PLAN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMAS DE LA CAJA DE COMPENSACIÓN FAMILIAR DEL CAUCA - COMFACAUCA, BASADO EN LA NORMA ISO 27001.

EDUARDO ANTONIO MONTILLA LEDEZMA

YENNY CAROLINA MORALES LEON

TRABAJO DE GRADO

DIPLOMADO EN IMPLEMENTACIÓN Y AUDITORÍA INTERNA EN SISTEMAS

FACULTAD DE INGENIERÍA DE SISTEMAS

2020

Nota de aceptación

_____
_____
_____
_____
_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

Popayán, 13 de Marzo de 2020

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

LISTA DE ANEXOS

GI -001 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

GI -002 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

GI -003 REPORTE DE VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

GI -004 PLAN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

GLOSARIO

ACCESO: resultado positivo de una autenticación.

ACTIVO: cualquier cosa que tenga valor para la organización.

AMENAZA: es una causa potencial de un incidente no deseado, el cual puede generar un daño a un sistema u organización.

ANÁLISIS FORENSE: conjunto de técnicas elaboradas para extraer información de cualquier soporte sin alterar su estado, permitiendo buscar evidencias en un proceso judicial.

ATAQUES INFORMÁTICOS: es un evento organizado por una o más personas con el fin de causar daño a un sistema informático o red.

CAJA DE COMPENSACIÓN FAMILIAR: son corporaciones, sin ánimo de lucro que cumplen con la función de brindar seguridad social y administrar el subsidio familiar.

CIBERACTIVO: dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información, así como aquellos elementos que permitan el acceso al mismo de forma local o remota.

CONFIDENCIALIDAD: garantizar que la información permita el acceso, sólo de aquellas personas autorizadas para tal fin.

DIAGNÓSTICO: proceso de reconocimiento, análisis y evaluación de una cosa o situación para solucionar un problema o remediar un mal.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

ERISI: equipo de respuesta a incidentes de seguridad de la información.

ESTÁNDAR: que sirve de patrón, modelo o punto de referencia para medir o valorar cosas de la misma especie.

EVENTO DE SEGURIDAD: acontecimiento que no presenta ningún tipo de cambio negativo.

EVIDENCIA: muestra verificada y certera obtenida en una investigación.

GESTIÓN DE INCIDENTES EN SEGURIDAD DE LA INFORMACIÓN: es un proceso que consiste en detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

GESTIÓN: administrar una tarea, proyecto o proceso.

GLPI: sistema de seguimiento de incidencias que maneja la caja de compensación Familiar del Cauca - Comfacauca.

HANGOUTS: aplicación de mensajería multiplataforma desarrollada por Google.

HARDWARE: conjunto de elementos físicos o materiales que componen una computadora o un sistema informático.

INCIDENTE EN SEGURIDAD DE LA INFORMACIÓN: es un evento de seguridad de la información no deseado o inesperado, que tiene una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información.

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud.

LOGS: registro de los sistemas de información que permite verificar las tareas o actividades realizadas por un determinado usuario o sistema.

MATRIZ DE RIESGOS: es una herramienta que aporta de manera rápida y sencilla una visión de los riesgos que afectan a la empresa.

OUTSOURCING: es la subcontratación de terceros para hacerse de ciertas actividades complementarias a la actividad principal.

PLAN: programa en el que se detalla el modo y conjunto de medios necesarios para llevar a cabo una idea.

PLATAFORMAS: sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible.

RIESGOS: posibilidad de que una amenaza concreta pueda generar una vulnerabilidad causando una pérdida o daño en un activo de información.

SALARIO INTEGRAL: integra todos los conceptos que puedan sustituir un salario en un solo monto o pago.

SEGURIDAD DE LA INFORMACIÓN: conjunto de medidas preventivas que aplican las organizaciones y sistemas tecnológicos, buscando resguardar y proteger la información bajo tres pilares fundamentales: Confidencialidad, Integridad y Disponibilidad.

SEGURIDAD DIGITAL: también conocida como ciberseguridad o seguridad de tecnología de la información, se enfoca en la protección de la infraestructura e información que se encuentran alojados en una computadora.

SERVIDORES: es un ordenador de gran potencia, encargado de transmitir la información pedida por sus clientes**.**

SEVENET: herramienta de software para apoyar la gestión documental de forma integral en Comfacauca.

SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN-SGSI: sistema de gestión diseñado para asegurar controles de seguridad suficiente y proporcional que protejan los activos de la información y brinden confianza a las partes interesadas.

SOFTWARE: conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

STAC TECNOLOGÍA: empresa outsorcing que apoya Comfacauca en los procesos de sistemas y tecnología de la información.

USUARIO: todo servidor público, contratista, ente regulador, socios de negocios y terceros entre otros, que tengan relación con la Caja de Compensación Familiar del Cauca - Comfacauca.

RESUMEN

Este proyecto de grado se orienta a la creación de un plan para la gestión de incidentes de seguridad de la información, con el objetivo de aportar a la empresa Comfacauca un mecanismo de gestión de los eventos de seguridad de la información que puedan presentarse, basado en los requerimientos especificados en la norma ISO 27001[1] en la gestión de incidentes de seguridad, teniendo en cuenta que en la actualidad no existe un plan de manejo de incidentes y solamente se cuenta con documentación básica sin ser manejada debidamente.

Comfacauca es una empresa que recibe el 4% de la nómina de los empleados del departamento del cauca [4] y para su operación maneja un gran volumen de datos y se hace necesario garantizar la confidencialidad, integridad y disponibilidad de su información con mecanismos como la gestión de incidentes, para que cuando se presente un evento de seguridad, se hayan establecido unos procedimientos para la contención de los impactos que puedan darse.

Para desarrollar el plan para la gestión de incidentes de seguridad de la información, se hace necesario realizar un diagnóstico bajo el criterio del Dominio A.16 Gestión de incidentes, de la Norma ISO 27001[1] donde se identifique el cumplimiento de los requisitos y en que se está fallando, posteriormente se realiza unas observaciones y recomendaciones de buenas prácticas basados en la guía ISO 27002[2], con esta información se entra al contexto de la empresa y se inicia la elaboración del plan para la gestión de incidentes de seguridad de la información, fundamentado en la metodología de técnicas de seguridad en la gestión de incidentes de la guía ISO 27035[3] donde se aplica el tratamiento de incidentes.

Con visión a la implementación de un sistema de gestión de seguridad de la información se deben ir creando este tipo de trabajos que ayuden al cumplimiento de la norma y generen valor en el tratamiento de la información.

Se espera que con la elaboración de este proyecto Comfacauca pueda tener unas bases sólidas respecto al tema de gestión de incidentes y el cumplimiento de la norma ISO 27001 en la gestión de incidentes, para una futura implementación de un SGSI.

ABSTRACT

This degree project is oriented to the creation of a plan for the management of information security incidents, with the aim of providing the Comfacauca company with a management mechanism for the information security events that may arise, based on the requirements specified in ISO 27001 [1] in the management of security incidents, taking into account that currently there is no incident management plan and only basic documentation is available without being handled duly.

Comfacauca is a company that receives 4% of the payroll of the employees of the department of Cauca [4] and for its operation it handles a large volume of data and it becomes necessary guarantee confidentiality, integrity and availability of its informationwith mechanisms such as management of incidents, so that when a security event occurs, procedures have been established for the containment of conflicts that may occur.

To develop the plan for the management of information security incidents, it is necessary to carry out a diagnosis under the criteria of Domain A.16 Incident Management, of the ISO 27001 Standard [1] where compliance with the requirements is identified and in which it is failing, subsequently some observations and recommendations of specific good practices are made in the ISO 27002 guide [2], with this information enters the context of the company and begins the elaboration of the plan for the management of security incidents of information, based on the methodology of security techniques in incident management of the ISO 27035 guide [3] where incident treatment is applied.

With a view to the implementation of an information security management system, this type of work must be created that helps to comply with the standard and the generate value in the treatment of information.

It is expected that with the elaboration of this project Comfacauca can have a solid foundation regarding the issue of incident management and compliance with the ISO 27001 standard in incident management, for a future implementation of an SGSI.

INTRODUCCIÓN

Cualquier tipo de empresa, sin importar su tamaño o naturaleza, debe tener en cuenta que actualmente existen diversidad de amenazas contra la seguridad y privacidad de la información. Al no tener claras estas advertencias, se genera para la organización ciertos riesgos, que al materializarse pueden ocasionar pérdidas económicas, sanciones legales y daños a su imagen, poniendo en peligro la continuidad del negocio. Junto a esto se relacionan los avances tecnológicos, los cuales cada día son más complejos de asegurar y administrar, exigiendo a cada organización designar responsables y encargados de velar por la protección y seguridad de los recursos, infraestructura e información.

Este documento presenta el trabajo de grado que tiene como objeto de estudio la elaboración de un plan para la gestión de incidentes de seguridad de la información en el área de Sistemas de la Caja de Compensación Familiar del Cauca - Comfacauca con el fin de tratar las insuficiencias o incapacidades que presenta el proceso de Incidentes para gestionar de manera correcta los eventos o incidentes de seguridad, de tal forma que se logre una adecuada gestión de los mismos y garantizar el cumplimiento de los requisitos de seguridad de la información planteados en el control A.16 Gestión de Incidentes de la norma ISO 27001.

La estructura del documento parte en primera instancia de la evaluación diagnóstica realizada al proceso de Gestión de Incidentes, teniendo como criterio la ISO 27001 según el anexo A.16, los cuales son de obligatorio cumplimiento para obtener un sistema certificado. y posteriormente se realizan unas observaciones y comunicación de buenas prácticas basadas en la guía ISO 27002, Finalmente se elabora el plan para la gestión de incidentes bajo la metodología del manejo de las fases de gestión de incidentes presentados en la guía especializada ISO 27035 que están orientadas a Planeación; Detección y reporte; Evaluación y decisión; Respuesta y lecciones aprendidas.

1. PLANTEAMIENTO DEL PROBLEMA

La evolución de la tecnología de la información enmarca cambios que generan múltiples riesgos y amenazas, por ello es necesario que las organizaciones implementen estrategias de seguridad basada en los riesgos y mantenga alineada las necesidades del negocio.

Basándose en el diagnóstico de la situación de la caja de compensación familiar del cauca Comfacauca, no cuenta con un SGSI establecido. El área de sistemas solo cuenta con algunas políticas y controles que no son suficientes para cubrir las reacciones necesarias cuando ocurran incidentes que puedan afectar la confidencialidad, integridad y disponibilidad de la información; buscando así planear la implementación de un control que sirva para fortalecer integralmente en la entidad, la seguridad de la información.

La implementación de un Sistema de Gestión de Seguridad de la Información, es un proceso que toma tiempo y requiere bastantes recursos que muchas veces la alta dirección no está consciente de la magnitud que pueda implicar la implementación de un SGSI y lo deja como un tema no prioritario.

Por lo tanto, se plantea la siguiente pregunta: ¿Cuál es la actividad dentro del proceso sistemas y TI que requiere un trato prioritario, basado en los requisitos establecidos por la norma ISO 27001?

2. JUSTIFICACIÓN

Las organizaciones mantienen una constante incertidumbre debido al crecimiento de los incidentes cibernéticos en el país, ya que la cifra establecida es del 54% con respecto al 2018 según registro de las autoridades, de los 28.827 casos reportados, 15.948 fueron denunciados como infracciones a la ley 1273 de 2009. [6] La cual tipifica los delitos informáticos en Colombia. [5]

En la actualidad, Colombia establece una Política general de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones mediante Resolución 512 de 2019.[7] En la cual se adoptan e implementan modelos de Seguridad y Privacidad de la información enmarcados en el SGSI, planteando como objetivo proteger, preservar y administrar la confidencialidad, integridad , disponibilidad, autenticidad y no repudio de la información, estableciendo una gestión integral de riesgos y la implementación de controles físicos y digitales, evitando así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y el alto desempeño del SGSI.

La gestión de los incidentes de seguridad de la información es un tema de gran importancia, dentro de los sistemas de gestión basados en la Norma estándar ISO 27001: 2013 ya que el comportamiento de estos permite evidenciar que tan probable es la

ocurrencia de los mismos y los posibles impactos que estos pueden generar a la empresa. Los incidentes de seguridad suministran información confiable y veraz, útil para gestionar ciertos riesgos de seguridad de la información, resaltando que este estándar precisamente está basado en un modelo de gestión de seguridad de la información.

Revisando los antecedentes de gestión de la información en Comfacauca bajo los lineamientos de la implementación de un SGSI, se identifica que se requiere trabajar en la Gestión de incidentes, debido a que es una actividad dentro del proceso Sistemas y TI que si bien se han hecho políticas, no han sido aplicadas de manera correcta por la empresa en los casos de respuesta a un incidente de seguridad, por lo tanto se propone realizar un plan para la gestión de incidentes.

El Plan para una correcta gestión de incidentes de seguridad de la información en el área de sistemas de la caja de Compensación Familiar del Cauca - Comfacauca inicia realizando un diagnóstico del manejo de los incidentes de S.I. actuales, aplicando el criterio del dominio A.16, seguidamente se revisa la documentación existente para validar el cumplimiento del dominio y se culmina presentado las recomendaciones o buenas prácticas en el manejo de los incidentes de seguridad de la información.

El presente proyecto busca, establecer un plan para que la empresa Comfacauca realice una correcta valoración y respuesta a los incidentes de seguridad de la información, evitando que se presenten de forma continua y se minimicen posibles impactos que afecten la seguridad de la información. Basándose en la norma ISO 27001, proyectando a futuro la implementación de un sistema de Gestión de Seguridad de la Información certificado.

3. OBJETIVOS

3.1 Objetivo general:

Elaborar un plan para la gestión de incidentes de seguridad de la información en el área de sistemas de la Caja de Compensación Familiar del Cauca - Comfacauca, basado en el cumplimiento del Dominio A.16 de la norma ISO 27001.

3.2 Objetivos específicos:

3.2.1 Realizar diagnóstico del manejo actual de los incidentes de seguridad de la información, aplicando el criterio del dominio A.16

3.2.2 Presentar recomendaciones para el cumplimiento del dominio A.16 y buenas prácticas de seguridad de la información basadas en la guía ISO 27002.

3.2.3 Elaborar el plan de manejo de los incidentes de seguridad de la información.

4. MARCO TEÓRICO

El auge de las tecnologías de la comunicación y la información trae consigo una serie de vulnerabilidades que al no ser tratadas pueden materializarse y generar afectación a grandes sistemas de información por parte de ciberdelincuentes que están listos para detectar dichas vulnerabilidades con el fin de hacer daño y cometer todo tipo de delitos cibernéticos.

4.1 Norma NTC ISO/IEC 27001

Existe la norma ISO 27001 la cual es un marco de gestión de la seguridad de la información, que puede ser utilizada en cualquier tipo de organización, buscando una participación de todo el personal de la empresa, para que estén enterados de la seguridad y el conocimiento de los riesgos que puedan generar en los diferentes procesos, buscando así disminuir el impacto de ocurrencia en incidencias presentadas por los sistemas de información.

Dentro de la norma ISO 27001 se encuentran los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI), son de obligatorio cumplimiento los numerales 4 al 10 y según el contexto de la organización y declaración de aplicabilidad se deben cumplir con el anexo A, Dominios, objetivos de control y controles de referencia que van desde el numeral 5 al 18.

Dentro del Anexo A, se encuentra el Dominio A.16, *Gestión de incidentes de seguridad de la información* y cuenta con un objetivo de control A.16.1, *Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.* De igual manera contiene los siguientes controles de referencia:

- *A.16.1.1 Responsabilidades y procedimientos:*
  Se deben Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- *A.16.1.2 Reporte de Eventos de Seguridad de la Información:*
  Reportar oportunamente los eventos de seguridad de la información por los canales dispuestos para tal fin.

- *A.16.1.3 Reporte de debilidades de Seguridad de la Información:*
  Reportar debilidades o vulnerabilidades de seguridad de la información observadas o sospechadas sobre los servicios o sistemas de información de la organización.

- *A.16.1.4 Evaluación de Eventos de Seguridad de la Información y Decisiones sobre ellos:*
  Evaluar los eventos y decidir si se van a clasificar como incidentes de seguridad de la información.

- *A.16.1.5 Respuesta a Incidentes de Seguridad de la Información:*
  Dar respuesta a los incidentes de acuerdo con los procedimientos documentados.

- *A.16.1.6 Aprendizaje Obtenido de los Incidentes de Seguridad de la Información:*
  Documentar el conocimiento adquirido al analizar y resolver los incidentes de seguridad para que pueda ser usado para reducir la probabilidad y el impacto de incidentes futuros, "Documentar las lecciones aprendidas".

- *A.16.1.7 Recolección de Evidencia:*
  Recolectar la evidencia a través de la identificación, recolección, adquisición y preservación de la información que pueda servir como evidencia.

La gestión de los incidentes de seguridad de la información es un aspecto muy importante dentro de los sistemas de gestión de seguridad de la información basados en ISO 27001 ya que sí son tratados oportunamente se pueden disminuir los impactos a la organización, adicionalmente el estudio y análisis del comportamiento de estos permite obtener una experiencia, aportando en la disminución de probabilidad de ocurrencia, siempre y cuando se apliquen nuevos controles o los existentes se modifiquen.[8]

4.2 Guía GTC - ISO/IEC 27002

La guía ISO/IEC 27002 suministra directrices para las normas de seguridad de la información en las organizaciones y las buenas prácticas sobre la gestión de la seguridad de la información, incluida la selección, la implementación y la gestión de controles, tomando en consideración los entornos del riesgo de seguridad de la información dentro de la organización.

Esta guía está planteada por organizaciones que tienen la intención de:

- Elegir controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información con base en la norma NTC-ISO/IEC 27001

- Implementar los controles de seguridad de la información regularmente aceptados.

- Crear sus propias políticas de gestión de la Seguridad de la Información.

La guía, en la que hacemos énfasis contiene 14 numerales de control de seguridad de la información que en su conjunto establece más de 35 categorías de seguridad principales y 114 controles, cada numeral que determina controles de seguridad contiene una o más categorías de seguridad que son fundamentales. Dependiendo de cada situación, los

controles de seguridad de alguno o de todos los numerales pueden ser importantes; por esta razón, cada organización que decida aplicar esta guía debería identificar inicialmente, los controles aplicables, su nivel de importancia y su ajuste dentro de cada proceso individual de la empresa. Cabe aclarar, que cada categoría de control contiene:

- Un objetivo de control que condiciona lo que se va a lograr.

- La cantidad de controles que se pueden aplicar para alcanzar el cumplimiento del objetivo de control.

4.3 GTC-ISO/IEC 27035

FASES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad de la información consiste en cinco fases según ISO 27035

Planeación y Preparación.
Detección y Reporte
Valoración y Decisión.
Respuesta
Lecciones aprendidas.

En cada fase se consideran aspectos relevantes, los cuales son:

Planeación y Preparación

- Política de gestión de incidentes de la información y compromiso de la alta dirección
- Políticas de seguridad de la información incluyendo la de gestión de riesgos
- Plan de gestión de incidentes de seguridad de la información
- Establecimiento del IRT
- Relacionamiento y conexión con organizaciones internas y externas
- Soporte técnico, organizacional, operacional y otros requeridos
- Concienciación y entrenamiento sobre la gestión de incidentes SI
- Pruebas al plan de gestión de incidentes SI

Detección y reporte

- Recolección de información del conocimiento de la situación desde entornos locales, fuente de datos externas y otras entradas
- Monitoreo de los sistemas y las redes
- Detección y notificación de alertas de actividades anómalas, sospechosas o maliciosas.
- Colección de los reportes de eventos de seguridad de la información.

- Reportando eventos de seguridad de la información

Valoración y decisión

Valoración de seguridad de la información y determinación sobre los incidentes de seguridad de la información

Respuesta

- Determinar si los incidentes SI están bajo el control de una investigación
- Contener y erradicar los incidentes SI
- Recuperarse de los incidentes SI
- Solución y cierre de los incidentes SI

Lecciones aprendidas

- Identificación de lecciones aprendidas
- Identificación y aplicación de mejoras a la seguridad de la información
- Identificación y aplicación de mejoras a la gestión de riesgos SI y de los resultados de las revisiones por la dirección
- Identificación y aplicación de mejoras al plan de gestión de incidentes SI
- Evaluación del desempeño y efectividad del IRT.

5. ORGANIZACIÓN DEL DOCUMENTO

El trabajo se inicia con un glosario de palabras utilizadas dentro del desarrollo del proyecto, seguido de un resumen tipo ejecutivo donde se indican los aspectos más importantes del documento. Se realiza la introducción de la temática a tratar, planteamiento del problema, justificación y objetivos.
El desarrollo del trabajo consiste en realizar un diagnóstico inicial bajo los requerimientos del Dominio A.16 de la norma ISO 27001, para ello se emplea una tabla de planeación del diagnóstico, y posterior una nueva tabla para la evaluación de cada objetivo de control. A fin de obtener un resultado de esa evaluación determinando unas observaciones y recomendaciones de buenas prácticas. Finalmente se presenta el esquema anexo GI-004 plan para la gestión de incidentes de seguridad de la información.

6. DESARROLLO DEL TRABAJO

6.1 **Metodología:**

El método que se utilizará en este trabajo será alineado a la norma ISO 27001 Dominio A.16 y la guía ISO 27002 numeral 16 Gestión de incidentes de seguridad de la información, se ejecuta en tres etapas, dos de ellas se desarrollaron anteriormente y la última es el plan para la gestión de incidentes seguridad de la información que utilizará la guía ISO 27035.

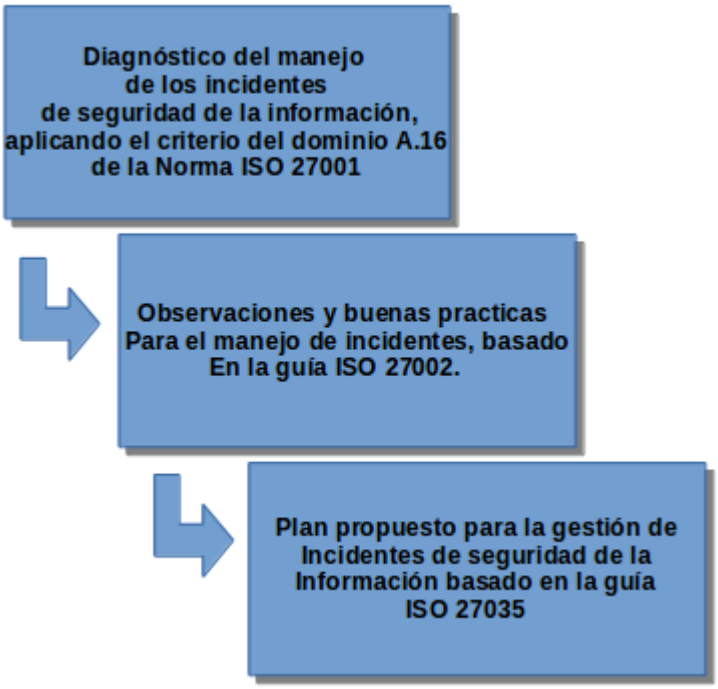

Ilustración 1 *Etapas para el desarrollo del proyecto - Fuente propia.*

6.2 **Diagnóstico del manejo actual de incidentes de S.I:**

Para iniciar con la solución al problema planteado se realizó el diagnóstico de la manera en que actualmente se gestionan los incidentes de S.I en el área de sistemas, a continuación, se presenta el plan que trata los temas solicitados por el Dominio A.16 y fue aceptado por el encargado de asuntos de seguridad del área de sistemas, Ing. Rodrigo Carreño.

PLAN REUNIÓN DE DIAGNÓSTICO			
Objetivo:	DETERMINAR EL CUMPLIMENTO DE LOS OBJETIVOS DE CONTROL ESTABLECIDOS POR EL DOMINIO A.16 DE LA NORMA ISO 27001 EN EL ÁREA DE SISTEMAS DE COMFACAUCA		
Alcance:	LA ACTIVIDAD GESTIÓN DE INCIDENTES DEL PROCESO DE T.I		
Criterios:	ANEXO A.16 DE LA NORMA ISO 27001		
Responsables:	EDUARDO MONTILLA - YENNY MORALES		
Fecha Reunión:	29/nov./2019	**Entrevistado:**	Ing. Rodrigo Carreño
Fecha	**Hora**	**Proceso / actividad**	**Observaciones**
29/nov./2019	8 am	Entrevista al coordinador de sistemas, encargado de la actividad gestión de incidentes.	Contexto y funcionamiento del área de Sistemas
29/nov./2019	9am - 12m	Verificación de procedimientos en la atención de un incidente y responsables	Control A.16.1.1
29/nov./2019	9am - 12m	Verificación de canales de gestión y método de reporte de incidentes	Control A.16.1.2
29/nov./2019	9am - 12m	Revisión de capacitaciones realizadas a los empleados en el reporte de eventos e incidentes	Control A.16.1.3
29/nov./2019	9am - 12m	Revisión de la evaluación de un evento de seguridad de la información y decisión sobre ellos	Control A.16.1.4

29/nov./2019	9am - 12m	Verificación de respuesta a incidentes	Control A.16.1.5
29/nov./2019	9am - 12m	Revisión de Aprendizaje obtenido de los incidentes de seguridad de la información	Control A.16.1.6
29/nov./2019	9am - 12m	Verificación de Recolección de evidencia	Control A.16.1.7
Observaciones:			
Elaborado por:	Eduardo Montilla	**Aceptado:**	
	Yenny Morales		Rodrigo Carreño

Tabla 1 *Plan Reunión de Diagnóstico*

Posterior a la aceptación del plan de los temas a tratar en la reunión diagnóstica se determina lo siguiente:

Comfacauca es una caja de compensación familiar que recibe aportes del 4% del salario integral de trabajadores de las empresas afiliadas, por esta razón utiliza información de tipo laboral y personal con el fin de operar su misión que es la de pagar el subsidio monetario a los trabajadores con personas a cargo y brindar servicios sociales a los mismos, para que todos estos procesos funcionen se necesita contar con infraestructura tecnológica que va desde equipos de cómputo básicos hasta servidores locales y en la nube a través de outsourcing, en ellos se alojan los diferentes sistemas de información y bases de datos, toda esa infraestructura tecnológica está a cargo del área de sistemas.

A continuación, se muestra el mapa de procesos general de Comfacauca.

MAPA DE PROCESOS COMFACAUCA

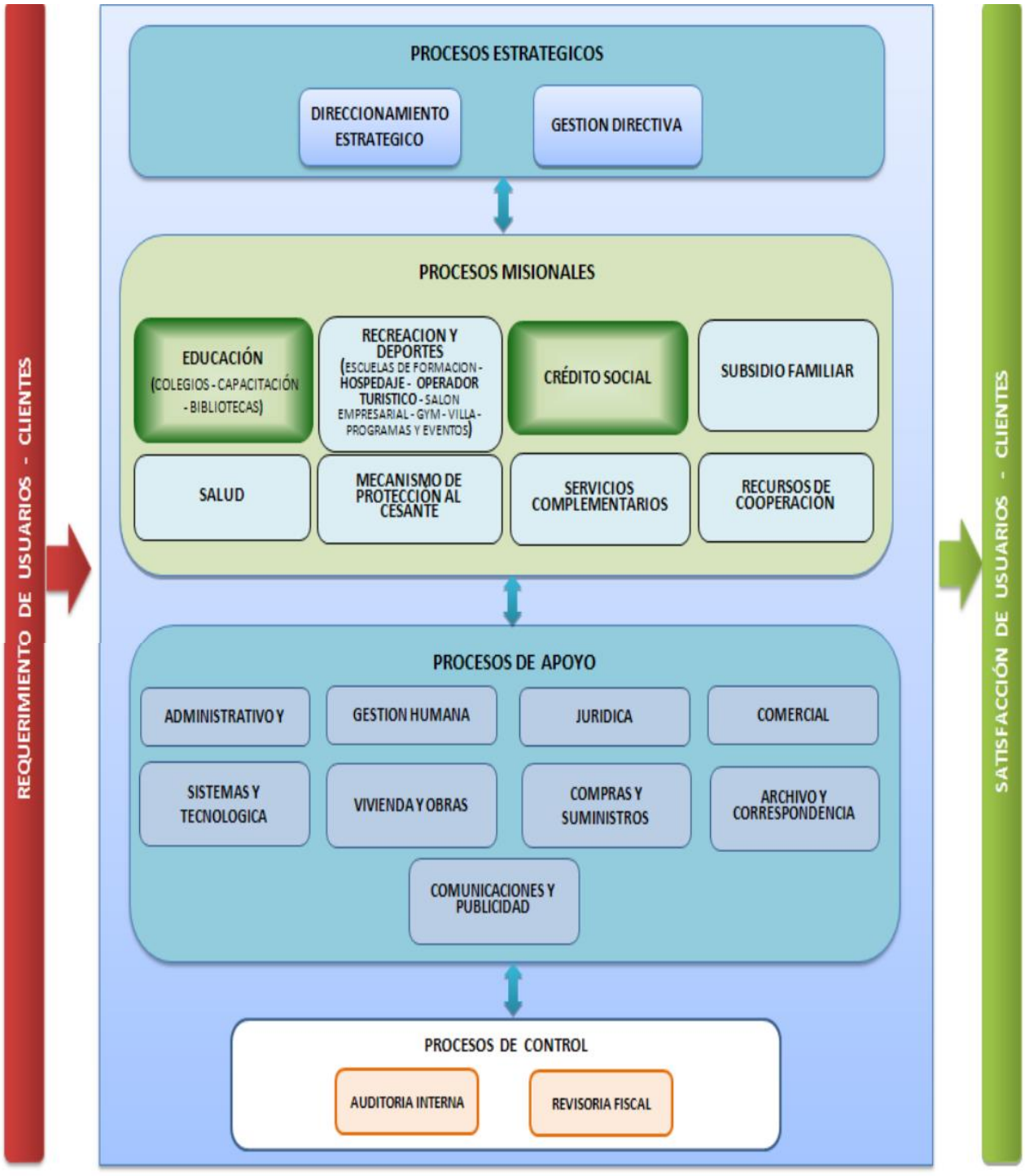

Ilustración 2 *Mapa de procesos Comfacauca - Fuente: Comfacauca*

El área de sistemas es un proceso de apoyo y que se involucra con todos los demás procesos siendo su gestor de tecnología, a continuación, se mencionan las actividades realizadas por el área.

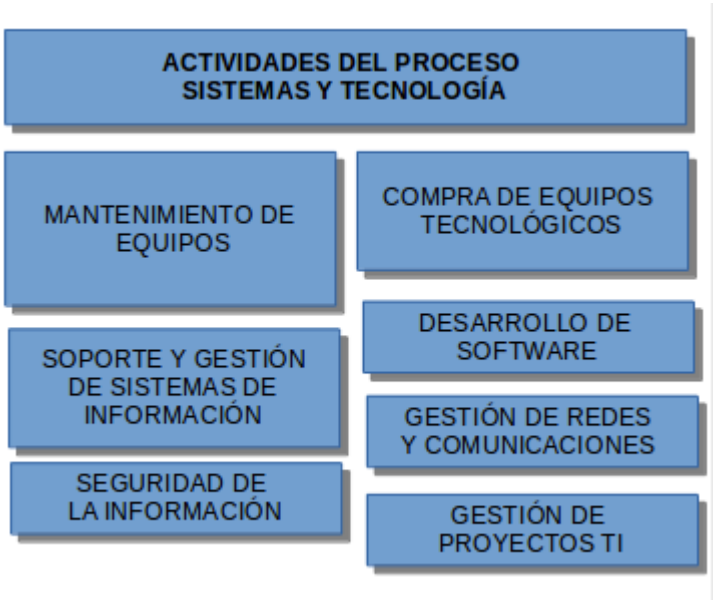

Ilustración 3 *Mapa de actividades Sistemas y Tecnología – Fuente: propia*

En la actividad de seguridad de la información no se cuenta con un sistema de gestión de seguridad de la información SGSI, que sería lo idóneo para el desarrollo de la actividad en consecuencia se requiere disminuir la brecha de la implementación de un SGSI, de modo que se debe trabajar en un aspecto bastante importante para la empresa que no existe, es el caso de la gestión de incidentes de seguridad de la información y como referencia se tomará el dominio A.16 de la norma ISO 27001 para una futura implementación y posterior certificación, a continuación se presenta la entrevista realizada al encargado de asuntos de seguridad de la información, Ing. Rodrigo Carreño.

EVALUACIÓN DIAGNÓSTICA						
Ítem	**Pregunta**	**Requerimiento o control**	**Respuesta**	**Cumple**		
				Si	**No**	**Parcial**
1	¿Existen procedimientos para la gestión de incidentes de seguridad de la información? si existen ¿Que contienen?	A.16.1.1	Existe un plan de tratamiento de incidentes, un análisis y evaluación de riesgos ambos documentos se emitieron a partir de una auditoría que realizó la empresa STAC Tecnología	✘		

2	¿Existen responsabilidades establecidas para la gestión de incidentes? si existen ¿quiénes son los encargados y cómo las aplican?	A.16.1.1	Actualmente planeación maneja una matriz de riesgos e incidentes donde responsabiliza al jefe de la sección mantener actualizada y controlada.	✘		
3	¿Se ha definido un canal para el reporte de incidentes? si existe ¿cómo funciona?	A.16.1.2	La caja tiene varios medios de comunicación y divulgación de información (hangouts, sevenet, correo electrónico, extensiones telefónicas) entre otros, pero oficialmente no existe un plan de comunicaciones o un paso a paso para reportar incidentes.		✘	
4	¿Se brindan capacitaciones de identificación y reporte de incidentes a los empleados? si la respuesta es sí ¿cómo lo hacen?	A.16.1.3	No, actualmente se envían ocasionalmente circulares por sevenet o correo electrónico de posibles amenazas que puedan tener los sistemas.		✘	
5	¿Cómo evalúan si un evento de seguridad de la información corresponde a un incidente?	A.16.1.4	Los eventos que suceden o han sucedido en la actualidad se verifican por medio de los logs de las plataformas de sistemas que tiene la caja, si se evidencia este acceso no autorizado se reporta como un incidente.			✘
6	¿Cómo se da respuesta a los incidentes? ¿Existe algún procedimiento documentado?	A.16.1.5	Existe un formato de incidentes y fallas elaborado por la empresa STAC Tecnología, pero no se ha legalizado, divulgado o utilizado dentro de la organización.		✘	
7	¿Cómo se utiliza el aprendizaje de un incidente, para reducir la posibilidad o el impacto de incidentes futuros?	A.16.1.6	La retroalimentación dentro de la sección se maneja de una manera no formal, se comenta el incidente y la solución, pero no se almacena en un árbol de conocimientos (El GLPI si tiene un módulo donde se podría		✘	

			almacenar esta información)			
8	¿Existen mecanismos de cuantificación y seguimiento de todos los tipos, cantidad y costos de incidentes?	A.16.1.6	El activo de Hardware y Software si se tiene cuantificado en el inventario de la caja (Cantidad, precio, año que fue adquirido etc), pero no se tiene cuantificado el activo de la información. Por eso no se puede cuantificar el costo de un incidente		✘	
9	¿Existen procedimientos cuando se tiene evidencia de los incidentes para fines legales o disciplinarios? ¿Cómo funciona?	A.16.1.7	No hay un proceso o procedimiento de análisis forense como tal para hacer tratamiento a la evidencia de un un incidente, si se descubre un incidente de seguridad y se evidencia que fue un funcionario de la empresa, se reporta a la sección y/o jefatura respectiva con su debida evidencia para realizar el proceso disciplinario interno y las sanciones legales y/o económicas que dieran a lugar. Los logs o accesos del sistema se envían a talento humano como evidencia de un incidente		✘	

Tabla 2 *Evaluación Diagnostica*

6.3 **Observaciones y Recomendaciones de Buenas Prácticas**

1. Cumple porque existe un plan para la gestión de incidentes y se realizó la revisión del documento “Procedimiento de manejo de incidentes” y de “Política de manejo de incidentes” ambos emitidos por la empresa contratista STAC tecnología los cuales contienen los lineamientos mínimos requeridos por la norma, son aceptados por la alta dirección y han sido comunicados a los jefes de cada dependencia.

2. Cumple porque existe el documento y está basado en lo requerido por la norma,

donde se establecen responsabilidades de cada uno de los actores y se gestiona desde el departamento de planeación, la actualización y monitoreo del cumplimiento de lo ya pactado.

3. No cumple, porque no se ha determinado un canal oficial para el reporte de incidentes ni se establece gestión del mismo, teniendo en cuenta las recomendaciones de buenas prácticas del objetivo de control 16.1.2, sobre este tema se debería:

   - ➔ Tener un canal apropiado y rápido donde se puedan registrar los eventos de seguridad de la información para su tratamiento.
   - ➔ Concientizar a los empleados sobre el reporte de eventos de seguridad lo más pronto posible e informarles las diferentes situaciones que pueden ser consideradas eventos de seguridad como:
     - ❑ Controles de seguridad ineficaces;
     - ❑ Violación de la integridad, confidencialidad y disponibilidad de la información;
     - ❑ Errores humanos;
     - ❑ No acatamiento de políticas y directrices;
     - ❑ Violaciones de acuerdo de seguridad física;
     - ❑ Cambios no controlados en el sistema;
     - ❑ Mal funcionamiento en el software o hardware;
     - ❑ Violaciones de acceso.

   y en general todo comportamiento sospechoso que afecte el funcionamiento normal de cualquier sistema puede ser tomado como evento, siendo un posible ataque de seguridad.

4. No cumple, no se ha estructurado un plan de capacitaciones para la identificación de eventos de seguridad y concientización del reporte de ellos. por lo tanto, siguiendo las recomendaciones del objetivo de control 16.1.3 se sugiere lo siguiente:

   - ➔ se debería exigir a empleados y contratistas que usan los servicios y sistemas de información de Comfacauca, que observen y reporten al canal de atención destinado, cualquier debilidad que puedan evidenciar en los sistemas y servicios.

   - ➔ se debería advertir a los contratistas y empleados no poner a prueba las debilidades de seguridad sospechadas ya que puede ser interpretado como un ataque, además de hacer daños al sistema y tendría repercusiones legales para el que lo haga.

5. Cumple parcialmente, no se tiene un método ordenado para la evaluación de sí un evento pasa a ser incidente. por lo tanto, se recomienda lo siguiente según el objetivo de control 16.1.4:

    - ➔ El punto de contacto debería evaluar cada evento de seguridad y catalogar su nivel de prioridad, impacto y si es necesario extenderlo a otra instancia como lo son las autoridades judiciales.
    - ➔ Los resultados y registro de eventos deberían ser almacenados y tratados para evitar futuros eventos relacionados, reduciendo de esta manera los indicadores de ocurrencia.

6. No cumple, la empresa STAC Tecnología elaboró un formato para el registro de eventos de seguridad como insumo principal para dar respuesta, pero no está autorizado, y en la actualidad no se utiliza. Se realizó una revisión de dicho formato y del proceso de respuesta al incidente encontrando que el formato es multiuso ya que también contiene información de soporte general de TI y no es exclusivo para los incidentes de seguridad; por lo tanto, le hace falta algunas secciones para categorizar el tipo de incidente, prioridad, nivel de afectación y que indique el manejo de evidencia según el caso para un posible análisis forense. Adecuar un espacio para el mismo donde se debe escalar, si es necesario, e indicar a qué entidad se escala.

    Entre tanto se hacen las siguientes recomendaciones de acuerdo al objetivo de control 16.1.5:

    - ➔ recolectar la evidencia lo más pronto posible después de ocurrido el incidente;
    - ➔ llevar a cabo el análisis forense, según se requiera;
    - ➔ llevar el asunto a instancias mayores cuando se requiera, por ejemplo, a las autoridades judiciales;
    - ➔ asegurarse de que todas las actividades de respuesta sean registradas para un posterior análisis;
    - ➔ comunicar la existencia del incidente de seguridad de la información con el personal interno o externo a Comfacauca que deban saberlo;
    - ➔ tratar las debilidades de seguridad de la información encontradas y que causaron o contribuyeron al incidente;
    - ➔ una vez se cierre el tratamiento del incidente de seguridad, se debe registrar;
    - ➔ por último, se deberían hacer análisis posteriores a los incidentes para identificar su origen.

7. No cumple, debido a que no se tiene un mecanismo formal a los interesados sobre la ocurrencia de incidentes y la manera de poder evitarlos, a continuación, se

muestran las recomendaciones de acuerdo al objetivo de control 16.1.6:

- ➔ el conocimiento obtenido de la resolución de incidentes debería servir para reducir la posibilidad o impacto de futuros incidentes;
- ➔ se debería contar con mecanismos para el seguimiento, cuantificación de tipos, volúmenes y costos de los incidentes, esta información se utilizará para evaluar cuáles son los incidentes recurrentes y su impacto;
- ➔ La evaluación de los incidentes indicará si se requieren nuevos controles o sí se deben reforzar los existentes, además de tener en cuenta la opinión de las personas que estén implicadas en los incidentes seguridad puedan dar formación a los demás empleados concientizando a la manera de respuesta y como evitarlos a futuro.

8. No cumple, no se cuenta con un mecanismo para la valorización de los incidentes y el nivel de afectación que estos tienen en la organización, en el ítem anterior se dieron las recomendaciones sobre este tema perteneciente al objetivo de control 16.1.6.

9. No cumple, las actividades relacionadas con el correcto tratamiento de la evidencia son mínimas y no son organizadas de tal manera que se preserve la evidencia como es debido, a continuación, se plantean las recomendaciones basadas en el objetivo de control 16.1.7:

   - ➔ Comfacauca debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la evidencia en sus diferentes tipos de estados y tipos de elementos probatorios el procedimiento debería tener en cuenta.
     - ❏ *La cadena de custodia;*
     - ❏ *La seguridad de la evidencia;*
     - ❏ *La seguridad del personal;*
     - ❏ *Los roles y responsabilidades del personal involucrado;*
     - ❏ *La competencia del personal;*
     - ❏ *La documentación;*
     - ❏ *Las sesiones informativas;*

7. RESULTADOS ALCANZADOS Y DISCUSIÓN DE LOS MISMOS:

7.1 PLAN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

La guía GTC-ISO/IEC 27035 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN nos brinda orientación sobre la gestión de incidentes de seguridad de la información como parte de un plan integral a través de la preparación, reconocimiento, evaluación,

respuesta y toma de experiencias de lo sucedido con los incidentes de seguridad generando una mejora continua de la seguridad de la información en el área de sistemas de Comfacauca. Ver Anexo **GI-004**.

8**. Conclusiones y trabajos futuros:**

- ❑ De acuerdo con lo establecido en la guía ISO 27035 y las fases que la componen se plantean recomendaciones para un correcto tratamiento de los incidentes de seguridad de la información que se presenten de forma recurrente o relativa.
- ❑ Mediante el desarrollo del presente trabajo se estableció un plan para el correcto tratamiento de los incidentes de la información que ocurran dentro de la organización, buscando así lograr la implementación en Seguridad de la Información, Gestión de incidentes bajo la Norma ISO 27001.
- ❑ Este trabajo aporta de manera significativa para la adquisición de experiencia en aplicación de las normas y guías emitidas por el Icontec trabajadas, y nos vincula al sector empresarial, donde se pondrá en marcha toda la teoría enseñada durante el transcurso del diplomado.

9**. Recomendaciones**

- ❑ Incentivar y promover la certificación en NTC-ISO/IEC 27001:2013 de los procesos misionales de la entidad.
- ❑ Mediante el fortalecimiento de los procesos de Comfacauca, crear una cultura de la entidad, enfocada a resguardar permanentemente la confidencialidad, integridad y disponibilidad de la información.
- ❑ Con el apoyo de la alta dirección, promover la implementación y aplicación de buenas prácticas para un manejo seguro de la información.
- ❑ Se sugiere continuar trabajando en los demás dominios de la norma ISO 27001, con el fin de ir logrando el cumplimiento de los requerimientos para lograr una implementación de un SGSI y su posterior certificación cuando tenga un grado de madurez significativo.

BIBLIOGRAFÍA

[1]INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnologías de la información. Técnicas de seguridad. Sistema de Gestión de la Seguridad de la Información. Requisitos. NTC-ISO/IEC 27001. Bogotá: ICONTEC, 2013.

[2] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Código de buenas prácticas para controles de seguridad de la información. NTC-ISO/IEC 27002. Bogotá: ICONTEC, 2013.

[3]INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnologías de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. GTCC-ISO/IEC 27035. Bogotá: ICONTEC, 2012.

[4] CAJA DE COMPENSACION FAMILIAR DEL CAUCA- COMFACAUCA
Sitio web: Comfacauca-2015
http://www.comfacauca.com/nuestra-empresa

[5] El TIEMPO
Sitio web: en 2019 se reportaron más de 28.000 casos de ciberataques en Colombia.
Por: Tecnosfera- 30 de octubre de 2019.
https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

[6] MINTIC
Ley 1273 de 2009
Dirección de apropiación de las TICS, Bogotá 04 de enero de 2009
https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[7] MINTIC
MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y TELECOMUNICACIONES
Resolución 512 de 2019
Normograma MinTic, Bogotá 14 de marzo de 2019
https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0512_2019.html

[8] GUÍA DE CIBERSEGURIDAD
Propuestas Guía de Ciberseguridad para comentario
https://cnostatic.s3.amazonaws.com/cno-public/archivosAdjuntos/propuesta_guia_de_ciberseguridad_para_comentarios.pdf

CONTROL DE CAMBIOS

VERSIÓN	FECHA	MOTIVO CAMBIO
1	14 de Febrero de 2020	Creación
1.2	13 de Marzo de 2020	Adición de anexos