1. INTRODUCCIÓN

En Colombia, se viene presentado una rápida evolución y adopción de las TIC's (Tecnologías de la Información y Comunicaciones) como base para cualquier actividad socioeconómica, se ha incrementado el uso de las mismas por toda la sociedad se ha expandido las redes de telecomunicaciones, y la convergencia, han marcado la dinámica del sector de las TIC y en las economías de los países durante los últimos años, ya que las tendencias internacionales muestran que el entorno digital es dinámico y crece continuamente. Dicha evolución y maduración genera impactos positivos en todos los ámbitos de la sociedad y en todos los sectores económicos que han estado a la vanguardia de esta tendencia para lograr mayor conocimiento de sus clientes, mayor productividad, competitividad y creación de nuevos modelos de negocio.

Según el Consejo Nacional de política económica y social de la república de Colombia (CONPES)[1],la creciente relevancia del entorno digital sobre las actividades socioeconómicas, y su alto dinamismo, ha traído consigo un conjunto de incertidumbres, riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos, a los que se encuentran expuestos los individuos y las organizaciones, públicas y privadas

Muchas de esas organizaciones han considerado la seguridad informática como algo secundario y han prestado poca atención a los riesgos que en la actualidad existen, como pueden ser: amenazas internas, una de ellas, errores de los usuarios y amenazas externas dentro de las cuales podemos nombrar un Ransomware. Esto se ve sustentado en la publicación del día 6 de septiembre de 2016 de la revista Semana[2] que dice: “Las empresas en Colombia no invierten en seguridad digital” e informa que sólo invierten el 10% del presupuesto en la seguridad informática. Así mismo en su publicación del día 22 de marzo informa que “Las empresas colombianas no están preparadas para los ciberataques”.

Confa no ha sido ajeno al crecimiento y uso de las TIC's[3] que juega un papel fundamental en el mejoramiento de la calidad de vida de los afiliados y beneficiarios en el Departamento de Caldas, convirtiendo así la información en un activo cada vez más valioso y sensible frente a

---

[1] CONPES: Consejo Nacional de Política Económica y Social, fue creado por la Ley 19 de 1958. Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[2] SEMANA: es una revista colombiana de política y actualidad. Es propiedad de Felipe López.[1]Su director actual es Alejandro Santos.
http://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724

[3] TIC's: Tecnologías de la información y la comunicación (TIC o TICs)

las amenazas y riesgos que su gestión conlleva y es por ello que dicha información se debe mantener segura.

Las amenazas recientes a la información han generado un mayor sentido de urgencia que antes con respecto a la necesidad de tener mayor seguridad en la información de Confa y ha venido reforzando dichas medidas de seguridad, con el fin de prepararse para recibirlos y contrarrestarlos, pues solo con un clic, las amenazas en la red pueden llegar a causar daños en la información y por ello ha considerado importante que los colaboradores desarrollen hábitos de seguridad para cerrar las puertas virtuales e impedir el paso de los cibercriminales.

Para Confa contrarrestar, los efectos que puede acarrear la falta de seguridad informática, se presenta este trabajo que consiste en diseñar un plan estratégico de seguridad de información, que se debe convertir en la carta de navegación en un corto, mediano y largo plazo para gestionar de forma adecuada y mejorar la seguridad de la información. Este plan debe ser proactivo que indique cómo sobrevivir a los múltiples escenarios y también prepararla en el manejo de las amenazas inesperadas que podría afrontar en el futuro.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Diseñar y establecer un Plan de Seguridad de la Información (PSI) que permita desarrollar operaciones, acorde con los requerimientos del negocio, las políticas de seguridad de la información, los lineamientos del modelo de seguridad y privacidad de la estrategia de Gobierno en Línea y en cumplimiento a las disposiciones legales vigentes.

2.2. OBJETIVOS ESPECÍFICOS

Los siguientes son los objetivos específicos del plan de seguridad de la información que apoya el cumplimiento del objetivo general:

1. Identificar los recursos críticos dentro de la operación de los Servicios de Confa
2. Identificar las amenazas y vulnerabilidades a las que están supeditados los procesos activos y críticos durante su operación.

3. Identificar la probabilidad de materialización de cada una de las amenazas identificadas al explotar vulnerabilidades existentes.
4. Identificar las consecuencias por afectación interna o externa de las operaciones del negocio y la seguridad de la información de la compañía.
5. Identificar los controles que actualmente se tienen implementados y que permiten la mitigación en mayor o menor medida de las fuentes de riesgo.
6. Conocer los niveles de riesgo residual a los cuales aún se encuentra expuesta la operación de Confa.
7. identificar los hallazgos y recomendaciones de mejora.
8. Disponer de las bases suficientes para establecer y mantener una política y estándares de seguridad de información que cubra toda la organización.
9. Tener una metodología estándar de evaluación a procesos y actividades relacionados con la seguridad de la información.
10. Establecer un programa de evaluación periódica de vulnerabilidades sobre los activos de la organización.
11. Administrar conscientemente el programa de identificación y clasificación de activos de información.
12. Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de información.
13. Mejorar los procesos de control de incidentes de seguridad o violaciones de seguridad.
14. Coordinar todas las funciones relacionadas a seguridad, como seguridad física, seguridad personal y seguridad de información.
15. Tener una visión clara para el desarrollo y administración del presupuesto de seguridad de información.
16. Generar y ejecutar programas periódicos de concienciación para comunicar aspectos básicos de seguridad de información y alineamientos.

3. ALCANCE

El Plan de Seguridad de la Información (PSI) aplica para todas las áreas de Confa y busca dar una visión del estado actual de la seguridad de la información en la organización para posteriormente identificar la brecha e implementar del modelo de seguridad. Igualmente crea unos lineamientos del estado que manejan información clasificada como crítica, sensible y confidencial, con el fin de preservar la continuidad de la operación ante cualquier incidente. Así mismo aplica a todos los activos de información entre los cuales están los sistemas de información, bases de datos, dispositivos de telecomunicaciones, documentación física y digital, personas y servicios tercerizados. Por lo tanto, todas las personas que utilicen los servicios Tecnológicos de CONFA, deberán conocer y aceptar el siguiente Plan de la Seguridad de la Información y su uso. El desconocimiento del mismo, no

exonera de las responsabilidades asignadas.

4. METODOLOGÍA

4.1. CICLO OPERACIÓN

El modelo de seguridad de la información de CONFA se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea[4]:

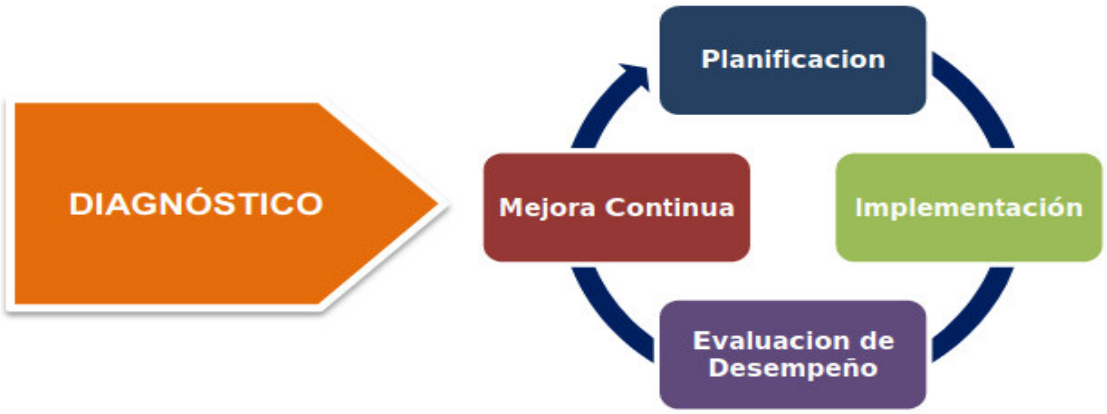

Figura 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información

- **Fase Diagnóstico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- **Fase Planificación (Planear):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

[4] Modelo de Seguridad y Privacidad, MINTIC, Pág. 20

4.2 ALINEACIÓN NORMA ISO 27001:2013

Esta nueva versión de ISO/IEC 27001:2013 se adapta con una serie de lineamientos que sirven para el desarrollo de un sistema de gestión de la seguridad de la información, que sin importar el tipo de empresa, se pueda alinear con otros sistemas de gestión en la empresa. Esta nueva estructura propuesta, alineada con el ciclo de la Mejora Continua tiene la siguiente estructura:

Figura 2: Norma ISO 27001:2013 alineado al Ciclo de mejora continua
Fuente: Elaborada con base en la información publicada en la página web http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnóstico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Ciclo Operación	Capitulo ISO 27001:2013

Diagnóstico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

Tabla 1. Fases Ciclo Operación vs. Estructura ISO 27001:2013

4.3. METODOLOGÍA USADA

La metodología utilizada para el desarrollo del Plan de Seguridad en Confa se explica a continuación

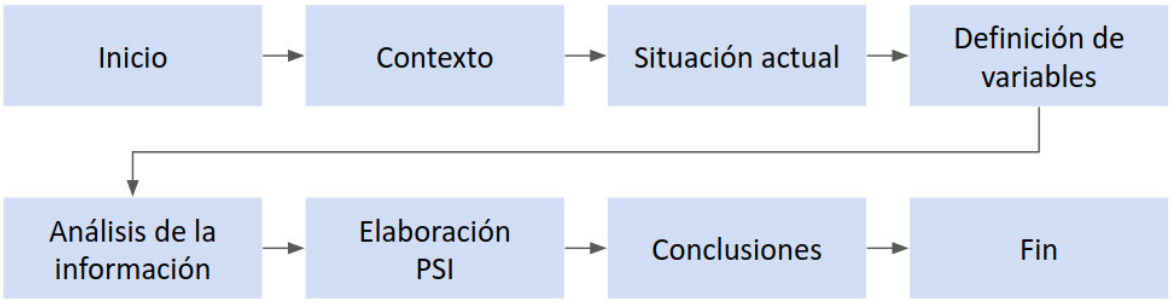

Figura 3. Metodología usada

5. CONTEXTUALIZACIÓN DE LA ORGANIZACIÓN

5.1 MISIÓN

Contribuimos con la construcción de una mejor sociedad, apoyando a las familias en el mejoramiento de su calidad de vida.

5.2. VISIÓN

Seremos una organización innovadora y sostenible, reconocida por el impacto que genera en la calidad de vida y en el desarrollo social de la región.

5.3. HISTORIA

La historia de las Cajas de Compensación en Caldas, se remonta al año 1957, cuando en junio se inició la primera que existió en el departamento denominada CAJA DE COMPENSACIÓN FAMILIAR DE CALDAS - ANDI, siendo además la segunda existente en el país.

Después de la aparición de esta Caja, surgieron la Caja de Compensación Familiar de Fenalco, seccional Manizales (Octubre de 1957 y que en 1961 pasó a llamarse Caja de Compensación Familiar de Manizales), la Caja de Compensación Familiar del Comercio Cajacom (1961), la Caja Comercial de Compensación Familiar, la Caja Integral de Compensación Familiar (1961).

Ante la necesidad de crecimiento y de prestar un mejor servicio a la comunidad Caldense, estas Cajas se fusionaron así:

Caja de Compensación Familiar de Caldas - Andi y Caja de Compensación Familiar de Manizales, creando en el año 1974 la Caja de Compensación Familiar Comfamiliar.

La Caja Comercial de Compensación Familiar, se liquidó, dejando sus clientes más importantes a la Caja Integral de Compensación Familiar, que posteriormente fue absorbida por la Caja de Compensación Familiar del Comercio -Cajacom.

A partir de 1975 quedaron dos Cajas en el escenario social caldense: Comfamiliar y Cajacom. Mediante resolución N°0064 de febrero 9 de 1984, expedida por la Superintendencia del Subsidio Familiar, nace la Caja de Compensación Familiar de Caldas - Confamiliares, como resultado de la fusión de las Cajas de Compensación Comfamiliar y Cajacom.

Los principales gestores de esta unión fueron el señor Hernando Aristizábal Botero y el Señor Emilio Restrepo Aguirre.

Las expectativas que en aquel entonces impulsaron la realización de esta integración institucional, revelan hoy una entidad fortalecida y sólida que ofrece a las familias de los trabajadores caldenses un conjunto de servicios y programas que contribuyen al mejoramiento de su calidad de vida.

5.4. ESTRUCTURA ORGANIZACIONAL

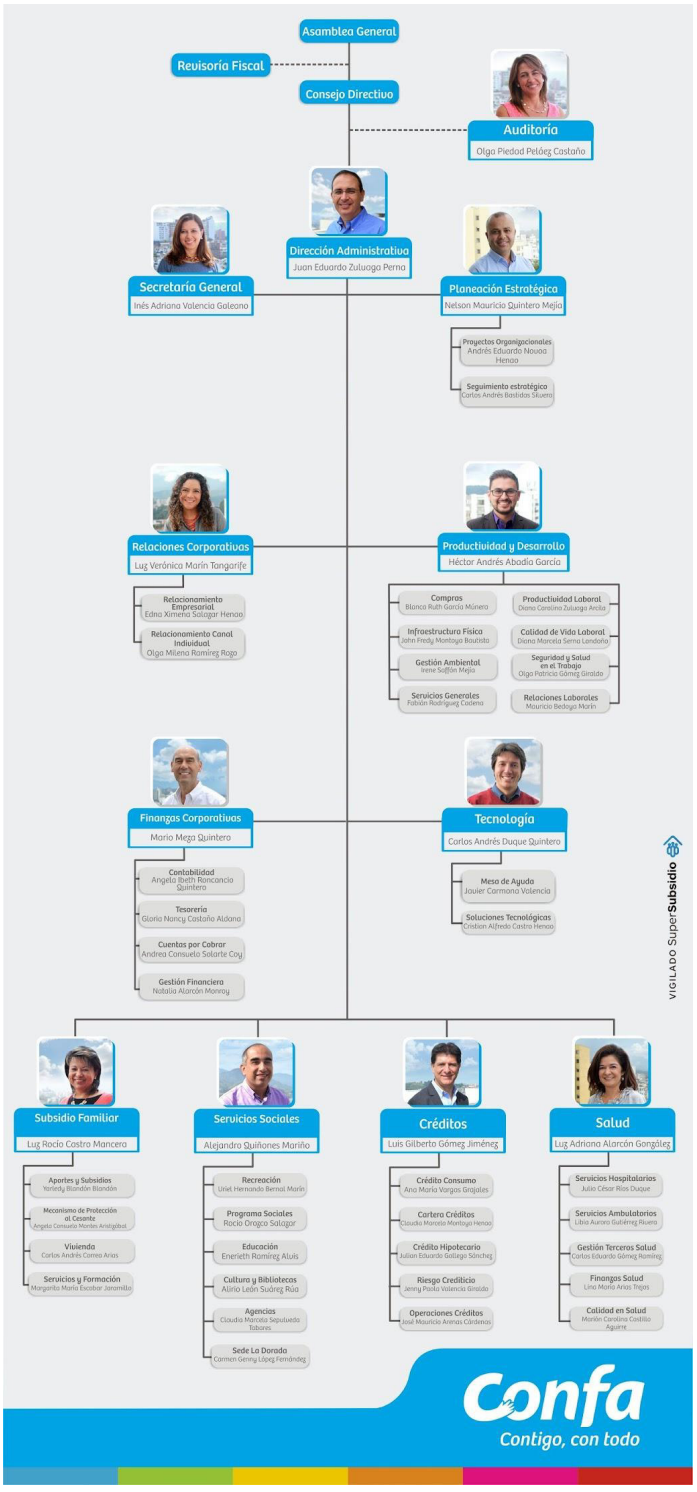

Figura 4. Estructura organizacional de Confa

6. ESCALAS DE VALORACIÓN

6.1. Análisis GAP o brecha anexo A ISO27001:2013

Las metodologías de análisis GAP se fundamentan en la detección de las diferencias existentes entre la situación actual en la que se encuentra un determinado elemento y la deseable. De este modo, nos da una idea de cuál es el esfuerzo de adaptación de la realidad actual y qué es necesario poner en marcha para alcanzar ese ideal.

En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013 y la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo correspondiente a cada año estipulada en el Manual de Gobierno en Línea así:

Tipo de Entidad	2015	2016	2017	2018	2019	2020
De orden Nacional	40 %	60%	80%	100%	Mantener 100%	Mantener 100%
De orden Territorial A	35 %	50%	80%	100%	Mantener 100%	Mantener 100%
De orden Territorial B y C	10 %	30%	50%	65%	80%	100%

Tabla 2. Escala de evaluación definida cada año en el Manual de Gobierno en Línea

6.2. Escala de Evaluación:

Es el punto de referencia para calificar los controles de las hojas administrativas, técnicas, PHVA, ciberseguridad.

Tabla de Escala Nivel de Madurez ISO 27001 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No Aplica

Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores
Definido	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 3. Hoja de escala de evaluación