisis de la situación actual de la seguridad de la información de conformidad con los dominios y objetivos de control de la norma NTC/ISO 27001:2013.

- Identificar los activos y recursos que se deben proteger mediante el análisis basado en metodologías sistémicas de evaluación de riesgos.

- Proponer el diseño de la política de la seguridad de la información de acuerdo con los procesos y lineamientos organizacionales.

3. ALCANCE

Es importante resaltar que el objeto de este proyecto es proporcionar un documento para la Caja de Compensación Familiar Comfenalco Quindío que sirva como base para el diseño del Sistema de Seguridad de la Información sin llegar a la etapa de implementación propiamente dicha.

Debido a la magnitud organizacional de Comfenalco Quindío el proyecto se lleva a cabo sobre el área de la Oficina de Sistemas (TIC/IPS) porque es la responsable del buen funcionamiento de la infraestructura tecnológica de la empresa. El

proyecto no cubre un Plan para Recuperación de Desastres ni tampoco un Plan para Continuidad de Negocio, los cuales quedarán para nuevos proyectos investigativos.

4. DESCRIPCION DE LA ORGANIZACIÓN A TRATAR

Comfenalco Quindío fue fundada el 6 de febrero de 1967 por un grupo de comerciantes quindianos, agremiados de la Federación Nacional de Comerciantes, (Fenalco), cuyo propósito es el de apoyar y beneficiar a los trabajadores y sus familias. Cincuenta y una empresas acompañaron el comienzo, de la Caja, siendo hoy en día una de las empresas más representativas de la región, por su labor social y por ser una de las empresas más grandes del Quindío.

Misión

Contribuir al mejoramiento de la calidad de vida de los trabajadores afiliados, sus familias y la comunidad, a través de la prestación de servicios integrales, con criterios de eficacia y eficiencia bajo un enfoque socialmente responsable.

Visión

Comfenalco Quindío será una organización líder, competitiva, innovadora y autosostenible; generadora de oportunidades y bienestar social para la familia y la comunidad.

Política de Gestión Integral

Prestar servicios competitivos que garanticen la satisfacción de los clientes y el logro de los objetivos de la organización, mediante la mejora continua de los procesos, el cumplimiento de los requisitos, la eficaz administración de los riesgos; el desarrollo integral de los funcionarios, el mantenimiento de ambientes de trabajo saludables y seguros, el uso eficiente de los recursos, la preservación del medio ambiente y la responsabilidad social empresarial.

Valores Corporativos

La Integridad

La integridad se manifiesta en la rectitud al obrar y en la honradez en todos los ámbitos. Para Comfenalco este valor es fundamental, tanto en su dimensión de

práctica personal, como en la filosofía y cultura corporativa, pues nuestra conducta y comportamiento ético en el manejo de los recursos y en la prestación de los servicios, debe asegurar la confianza de nuestros clientes y partes interesadas.

La Solidaridad

Entendida como una actitud generosa, participativa y cooperadora, la solidaridad constituye una unión de esfuerzos que hace posible el bienestar, la compensación y la ayuda mutua.

El Respeto

Su ejercicio, base fundamental de una convivencia sana y pacífica, inspira nuestra diaria labor y nos estimula a responder con eficiencia, oportunidad y comprensión a los compromisos adquiridos con los clientes, a respetar sus derechos y a cumplir la normatividad vigente.

La Responsabilidad Social

En el marco de nuestros valores corporativos, nos esforzamos por apoyar el desarrollo local, a través de acciones sociales, comunitarias y ambientales que generen una cultura de transformación y contribuyan a mejorar los contextos en los que vivimos.

La Vocación de Servicio

Promovemos una cultura de servicio, calidad e innovación, a través de una atención integral y diferenciada y la gestión de procesos eficaces, dirigidos a la satisfacción de los clientes y al cumplimiento de la misión, la visión y las metas de la organización, para avanzar por el camino del mejoramiento continuo.

Cumplimiento

En la actualidad, Comfenalco Quindío cuenta con un Sistema de Gestión Integral certificado bajo la Norma Técnica Colombiana ISO 9001:2008 gracias al cual se asegura el cumplimiento de los requisitos legales, del cliente y la organización y aporta de manera positiva al control, a la adecuada gestión de los procesos y al cumplimiento de las metas y objetivos corporativos.

5. PLANTEAMIENTO DEL PROBLEMA

5.1. Definición del problema

Las redes informáticas como soporte fundamental a las operaciones de procesamiento de datos, deben ser protegidas no sólo de forma lógica sino también física; implementar las técnicas necesarias enfocadas a la salvaguarda de la red, resulta ser un objetivo primordial frente a la seguridad informática de las organizaciones, el cual lamentablemente es relegado en muchas de ellas[1].

La Caja de Compensación Familiar Comfenalco Quindío, contrató recientemente con una empresa externa una consultoría para determinar el grado de madurez del área de Tecnologías de la Información. El Informe final de Resultados de la consultoría, en su sección de Planes de Mejora, recomienda el inicio de proyectos a mediano plazo tendientes a crear una arquitectura para la seguridad de la información dado que el análisis realizado encontró un 0% de madurez en dicha área.

Al no tener diseñado ni implementado un Sistema de Gestión de la Seguridad, Comfenalco Quindío enfrenta una situación de riesgo permanente de sufrir pérdidas, modificaciones, violaciones de la confidencialidad en su información. En este contexto en el presente documento se expone una propuesta solamente para el diseño de un SGSI para Comfenalco Quindío que brinde a la alta dirección de la Caja una oportunidad real de cumplir con lo recomendado por la empresa consultora al llevarlo a la fase de implementación.

A pesar de no tener definida una política de Gestión de la Seguridad de la Información la Caja de Compensación Familiar Comfenalco Quindío cuenta con unas directrices y controles para la seguridad de su red informática que a la luz del Informe de Resultados obtenido por la Auditoría Informática a la que fue sometida resultan ser insuficientes para garantizar dicha seguridad.

Dados los anteriores antecedentes y con los conocimientos adquiridos durante el desarrollo de la Especialización en Seguridad Informática, se cuentan con los elementos necesarios para desarrollar una propuesta enfocada a la Seguridad de la Red Informática de Comfenalco Quindío.

5.2. Justificación

Los servicios de recreación, educación, deportes y el pago del subsidio familiar

[1] Herath, Tejaswini. Essays on information security practices in organizations. State University of New York at Buffalo: ProQuest Dissertations Publishing. p.14.

revisten una importancia trascendental para cientos de familias cobijadas por los planes y beneficios de Comfenalco Quindío de tal manera que el cumplimiento de estos invaluables servicios se ubican en el centro mismo de la Misión la Caja.

Es por esta razón que este proyecto busca proporcionar las herramientas técnicas y metodológicas suficientes para que la organización objeto de estudio, pueda llevar a la fase de implementación las acciones pertinentes para la seguridad de su red informática, según lo sugerido por la Auditoría externa dado que ésta se constituye como el medio principal para el procesamiento de casi toda la información de la empresa, acciones enfocadas a contrarrestar cualquier ataque interno o externo, además de minimizar al máximo el impacto ante la materialización de cualquier amenaza, capaz de interrumpir los servicios de Comfenalco Quindío.

Por lo anterior, y ante la evolución que con las herramientas de protección tienen las amenazas, se hace necesario generar un modelo de seguridad informática para la red de Comfenalco Quindío, con el fin de garantizar la confidencialidad, seguridad y protección de la información que maneja y que produce dicha entidad de tal manera que pueda garantizar sus valiosos servicios a todos los beneficiarios de la Caja.

5.3. Marco teórico

El reconocimiento amplio y generalizado de la información como un activo estratégico importante para las organizaciones sirve de sustento a la necesidad de mantenerla protegida contra los eventos adversos originados en la intervención humana, en los fallos tecnológicos o en desastres naturales que amenacen su integridad, disponibilidad y confidencialidad.

En la consecución de este objetivo se han creado una serie de métodos, metodologías, herramientas y normas por parte de distintas instituciones y entidades que actualmente gozan del aval y la aceptación internacional entre las cuales mencionamos: **International Organization for Standardization (ISO)** a quien debemos el conjunto de las normas ISO; **Computer Emergency Response Team (CERT)** creadores de la metodología conocida como OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation); El **Consejo Superior de Administración Electrónica** de España desarrolladores de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones).

NTC/ISO 27001

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Originada en la BS 7799-2:2002 es la norma base aplicada para las certificaciones de los SGSI implementados en las organizaciones por parte de auditores externos. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. En la norma se considera como no obligatoria la implementación de la totalidad de los controles enumerados en el anexo pero recomienda que la organización deberá sustentar la no aplicabilidad de los controles no implementados.

Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-NTC/ISO 27001:2014. En 2015, se publicó un documento adicional de modificaciones (UNE-NTC/ISO 27001:2014/Cor 1:2015). En Colombia ha sido: publicada como NTC-ISO-IEC 27001, En Chile se denomina NCh-ISO27001) y en Uruguay UNIT-NTC/ISO 27001.

Para las empresas que desean obtener una certificación en la norma ISO 27701 los auditores solicitan un conjunto de documentos y registros de carácter obligatorio que son los siguientes:

- ✓ Alcance del SGSI (punto 4.3).
- ✓ Objetivos y política de seguridad de la información (puntos 5.2 y 6.2).
- ✓ Metodología de evaluación y tratamiento de riesgos (punto 6.1.2).
- ✓ Declaración de aplicabilidad (punto 6.1.3).
- ✓ Plan de tratamiento de riesgos (puntos 6.1.3 y 6.2).
- ✓ Informe de evaluación de riesgos (punto 8.2).
- ✓ Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4).
- ✓ Inventario de activos (punto A.8.1.1).
- ✓ Uso aceptable de los activos (punto A.8.1.3).
- ✓ Política de control de acceso (punto A.9.1.1).
- ✓ Procedimientos operativos para gestión de TI (punto A.12.1.1).
- ✓ Principios de ingeniería para sistema seguro (punto A.14.2.5).
- ✓ Política de seguridad para proveedores (punto A.15.1.1).
- ✓ Procedimiento para gestión de incidentes (punto A.16.1.5).
- ✓ Procedimientos para continuidad del negocio (punto A.17.1.2).
- ✓ Requisitos legales, normativos y contractuales (punto A.18.1.1)[2].

[2] KOSUTIC, D. Lista de documentos obligatorios exigidos por la Norma ISO 27001(Revisión 2013). En Línea. 2 de Abril de 2017. Disponible en ISO 27001 & ISO 22301. Base de Conocimientos. https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/) /

OCTAVE. Operationally Critical Threat, Asset, and Vulnerability Evaluation, Evaluación Crítica Operacional de Amenazas, Activos y Vulnerabilidades. Contiene un conjunto de herramientas, métodos y técnicas para la valoración de riesgos de la seguridad informática. Fue desarrollada por la Carnegie Mellon University y cuenta en la actualidad con tres versiones, incluída una para PYMES llamada Octave – S. La versión Octave-Allegro es la más reciente y trae una serie de formatos y hojas de cálculo para facilitar la evaluación del riesgo en las organizaciones. Una característica de Octave es que asume que las personas que realizan la evaluación de riesgos conocen los riesgos a los que están expuestos los activos de información y por lo tanto no hace falta entrevistas ni herramientas para identificar las amenazas.

NIST SP800-30: Risk Management Guide for Information Technology Systems, Fué creada por el NIST (National Institute for Standards and Technology, Instituto Nacional para los Estándares y Tecnología). Se caracteriza por su flexibilidad y su facilidad de usos e implementación en organizaciones de cualquier tamaño. Divide la gestión de riesgos en 9 aspectos: Determinación del Sistema, Determinación de Amenazas, Identificación de vulnerabilidades, Análisis de Control, Cálculo de Probabilidades, Análisis de Impacto, Determinación del riesgo, Recomendaciones de controles, Documentación de los resultados[3].

EBIOS. (Expression des Besoins et Identification des Objectifs de Sécurité, Expresión de Necesidades e Identificación de los Objetivos de Seguridad). Es un método creado por la francesa Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI) que adopta un enfoque basado en los elementos constitutivos de los riesgos para orientar la evaluación y tratamiento. EBIOS propone cubrir el análisis de riesgos en cinco fases: establecimiento del contexto, análisis de eventos de seguridad, análisis de escenarios de amenazas, análisis de riesgos y determinación de controles de seguridad. Para el desarrollo de las fases, además de un conjunto de guías, la ANSSI pone a disposición de los gestores de seguridad una herramienta software gratuita.[4]

MAGERIT. Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica. La razón de ser de MAGERIT está fundamentada en la generalización del uso de las tecnologías de la

---

[3] NIST SP800-35. Guide to Information Technology Security Services, Special Publication 800-35 .National Institute of Standards and Technology,p.6.

[4] Republique Francaise, Premier Ministre, Secrétariat général de la défense nationale, El método EBIOS, En línea. Septiembe 2013 Disponible en:https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

información lo cual supone unos beneficios evidentes para los ciudadanos pero que también implica ciertos riesgos que deben minimizarse con la aplicación medidas de seguridad que generen confianza.

El público al que está dirigido MAGERIT está formado por todos aquellos que trabajan con sistemas informáticos para el procesamiento de información digital. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.[5]

En este trabajo utilizaremos MAGERIT, porque además de su amplía acogida en el mundo hispanohablante y ser un producto libre y gratuito, es totalmente coherente con lo propuesto por la Organización Internacional de Estándares (International Organization for Standardization, ISO) de tal manera que se convierte en una buena elección para empresas que a futuro piensan en obtener una certificación. Por otro lado, para la gestión de riesgos, las guías de MAGERIT para el análisis de riesgos son muy completas y sistemáticas. Por esta razón, profundizaremos un poco en su contenido y estructura.

MAGERIT versión 3 se ha estructurado en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas".

Método

- Se estructura de la siguiente forma:
- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un

[5] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.p. 12.

sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Los apéndices recogen material de consulta:

1. Un glosario,
2. Referencias bibliográficas consideradas para el desarrollo de esta metodología,
3. Referencias al marco legal que encuadra las tareas de análisis y gestión en la Administración Pública Española,
4. El marco normativo de evaluación y certificación
5. Las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos,
6. Una guía comparativa de cómo Magerit versión 1 ha evolucionado a la versión 2 y a esta versión 3

Catálogo de Elementos

Marca unas pautas en cuanto a:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información

Se persiguen los siguientes objetivos:

Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.[6]

[6] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.6.

Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Cada sección incluye una notación XML que se empleará para publicar regularmente los elementos en un formato estándar capaz de ser procesado automáticamente por herramientas de análisis y gestión.
Si el lector usa una herramienta de análisis y gestión de riesgos, este catálogo será parte de la misma; si el análisis se realiza manualmente, este catálogo proporciona una amplia base de partida para avanzar rápidamente sin distracciones ni olvidos.

Guía de Técnicas

Aporta adicional orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

Valoración Delphi: Se trata de una guía de consulta con recomendaciones sobre el uso de ciertas técnicas específicas de las que esta guía busca ser una introducción. También proporciona referencias para que el lector profundice en las técnicas presentadas.[7]

5.4. Materiales y métodos

Para la realización del proyecto se hizo necesaria la recolección y acceso a los siguientes materiales:

- **ISO / IEC 27000:2013** (Tecnología de la Información – Técnicas de

[7] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.14.

Seguridad – Sistemas de Gestión de la Seguridad de la Información – **Generalidades y Vocabulario**)

- **ISO / IEC 27001:2013** (Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – **Requerimientos**)

- **ISO / IEC 27002:2013** (Tecnología de la Información – **Código de Prácticas para los Controles de la Seguridad de la Información**)

- **NTC – ISO / IEC 27001:2013** (**Norma Técnica Colombiana -Icontec -** Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – **Requerimientos**)

- **MAGERIT** – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – **Método.**

- **MAGERIT** – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – **Catálogo de elementos.**

- **MAGERIT** – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – **Guía de Técnicas.**

6. DESARROLLO DEL PROYECTO

Teniendo como referencia la NTC/ISO 27001:2013, la metodología para Análisis y Gestión de Riesgos Magerit y los objetivos planteados para el desarrollo del presente proyecto, a continuación se documentará la construcción del mismo.

6.1 Situación actual de la organización a nivel de seguridad de la red informática.

Comfenalco Quindío, pese a que es una organización debidamente organizada según los lineamientos de las leyes que la regulan, tales como las emanadas de la Superintendencia del Subsidio Familiar, Supersalud, Ministerio de Salud y del Gobierno Nacional en general, cuenta con unas políticas de seguridad informática insuficientes frente al volumen de activos que la misma posee y frente al grado de importancia de los procesos que en su interior se desarrollan. Se puede decir que actualmente la organización se encuentra en un nivel de seguridad medio-bajo. Lo

anterior se puede evidenciar en la evaluación realizada inicialmente a la organización.

6.2 Análisis Diferencial

El Análisis diferencial es una matriz que sirve para comparar y establecer el grado de cumplimiento existente en la organización respecto al conjunto de dominios, objetivos de control y controles presentes en el Anexo A de la norma ISO 27001:2013. De esta manera permite conocer el estado actual en cuanto a seguridad de la información y tener una visión muy clara acerca de las áreas relativamente desprotegidas y los controles que deben implementarse para protegerlas.

En el contexto organizacional, la Norma NTC/ISO 27001:2013 presenta un conjunto de requisitos indispensables para establecer, implementar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

Desde esta perspectiva, y tal como se detalla en el Anexo A, se realiza un análisis diferencial que permita conocer el grado de cumplimiento actual que presenta Comfenalco Quindío respecto a los Dominios, Objetivos de Control y Controles establecidos en los numerales 1 al 15 de la norma que permita identificar las falencias o debilidades actuales en el área de seguridad de la información para diseñar un plan de mejoramiento acorde con los objetivos que a este nivel se desean para la empresa.

Un resumen acerca del nivel de cumplimiento frente a cada dominio y sus controles puede apreciarse en la Tabla 1 y de modo gráfico en la Gráfica 1.

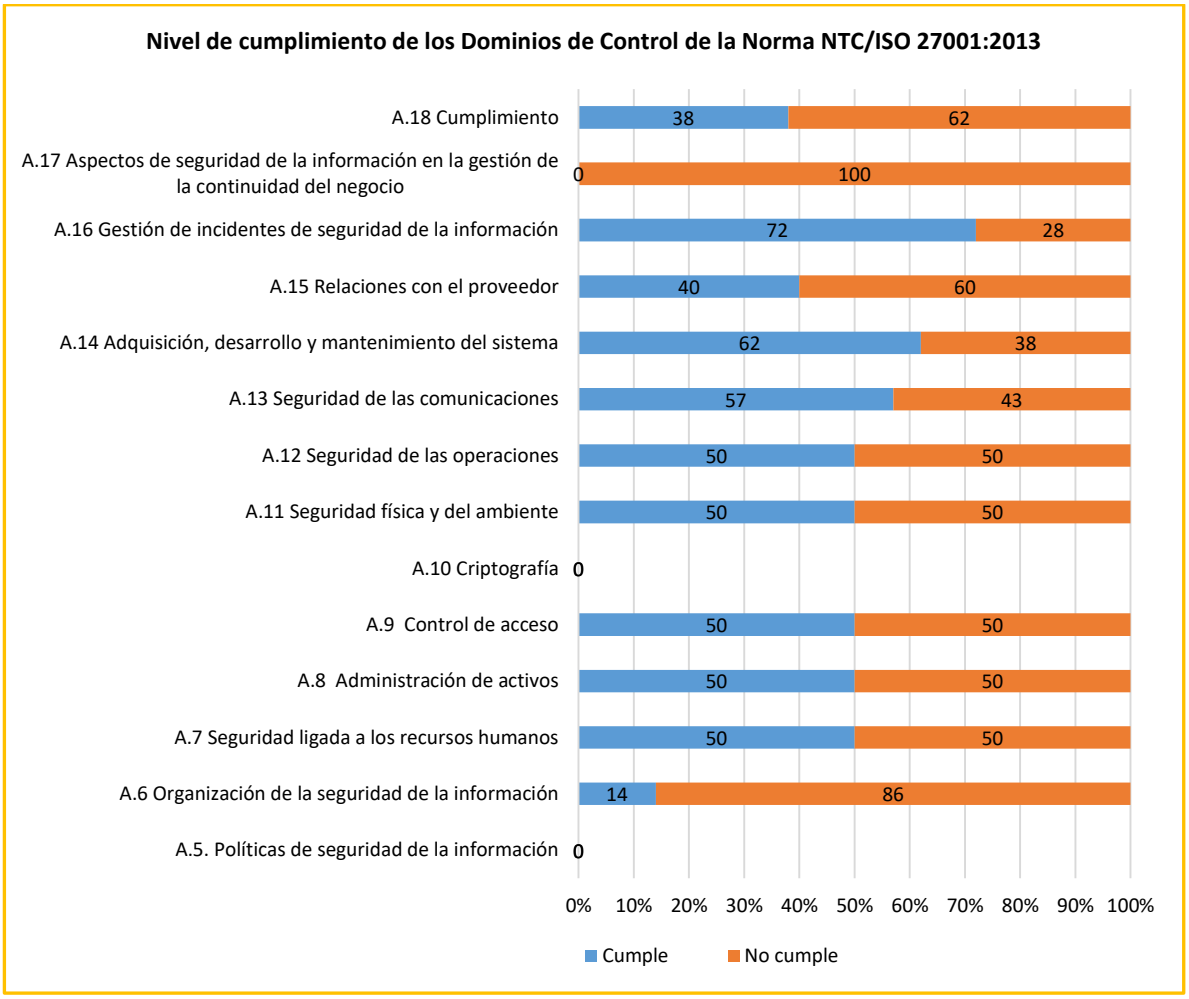
Tabla 1. Nivel de Cumplimiento de los Dominios según la Norma NTC/ISO 27001:2013

DOMINIOS	CUMPLE (%)	NO CUMPLE (%)
A.5. Políticas de seguridad de la información	**0**	**100**
A.6 Organización de la seguridad de la información	**14**	**86**
A.7 Seguridad ligada a los recursos humanos	**50**	**50**
A.8 Administración de activos	**50**	**50**
A.9 Control de acceso	**50**	**50**
A.10 Criptografía	**0**	**100**
A.11 Seguridad física y del ambiente	**50**	**50**
A.12 Seguridad de las operaciones	**50**	**50**
A.13 Seguridad de las comunicaciones	**57**	**43**
A.14 Adquisición, desarrollo y mantenimiento del sistema	**62**	**38**
A.15 Relaciones con el proveedor	**40**	**60**

A.16 Gestión de incidentes de seguridad de la información	**72**	**28**
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**0**	**100**
A.18 Cumplimiento	**38**	**62**

Fuente: La Autora

Figura 1. Nivel de Cumplimiento de los Dominios según la Norma NTC/ISO 27001:2013



Fuente: La Autora

El resultado del análisis diferencial muestra claramente que Comfenalco Quindío no cumple con la mayor parte de los Dominios y de los Objetivos de Control y Controles expuestos en la Norma.

Adicionalmente, el análisis diferencial revela que si bien existen controles aplicables e implementados en A.14. Adquisición, desarrollo y mantenimiento del sistema y en A.16. Gestión de incidentes de seguridad, que superan el 60% de cumplimiento, la carencia de una Política de seguridad de la información, evidenciada en A.5, indica que todos los controles carecen actualmente de un elemento unificador y señalan la urgente necesidad de diseñar e implementar dicha política que se constituya en la columna vertebral del Sistema de Gestión de Seguridad de la Información de Comfenalco Quindío.

El resultado global en cuanto al cumplimiento de la norma puede apreciarse en la Gráfica No.2.

Figura 2. Porcentaje de Cumplimiento de los Dominios según la Norma NTC/ISO 27001:2013

Fuente: La Autora

6.3 Análisis de Riesgos

Tabla 2. Análisis de Riesgos

OBJETIVO	Realizar la identificación, análisis y evaluación de activos y riesgos de la seguridad de la información
ALCANCE	Aplica para los activos de la empresa
EMPRESA	Caja de Compensación Comfenalco Quindío
SITIO WEB	www.comfenalcoquindio.com
CONTEXTO LEGAL	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la Metodología MAGERIT
TRATAMIENTO	Se tratarán los riesgos cuyo resultado después de la valoración de riesgos sean:
	• **Inaceptable** • **Inadmisible**
	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a15 moderado (M), 16 a 26 inaceptable (I)
	Una vez aplicados los controles, se acepta un riesgo residual en niveles APRECIABLE e IMPORTANTE
	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico (C)

Fuente: La Autora

Antes de proceder con la identificación de los riesgos que a nivel de seguridad se encuentra expuesta la organización, se procede en primer término a identificar los activos de la misma, tal y como se muestra en la Tabla 3:

Tabla 3. Lista de Activos Identificados

CÓDIGO	ACTIVO	CLASE DE ACTIVO	RESPONSABLE
1	Base de datos Subsidio Familiar	D	Gestión TIC
2	Programa subsidio familiar	SW	Gestión TIC
3	Windows 7	SW	Gestión TIC
4	McAfee VirusScan	SW	Gestión TIC
5	Ultra VNC (Escritorio Remoto)	SW	Gestión TIC
7	Term Vision (emulador windows y un servidor unix) aplicativo subsidio cobol	SW	Gestión TIC
8	Net Term (emulador windows y un servidor unix) aplicativo subsidio cobol	SW	Gestión TIC

9	Mandrake 7.2	SW	Gestión TIC
10	Windows Server 2008 standard Service pack 2	SW	Gestión TIC
11	SQL Server 2008 Management Studio	SW	Gestión TIC
13	Open server 6.0	SW	Gestión TIC
14	RM COBOL 12	SW	Gestión TIC
15	Windows server 2000 Service pack 4.	SW	Gestión TIC
16	Servidor Web: Apache 2,0, PHP 4.4.0	SW	Gestión TIC
17	Windows XP Professional Service pack 3	SW	Gestión TIC
18	Open Office	SW	Subsidio Familiar
19	Zip Genius	SW	Subsidio Familiar
20	Nero	SW	Subsidio Familiar
21	Roxio	SW	Subsidio Familiar
22	Sevenet 1.0	SW	Gestión Documental
23	Proxy plus	SW	Gestión TIC
24	Equipos de computo	HW	Subsidio Familiar – Gestión TIC
25	Impresora	HW	Subsidio Familiar
26	Teléfono conmutador	HW	Subsidio Familiar
27	Servidor correo electrónico	HW	Gestión TIC
28	Servidor vivienda	HW	Gestión TIC
29	Servidor subsidio	HW	Gestión TIC
30	Servidor intranet	HW	Gestión TIC
31	Servidor internet	HW	Gestión TIC
32	Switch	HW	Gestión TIC
33	Red Telefónica	COM	Mantenimiento y Servicios Generales
34	Red de Datos	COM	Gestión TIC
35	Red Local	COM	Gestión TIC
36	Internet	COM	Gestión TIC
37	Funcionarios	P	Gestión Humana
54	Correo electrónico interno	S	Gestión TIC
55	Correo electrónico vía web	S	Gestión TIC
57	Fuentes de Alimentación	AUX	Mantenimiento y Servicios Generales
58	Cableado	AUX	Gestión TIC
59	Sistemas de alimentación ininterrumpida	AUX	Mantenimiento y Servicios Generales
60	Muebles de oficina	AUX	Subsidio Familiar
61	Edificio Sede	L	Dirección Administrativa

62	Documentación de los procesos, procedimientos, políticas, instructivos, manuales, formularios, actas, contratos, inventarios, documentos contables, registros y comunicaciones con empresas y trabajadores afiliados.	SI	Subsidio Familiar – Gestión TIC - Calidad

Fuente: La Autora

Dichos activos fueron agrupados de acuerdo a su naturaleza, obteniendo los siguientes grupos de activos:

- D: Datos/Información.
- SW: Software (aplicaciones).
- HW: Hardware.
- COM: Redes de Comunicaciones.
- P: Personal.
- S: Servicios.
- AUX: Equipamiento auxiliar.
- L: Instalaciones físicas.
- SI: Soportes de Información (en papel, medio magnético, etc.).

Lo anterior, se hizo tomando como referencia el Catálogo de Elementos de MAGERIT.

Relación de dimensiones de seguridad

Teniendo en cuenta las dimensiones de seguridad proporcionadas por la metodología para análisis y gestión de riesgos MAGERIT, éstas serán las que se evalúen durante el análisis de riesgos:

Tabla 4. Relación de Dimensiones de Seguridad

DIMENSIONES	
D	Disponibilidad
I	Integridad
C	Confidencialidad
A_S	Autenticidad del servicio
A_D	Autenticidad de los datos
T_S	Trazabilidad de los servicios
T_D	Trazabilidad de los datos

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.15.

Criterios de valoración

Como primera medida se identificaron los tipos de elementos a valorar en la etapa de valoración de los activos, resultando los siguientes:

1. Valoración de activos: donde se le da un valor al activo, de acuerdo a la importancia que éste tenga para la organización.
2. Valoración de Amenazas: donde se da un valor a la amenaza, de acuerdo a su tipo, al impacto que tendría sobre determinado activo (si llegase a materializarse), a las condiciones del medio (sociales, económicas, climáticas, ambientales), a la ocurrencia de incidentes relacionados con la amenaza (sociales, económicas, climáticas, ambientales), a los controles ya implementados dentro de la organización para mitigar el impacto de ciertas amenazas, entre otros.
3. Valoración de las siete dimensiones, según MAGERIT:
    a. Disponibilidad.
    b. Integridad.
    c. Confidencialidad.
    d. Autenticidad del Servicio.
    e. Autenticidad de los Datos.
    f. Trazabilidad del Servicio.
    g. Trazabilidad de los Datos.

Posterior a la identificación de los elementos a valorar, se dio paso a la definición de los criterios de valoración de cada uno de esos elementos:

1. Valoración de activos: teniendo en cuenta el criterio que se utiliza para valorar los procesos dentro del Sistema de Administración del Riesgo – SAR, implementado por Comfenalco Quindío, se decidió que para valorar los activos se utilizaría una escala de importancia del 1 al 5, donde 1 es Muy Bajo y 5 es Muy Alto, así:

Tabla 5. Escala de Valoración

5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo

Fuente: Comfenalco Quindío.

2. Valoración de amenazas: teniendo en cuenta los factores anteriormente relacionados, se decidió manejar una escala de 1 al 10, de acuerdo al impacto de la amenaza sobre el activo.

3. Valoración de las siete dimensiones, según MAGERIT: teniendo en cuenta que cada dimensión representa igual importancia para cada activo, se decidió dar un valor de 10 a cada una, de modo que si un activo tiene relacionadas 5 dimensiones, su valor sería de 50 (10 por cada dimensión que se relacione con el activo a evaluar) y así sucesivamente.

Definido lo anterior, se obtuvo un esquema de evaluación con la siguiente estructura:

Tabla 6. Esquema de Evaluación

<table>
<tr><td rowspan="2">Valor del activo para la organización (VAO)</td><td>Valor Amenaza(VA)</td><td>Valor Dimensiones(VD)</td></tr>
<tr><td colspan="2">Total (VAO*VA*VD)</td></tr>
</table>

Fuente: La Autora.

De igual manera se aplicó un criterio de evaluación a la operación antes descrita (VAO*VA*VD), de la siguiente manera:

Tabla 7. Criterio de Evaluación

Muy Alto	Entre 1681 y 3500	
Alto	Entre 601 y 1680	
Medio	Entre 121 y 600	
Bajo	Entre 11 y 120	
Muy Bajo	Entre 1 y 10	

Fuente: La Autora.

Una vez definidos los tipos de elementos a evaluar y los criterios de evaluación, se dio paso a la fase de valoración de activos, donde se obtuvo una matriz, la cual contiene cada uno de los activos identificados, su valor para la organización, el valor de la amenaza, el valor de la dimensión que le corresponden de acuerdo al tipo de amenaza y el resultado final de la multiplicación entre cada una de las valoraciones hechas. Dicha matriz, cuya descripción se hace en el Anexo E, hace parte integral del cuerpo del proyecto de Análisis y Gestión de Riesgos,

desarrollado en marco a las actividades propias del proyecto “DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMFENALCO QUINDÍO”.

Posterior a la valoración de activos de dio paso a la definición de cómo se evaluaría la frecuencia de ocurrencia de la amenaza frente al activo, determinando una escala de valor, así:

MF: muy frecuente (a diario)	100
F: frecuente (mensual)	75
FN: frecuencia normal (anual)	50
PF: poco frecuente (cada varios años)	25

Para esta valoración se tuvieron en cuenta aspectos como el historial de la organización frente a la materialización de cada amenaza, el entorno social, ambiental, económico, político, entre otros, los cuales proporcionaron el criterio para determinar el porcentaje de frecuencia de ocurrencia de cada amenaza frente a cada activo, determinando entonces, más que la frecuencia, la probabilidad de ocurrencia o de materialización de las amenazas. Ver Anexo F.

Realizada la valoración amenaza vs. frecuencia de ocurrencia, se procedió a ubicar cada activo en la respectiva matriz de riesgo, teniendo como referencia el siguiente esquema, proporcionado por MAGERIT[8]:

Tabla 8. Esquema Matriz de Riesgo

	FRECUENCIA			
IMPACTO	PF	FN	F	MF
MA	A	MA	MA	MA
A	M	A	MA	MA
M	B	M	A	MA
B	MB	B	M	A
MB	MB	MB	B	M

Fuente: La Autora

Finalmente, el Criterio de Aceptabilidad del Riesgo se definió tomando como referencia el que la Caja de Compensación Familiar maneja dentro de su Sistema de Administración del Riesgo – SAR, quedando el siguiente criterio:

[8] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.p. 28.

Tabla 9. Criterio de Aceptabilidad del Riesgo

Criterio de Aceptabilidad	Nivel de Riesgo con Control	Descripción
Admisible	• Impacto entre 1 y 12. Frecuencia entre 25 y 50. • Impacto entre 13 y 120. Frecuencia de 25.	No requiere tratamiento de riesgos, los controles existentes son suficientes para asumir el riesgo.
Aceptable	• Impacto entre 1 y 12. Frecuencia de 75. • Impacto entre 13 y 120. Frecuencia de 50. • Impacto entre 121 y 600. Frecuencia de 25.	El riesgo se encuentra en un nivel que puede asumirse sin necesidad de tomar otras medidas de control diferentes a las que se poseen.
Tolerable	• Impacto entre 1 y 12. Frecuencia de 100. • Impacto entre 13 y 120. Frecuencia de 75. • Impacto entre 121 y 600. Frecuencia de 50. • Impacto entre 601 y 1680. Frecuencia de 25.	Se deben tomar acciones para mejorar o rediseñar los controles existentes o diseñar nuevos controles, sin embargo, tienen una prioridad de segundo nivel, por lo tanto las acciones pueden ser tomadas a mediano plazo y realizarse con los recursos ordinarios del proceso.
Inaceptable	• Impacto entre 13 y 120. Frecuencia de 100. • Impacto entre 121 y 600. Frecuencia de 75. • Impacto entre 601 y 1680. Frecuencia de 50. • Impacto entre 1681 y 3500. Frecuencia de 25.	Debido al alto impacto que tendrían en el proceso, se deben tomar acciones para mejorar o rediseñar los controles existentes o diseñar nuevos controles. Estas acciones se deben tomar en el corto plazo y pueden implicar recursos extraordinarios del proceso.
Inadmisible	• Impacto entre 121 y 600. Frecuencia de 100. • Impacto entre 601 y 1680. Frecuencia entre 75 y 100. • Impacto entre 1681 y 3500. Frecuencia entre 50 y 100.	Dado su impacto en el logro de los objetivos deben ser intervenidos en forma inmediata y por lo tanto se deben tomar acciones para mejorar o rediseñar los controles existentes o diseñar nuevos controles. La intervención de este nivel de riesgo es de alta prioridad.

Fuente: La Autora

Dependencia de activos

En razón al volumen de activos identificados, a continuación se mostrará la dependencia de activos, agrupándolos por tipo de activo sin especificar cada uno.

Tabla 10. Dependencia de Activos

Activo	Datos/ Información	Personas	Hardware	Software	Soportes de Información	Equipamiento Auxiliar	Servicios	Instalaciones	Redes de Comunicación
Datos/ Información									
Personas									
Hardware									
Software									
Soportes de Información									
Equipamiento Auxiliar									
Servicios									
Instalaciones									
Redes de Comunicación									

Fuente: La Autora

Identificación de las amenazas

Para la identificación de las amenazas, se tomó como referencia el listado de amenazas[9] que MAGERIT presenta, el cual se describe a continuación:

Tabla 11. Listado de amenazas

CODIGO	AMENAZA
N.1	Fuego
N.2	Daños por agua
N.*	Desastres naturales
I.1	Fuego
I.2	Daños por agua
I.*	Desastres industriales

[9] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.25.

I.3	Contaminación mecánica
I.4	Contaminación electromagnética
I.5	Avería de origen físico o lógico
I.6	Corte del suministro eléctrico
I.7	Condiciones inadecuadas de temperatura y/o humedad
I.8	Fallo de servicios de comunicaciones
I.9	Interrupción de otros servicios y suministros esenciales
I.10	Degradación de los soportes de almacenamiento de la información
I.11	Emanaciones electromagnéticas
E.1	Errores de los usuarios
E.2	Errores del administrador
E.3	Errores de monitorización (log)
E.4	Errores de configuración
E.7	Deficiencias en la organización
E.8	Difusión de software dañino
E.9	Errores de [re-]encaminamiento
E.10	Errores de secuencia
E.14	Escapes de información
E.15	Alteración de la información
E.16	Introducción de información incorrecta
E.17	Degradación de la información
E.18	Destrucción de información
E.19	Divulgación de información
E.20	Vulnerabilidades de los programas (software)
E.21	Errores de mantenimiento / actualización de programas (software)
E.23	Errores de mantenimiento / actualización de programas (hardware)
E.24	Caída del sistema por agotamiento de recursos
E.28	indisponibilidad de personal
A.4	Manipulación de la configuración
A.5	Suplantación de la identidad del usuario
A.6	Abuso de privilegios de acceso
A.7	Uso no previsto
A.8	Difusión de software dañino
A.9	[Re-]encaminamiento de mensajes
A.10	Alteración de secuencia
A.11	Acceso no autorizado
A.12	Análisis de tráfico
A.13	Repudio
A.14	Interceptación de información (escucha)
A.15	Modificación de la información

A.16	Introducción de falsa información
A.17	Corrupción de la información
A.18	Destrucción la información
A.19	Divulgación de información
A.22	Manipulación de programas
A.24	Denegación de servicio
A.25	Robo
A.26	Ataque destructivo
A.27	ocupación enemiga
A.28	indisponibilidad de personal
A.29	Extorsión
A.30	Ingeniería social

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.6.

[N] Desastres naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataques intencionados

En el Anexo E, se presenta la matriz Activos vs. Amenazas, donde se hace la respectiva valoración de los activos y de las amenazas, aplicando allí el esquema de evaluación que se detalla a continuación. Los resultados de la evaluación nos dan como resultado el impacto de la amenaza sobre el activo, lo que se traduce como Estimación del impacto, el cual hace parte de las tareas propuestas por MAGERIT.[10]

Tabla 12. Esquema de Evaluación

<table>
<tr><td rowspan="2">Valor del activo para la organización (VAO)</td><td>Valor Amenaza(VA)</td><td>Valor Dimensiones(VD)</td></tr>
<tr><td colspan="2">Total (VAO*VA*VD)</td></tr>
</table>

Fuente: La Autora.

[10] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.6.

Dados los activos identificados y las amenazas asociadas a estos activos, dichas políticas son insuficientes para mitigar el impacto frente a una posible materialización de esas amenazas, razón por la cual se desarrollará el Anexo A de la NTC/ISO27001:2013, donde se generarán las políticas necesarias para blindar a la organización frente a las amenazas.

Estimación del riesgo

En el Anexo F, se presenta la matriz Impacto vs. Frecuencia, con el fin de hacer la estimación del riesgo. Para dicha estimación se tuvo en cuenta la siguiente escala de valor, la cual fue previamente explicada en la Fase de Planificación:

MF: muy frecuente (a diario) *100*
F: frecuente (mensual) *75*
FN: frecuencia normal (anual) *50*
PF: poco frecuente (cada varios años) *25*

Calificación de los riesgos

Una vez realizada la Estimación del riesgo, se obtuvo la siguiente matriz de riesgos, donde vemos claramente que todos los activos se encuentran en riesgo, para el caso específico se trabajará sólo con aquellos activos que se encuentren en rojo y en naranja. Para dichos activos aplicarán las políticas propuestas en el siguiente numeral, teniendo como referencia el Anexo A de la NTC/ISO 27001:2013.

Tabla 13. Matriz de Riesgos

RIESGO		FRECUENCIA			
		PF	FN	F	MF
IMPACTO	MA				
	A		24-27-28-29-30-31	1-2-3-7-8-9-10-11-13-14-15-16-17-22-23	
	M		4-18-19-20-21-25-26-32-33-57-58-59-60-62	5-34-35-36-37-54-55-61	
	B				
	MB				

Fuente: La Autora.

6.4 Alcance del Sistema de Gestión de Seguridad de la Información

CAJA DE COMPENSACION FAMILIAR COMFENALCO QUINDIO
ALCANCE DEL SGSI

1. PROPÓSITO, ALCANCE Y USUARIOS

El objetivo de este documento consiste en delimitar claramente el alcance y límite de la planeación del Sistema de Gestión de la Seguridad de la Información en las áreas señaladas por el Comité de Seguridad de la Información de la Caja de Compensación Familiar, Comfenalco Quindío.

El documento es aplicable al personal que labora en la Comfenalco Quindío ya sea en calidad de empleados de planta o como contratistas; a la documentación y al conjunto de actividades propias del proceso de planeación del SGSI para Comfenalco Quindío.

2. DEFINICIÓN DEL ALCANCE DEL SGSI

La Caja de Compensación Familiar, Comfenalco Quindío necesita delimitar el alcance de la planeación del SGSI para brindar protección a los activos informáticos que prestan el servicio a la institución. En la consecución de este objetivo, se ha propuesto el desarrollo de la fase de planeación de un SGSI guiado por el estándar ISO/IEC 27001:2013 teniendo en cuenta las regulaciones que cobijan a la Caja de Compensación Familiar, Comfenalco Quindío.

La fase de planeación del SGSI abarcará las siguientes áreas:

- Dirección Administrativa
- División Administrativa
- Talento Humano
- Oficina de Tecnologías de la Información y Telecomunicaciones.

6.5 Declaración de Aplicabilidad

La Declaración de Aplicabilidad tiene como fundamento principal el análisis de riesgos y el tratamiento que se dará a los mismos. Es un documento donde se registran los controles del Anexo A de la norma ISO 27001:2013 que se consideran apropiados para satisfacer las necesidades organizacionales en cuanto a seguridad de la información y se eligen para su implementación, por tal razón la declaración requiere tener conocimiento del estado actual de dichos controles en caso de estar ya operativos bien sea parcial o totalmente.

En el Anexo 3 se detallan los controles aplicables al Sistema de Seguridad de la Información propuesto para Comfenalco, Quindío. En este contexto se incluyen los controles enunciados en el Anexo A del estándar ISO/IEC 27001:2013.

6.6. Propuesta de Política General de Seguridad teniendo en cuenta los controles postulados en el anexo A de la NTC/ISO 27001:2013.

La política de seguridad debe quedar plasmada en un documento donde claramente se delimiten las áreas donde se implementará el sistema de seguridad, los activos objeto de protección y el grado de aplicación de las soluciones para que puedan ofrecer y garantizar los niveles adecuados de protección a la confidencialidad, integridad y oportunidad. En el documento se estipulan las áreas más críticas para el funcionamiento de la organización y se eligen los activos que la dirección considera más importantes tanto desde el punto de vista económico como funcional.

Según el tipo de organización, pública, privada o de economía mixta, el contenido de este documento expresa en menor o mayor grado las regulaciones estatales sobre seguridad de la información; los niveles de compromiso, actuación y comportamientos esperados por parte de los empleados en cuanto al uso de los activos de información desde la perspectiva de la dirección de la empresa así como también puede expresar las expectativas de terceras partes con las cuales la organización se encuentre vinculada contractualmente.

Las políticas en materia de seguridad de la información de la Caja de Compensación Familiar Comfenalco Quindío, establecerán los objetivos de seguridad de la información, para el manejo y uso adecuado, y se adaptaran a los requerimientos de la organización y contendrán los siguientes elementos:

Políticas para la seguridad de la información

- ✓ Se elaborará un Documento con las Políticas para la seguridad de la información de Comfenalco Quindío para el conocimiento de los Empleados y de las partes externas.

- ✓ Los documentos contentivos de las políticas de seguridad deben ser dinámicos, por lo que las máximas autoridades deben estar en conocimiento de todos los eventos que pudieran violar la seguridad del sistema, los lineamientos deben ajustarse y mejorarse continuamente, siendo necesaria la revisión periódica del documento con las políticas de seguridad.

Organización de la Seguridad de la Información

- ✓ Determinar los responsables del cumplimiento de las políticas establecidas y las medidas que se aplicaran en caso de algún incumplimiento, tales como robo, fraude, mal uso de la información y de los recursos e instalaciones.

- ✓ Se establecerán los roles de los actores comprometidos con el cumplimiento de las políticas de Seguridad de la Información, determinando las funciones y las áreas de responsabilidad, los niveles autorizados de modificación y uso adecuado de la información y los sistemas de información.

- ✓ Mantener contacto con las autoridades pertinentes para el manejo adecuado de los incidentes que pudieran suscitarse en materia de seguridad de la información, permitir igualmente la acción de profesionales especializados en Seguridad de información.

Seguridad ligada a los recursos humanos

- ✓ Para preservar la información y los sistemas adquiridos por la Caja de Compensación, se debe garantizar que el personal de la organización a través de la Dirección de Gestión Humana conozca de manera explícita las políticas establecidas para salvaguardar la integridad y la confidencialidad de los datos y los recursos dirigidos al mantenimiento de la información, el personal debe identificarse y comprometerse con los objetivos de seguridad y protección de Comfenalco Quindío.

- ✓ Los Empleados de la Organización y Contratistas deberán recibir la información adecuada a través de actividades de formación en seguridad de información, del mismo modo, sean concientizados y actualizados regularmente sobre las políticas establecidas y las posible modificaciones en los procedimientos y procesos relacionados con la seguridad de los Sistemas de Información.

- ✓ Aplicación de Normas y Procedimientos correspondientes a la desvinculación del personal adscrito a las áreas de Sistemas o cambio de la relación laboral dentro de la Institución, que definan los criterios que permitan la continuidad de la responsabilidad en el mantenimiento de las políticas de seguridad de la información.

Administración de activos

- ✓ Establecer un inventario de los activos de la organización, a fin de mantener un control de los mismos, mediante su clasificación y el aseguramiento en caso de desastre. Definir del mismo modo cuales serán los procedimientos a seguir para la protección de los equipos de procesamiento, de almacenamiento y de trasmisión de información desarrollando un Manual de Inventarios y Clasificación de Activos.

- ✓ Se debe desarrollar e implementar de acuerdo al esquema adoptado, los procedimientos detallados para el manejo de los activos propiedad de la Caja de Compensación.

- ✓ Se reglamentará el acceso a los recursos mediante una correcta administración de usuarios. se elaborará un manual con el procedimiento a seguir para asegurar el mantenimiento de la información y la recuperación de la misma en caso de pérdida, a través de copias de respaldo u otra metodología adecuada, del mismo modo se reglamentará el uso de dispositivos móviles dentro de las instalaciones.

- ✓ Las Dependencias encargadas de garantizar la custodia de la información, se encargarán de proteger, mantener y actualizar el inventario de los Activos a fin de instaurar los controles necesarios para el cumplimiento de los reglamentos construidos para la correcta integración de la información, software, hardware y recursos humanos.

- ✓ Los Activos enumerados en el Inventario, se mantendrán bajo la propiedad de la Caja de Compensación, siendo esta la garante del resguardo de los mismos.

- ✓ Implementar procedimientos para la eliminación de Los medios removibles que por condiciones de obsolescencia y deterioro deban ser alejados del ambiente de procesamiento, así como la protección de estos al ser transportados.

- ✓ Establecer procedimientos que permitan la eliminación de los medios de manera segura y que no impliquen un peligro cuando los mismos no sean ya necesarios.

- ✓ Los medios que contengan información y que requieran ser transportados para su eliminación o transferencia, deberán ser protegidos ante personas no autorizadas para su uso, ante el uso indebido o la corrupción de los mismos.

Políticas de Control de Acceso

- ✓ Documentar y establecer el carácter obligatorio del cumplimiento de la política de acceso y el uso debido de la información.

- ✓ Los usuarios deberán tener acceso al uso de las redes construidas para el manejo y uso de la información, a los fines del cumplimiento de las funciones inherentes a las diferentes áreas de la organización.

- ✓ Se realizarán los correspondientes registros los usuarios para garantizar el derecho de los empleados al acceso de la información, a quienes se les creará un identificador único para el acceso a los sistemas.

- ✓ Se establecerá el procedimiento necesario para la asignación y revocación del derecho al acceso a los sistemas y revisarlos periódicamente para garantizar el acceso con la vinculación del personal o de los usuarios externos de la información o el retiro del derecho al término de la relación laboral o contrato.

- ✓ Los sistemas de gestión de contraseñas, generarán y asignar contraseñas validas y de calidad, personales e intransferibles.

- ✓ En cuanto al tratamiento de la información, utilizar metodologías ajustadas a la detección de riesgos a fin de considerar las amenazas que puedan surgir tanto a nivel externo como interno de la institución, de igual manera, se establecerán un conjunto de reglas en cuanto a dispositivos de almacenamiento utilizados y para acceder a la información y a los recursos que maneja la organización.

Política de Criptografía

- ✓ Integrar técnicas de ayuda criptográficas con la finalidad de proteger la confidencialidad de la información, de igual manera configurar un soporte en el manejo de claves criptográficas.

- ✓ Documentar los procedimientos indispensables para la implantación de controles criptográficos.

- ✓ Se establecerán criterios para el uso y la protección de las claves criptográficas y su vida útil dentro de la Institución.

Seguridad Física y del Ambiente

- ✓ Diseñar y aplicar métodos seguros de protección en los ambientes de procesamiento, tales como Controles de acceso físico, Seguridad de oficinas, salas e instalaciones, protección física ante desastres naturales, accidentes o ataques maliciosos.

- ✓ Definir los perímetros de los establecimientos físicos que contengan información sensible y que pueda ser vulnerada por personas ajenas al manejo y control de la misma, resguardar los espacios necesarios para mantener la información y restringir el acceso al código fuente de los programas utilizados por Comfenalco.

- ✓ Establecer los controles para el ingreso apropiado de personal totalmente autorizado.

- ✓ Integrar mecanismos de control de entrada a las oficinas, salas instalaciones comprometidos en las áreas de sistemas, tales como tarjetas magnéticas de entrada, claves o lector de huella digitalizada.

- ✓ Garantizar áreas e instalaciones seguras que prevean el mantenimiento de los equipos y accesorios de informática.

Seguridad del Equipamiento

- ✓ Se garantizará el mantenimiento de los equipos en condiciones óptimas, en especial aquellos que contengan medios de almacenamiento, se revisaran continuamente los datos y software a fin de evitar su deterioro y corrupción, así mismo, se establecerán los procedimientos necesarios para la reutilización y el descarte de los equipos.

- ✓ Los equipos deben ubicarse en espacios, mesas y escritorios limpios, se establecerán normas de ordenamiento y limpieza para pantallas, escritorios, organización y resguardo de papeles en gabinetes o compartimientos adecuados para su archivo.

Seguridad de las operaciones

- ✓ Todas las operaciones que se realizan en los sistemas de información deben ser documentadas para ser puestas a disposición de los usuarios que requieran esta información.

- ✓ Los cambios en la organización, en los procesos, así como en el procesamiento de la información y sistemas, deben ser controlados mediante una gestión adecuada que implique la revisión constante.
- ✓ supervisar y adaptar el uso de los recursos, mediante el monitoreo permanente y prever la necesidad de nuevos requisitos de capacidad para el buen desempeño del sistema.

- ✓ Establecer una separación de los ambientes en pro de mantener las áreas de desarrollo, prueba y operación bien definidas para sus correspondientes funcionalidades.

- ✓ Sincronizar a una sola fuente horaria de referencia, los relojes de todos los sistemas de procesamiento de información dentro de la institución.

- ✓ Se Implementaran los procedimientos para el control de la instalación del software en los sistemas operacionales.

- ✓ Tomar las medidas adecuadas para evitar que se vulneren los sistemas de información usados, de manera oportuna, además, evaluar la exposición de la Caja de Compensación a estas vulnerabilidades y el riesgo asociado a esta vulnerabilidad.

- ✓ Establecer Auditoría para el control de eventos de seguridad de los sistemas.

- ✓ La organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información), debe avalar la revisión por parte de Empresas de Auditoría independientes, a intervalos planificados, o cuando ocurran cambios significativos, que certifiquen la Seguridad de la Información.

- ✓ Verificar los sistemas operacionales estableciendo una planificación detallada y minuciosa para minimizar el riesgo de la interrupción en los procesos de la institución.

Seguridad de las comunicaciones

- ✓ Documentar los procedimientos relacionados con la protección en caso de transferencia de la información.

- ✓ Establecer acuerdos para la transferencia segura de la información entre la institución y terceras partes.

- ✓ Generar mecanismos de encriptación de la información a fin de reducir el riesgo de vulneración y proteger la mensajería electrónica tanto a nivel interno como externo.

- ✓ El uso del servicio de internet y del correo electrónico como una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, deberá ser utilizado únicamente para fines laborales o institucionales, los mensajes emitidos a través de estos medios de comunicación deberán ser estrictamente relacionados con los propósitos de la institución.

    - Se detallará por escrito las reglas a seguir en cuanto el uso del internet y el correo electrónico, en cuanto a la Eficiencia Administrativa.

    - Establecer las circunstancias en las cuales el uso del papel para el envío de documentos físicos sea indispensable y permitido por la Ley.

- Reglamentar el acceso y el uso de documento digitales, así como el establecimiento de entidades de certificación de firmas digitales, el esclarecimiento de la legalidad de los mensajes y las implicaciones legales del mal uso de los mismos.

- Se establecerán lineamientos y sanciones, sobre el uso indebido de mensajes no institucionales, tales como: cadenas, correos masivos, que atenten contra la privacidad de la institución y contra la moral y principios del receptor o los receptores. Además de la recepción de correos con características de software malicioso.

- La Dirección de Tecnología establecerá las políticas de navegación y los niveles de usuarios, establecidas las funciones y la jerarquía de los mismos. También se determinarán los permisos a páginas autorizadas para el cumplimiento de las funciones dentro de la institución.

- Los incidentes relacionados con mensajes sospechosos o contenido que afecte la seguridad e integridad de los sistemas, deberá ser reportado de manera inmediata a la Comité de Seguridad de la Información de Comfenalco Quindío.

- Se consideran estrictamente confidenciales las cuentas de correo institucional, las cuales no deben ser reveladas en páginas web públicas, ni en ningún otro sitio de internet o entidad ajena, que implique un riesgo para la seguridad de la institución.

- La información destacada como privada de la institución debe ser autorizada para su publicación o distribución por las autoridades competentes para ello.

- La información clasificada como confidencial debe ser cifrada a fines de mantener la debida discrecionalidad.

- Solamente podrán divulgar datos o cifras oficiales de la institución, las Direcciones y oficinas encargadas o autorizadas para ese fin.

- La información relacionada con la Caja de Compensación solo podrá ser distribuida mediante correos personales o sitios web diferentes a los institucionales si son autorizados por la Comité de Seguridad de la Información.

- Los servicios a los que un usuario puede acceder, dependerá del rol o función que cumple dentro de la institución para los cuales estará formal y expresamente autorizado.

- El monitoreo del acceso de los usuarios tanto internos como externos, generará ciertos límites de uso, tales como horarios de conexión, el acceso a determinadas páginas y descarga de archivos no permitidos.

Adquisición, desarrollo y mantenimiento del sistema

- ✓ Se incluirán los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.

- ✓ Será responsabilidad de la Comité de Seguridad de la Información, avalar la adquisición y recepción del software que demanden las dependencias de la institución, y de igual modo que estos cumplan con los requisitos de seguridad, de soporte y salvaguarda.

- ✓ La Comité de Seguridad de la Información tendrá responsabilidad de velar por el desarrollo interno y externo de sistemas de información y del cumplimiento de los requerimientos de seguridad apropiados de protección de la información de la Caja de Compensación familiar.

- ✓ Velará también la Dirección de Información y Tecnología por la protección ante actos fraudulentos, diferencias en los contratos y divulgación no autorizada de La información relacionada a servicios de aplicación que pasan por redes públicas.

- ✓ Toda información de servicio trasmitida, debe ser monitoreada a los fines de que se cumpla que la misma sea enviada en forma completa, sin ningún tipo de omisión, alteración o en cualquier caso duplicación o repetición inadecuada.

- ✓ Se Definirán, documentaran y mantendrán los principios que garanticen la seguridad en los sistemas.

- ✓ La institución garantizará la existencia de entornos de desarrollo software seguros, que permitan la seguridad del mismo en todas las fases del desarrollo.

- ✓ Se incluirán en los documentos de acuerdos con los proveedores, los requisitos para abordar los riesgos de seguridad de la información asociados a la prestación de servicios de tecnología de la información y comunicaciones y a la cadena de suministro de productos.

- ✓ Realizar supervisiones y auditorías a los servicios contratados con los proveedores para mantener un control en las relaciones de estos con la institución, asegurando que los convenios y contratos estén enmarcados dentro de las políticas y procedimientos de seguridad de la información.

- ✓ Mantener y mejorar las políticas de seguridad de información existentes, mediante una gestión adecuada de los cambios en el suministro de los servicios por parte de los proveedores, igualmente se mejorarán los procedimientos y controles en seguridad de la información, de los sistemas, procesos involucrados y de los riesgos que implicaran los cambios originados por terceras partes.

Gestión de incidentes de seguridad de la información

- ✓ La Caja de Compensación Familiar Comfenalco Quindío promoverá la disminución de incidentes entre funcionarios y contratistas, a través del seguimiento y la elaboración de reportes de los incidentes suscitados que incidan en la seguridad de los sistemas de información, aportando soluciones y generando investigaciones de acuerdo con su criticidad.

- ✓ Los eventos o incidentes observados, deberán ser evaluados y analizados a fin de que sea emitido por parte de la Máxima Autoridad de la Institución o de la(s) personas designadas por esta un pronunciamiento oficial ante las entidades externas o ante terceros.

- ✓ Elaborar un Manual o Guía con la normativa con los procedimientos para la atención adecuada de los incidentes con los Contratistas y Proveedores.

Seguridad de la información en la gestión de la continuidad de las Tecnologías de Información.

- ✓ La Caja de Compensación Familiar de Quindío, dispondrá de la planificación necesaria que dé continuidad a la Seguridad de los Sistemas de Información así como de los servicios de páginas WEB, telefonía, Correo electrónico Institucional, además del mantenimiento de la infraestructura tecnológica necesaria para el soporte en los sistemas, en aras de seguir manteniendo la operatividad y funcionalidad de la organización.

- ✓ Comfenalco dispondrá igualmente la documentación necesaria para el mantenimiento de la continuidad de lo planificado en materia de seguridad de la información en caso de situaciones adversas.

Cumplimiento

- ✓ Además de cumplir con la Normativa Legal Vigente, Comfenalco velará por el cumplimiento de los requisitos legales enmarcados en la Seguridad de la Información del Estado Colombiano, entre ellos los Derechos de Autor y Propiedad Intelectual, protección de los datos confidenciales, la Ley de

Transparencia y Derecho de acceso a la Información Pública Nacional y los lineamientos que se describan en los Manuales de Normas y Procedimientos de la Organización.

6.7. Plantear los procedimientos necesarios que permitan implantar los controles seleccionados para la medida y gestión de los riesgos a nivel de la red informática de la empresa.

a. Actualización del proceso de Sistemas (Gestión TIC), el cual en gran medida es el responsable de la seguridad informática de la organización, dado que no se encuentran documentadas y/estandarizadas la mayoría de operaciones que diariamente allí se desarrollan, lo que no hace viable la medición de la efectividad del proceso de seguridad informática.

b. Revisar la propuesta de Política General de Seguridad de la Información planteada en este proyecto, y cualquier otro tipo de políticas, que apoyen la seguridad informática de la organización, revisión que incluye las siguientes actividades a fin de llevar a cabo su posible aplicación:

   - ✓ Establecer un procedimiento claro para el manejo de dispositivos móviles, que incluya protocolo a seguir en caso de que se extravíe y en el cual quede indicado que no se debe almacenar información sensible de la organización en este tipo de dispositivos.
   - ✓ Establecer un procedimiento claro para evaluar los funcionarios aptos para el teletrabajo, donde participen el área de Gestión Humana, Salud Ocupacional, Sistemas y el Jefe del área a la que pertenece el funcionario.
   - ✓ Establecer un procedimiento claro donde se definan todas las actividades a realizar antes, durante y después de la contratación de personal. Este procedimiento debe incluir la entrega y devolución formal de activos otorgados para el desarrollo de funciones (bases de datos, documentos, hardware, software, etc.), firma de acuerdos de confidencialidad, propiedad industrial e intelectual y demás documentos que garanticen el compromiso de los funcionarios con la seguridad de la información de la organización.
   - ✓ Establecer un procedimiento formal para la entrega, responsabilidad, traslado y destrucción de activos, que incluya protocolos para dar de baja activos teniendo en cuenta el concepto técnico a que haya lugar y su disposición final. También es importante clasificar los activos (críticos, de uso común, etc.), para así proceder con su protección y custodia. De esta misma manera se debe incluir la entrega, responsabilidad, traslado y disposición de la información que manejan los funcionarios de la Caja, a fin de que esta sea clasificada y poder determinar su protección, custodia y disposición final.
   - ✓ Establecer un procedimiento formal para otorgar acceso a la red

informática de la Caja, a través de los diferentes dispositivos designados para tal fil, donde participen el área de Gestión Humana, Sistemas y el Jefe del área a la que pertenece el funcionario, a fin de que teniendo en cuenta la labor a desarrollar, así mismo se establezca su acceso a la red informática y a las diferentes aplicaciones y sistemas de información de la organización. Es importante que todas las aplicaciones y sistemas de información de la Caja tengan un protocolo de acceso seguro (usuario y contraseña) y que no se compartan usuarios, a fin de establecer responsabilidades cuando así se requiera.

- ✓ Revisar el protocolo de seguridad de acceso físico a las instalaciones de la organización, sugiriendo recopilar de los visitantes algún tipo de documento que lo identifique claramente ante una eventual situación que así lo requiera.
- ✓ Establecer un procedimiento para el retiro de activos físicos de la organización, donde el área de Sistemas y el Jefe del área correspondiente autoricen la salida de dichos activos.
- ✓ Restringir completamente la descarga e instalación de aplicaciones por parte de los funcionarios de la organización. Dicha actividad corresponde única y exclusivamente al área de Sistemas de la Caja. Lo anterior a fin de garantizar un buen uso de los recursos de red y de que se cumplan con las leyes de derechos de autor que rigen a todas las organizaciones del país.
- ✓ Establecer una política clara para el uso del correo electrónico tanto interno como externo.
- ✓ Incluir dentro de los contratos con terceros la firma de acuerdos de confidencialidad, propiedad industrial e intelectual.
- ✓ Establecer un protocolo para la generación de copias de respaldo de la información y del sistema que soporta la operación de la Caja, que incluya el análisis, custodia y conservación de los log de auditoría, de las pruebas que se realizan a las copias de seguridad y de las diferentes novedades presentadas, lo cual apoya la toma de decisiones para minimizar el impacto ante la eventual materialización de las amenazas a las que se encuentra expuesta la organización.

c. Socializar a todos y cada uno de los funcionarios de la Caja de las políticas que la misma implemente en marco de la seguridad informática, dado que es responsabilidad de todos el garantizar la confidencialidad, disponibilidad e integridad de la información que al interior de la organización se gestiona.

d. Fortalecer las herramientas de control para la detección, prevención y recuperación para proteger contra código malicioso, para mantener y controlar las redes protegiéndolas de amenazas y mantener la seguridad de los sistemas, incluyendo la información en tránsito y controles que eviten la divulgación, modificación, retiro o destrucción de activos no autorizada, entre otros.

e. Establecer un Plan de Continuidad del Negocio dado que, ante la eventual materialización de una amenaza, la Caja no cuenta con un plan que le permita reanudar operaciones con el mínimo de tiempo fuera de servicio.
f. Actualización de los sistemas operativos tanto de equipos de escritorio como de los servidores, dado que las versiones de algunos de ellos no cuentan con el soporte del fabricante (ejemplo: Windows XP).
g. Implementación de un Directorio Activo que permita la autenticación de todos los usuarios de la red de la Caja, tanto a la red informática como a las diferentes aplicaciones y sistemas de información que se gestionan en la misma.

6.8. Formular un plan de tratamiento del riesgo que identifique las acciones, responsables y prioridades de la Dirección para la gestión de los riesgos de la seguridad de la red informática de la Caja.

Identificadas las amenazas a las cuales se encuentran expuestos los activos previamente evaluados, se proponen las siguientes salvaguardas:

Tabla 14. Amenazas y Salvaguardas

CODIGO	AMENAZA	TIPO DE ACTIVO QUE AFECTA	SALVAGUARDAS PROPUESTA
N.1	Fuego	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	Para los activos de tipo Datos: • Implementar controles de acceso a la información • Implementar la firma electrónica • Llevar registro de actuaciones • Llevar registro de incidencias • Realizar copias de seguridad Para los activos de tipo Hardware: • Tener inventario del hardware • Realizar control de entradas y salidas del hardware
N.2	Daños por agua	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
N.*	Desastres naturales	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
I.1	Fuego	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
I.2	Daños por agua	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	

I.*	Desastres industriales	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	• Destrucción segura del hardware • Configuración del hardware sólo por personal autorizado • Realizar mantenimiento preventivo al hardware • Protección frente a código dañino: virus, espías, etc. • Detección de intrusión • Llevar registro de actuaciones • Gestión adecuada de privilegios • Implementar controles de acceso al hardware Para los activos de tipo Software: • Protección frente a código dañino: virus, troyanos, puertas traseras, etc. • Implementar controles de acceso al software • Llevar registro de actuaciones Para los activos de tipo Servicios: • Implementar un sistema de identificación y autenticación de usuarios • Implementar sistema de transferencia automática para la alimentación eléctrica
I.3	Contaminación mecánica	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar	
I.4	Contaminación electromagnética	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar	
I.5	Avería de origen físico o lógico	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar	
I.6	Corte del suministro eléctrico	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar	
I.7	Condiciones inadecuadas de temperatura y/o humedad	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar	
I.8	Fallo de servicios de comunicaciones	Redes de Comunicaciones	
I.9	Interrupción de otros servicios y suministros esenciales	Equipamiento Auxiliar	
I.10	Degradación de los soportes de almacenamiento de la información	Soportes de Información	
I.11	Emanaciones electromagnéticas	Hardware Redes de Comunicaciones	
E.1	Errores de los usuarios	Servicios Datos Software	
E.2	Errores del administrador	Servicios Datos Software Hardware Redes de Comunicaciones	
E.3	Errores de monitorización (log)	Servicios Datos Software	

E.4	Errores de configuración	Servicios Datos Software Hardware Redes de Comunicaciones	de la organización Para los activos de tipo Redes de Comunicaciones • Realización de mantenimiento preventivo • Configuración sólo por personal autorizado • Segregar la red • Configurar *Reuters* • Configurar cortafuegos • Gestión de claves, si se emplea cifrado • Sistemas para detección de intrusión • Realizar monitoreo de uso Para los activos de tipo equipamiento auxiliar • Implementar sistema de transferencia automática para la alimentación eléctrica de la organización Para activos de tipo Instalaciones • Protección frente a accidentes naturales como terremotos, riadas, incendios, tormentas, etc. • Protección frente a accidentes industriales como incendio, inundación, etc. • Protección
E.7	Deficiencias en la organización	Personal	
E.8	Difusión de software dañino	Software	
E.9	Errores de [re-]encaminamiento	Servicios Software Redes de Comunicaciones	
E.10	Errores de secuencia	Servicios Software Redes de Comunicaciones	
E.14	Escapes de información	Datos Software Redes de Comunicaciones	
E.15	Alteración de la información	Datos	
E.16	Introducción de información incorrecta	Datos	
E.17	Degradación de la información	Datos	
E.18	Destrucción de información	Datos	
E.19	Divulgación de información	Datos	
E.20	Vulnerabilidades de los programas (software)	Software	
E.21	Errores de mantenimiento / actualización de programas (software)	Software	
E.23	Errores de mantenimiento / actualización de programas (hardware)	Hardware	
E.24	Caída del sistema por agotamiento de recursos	Servicios Hardware Redes de Comunicaciones	
E.28	indisponibilidad de personal	Personal	
A.4	Manipulación de la	Servicios	

	configuración	Datos Software Hardware Redes de Comunicaciones	contaminación mecánica: polvo, vibraciones • Protección contra contaminación electromagnética • Protección frente a emanaciones electromagnéticas • Protección del recinto: edificios, locales y áreas de trabajo • Protección del cableado • Control de acceso: entrada y salida de personas, equipos, soportes de información, etc. Para activos de tipo Personal: • Implementación de políticas de personal que cubran desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua.
A.5	Suplantación de la identidad del usuario	Servicios Software Redes de Comunicaciones	
A.6	Abuso de privilegios de acceso	Servicios Software Hardware Redes de Comunicaciones	
A.7	Uso no previsto	Servicios Software Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
A.8	Difusión de software dañino	Software	
A.9	[Re-]encaminamiento de mensajes	Servicios Software Redes de Comunicaciones	
A.10	Alteración de secuencia	Servicios Software Redes de Comunicaciones	
A.11	Acceso no autorizado	Servicios Datos Software Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
A.12	Análisis de tráfico	Redes de Comunicaciones	
A.13	Repudio	Servicios	
A.14	Interceptación de información (escucha)	Datos Software Hardware Redes de Comunicaciones	
A.15	Modificación de la información	Datos	
A.16	Introducción de falsa información	Datos	
A.17	Corrupción de la información	Datos	
A.18	Destrucción la información	Datos	

A.19	Divulgación de información	Datos	
A.22	Manipulación de programas	Software	
A.24	Denegación de servicio	Servicios Redes de Comunicaciones	
A.25	Robo	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar	
A.26	Ataque destructivo	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
A.27	Ocupación enemiga	Hardware Redes de Comunicaciones Soportes de Información Equipamiento Auxiliar Instalaciones	
A.28	Indisponibilidad de personal	Personal	
A.29	Extorsión	Personal	
A.30	Ingeniería social	Personal	

Fuente: La Autora

6.9. Plan de tratamiento de riesgos

El propósito de este Plan es permitir a la Caja de Compensación Comfenalco Quindío, alcanzar los objetivos de seguridad del Sistema De Gestión de Seguridad de la Información mediante la definición de los controles aplicables para las amenazas identificadas sobre los activos desde la perspectiva de la metodología MAGERIT con el fin de mitigar los riesgos asociados a cada uno de los activos y establecer el tratamiento adecuado, el cual se regirá por los siguientes criterios: **Asumirlos (AS), Diseñar los Controles(DC) o Transferirlos a Terceros (TT)**, tal y como se muestra en la Tabla 15:

Tabla 15. Plan de Tratamiento de Riesgos

COD	ACTIVO	TIPO	AMENAZA	RIESGO	TRATAMIENTO	SALVAGUARDAS
1	Base de datos Subsidio Familiar	D	E*, A*	Inaceptable	DC	• Protección de la información. • Copias de seguridad • Cifrado de la Información

2	Programa subsidio familiar	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
3	Windows 7	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
4	McAfee VirusScan	SW	I*,E*, A*	Tolerable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
5	Ultra VNC (Escritorio Remoto)	SW	I*,E*, A*	Inadmisible	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
7	Term Vision (emulador 58 windows y un servidor unix) aplicativo subsidio cobol	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
8	Net Term (emulador 58 windows y un servidor unix) aplicativo subsidio cobol	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
9	Mandrake 7.2	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
10	Windows Server 2008 standard Service pack 2	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
11	SQL Server 2008 Management Studio	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
13	Open server 6.0	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
14	RM COBOL 12	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
15	Windows server 2000 Service pack 4.	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
16	Servidor Web: Apache 2,0, PHP 4.4.0	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad

						• Copias de seguridad
17	Windows XP Professional Service pack 3	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
18	Open Office	SW	I*,E*, A*	Tolerable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
19	Zip Genius	SW	I*,E*, A*	Tolerable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
20	Nero	SW	I*,E*, A*	Tolerable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
21	Roxio	SW	I*,E*, A*	Tolerable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
22	Sevenet 1.0	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
23	Proxy plus	SW	I*,E*, A*	Inaceptable	DC	• Protección de las aplicaciones • Aplicar perfiles de seguridad • Copias de seguridad
24	Equipos de computo	HW	I*,E*, A*	Inadmisible	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad
25	Impresora	HW	I*,E*, A*	Tolerable	DC	• Protección de los equipos informáticos
26	Teléfono conmutador	HW	I*,E*, A*	Tolerable	DC	• Protección de los equipos informáticos
27	Servidor correo electrónico	HW	I*,E*, A*	Inadmisible	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad
28	Servidor vivienda	HW	I*,E*, A*	Inadmisible	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad
29	Servidor subsidio	HW	I*,E*, A*	Inadmisible	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad
30	Servidor intranet	HW	I*,E*, A*	Inadmisible	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad

31	Servidor internet	HW	I*,E*, A*	Inadmisible	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad
32	Switch	HW	I*,E*, A*	Tolerable	DC	• Protección de los equipos informáticos • Aplicar perfiles de seguridad • Garantizar la disponibilidad
33	Red Telefónica	COM	E*, A*	Tolerable	DC	• Protección de las comunicaciones
34	Red de Datos	COM	E*, A*	Inadmisible	DC	• Protección de las comunicaciones • Protección criptográfica a los intercambios de información • Garantizar la disponibilidad
35	Red Local	COM	E*, A*	Inadmisible	DC	• Protección de las comunicaciones • Protección criptográfica a los intercambios de información • Garantizar la disponibilidad
36	Internet	COM	E*, A*	Inadmisible	DC	• Protección de las comunicaciones • Protección criptográfica a los intercambios de información • Garantizar la disponibilidad
37	Funcionarios	P	E*, A*	Inadmisible	DC	• Capacitación, entrenamiento, sensibilización • Garantizar disponibilidad • Administración del personal
54	Correo electrónico interno	S	E*, A*	Inadmisible	DC	• Protección del correo electrónico • Protección de servicios Web
55	Correo electrónico vía web	S	E*, A*	Inadmisible	DC	• Protección del correo electrónico • Protección de servicios Web
57	Fuentes de Alimentación	AUX	E*, A*	Tolerable	DC	• Garantizar disponibilidad • Suministro eléctrico
58	Cableado	AUX	E*, A*	Tolerable	DC	• Garantizar disponibilidad • Protección física del cableado
59	Sistemas de alimentación ininterrumpida	AUX	E*, A*	Tolerable	DC	• Garantizar disponibilidad • Suministro eléctrico
60	Muebles de oficina	AUX	E*, A*	Tolerable	DC	• Garantizar disponibilidad
61	Edificio Sede	L	E*, A*	Inadmisible	DC	• Controles al acceso físico • Protección de las instalaciones • Garantizar disponibilidad

62	Documentación de los procesos, procedimientos, políticas, instructivos, manuales, formularios, actas, contratos, inventarios, documentos contables, registros y comunicaciones con empresas y trabajadores afiliados.	SI	E*, A*	Tolerable	DC	

Fuente: La Autora

Una vez establecida la propuesta para la Política General de Seguridad e identificadas las salvaguardas para minimizar el impacto de la eventual materialización de las amenazas previamente identificadas, la organización en cabeza de su Dirección Administrativa deberá definir los responsables de la creación, modificación, actualización, socialización y todas aquellas actividades relacionadas con la seguridad informática, su aplicación y seguimiento dentro de la organización. Por lo anterior, se proponen los siguientes responsables:

Comité de Seguridad Informática

Conformado por los responsables de las áreas transversales a todos los procesos de la Caja, incluyendo también a los líderes de cada proceso de acuerdo al caso específico, los cuales tendrán unos roles comunes:

Dicho comité tendrá unos roles comunes:

- Revisar y proponer cambios de la política de seguridad e igualmente informará todo lo relacionado en materia de seguridad.
- Monitorear los cambios que surjan de los riesgos que afectan los activos de la organización.
- Analizar y aprobar iniciativas que apalanquen la política y los objetivos de la Seguridad Informática.
- Evaluar y coordinar la planificación e implementación de controles.
- Difundir la política, los objetivos, controles y todo lo relacionado con la Seguridad Informática.
- Promover la mejora continua y la aplicación de todas las actividades que se establecen para mantener la Seguridad Informática de la Caja.

Teniendo en cuenta lo anterior, se proponen los siguientes roles:

Coordinador: Coordinara todas las acciones del comité de seguridad e impulsará la implementación de las políticas que se impulsen al interior de dicho comité, a fin de garantizar la seguridad informática dentro de la organización.

Responsable de Sistemas: Cumplirá las acciones relacionadas con la seguridad de todos los sistemas de información, de la red informática, la red de comunicaciones y todos los recursos hardware y software con los que cuenta la Caja, de tal forma que se encuentren alineados con la política y objetivos de la Seguridad Informática de la misma.

También desarrollará con su equipo de trabajo, los requerimientos de Seguridad Informática establecidos para la administración, operación y mantenimiento de todos los recursos informáticos de acuerdo a lo establecido en los lineamientos para el cumplimiento de la Seguridad Informática.

Responsable de Gestión Humana: Comunicará a todos los funcionarios de la Caja las responsabilidades que tiene cada uno en cuanto al cumplimiento de normas, procedimientos y políticas relacionadas con la seguridad informática.

Igualmente será el encargado de notificar los cambios que surjan en todos los documentos relacionados con la Seguridad Informática, velará por las firmas de los acuerdos de confidencialidad y todas las capacitaciones que hubiese lugar en materia de seguridad.

Responsable Legal: Verificará el cumplimiento de todos los contratos, acuerdos u otra documentación con los empleados y terceros, también prestará asesoría cuando sea necesario en materia de Seguridad Informática.

Propietarios de información: Clasificarán la información de acuerdo al grado de confidencialidad necesario, y dicha clasificación deberá ser documentada y constantemente actualizada, definirán los permisos de acceso de acuerdo a sus roles y responsabilidades dentro de la Organización.

8. CONCLUSIONES

Este proyecto permitió conocer la importancia que tiene la aplicación de un Sistema de Seguridad de la Información para la Caja de Compensación Familiar, Comfenalco Quindío como organización que contribuye en la elevación de la calidad de vida de los trabajadores, de sus familias y de la comunidad, mediante la prestación de un conjunto de servicios apreciados y valorados por la población del departamento.

La ejecución del Análisis Diferencial realizado brindó la oportunidad de diagnosticar con bastante precisión el estado actual de la seguridad de la información en la Caja y conocer el estado de los dominios, objetivos de control y los controles existentes, así como también su grado de cumplimiento con relación al Anexo A de la norma.

Otro logro importante de la realización del proyecto se obtuvo al identificar los activos de información críticos, elegir adecuadamente una metodología para el análisis de los riesgos que gravitan sobre los mismos y proponer un Plan de Tratamiento de riesgos que permita mantenerlos en un nivel aceptable sin comprometer las operaciones de la Caja en caso de presentarse una concreción de una amenaza.

Finalmente cabe destacar la redacción de manera muy clara y completa de la Política de Seguridad de la Información, el cual es el documento central para todo el proceso de gestión de un SGSI.

9. RECOMENDACIONES

La alta Dirección de Comfenalco, Quindío y Comité de Seguridad Informática deben intensificar y ahondar en su compromiso por implantar un SGSI que sea piedra angular de la seguridad de la información, reconocida por todos los empleados; en este sentido se debe trabajar por la creación de una cultura organizativa de la seguridad de la información basada en la capacitación y sensibilización del personal como eje central del éxito de un SGSI[11].

Se recomienda la implementación de los controles relativos a la organización de la seguridad de la información (A.6.del Anexo a la norma) en cuanto a la clara definición de roles de los funcionarios, la separación de responsabilidades y deberes e igualmente definir los procedimientos para mejorar los contactos con las autoridades externas. Se debe verificar con frecuencia la aplicación de los controles sobre el uso de dispositivos móviles al interior de la empresa.

Reviste importancia especial la ausencia de planes documentados y detallados para garantizar la continuidad del negocio, según se desprende del resultado del punto A.17 del Anexo A de la norma por lo cual se recomienda iniciar un trabajo que coadyuve a superar esta falencia.

A mediano plazo debe contemplarse la factibilidad económica y técnica de dotar a la Caja con la infraestructura necesaria que le permita implementar sistemas protectores de información redundante. A corto plazo, evaluar la posibilidad de pasar a la fase de implementación de este proyecto que permita diseñar y aplicar los controles específicos que aún se encuentran en nivel de “inexistentes” según lo detectado a lo largo de este trabajo.

[11] Kayworth, Tim; Whitten, Dwayne (2012). “Effective information security requires a balance of social and technology factors”. MIS quarterly executive, v. 9, n. 3, p. 164.

10. REFERENCIAS BIBLIOGRAFICAS

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.6.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.p. 12.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.14.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.p. 28.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.42.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.127

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.6.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.15.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.25.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p.75.

Herath, Tejaswini. Essays on information security practices in organizations. State University of New York at Buffalo: ProQuest Dissertations Publishing. p.14.

Herath, Tejaswini. Essays on information security practices in organizations. State University of New York at Buffalo: ProQuest Dissertations Publishing. p. 125.

Kayworth, Tim; Whitten, Dwayne (2012). “Effective information security requires a balance of social and technology factors”. MIS quarterly executive, v. 9, n. 3, pp. 163-175

Kayworth, Tim; Whitten, Dwayne (2012). “Effective information security requires a balance of social and technology factors”. MIS quarterly executive, v. 9, n. 3, p. 164.

KOSUTIC, D. Lista de documentos obligatorios exigidos por la Norma ISO 27001(Revisión 2013). En Línea. 2 de Abril de 2017. Disponible en ISO 27001 & ISO 22301. Base de Conocimientos. https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/) /

NIST SP800-35. Guide to Information Technology Security Services, Special Publication 800-35 .National Institute of Standards and Technology,p.6.

NIST SP800-35. Guide to Information Technology Security Services, Special Publication 800-35 .National Institute of Standards and Technology,P.84.

Norma NTC-ISO 27001 (2013). Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información – Requerimientos). Bogotá. 2013 Editorial: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)

Republique Francaise, Premier Ministre, Secrétariat général de la défense nationale, El método EBIOS, En línea. Septiembe 2013 Disponible en:https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

Zubieta, J. (2015). Ciberdiccionario: Conceptos de seguridad en lenguaje entendible. España, Editorial: AutorEditor,2015. p.99.

Anexo A

Análisis Diferencial Comfenalco Quindío respecto a la norma ISO 20007:2013

A.5 Políticas de seguridad de la información		
A.5.1 Orientación de la dirección para la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información. APLICABLE: SI IMPLEMENTADO: NO No existe un documento donde se exponga la política de Comfenalco Quindío respecto a la seguridad de la información.
A.5.1.2	Revisión de las políticas de seguridad de la información	*Control* Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas. APLICABLE: SI IMPLEMENTADO: NO No se hace revisión periódica porque se carece del documento referenciado en A.5.1.1
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	*Control* Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas. APLICABLE: SI IMPLEMENTADO: NO No están definidas responsabilidades ni roles porque no está implementado el SGSI

A.6.1.2	Segregación de funciones	*Control* Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización. APLICABLE: SI IMPLEMENTADO: SI Existe la separación del personal por áreas de trabajo y el acceso a los activos se otorga sólo según lo indique la necesidad para el desarrollo de los trabajos
A.6.1.3	Contacto con autoridades	*Control* Se deben mantener los contactos apropiados con las autoridades pertinentes. APLICABLE: SI IMPLEMENTADO: NO Los incidentes de seguridad de la información se manejan y resuelven al interior de la empresa
A.6.1.4	Contacto con grupos especiales de interés	*Control* Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales. APLICABLE: SI IMPLEMENTADO: NO Se carece de contactos formales con autoridades o grupos de interés para manejar los incidentes de seguridad de la información
A.6.1.5	Seguridad de la información en la gestión de proyecto	*Control* Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto. APLICABLE: SI IMPLEMENTADO: NO Al iniciar un proyecto no se vislumbran los riesgos asociados a la seguridad de la información.
A.6.2 Dispositivos móviles y trabajo remoto		
Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.		

A.6.2.1	Política de dispositivos móviles	*Control* Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles. APLICABLE: SI IMPLEMENTADO: NO No existe política de seguridad en cuanto al uso de dispositivos móviles al interior de la empresa en las jornadas laborales.
A.6.2.2	Trabajo remoto	*Control* Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto. APLICABLE: SI IMPLEMENTADO: NO No se utiliza trabajo remoto
A.7 Seguridad ligada a los recursos humanos		
A.7.1 Previo al empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.		
A.7.1.1	Selección	*Control* Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos. APLICABLE: SI IMPLEMENTADO: SI Los empleados se seleccionan cuidadosamente de acuerdo con los requerimientos exigidos por el cargo
A.7.1.2	Términos y condiciones de la relación laboral	*Control* Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información. APLICABLE: SI IMPLEMENTADO: SI Los contratos concedidos incluyen cláusulas relativas a la seguridad de la información
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.		

A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. APLICABLE: SI IMPLEMENTADO: NO No existe una política definida sobre la seguridad de la información
A.7.2.2	Concientización, educación y formación en seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral. APLICABLE: SI IMPLEMENTADO: NO No existe un SGSI ni programas de sensibilización y concientización dirigidos los empleados sobre seguridad de la información.
A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información. APLICABLE: SI IMPLEMENTADO: SI Aunque no existe un SGSI los empleados saben que afrontarían un proceso disciplinario si incurren en faltas relativas a la seguridad de la información.
A.7.3 Desvinculación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.		
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	*Control* Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral. APLICABLE: SI IMPLEMENTADO: NO Al producirse la desvinculación al empleado no se le notifica acerca de la continuidad de sus responsabilidades vigentes sobre seguridad de la información.
A.8 Administración de activos		
A.8.1 Responsabilidad por los activos		

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.		
A.8.1.1	Inventario de activos	*Control* Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos. APLICABLE: SI IMPLEMENTADO: SI Actualmente se cuenta con un documento sobre activos de información de Comfenalco Quindío.
A.8.1.2	Propiedad de los activos	*Control* Los activos que se mantienen en inventario deben pertenecer a un dueño. APLICABLE: SI IMPLEMENTADO: NO En el documento referenciado en A.8.1.1 no se declaran los propietarios de dichos activos.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información. APLICABLE: SI IMPLEMENTADO: SI Se tiene un documento con reglas sobre buen uso de los activos aunque no cubre todas las áreas
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo. APLICABLE: SI IMPLEMENTADO: SI La devolución de un activo es registrada mediante acta al efectuarse una desvinculación.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.		

A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización. APLICABLE: SI IMPLEMENTADO: SI Existe documento sobre la clasificación.
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con esquema de clasificación de información adoptado por la organización. APLICABLE: SI IMPLEMENTADO: SI Existe documento para el etiquetado de la información.
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización. APLICABLE: SI IMPLEMENTADO: NO Se debe implementar con alcance a toda la empresa.
A.8.3 Manejo de los medios		
Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.		
A.8.3.1	Gestión de los medios removibles	*Control* Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización. APLICABLE: SI IMPLEMENTADO: NO No se tienen implementados estos procedimientos
A.8.3.2	Eliminación de los medios	*Control* Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales APLICABLE: SI IMPLEMENTADO: NO No se tienen implementados estos procedimientos

A.8.3.3	Transferencia física de medios	*Control* Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte. APLICABLE: SI IMPLEMENTADO: NO No se tienen implementados estos procedimientos
A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información. APLICABLE: SI IMPLEMENTADO: NO Se tiene la política pero no se ejecuta su cumplimento.
A.9.1.2	Accesos a las redes y a los servicios de la red	*Control* Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente. APLICABLE: SI IMPLEMENTADO: NO Se tiene la política pero no se evidencia su cumplimiento
A.9.2 Gestión de acceso del usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.		
A.9.2.1	Registro y cancelación de registro de usuario	*Control* Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso. APLICABLE: SI IMPLEMENTADO: NO Los empleados carecen de un Identificador único para los accesos a los sistemas

A.9.2.2	Asignación de acceso de usuario	*Control* Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios. APLICABLE: SI IMPLEMENTADO: NO Los empleados carecen de un Identificador único para los accesos a los sistemas
A.9.2.3	Gestión de derechos de acceso privilegiados	*Control* Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado. APLICABLE: SI IMPLEMENTADO: SI El acceso privilegiado se permite de acuerdo con las necesidades del cargo y del servicio prestado por el empleado.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	*Control* Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal. APLICABLE: SI IMPLEMENTADO: SI La asignación de claves es personal y al empleado se le hacen recomendaciones de buen uso, cambio inmediato y no divulgación de las mismas.
A.9.2.5	Revisión de los derechos de acceso de usuario	*Control* Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica. APLICABLE: SI IMPLEMENTADO: NO Se tiene la política pero no se hacen verificaciones periódicas de su cumplimiento

A.9.2.6	Eliminación o ajuste de los derechos de acceso	*Control* Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio. APLICABLE: SI IMPLEMENTADO: NO No hay un procedimiento documentado para la revocación de derechos de acceso al producirse una desvinculación.
A.9.3 Responsabilidades del usuario		
Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta. APLICABLE: SI IMPLEMENTADO: SI Se preserva la confidencialidad sobre la información de acceso y autenticación a los sistemas.
A.9.4 Control de acceso al sistema y aplicaciones		
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso. APLICABLE: SI IMPLEMENTADO: SI El acceso se controla de acuerdo al rol y responsabilidad del cargo.
A.9.4.2	Procedimientos de inicio de sesión seguro	*Control* Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro. APLICABLE: SI IMPLEMENTADO: SI Se evidencia el control mediante la aplicación de inicio de sesión seguro.

A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. APLICABLE: SI IMPLEMENTADO: NO Las contraseñas se implementan de manera personal y manualmente.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación. APLICABLE: SI IMPLEMENTADO: SI Sólo se permite instalar software licenciado
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas. APLICABLE: SI IMPLEMENTADO: SI El acceso al código fuente sólo se permite al personal autorizado
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. APLICABLE: SI IMPLEMENTADO: NO No existe política ni documentación sobre implantación y uso de controles criptográficos.
A.10.1.2	Gestión de claves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil. APLICABLE: SI IMPLEMENTADO: NO No existe política ni documentación sobre implantación y uso de controles criptográficos
A.11 Seguridad física y del ambiente		

A.11.1 Áreas seguras		
Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información. Se debe restringir el acceso al código fuente de los programas. APLICABLE: SI IMPLEMENTADO: SI Se evidencia en la Sede principal. Debe extenderse a los Centros alternos
A.11.1.2	Controles de acceso físico	*Control* Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado. APLICABLE: SI IMPLEMENTADO: SI Se controla el acceso físico a las áreas seguras mediante diversos métodos
A.11.1.3	Seguridad de oficinas, salas e instalaciones	*Control* Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones. APLICABLE: SI IMPLEMENTADO: NO No todas las oficinas y otras áreas están protegidas con control de acceso físico.
A.11.1.4	Protección contra amenazas externas y del ambiente	*Control* Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes. APLICABLE: SI IMPLEMENTADO: NO No hay protección física ante desastres naturales, accidentes o ataques maliciosos.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras. APLICABLE: SI IMPLEMENTADO: NO No se tienen áreas que requieran ser aseguradas físicamente.

A.11.1.6	Áreas de entrega y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado. APLICABLE: SI IMPLEMENTADO: SI Se ejerce control físico y monitoreo sobre estas áreas.
A.11.2 Equipamiento		
Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los activos así como la interrupción de las actividades de la organización.		
A.11.2.1	Ubicación y protección del equipamiento	*Control* El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado. APLICABLE: SI IMPLEMENTADO: SI Los equipos gozan de protección contra amenazas de tipo ambiental.
A.11.2.2	Elementos de soporte	*Control* Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte. APLICABLE: SI IMPLEMENTADO: SI Los equipos están protegidos mediante sistema de UPS contra fallos en suministro de energía eléctrica. Igualmente existe soporte para acondicionamiento de aire para los equipos que lo ameritan.
A.11.2.3	Seguridad en el cableado	*Control* Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información contra interceptación, interferencia o daños. APLICABLE: SI IMPLEMENTADO: SI Existe separación entre los cableados eléctrico y estructurado para garantizar la no interferencia

A.11.2.4	Mantenimiento del equipamiento	*Control* El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad. APLICABLE: SI IMPLEMENTADO: SI Los equipos reciben mantenimiento en los períodos previamente programados por personal competente y autorizado.
A.11.2.5	Retiro de activos	*Control* El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización. APLICABLE: SI IMPLEMENTADO: SI Estas operaciones sólo las realiza personal autorizado
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	*Control* Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. APLICABLE: SI IMPLEMENTADO: SI Los activos de información sólo se utilizan al interior de la empresa.
A.11.2.7	Seguridad en la reutilización o descarte de equipos	*Control* Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización. APLICABLE: SI IMPLEMENTADO: NO No se tienen procedimientos que garanticen el borrado seguro para eventos de descarte o reutilización.
A.11.2.8	Equipo de usuario desatendido	*Control* Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada. APLICABLE: SI IMPLEMENTADO: NO No se tiene un procedimiento específico para asegurar esta protección.

A.11.2.9	Política de escritorio y pantalla limpios	*Control* Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información. APLICABLE: SI IMPLEMENTADO: NO No se tienen una política de pantalla o de escritorios limpios, aunque la información confidencial es asegurada en gabinetes con acceso restringido.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten. APLICABLE: SI IMPLEMENTADO: NO No se tiene documentados los procedimientos de operación porque falta el SGSI
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información. APLICABLE: SI IMPLEMENTADO: NO No existe control de cambios formalmente documentado
A.12.1.3	Gestión de la capacidad	*Control* Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema. APLICABLE: SI IMPLEMENTADO: NO No existe monitoreo constante sobre los recursos y su capacidad.

A.12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales	*Control* Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación. APLICABLE: SI IMPLEMENTADO: NO Los ambientes para desarrollo, prueba y operación no están debidamente separados
A.12.2 Protección contra código malicioso		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.		
A.12.2.1	Controles contra código malicioso	*Control* Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios. APLICABLE: SI IMPLEMENTADO: SI Existe protección software contra código malicioso y se destaca la conciencia que tienen los usuarios frente a este tipo de amenazas.
A.12.3 Respaldo		
Objetivo: Proteger en contra de la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada. APLICABLE: SI IMPLEMENTADO: SI Se ejecutan backups previamente programados de manera automática
A.12.4 Registro y monitoreo		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de evento	*Control* Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información. APLICABLE: SI IMPLEMENTADO: SI Se mantienen y revisan con cierta periodicidad los registros de eventos generados vía sistema operativo.

A.12.4.2	Protección de la información de registros	*Control* Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados. APLICABLE: SI IMPLEMENTADO: SI La información de registro está debidamente protegida
A.12.4.3	Registros del administrador y el operador	*Control* Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad. APLICABLE: SI IMPLEMENTADO: SI Existen registros sobre estas actividades los cuales se protegen y revisan periódicamente.
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia. APLICABLE: SI IMPLEMENTADO: NO No existe un mecanismo diseñado explícitamente para sincronizar la fuente horaria.
A.12.5 Control del software de operación		
Objetivo: Asegurar la integridad de los sistemas operacionales.		
A.12.5.1	Instalación del software en sistemas operacionales	*Control* Se deben implementar los procedimientos para controlar la instalación del software en los sistemas operacionales. APLICABLE: SI IMPLEMENTADO: SI Aunque no existe la política documentada si se ejerce control sobre la instalación de software.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas.		

A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado. APLICABLE: SI IMPLEMENTADO: NO No existen procesos/procedimientos para evaluar la exposición de los activos a este tipo de amenazas
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios. APLICABLE: SI IMPLEMENTADO: SI Aunque no existe la política documentada la instalación de software se hace por personal autorizado y se vigila que sea software licenciado.
A.12.7 Consideraciones de la auditoría de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.		
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio. APLICABLE: SI IMPLEMENTADO: NO No existen planes/procedimientos de auditoría tendientes a verificar los sistemas operacionales.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.		
A.13.1.1	Controles de red	*Control* Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones. APLICABLE: SI IMPLEMENTADO: SI Aunque no existe una infraestructura de Clave Pública si se protege la información de las aplicaciones y los sistemas.

A.13.1.2	Seguridad de los servicios de red	*Control* Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros. APLICABLE: SI IMPLEMENTADO: SI Se controla el acceso a la red y a los servicios prestados por proveedores de servicios.
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes. APLICABLE: SI IMPLEMENTADO: SI Existe una separación a través de Dominios y Unidades Organizativas, aunque debe extenderse a toda la empresa. No sólo a la sede principal.
.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación. APLICABLE: SI IMPLEMENTADO: NO No hay procedimientos documentados para proteger la transferencia de información.
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben abarcar la transferencia segura de la información del negocio entre la organización y terceros. APLICABLE: SI IMPLEMENTADO: NO No existen acuerdos formales para garantizar la transferencia segura de la información con terceras partes.

A.13.2.3	Mensajería electrónica	*Control* La información involucrada en la mensajería electrónica debe ser debidamente protegida. APLICABLE: SI IMPLEMENTADO: NO No existen mecanismos de encriptación para proteger debidamente la mensajería electrónica tanto a nivel interno como en relación con terceros.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	*Control* Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización. APLICABLE: SI IMPLEMENTADO: SI Se aplican acuerdos de no divulgación de información crítica tanto con contratistas como con empleados de la planta.
A.14 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes. APLICABLE: SI IMPLEMENTADO: NO No hay política de seguridad de la información aplicable a la adquisición de los nuevos sistemas de información.
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	*Control* La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada. APLICABLE: SI IMPLEMENTADO: NO No hay política de seguridad de la información aplicables al uso de redes públicas.

A.14.1.3	Protección de las transacciones de servicios de aplicación	*Control* La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje. APLICABLE: SI IMPLEMENTADO: NO No hay infraestructura de Clave Pública que garantice plenamente los atributos requeridos por el control.
A.14.2 Seguridad en procesos de desarrollo y soporte		
Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización. APLICABLE: SI IMPLEMENTADO: SI Se aplican controles internos al desarrollo de software.
A.14.2.2	Procedimientos de control de cambios del sistema	*Control* Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios. APLICABLE: SI IMPLEMENTADO: SI Se aplican controles, aunque mínimos, a los cambios en el proceso de desarrollo de software.
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	*Control* Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización. APLICABLE: SI IMPLEMENTADO: SI Se aplican controles de prueba a las aplicaciones críticas cuando se producen cambios en las plataformas de operación.

A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta. APLICABLE: SI IMPLEMENTADO: SI Las modificaciones al software se realizan y verifican internamente.
A.14.2.5	Principios de ingeniería de sistema seguro	*Control* Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información. APLICABLE: SI IMPLEMENTADO: NO No se cuenta con una política ni procedimientos orientados al desarrollo de software seguro.
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema. APLICABLE: SI IMPLEMENTADO: NO No se cuenta con una política ni procedimientos orientados al desarrollo de software seguro.
A.14.2.7	Desarrollo tercerizado	*Control* La organización debe supervisar y monitorear la actividad del desarrollo del sistema tercerizado. APLICABLE: SI IMPLEMENTADO: SI Se verifica que el software desarrollado por terceros cumpla con los parámetros del desarrollo seguro.

A.14.2.8	Prueba de seguridad del sistema	*Control* Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad. APLICABLE: SI IMPLEMENTADO: SI Se realizan la pruebas de funcionalidad de seguridad, aunque debe hacerse de manera más exhaustiva.
A.14.2.9	Prueba de aprobación del sistema	*Control* Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas. APLICABLE: SI IMPLEMENTADO: SI Se definen y practican los criterios de prueba de aceptación para el nuevo software y para las actualizaciones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para prueba.		
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa. APLICABLE: SI IMPLEMENTADO: SI Se seleccionan cuidadosamente los datos de prueba y se controlan de manera segura.
A.15 Relaciones con el proveedor		
A.15.1 Seguridad de la información en las relaciones con el proveedor		
Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	*Control* Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización. APLICABLE: SI IMPLEMENTADO: SI Se tienen acuerdos con los proveedores para garantizar los requisitos de seguridad de la información.

A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	*Control* Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización. APLICABLE: SI IMPLEMENTADO: SI Se tienen acuerdos con los proveedores para garantizar la seguridad de la información en las actividades de acceso, procesamiento, almacenamiento y comunicación.
A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	*Control* Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministro del producto. APLICABLE: SI IMPLEMENTADO: NO No todos los acuerdos con proveedores de suministros tienen en cuenta los requisitos relativos a los riesgos de seguridad de la información.
A.15.2 Gestión de entrega del servicio del proveedor		
Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.		
A.15.2.1	Supervisión y revisión de los servicios del proveedor	*Control* Las organizaciones deben supervisar, revisar y auditar la entrega del servicio del proveedor. APLICABLE: SI IMPLEMENTADO: NO No se cuenta con una política de seguridad de la información que permita el monitoreo y auditoría de los servicios entregados por la totalidad de los proveedores.
A.15.2.2	Gestión de cambios a los servicios del proveedor	*Control* Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos. APLICABLE: SI IMPLEMENTADO: NO No se cuenta con una política de seguridad de la información que permita el monitoreo y el control apropiados de cambios originados por terceras partes.

A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información. APLICABLE: SI IMPLEMENTADO: SI Se cuenta con procedimientos de gestión de incidentes aunque no son extensivos a toda la empresa.
A.16.1.2	Informe de eventos de seguridad de la información	*Control* Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados. APLICABLE: SI IMPLEMENTADO: SI No se cuenta con mecanismos o procedimientos formales para comunicar los incidentes de seguridad de la información, pero los empleados los reportan oportunamente.
A.16.1.3	Informe de las debilidades de seguridad de la información	*Control* Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios, observada o que se sospeche. APLICABLE: SI IMPLEMENTADO: SI No se cuenta con mecanismos o procedimientos formales para comunicar las debilidades observadas en la seguridad de la información, pero los empleados comunican oportunamente sus observaciones al respecto.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información. APLICABLE: SI IMPLEMENTADO: NO No existe una metodología para el análisis y evaluación de los riesgos que permita la clasificación adecuada del evento.

A.16.1.5	Respuesta ante incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados. APLICABLE: SI IMPLEMENTADO: NO No existe una documentación con el protocolo o guía de atención para atención de los incidentes por carencia señalada en A.16.1.4.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros. APLICABLE: SI IMPLEMENTADO: SI No se cuenta con mecanismos o procedimientos formales pero si se utiliza el conocimiento previamente adquirido en la resolución de eventos similares.
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia. APLICABLE: SI IMPLEMENTADO: SI La empresa si recolecta y preserva las evidencias necesarias que puedan aportarse en el marco legal.
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre. APLICABLE: SI IMPLEMENTADO: NO No hay políticas ni planes definidos para garantizar la Continuidad del Negocio.

A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa. APLICABLE: SI IMPLEMENTADO: NO No hay políticas ni planes definidos para garantizar la Continuidad del Negocio o Planes para Recuperación de desastres.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas. APLICABLE: SI IMPLEMENTADO: NO No hay políticas ni planes definidos para garantizar la Continuidad del Negocio o Planes para Recuperación ante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	*Control* Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad. APLICABLE: SI IMPLEMENTADO: NO La empresa no cuenta con infraestructura para implementar información redundante.
A.18 Cumplimiento		
A.18.1 Cumplimiento con los requisitos legales y contractuales		
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.		

A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	*Control* Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización. APLICABLE: SI IMPLEMENTADO: SI Los requisitos estatutarios, regulatorios y contractuales están identificados y la empresa cumple con los mismos.
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados. APLICABLE: SI IMPLEMENTADO: SI La empresa cumple con el marco legal regulatorio que protege la propiedad intelectual en sus procesos de desarrollo de software y en la adquisición de software de terceros y proveedores.
A.18.1.3	Protección de los registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. APLICABLE: SI IMPLEMENTADO: NO No hay una política claramente definida y documentada para garantizar plenamente esta protección.
A.18.1.4	Privacidad y protección de la información de identificación personal	*Control* Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda. APLICABLE: SI IMPLEMENTADO: SI La empresa cumple con el marco legal regulatorio sobre protección y confidencialidad de datos personales

A.18.1.5	Regulación de los controles criptográficos	*Control* Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones pertinentes. APLICABLE: SI IMPLEMENTADO: NO La empresa no cuenta con infraestructura para garantizar el encriptamiento de la información procesada o transmitida
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos. APLICABLE: SI IMPLEMENTADO: NO La empresa no tiene convenios con empresas de auditoría o certificación en Seguridad de la Información
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes. APLICABLE: SI IMPLEMENTADO: NO No existe una política definida de seguridad de la información que permita la revisión periódica para evaluar su grado de gestión y cumplimiento.
A.18.2.3	Verificación del cumplimiento técnico	*Control* Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización. APLICABLE: SI IMPLEMENTADO: NO No se realizan pruebas técnicas de penetración porque se carece de las herramientas pertinentes y del personal con el entrenamiento adecuado para llevarlos a cabo.

Anexo B

A.5.1 Orientación de la dirección para la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	De conformidad con los objetivos de seguridad acordados se elaboran las políticas de seguridad se ponen a disposición del público en general y de los empleados de la empresa.
A.5.1.2	Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información son revisadas a intervalos planificados o si se producen cambios significativos. Esta revisión es realizada por el Comité de Seguridad de Comfenalco Quindío.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de trabajo de la dirección para comenzar a controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Existe una definición de roles y responsabilidades respecto a la seguridad de la información.
A.6.1.2	Segregación de funciones	Existe la separación del personal por áreas de trabajo y el acceso a los activos se otorga sólo según lo indique la necesidad para el desarrollo de los trabajos
A.6.1.3	Contacto con autoridades	El Comité de Seguridad mantiene contactos con grupos de interés y autoridades nacionales para el manejo de incidentes de información
A.6.1.4	Contacto con grupos especiales de interés	El Comité de Seguridad mantiene actualizada la información sobre contactos con grupos de interés para el manejo de incidentes de información

Anexo C

CAJA DE COMPENSACION FAMILIAR COMFENALCO QUINDIO

DECLARACION DE APLICABILIDAD

A.6.1.5	Seguridad de la información en la gestión de proyecto	Al iniciar un proyecto el Jefe de Seguridad está atento y es responsable de la adopción de una metodología de análisis y evaluación de riesgos al interior del proyecto.
A.6.2 Dispositivos móviles y trabajo remoto		
Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Se documentan las políticas de seguridad en cuanto al uso de dispositivos móviles al interior de la empresa en las jornadas laborales.
A.6.2.2	Trabajo remoto	No se utiliza teletrabajo.
A.7 Seguridad ligada a los recursos humanos		
A.7.1 Previo al empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.		
A.7.1.1	Selección	Los empleados se seleccionan cuidadosamente de acuerdo con los requerimientos exigidos por el cargo
A.7.1.2	Términos y condiciones de la relación laboral	Los contratos concedidos incluyen cláusulas relativas a la seguridad de la información
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Responsabilidades de la dirección	La dirección, consciente de la importancia de la Seguridad de la Información, brinda el soporte necesario para que los empleados y contratistas la apliquen de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Concientización, educación y formación en seguridad de la información	El Comité de Seguridad regularmente ejecutan campañas tendientes a fomentar la educación y el grado de conciencia de los empleados respecto a la Seguridad de la Información.

A.7.2.3	Proceso disciplinario	Los empleados afrontan un proceso disciplinario si incurren en faltas relativas a la seguridad de la información.
A.7.3 Desvinculación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.		
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	Al producirse la desvinculación el empleado es notificado acerca de la continuidad de sus responsabilidades vigentes sobre seguridad de la información.
A.8 Administración de activos		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.		
A.8.1.1	Inventario de activos	Se cuenta con un documento sobre activos de información de Comfenalco Quindío.
A.8.1.2	Propiedad de los activos	En el documento referenciado en A.8.1.1 se declaran los propietarios de dichos activos.
A.8.1.3	Uso aceptable de los activos	Los empleados se comprometes a hacer buen uso de los activos.
A.8.1.4	Devolución de activos	La devolución de los activos es registrada mediante acta al efectuarse una desvinculación.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.		
A.8.2.1	Clasificación de la información	Existe documento sobre la clasificación de la información de acuerdo a los niveles de seguridad definidos para Comfenalco Quindío
A.8.2.2	Etiquetado de la información	Los activos referenciados en el inventario están etiquetados de conformidad con la categoría de la información asociada al activo
A.8.2.3	Manejo de activos	Existen procedimientos claros para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.8.3 Manejo de los medios		
Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.		

A.8.3.1	Gestión de los medios removibles	Se cuenta con las políticas y procedimientos definidos para la gestión de los medios removibles de acuerdo al esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de los medios	Los medios se eliminan de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales
A.8.3.3	Transferencia física de medios	Los medios con información importante se protegen contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.
A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de		
A.9.1.1	Política de control de acceso	Se cuenta con la política de control de acceso definida en las Políticas de Seguridad de la Información.
A.9.1.2	Accesos a las redes y a los servicios de la red	El acceso directo a la red y a los servicios se encuentra protegido para que sean utilizados por las personas autorizadas.
A.9.2 Gestión de acceso del usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.		
A.9.2.1	Registro y cancelación de registro de usuario	Los empleados cuentan con un Identificador único para los accesos a los sistemas
A.9.2.2	Asignación de acceso de usuario	Los empleados cuentan un Identificador único para los accesos a los sistemas
A.9.2.3	Gestión de derechos de acceso privilegiados	El acceso privilegiado se permite de acuerdo con las necesidades del cargo y del servicio prestado por el empleado.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	La asignación de claves es personal y al empleado se le hacen recomendaciones de buen uso, cambio inmediato y no divulgación de las mismas.
A.9.2.5	Revisión de los derechos de acceso de usuario	El Jefe de Seguridad hace verificaciones periódicas de su cumplimiento y documenta las anormalidades observadas.
A.9.2.6	Eliminación o ajuste de los derechos de acceso	El Jefe de Seguridad verifica que al personal retirado le sean revocados los permisos de acceso.
A.9.3 Responsabilidades del usuario		

Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	Se preserva la confidencialidad sobre la información de acceso y autenticación a los sistemas.
A.9.4 Control de acceso al sistema y aplicaciones		
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	El acceso se controla de acuerdo con el rol y responsabilidad del cargo.
A.9.4.2	Procedimientos de inicio de sesión seguro	Se evidencia el control mediante la aplicación de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	Las contraseñas se implementan de manera personal y manualmente garantizando que éstas cumplan con los requisitos de seguridad definidos en la Política de Seguridad de la Información.
A.9.4.4	Uso de programas utilitarios privilegiados	Sólo se permite instalar software licenciado
A.9.4.5	Control de acceso al código fuente de los programas	El acceso al código fuente sólo se permite al personal autorizado
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	En la Política de Seguridad se documenta el uso de los controles criptográficos
A.10.1.2	Gestión de claves	Existe una política sobre el uso, protección y vida útil de las claves criptográficas.
A.11 Seguridad física y del ambiente		
A.11.1 Áreas seguras		
Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.		
A.11.1.1	Perímetro de seguridad física	El perímetro físico es controlado por personal de seguridad para prevenir accesos no autorizados al área donde se encuentran los equipos que soportan operaciones críticas
A.11.1.2	Controles de acceso físico	Se controla el acceso físico a las áreas seguras mediante diversos métodos
A.11.1.3	Seguridad de oficinas, salas e instalaciones	Las oficinas y otras áreas están protegidas con control de acceso físico.
A.11.1.4	Protección contra amenazas externas y del ambiente	No aplicable

A.11.1.5	Trabajo en áreas seguras	No aplicable
A.11.1.6	Áreas de entrega y carga	Se ejerce control físico y monitoreo sobre estas áreas.
A.11.2 Equipamiento		
Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los activos así como la interrupción de las actividades de la organización.		
A.11.2.1	Ubicación y protección del equipamiento	Los equipos gozan de protección contra amenazas de tipo ambiental como fuego, agua, humo, etc.
A.11.2.2	Elementos de soporte	Los equipos están protegidos mediante sistema de UPS contra fallos en suministro de energía eléctrica. Igualmente existe soporte para acondicionamiento de aire para los equipos que lo ameritan.
A.11.2.3	Seguridad en el cableado	Existe separación entre los cableados eléctrico y estructurado para garantizar la no interferencia
A.11.2.4	Mantenimiento del equipamiento	Los equipos reciben mantenimiento en los períodos previamente programados por personal competente y autorizado.
A.11.2.5	Retiro de activos	Estas operaciones sólo las realiza personal autorizado
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	Los activos de información sólo se utilizan al interior de la empresa.
A.11.2.7	Seguridad en la reutilización o descarte de equipos	El Jefe de Seguridad realiza un procedimiento para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su disposición final o reutilización.
A.11.2.8	Equipo de usuario desatendido	Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio y pantalla limpios	El Comité de Seguridad garantiza la política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos operacionales y responsabilidades		

Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	Los miembros del Comité de Seguridad documentan las actividades y procedimientos relativos a la Seguridad de la Información para cada uno de los activos de información.
A.12.1.2	Gestión de cambios	Los miembros del Comité de Seguridad velan porque los cambios en los activos de información sean debidamente planeados, aprobados y documentados.
A.12.1.3	Gestión de la capacidad	Los miembros del Comité de Seguridad supervisan el uso de los recursos, y están atentos a que la adquisición de nuevos recursos obedezcan a las necesidades reales de la organización
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales	Los ambientes para desarrollo, prueba y operación están debidamente separados
A.12.2 Protección contra código malicioso		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.		
A.12.2.1	Controles contra código malicioso	Existe protección software contra código malicioso y se destaca la conciencia que tienen los usuarios frente a este tipo de amenazas.
A.12.3 Respaldo		
Objetivo: Proteger en contra de la pérdida de datos.		
A.12.3.1	Respaldo de la información	Se ejecutan backups previamente programados de manera automática
A.12.4 Registro y monitoreo		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de evento	Se mantienen y revisan con cierta periodicidad los registros de eventos generados vía sistema operativo.
A.12.4.2	Protección de la información de registros	La información de registro está debidamente protegida
A.12.4.3	Registros del administrador y el operador	Existen registros sobre las actividades de los administradores los cuales se almacenan, protegen y revisan periódicamente.
A.12.4.4	Sincronización de relojes	El Comité de Seguridad asegura que sólo exista una referencia de tiempo para todos los sistemas.

A.12.5 Control del software de operación		
Objetivo: Asegurar la integridad de los sistemas operacionales.		
A.12.5.1	Instalación del software en sistemas operacionales	Se cuenta con documentación en forma de instructivos que guían y aseguran el control sobre la instalación de software operacional.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	El análisis y evaluación de los riesgos es guiado por Metodologías internacionalmente aceptadas.
A.12.6.2	Restricciones sobre la instalación de software	La instalación de software se hace por personal autorizado y se vigila que sea software licenciado.
A.12.7 Consideraciones de la auditoría de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.		
A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se planifican y despliegan cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio. El procedimiento es registrado y documentado.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.		
A.13.1.1	Controles de red	Aunque no existe una infraestructura de Clave Pública si se protege la información de las aplicaciones y los sistemas.
A.13.1.2	Seguridad de los servicios de red	Se controla el acceso a la red y a los servicios prestados por proveedores de servicios.
A.13.1.3	Separación en las redes	Existe una separación a través de Dominios y Unidades Organizativas.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	Las políticas, procedimientos y controles para transferencia de información están formalmente documentados y vigentes.
A.13.2.2	Acuerdos sobre transferencia de información	Existen acuerdos formales para garantizar la transferencia segura de la información con terceras partes.

A.13.2.3	Mensajería electrónica	Los miembros del Comité de Seguridad utilizan una infraestructura de Clave Pública (PKI) para garantizar la seguridad de la información transmitida por las redes.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Se aplican acuerdos de no divulgación de información crítica tanto con contratistas como con empleados de la planta.
A.14 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Existe una política que define los criterios de la seguridad de la información que deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Los miembros del Comité de Seguridad utilizan una infraestructura de Clave Pública (PKI) para garantizar la seguridad de la información transmitida por las redes.
A.14.1.3	Protección de las transacciones de servicios de aplicación	Los miembros del Comité de Seguridad utilizan una infraestructura de Clave Pública (PKI) para garantizar la seguridad de la información transmitida por las redes.
A.14.2 Seguridad en procesos de desarrollo y soporte		
Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Se tiene documentada la política y se aplican los procedimientos y controles internos al desarrollo de software.
A.14.2.2	Procedimientos de control de cambios del sistema	Se tiene documentada la política y se aplican controles para asegurar la gestión a los cambios en el proceso de desarrollo de software.
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	De conformidad con la política y los procedimientos documentados y establecidos se aplican controles de prueba a las aplicaciones críticas cuando se producen cambios en las plataformas de operación.

A.14.2.4	Restricciones en los cambios a los paquetes de software	Las modificaciones al software se realizan y verifican internamente.
A.14.2.5	Principios de ingeniería de sistema seguro	Existen documentos que establecen procedimientos para el desarrollo seguro a partir de los principios de desarrollo seguro
A.14.2.6	Entorno de desarrollo seguro	Existen documentos que establecen políticas para asegurar ambientes seguros a partir de los principios de desarrollo seguro.
A.14.2.7	Desarrollo tercerizado	El Comité de Seguridad verifica que el software desarrollado por terceros cumpla con los parámetros y requisitos establecidos por la Seguridad de la Información.
A.14.2.8	Prueba de seguridad del sistema	Se realizan las pruebas de funcionalidad de seguridad, aunque debe hacerse de manera más exhaustiva.
A.14.2.9	Prueba de aprobación del sistema	Se definen y practican los criterios de prueba de aceptación para el nuevo software y para las actualizaciones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para prueba.		
A.14.3.1	Protección de datos de prueba	Se seleccionan cuidadosamente los datos de prueba y se controlan de manera segura.
A.15 Relaciones con el proveedor		
A.15.1 Seguridad de la información en las relaciones con el proveedor		
Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	Se tiene la política de seguridad de la información relativa a los acuerdos con los proveedores para garantizar los requisitos de seguridad de la información.
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	Los acuerdos con los proveedores incluyen cláusulas para garantizar la seguridad de la información en las actividades de acceso, procesamiento, almacenamiento y comunicación.
A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	Los acuerdos con los proveedores de suministros tienen en cuenta los requisitos relativos a los riesgos de seguridad de la información definidos en las políticas de la Seguridad de la Información.
A.15.2 Gestión de entrega del servicio del proveedor		

Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.		
A.15.2.1	Supervisión y revisión de los servicios del proveedor	Se tiene la documentación de los acuerdos sobre la aplicación de la política de seguridad de la información que permiten el monitoreo y auditoría de los servicios entregados por la totalidad de los proveedores.
A.15.2.2	Gestión de cambios a los servicios del proveedor	Se tiene la documentación de los acuerdos sobre la aplicación de la política de seguridad de la información que permiten el monitoreo y auditoría de los cambios que se presenten en los servicios entregados por la totalidad de los proveedores
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	Se cuenta con procedimientos documentados para la gestión de incidentes
A.16.1.2	Informe de eventos de seguridad de la información	Los empleados reportan oportunamente los eventos de seguridad de la información mediante canales de gestión apropiados.
A.16.1.3	Informe de las debilidades de seguridad de la información	Los empleados y contratistas que usen los sistemas y servicios de información de la organización observan e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se registran en formatos establecidos con el fin de facilitar su evaluación y decidir si van a ser clasificados como incidentes de seguridad de la información.
A.16.1.5	Respuesta ante incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se utiliza el conocimiento previamente adquirido en la resolución de eventos similares.
A.16.1.7	Recolección de evidencia	La empresa si recolecta y preserva las evidencias necesarias que puedan aportarse en el marco legal.

A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Los miembros del Comité de Seguridad han documentado los procedimientos y actividades para la gestión de los problemas e incidentes de la seguridad de la información desde la perspectiva de la continuidad del negocio
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Los miembros del Comité de Seguridad han documentado los procedimientos y actividades para la gestión de los problemas e incidentes de la seguridad de la información desde la perspectiva de la continuidad del negocio
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Los miembros del Comité de Seguridad han documentado los planes y procedimientos para la gestión de incidentes de la seguridad de la información desde la perspectiva de la continuidad del negocio y los verifican y regularmente.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Se cuenta con los planes documentados para suplir infraestructura necesaria ante carencias importantes en el entorno habitual que impidan o dificulten el procesamiento de información.
A.18 Cumplimiento		
A.18.1 Cumplimiento con los requisitos legales y contractuales		
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Los requisitos estatutarios, regulatorios y contractuales están identificados, documentados y publicados y la empresa cumple con los mismos.

A.18.1.2	Derechos de propiedad intelectual	La empresa cumple con el marco legal regulatorio que protege la propiedad intelectual en sus procesos de desarrollo de software y en la adquisición de software de terceros y proveedores
A.18.1.3	Protección de los registros	Los registros, independientemente del medio, se encuentran protegidos físicamente contra alteraciones y pérdidas por parte de personal no autorizado.
A.18.1.4	Privacidad y protección de la información de identificación personal	La empresa cumple con el marco legal regulatorio sobre protección y confidencialidad de datos personales.
A.18.1.5	Regulación de los controles criptográficos	Los miembros del Comité de Seguridad utilizan una infraestructura de Clave Pública (PKI) para garantizar la seguridad de la información transmitida por las redes
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.		
A.18.2.1	Revisión independiente de la seguridad de la información	La organización tiene la documentación necesaria para la auditoría interna sobre la gestión de la seguridad de la información y su implementación.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	La organización tiene la documentación necesaria para la auditoría interna sobre la gestión de la seguridad de la información y su implementación que permiten verificar el nivel de cumplimiento de los dominios, objetivos de control y controles validables.
A.18.2.3	Verificación del cumplimiento técnico	Existe la documentación para ejecutar procedimientos y acciones de penetración y verificación de resultados mediante informes automatizados.

Anexo D

Identificación y valoración de las salvaguardas existentes

En cuanto a las salvaguardas existentes en la organización, la Caja cuenta con una serie de directrices de seguridad informáticas, las cuales se enuncian a continuación:

1. *Toda la información que se maneja en el área de sistemas es Confidencial y no puede ser entregada a terceros, salvo solicitud del encargado del área que maneja dicha información,*
2. *El software que se maneja en los equipos de cómputo de la entidad debe estar debidamente licenciado de acuerdo con la ley de derechos de autor. Todo equipo nuevo que ingresa a la Entidad debe ser grabado en el software de mantenimiento, así mismo cada licencia que se adquiera en la entidad.*
3. *Todos los equipos de la entidad deben ser usados para uso exclusivo en el trabajo asignado, no para asuntos personales.*
4. *El acceso a la información, en archivos físicos o electrónicos, debe restringirse exclusivamente a los que la necesitan.*
5. *Realizar diariamente copias de la información de los servidores …*
6. *Mensualmente se guardará una copia de seguridad de los datos de Sistemas y Droguerías.*
7. *Trimestralmente se hará una copia de los programas fuentes de la entidad.*
8. *Tener un proveedor de respaldo que pueda brindar soporte en hardware y software en caso requerirlo.*
9. *Las licencias originales serán fotocopiadas y se guardarán en la caja fuerte.*
10. *Hacer revisión de los espacios de discos una vez por mes.*
11. *Mantener una copia de discos de arranque de los servidores de la entidad.*
12. *Mantener una copia de la configuración de los servidores, routers y otros elementos que requieran configuración.*
13. *Cada que se cambian las claves de los equipos de los funcionarios de sistemas, se le informa al jefe de sistemas para mantener actualizada dicha información.*
14. *Todo equipo de la red corporativa deberá contar con antivirus y estar programado para que se actualice automáticamente un servidor de sistemas, el cual contendrá una carpeta con la actualización del antivirus.*
15. *Se harán inventarios físicos de los equipos para poder hacer verificación del*

software que tienen instalado y confrontarlos con la información de licenciamiento que se tiene en el área de sistemas. En la sala de sistemas del Instituto y del Colegio, se delegará la realización del inventario al encargado de la sala.

16. *El uso de Internet será exclusivamente para labores de trabajo y sólo se podrá descargar software de evaluación, drivers, parches de seguridad y actualización del antivirus.*
17. *Todo aplicativo con el cual se manejan los datos esenciales de la entidad deben contar con su respectivo Usuario y Contraseña"* ***es de la empresa anexo***

Anexo E

Matriz Activos versus Amenazas

CAJA DE COMPENSACION FAMILIAR COMFENALCO QUINDIO

Matriz Activos Vs Amenazas

ID	ACTIVO	CLASE DE ACTIVO	VALOR DEL ACTIVO	DESASTRES NATURALES						DE ORIGEN INDUSTRIAL																									
				A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A
				N.1		N.2		N.*		I.1		I.2		I.*		I.3		I.4		I.5		I.6		I.7		I.8		I.9		I.					
57	Fuentes de Alimentación	AUX	3	5	30	5	30	7	30	4	30	4	30	4	30	3	30	3	30	3	30	5	30	3	30			3	10						
				450		450		630		360		360		360		270		270		270		450		270				90							
58	cableado	AUX	3	5	30	5	30	7	30	4	30	4	30	4	30	3	30	3	30	3	30	5	30	3	30			3	10						
				450		450		630		360		360		360		270		270		270		450		270				90							
59	Sistemas de alimentación ininterrumpida	AUX	3	5	30	5	30	7	30	4	30	4	30	7	30	3	30	3	30	3	30	5	30	3	30			3	10						
				450		450		630		360		360		630		270		270		270		450		270				90							
60	Muebles de oficina	AUX	3	5	30	5	30	7	30	4	30	4	30	4	30	3	30	3	30	3	30	3	30	3	30			3	10						
				450		450		630		360		360		360		270		270		270		270		270				90							
33	Red Telefónica	COM	4	5	30	5	30	7	10	4	30	4	30	5	30	3	30	3	30	3	30	3	30	3	30	3	10								
				600		600		280		480		480		600		360		360		360		360		360		120								
34	Red de Datos	COM	4	5	30	5	30	7	30	4	30	4	30	4	30	3	30	3	30	3	30	5	30	3	30	3	10								
				600		600		840		480		480		480		360		360		360		600		360		120								
35	Red Local	COM	4	5	30	5	30	7	30	4	30	4	30	4	30	3	30	3	30	3	30	5	30	3	30	3	10								
				600		600		840		480		480		480		360		360		360		600		360		120								
36	Internet	COM	4	5	30	5	30	7	30	4	30	4	30	4	30	3	30	3	30	3	30	3	30	3	30	3	10								
				600		600		840		480		480		480		360		360		360		360		360		120								
1	Subsidio Familiar y Subsidio al Desempleo	D	5																															
2	Programa Subsidio Familiar	SW	5																															
24	EQUIPOS DE COMPUTO	HW	4	5	30	5	30	7	30	5	30	5	30	5	30	5	30	5	30	5	30	5	30	5	30										
				600		600		840		600		600		600		600		600		600		600		600											
25	IMPRESORA	HW	4	5	30	5	30	5	30	5	30	5	30	5	30	5	30	5	30	5	30	5	30	5	30										
				600		600		600		600		600		600		600		600		600		600		600											
26	TELEFONO CONMUTADOR	HW	4	5	30	5	30	6	30	5	30	5	30	5	30	5	30	5	30	5	30	3	30	3	30										
				600		600		720		600		600		600		600		600		600		360		360											

Anexo F

Matriz Impacto versus Frecuencia

CAJA DE COMPENSACION COMFENALCO QUINDIO

MATRIZ IMPACTO VERSUS FRECUENCIA

ID	ACTIVO	CLASE DE ACTIVO	VALOR DEL ACTIVO	DESASTRES NATURALES						DE ORIGEN INDUSTRIAL															
				I	F	I	F	I	F	I	F	I	F	I	F	I	F	I	F	I	F	I	F	I	F
				N.1		N.2		N.3		I.1		I.2		I.3		I.4		I.5		I.6		I.7			
57	Fuentes de Alimentación	AUX	3	450	25	450	25	630	75	360	50	360	50	360	25	270	25	270	25	270	50	450	25	270	25
58	cableado	AUX	3	450	25	450	25	630	75	360	50	360	50	360	25	270	25	270	25	270	50	450	25	270	25
59	Sistemas de alimentación ininterrumpida	AUX	3	450	25	450	25	630	75	360	50	360	50	630	25	270	25	270	25	270	50	450	25	270	25
60	Muebles de oficina	AUX	3	450	25	450	25	630	75	360	50	360	50	360	25	270	25	270	25	270	50	270	25	270	25
33	Red Telefónica	COM	4	600	25	600	25	280	75	480	50	480	50	600	25	360	25	360	25	360	50	360	25	360	25
34	Red de Datos	COM	4	600	25	600	25	840	75	480	50	480	50	480	25	360	25	360	25	360	50	600	25	360	25
35	Red Local	COM	4	600	25	600	25	840	75	480	50	480	50	480	25	360	25	360	25	360	50	600	25	360	25
36	Internet	COM	4	600	25	600	25	840	75	480	50	480	50	480	25	360	25	360	25	360	50	360	25	360	25
1	Subsidio Familiar y Subsidio al Desempleo	D	5																						
2	Programa Subsidio Familiar	D	5																						