RESUMEN – TRABAJO DE GRADO

AUTORES	**JOSÉ FABIÁN CHACÓN ORTIZ** **SERGIO DAVID RUBIO CASTILLO** **MARÍA DAYANA GONZÁLEZ RODRÍGUEZ**
FACULTAD	**FACULTAD DE INGENIERÍAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**Msc. YESSICA MARIA PEREZ PEREZ**
TÍTULO DE LA TESIS	**DISEÑO DE UN PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA UNA CAJA DE COMPENSACIÓN FAMILIAR, NORTE DE SANTANDER COMFANORTE, TENIENDO COMO REFERENCIA LA NORMA ISO/IEC 27035**

RESUMEN

(70 palabras aproximadamente)

LA PROPUESTA TIENE COMO FINALIDAD DISEÑAR UN PLAN DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27035 QUE MEJORARÁ LOS PROTOCOLOS DE RESPUESTA ANTE CUALQUIER TIPO DE ATAQUE, PROVOCARÁ UN CONJUNTO DE ALERTAS QUE CON LA INTERVENCIÓN DEL ISIRT-ERISI (EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN) TENDRÁN EL TRATAMIENTO ADECUADO Y SE PODRÁ RETROALIMENTAR A FUTUROS INCIDENTES.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:

DISEÑO DE UN PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA UNA CAJA DE COMPENSACIÓN FAMILIAR, NORTE DE SANTANDER COMFANORTE, TENIENDO COMO REFERENCIA LA NORMA ISO/IEC 27035

AUTORES:

JOSÉ FABIÁN CHACÓN ORTIZ

SERGIO DAVID RUBIO CASTILLO

MARÍA DAYANA GONZÁLEZ RODRÍGUEZ

Proyecto para optar al título de Especialistas en Auditoría de Sistemas

Directora:

Msc. YESSICA MARIA PEREZ PEREZ

Ingeniera de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia Diciembre de 2017

Índice

Lista de Tablas

Lista de Figuras

Introducción

La información ha cobrado vital importancia para las empresas y se ha posicionado como un activo principal en la toma de decisiones ayudando a conseguir el éxito o el fracaso. Los riesgos de seguridad pueden influir negativamente en la continuidad del negocio, imagen corporativa, relaciones con las partes interesadas, incumplimiento de normatividad y pérdidas económicas, entre otras, por lo tanto las organizaciones buscan proteger y asegurar la información para garantizar su integridad, confidencialidad y disponibilidad, para ello es esencialmente significativo implementar los controles preventivos de seguridad más idóneos que protejan la información de las amenazas a las que pueda estar expuesta.

La propuesta tiene como finalidad diseñar un plan de respuesta ante incidentes de seguridad de la información basado en la norma ISO/IEC 27035 que mejorará los protocolos de respuesta ante cualquier tipo de ataque, provocará un conjunto de alertas que con la intervención del ISIRT-ERISI (Equipo de respuesta ante incidentes de seguridad de la información) tendrán el tratamiento adecuado y se podrá retroalimentar a futuros incidentes.

Capítulo 1. Diseño de un plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander Comfanorte, teniendo como referencia la norma ISO/IEC 27035

1.1 Planteamiento del problema

"El crecimiento de las empresas y la sofisticación de las amenazas informáticas plantean un nuevo panorama en el cual cualquier entidad es propensa a padecer las consecuencias de algún incidente de seguridad, que podría estar relacionado con la información". (Mendoza, 2015) Actualmente las organizaciones le han dado importancia a la seguridad de la información preocupándose por implementar controles que las protejan, olvidando que los controles reducen el riesgo pero no lo eliminan, por lo anterior no es muy frecuente que se implementen planes y equipos de respuesta a incidentes que minimicen el impacto que pueda ocasionar un suceso de seguridad.

> A nivel latinoamericano la implementación de equipos de respuesta ante incidentes de seguridad ha tomado fuerza en los últimos años y existe al menos un grupo de respuesta a incidentes de seguridad (CSIRT) de este tipo en cada país de la región. (Andrade paredes, 2013)

En Colombia hay conformados ocho CSIRT que hacen parte del Foro para respuesta a incidentes y equipos de seguridad (FISRT, 2017), siendo el más representativo el CSIRT - PONAL Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional establecido para suministrar asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones.

La Caja de Compensación Familiar de Norte de Santander, COMFANORTE no cuenta actualmente con un equipo de respuesta ante incidencias de seguridad es decir, que al momento de presentarse alguna falla a nivel de seguridad de información en la corporación puede tener un impacto alto y se puede ver afectada la continuidad del negocio, lo anterior debido al aumento en tiempos de respuesta, falta de políticas definidas y falta de un equipo capacitado para dar solución a los incidentes cuando los controles implementados fallan o no sean efectivos.

Adicionalmente el diseño de un plan de respuesta a incidentes de seguridad de la información para la caja de compensación familiar de Norte de Santander, COMFANORTE da los lineamientos necesarios para controlar y restar cualquier tipo de perjuicio a la corporación referente a la información, así mismo para preservación de la evidencia y documentación sobre lo ocurrido. De esta forma, se conocerá el contexto del incidente que permitirá determinar su origen y posibles efectos; reducir las consecuencias del incidente de seguridad, minimizar la inversión de recursos, pérdida de confianza de clientes y disminuir el tiempo necesario para restaurar las operaciones a la normalidad.

La ISO es una de las entidades que proponen guías, marcos de trabajo y normas en diferentes áreas para que las organizaciones mejoren sus procesos.

> La organización de estándares internacionales para la normalización (ISO) es una red mundial que identifica cuáles normas internacionales son requeridas por el comercio, los gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial (ISO, sf).

Por lo anterior se tendrá como referencia la norma ISO/IEC 27035 gestión de incidentes de seguridad de la información para ayudar a fortalecer el actuar de la corporación en caso de la materialización de un riesgo.

1.2 **Formulación del problema**

¿El diseño de un plan de respuesta a incidentes de seguridad de la información teniendo como referencia la norma ISO/IEC 27035, puede contribuir a mejorar la seguridad de la información para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE?

1.3 **Objetivos**

1.3.1 Objetivo General. Diseñar un plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE, teniendo como referencia la norma ISO/IEC 27035.

1.3.2 Objetivos Específicos. Diagnosticar el estado actual de respuesta a incidentes de la caja de compensación familiar de Norte de Santander, COMFANORTE.

Realizar el análisis de riesgos y clasificación de incidentes de seguridad para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE.

Documentar plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE, teniendo como referencia la norma ISO/IEC 27035.

1.4 **Justificación**

La seguridad de la información es un aspecto muy importante debido a que reduce los riesgos en la disponibilidad, integridad y confidencialidad de la información uno de los activos más significativos para una organización, ya que cualquier incidente generado por algún agente interno o externo puede afectarla, Costas (2014) afirma:

> La seguridad de la información consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera en que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea

> posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. (p. 19).

Teniendo en cuenta que los equipos informáticos y los sistemas de información ya están siendo incorporados como un área de la empresa y que así como crece la información también aumentan los riesgos de seguridad, las entidades deben contar con controles para blindar los datos pero también deben tener un plan de respuesta que trate los incidentes de seguridad de la información que minimice el impacto a la Caja de Compensación Familiar en caso que fallen los controles y permita aprender de cada situación que se presente referente a seguridad de la información. Según (Georgia, 2003): "Las organizaciones han entendido que si los mecanismos de protección implementados fallan, es necesario contar con procesos estructurados y personal especializado que maneje los incidentes de seguridad de información y restablezca los sistemas en el menor tiempo posible". Por lo anterior se debe contar con un plan de respuesta ante incidentes, que le garantice una acción rápida ante cualquier suceso conocido o desconocido a las corporaciones, no siendo ajena a esta realidad la Caja de Compensación Familiar de Norte de Santander, COMFANORTE.

El proyecto del diseño de un plan de respuesta incidentes de seguridad de la información para la caja de compensación familiar de Norte de Santander, COMFANORTE tiene como finalidad mitigar el riesgo cuando sea materializado para que no se vea afectada la continuidad del negocio.

Del mismo modo en Colombia desde el 2008 el ministerio de comunicaciones documentó como estrategia de gobierno en línea el diseño de un equipo de respuesta ante incidentes de seguridad pero según el foro para respuesta a incidentes y equipos de seguridad (FIRST, 2017) existen en el país 8 CSIRT oficiales inscritos capacitados y en operación, por lo tanto también se pretende forjar un precedente de investigación que sirva de premisa a futuras indagaciones que

sobre la materia se desarrollen, para de esta forma facilitar el diseño e implementación de planes y equipos de respuesta ante incidentes.

1.5 **Hipótesis**

Con este estudio es importante diseñar un plan de respuesta ante incidentes de seguridad de la información basado en la norma ISO/IEC 27035 que mejorará los protocolos de respuesta ante cualquier tipo de ataque, provocará un conjunto de alertas que con la intervención del ISIRT-ERISI (Equipo de respuesta ante incidentes de seguridad de la información) tendrán el tratamiento adecuado y se podrá retroalimentar a futuros incidentes. Así se busca proteger y asegurar la información para garantizar su integridad, confidencialidad y disponibilidad, para ello es esencialmente significativo implementar los controles preventivos de seguridad más idóneos que protejan la información de las amenazas a las que pueda estar expuesta.

1.6 **Delimitaciones**

1.6.1 Geográficas: la presente investigación se realizó en las instalaciones físicas de la Caja de Compensación Familiar de Norte de Santander, COMFANORTE ubicada en Cúcuta, Norte de Santander, Colombia.

1.6.2 Temporales: El desarrollo del proyecto se realizará en tres (3) meses.

1.6.3 Conceptuales: Para la realización de ésta Investigación se tendrá en cuenta los siguientes conceptos: Seguridad de la información, incidente de seguridad de la información, equipo de respuesta a incidentes de seguridad de la Información ISIRT, ataque, vulnerabilidad, riesgo. Es necesario tener un conocimiento de la norma ISO/IEC 27035.

1.6.4 Operativas: Solo se realizará el diseño del plan de respuesta a incidentes para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE. Los posibles inconvenientes en el desarrollo de la investigación son: a) Inoportunidad en la entrega de

información por parte de la Caja de Compensación Familiar y b) Ausencia del personal de la caja de compensación cuando se realicen las visitas para la recolección de la información.

Capítulo 2. Marco Referencial

2.1 Marco histórico

2.1.1 Antecedentes. En la actualidad cuando se presentan incidentes de seguridad en una organización se recurre a personas especializadas, herramientas informáticas, consultas en línea o cualquier otro medio para dar solución, todas estas ayudas a las que se tiene acceso actualmente son el resultado de incidentes de seguridad que motivaron su aparición. En 1988 el "Gusano Morris" afectó Internet siendo el primer Malware que se replicara a 6.000 servidores de los 60.000 existentes en ese momento, lo que motivó la creación del primer Equipo de Emergencias ante Emergencias Informáticas (CERT, por su siglas en inglés) , poco después se creó el grupo de Asesoramiento de Capacidad de incidente informático (CIAC), a partir de este momento se tuvo en cuenta por parte del departamento de defensa de Estados Unidos el tema de la seguridad informática y encargó a la universidad de Carnegie Mellon la tarea la creación de un equipo CERT.

Un año después en 1989 se produjo el incidente del "Gusano WANK" en las oficinas de la NASA en GreenBelt Maryland que pretendía protestar en contra del uso de energía nuclear en los satélites y naves, lo cual aceleró la necesidad de comunicación y colaboración entre los CERT. Debido a lo anterior en 1990 se crea el foro de respuesta a incidentes y equipos de seguridad (FIRST, por sus siglas en inglés), el cual no ha dejado de crecer con las diferentes y cambiantes necesidades, hoy en día es la principal organización y líder mundial reconocida en respuesta a incidentes tanto reactivos como proactivos. Este foro fomenta la cooperación, el intercambio de información y estimula la reacción rápida a incidentes de seguridad.

En 1992 SURFNET creó el primer CSIRT de Europa el SURFNET-CERT, estos equipos experimentaron inconvenientes de diversa índole tales como zona horaria, lengua, estándares,

entre otros, a pesar de esto los equipos de respuesta a incidentes y seguridad continúan formándose en todo el mundo, cubriendo una serie de circunscripciones de países enteros, a organizaciones multinacionales. Los miembros FIRST se componen de equipos de una amplia variedad de organizaciones, incluyendo los ámbitos educativo, comercial, gobierno y militares. En 2002, Internet había crecido de 60.000 sistemas de computadora central a 150 millones en casi todos los países del mundo. Muchas compañías ahora confían en Internet en sus transacciones comerciales diarias.

Debido a que las instituciones tienen diferentes medios para almacenar información ya sea impreso o digital aparece el concepto de ISIRT, como se describe en la normaISO/IEC 27035: "El ISIRT, es una función organizacional que abarca el proceso para atender incidentes de seguridad de la información y se enfoca principalmente en incidentes relacionados con TI". (Organización internacional de normalización, [ISO], 2011**)**

Debido a la variedad de casos de incidentes de seguridad han aparecido grupos con características similares que varían ligeramente en su propósito, actualmente existen otras siglas usadas para el manejo de incidentes. Las siguientes siglas de uso común tienen un significado similar al del ISIRT, aunque no exactamente igual, según la norma ISO/270035, 2001:

> CERT "Equipo de respuesta ante emergencias de tecnología de información; se enfoca principalmente en incidentes de tecnología de información y comunicaciones y CSIRT "Equipo de respuesta a incidentes de seguridad de tecnología de la información; es una organización de servicio responsable de recibir, examinar y responder a reportes y actividades de incidentes de seguridad de tecnología de la información. (Organización internacional de normalización, [ISO], 2011)

Los Antecedentes son otros estudios relacionados a la investigación que se está desarrollando y que presenten aportes a ésta, su importancia radica en que indican un punto de referencia del conocimiento acerca de un tema específico de investigación. En este trabajo se

tomaron los antecedentes a nivel internacional y nacional con el fin de apoyar el diseño de un plan de respuesta a incidentes de seguridad de la información:

***2.1.1.1 Antecedentes Internacionales*.** Roberto Omar Andrade Paredes, en su proyecto de grado de maestría en gerencia de redes y telecomunicaciones con título "Diseño y Dimensionamiento de un Equipo De Respuesta Ante Incidentes De Seguridad Informática (Csirt) Para La Escuela Politécnica Del Ejército" para la Escuela Politécnica del Ejército de Ecuador. Propone presentar el marco teórico sobre el que se sustenta el estudio de factibilidad para la implementación del CSIRT de la ESPE. Inicialmente se realiza un análisis de la situación actual de los ataques informáticos y códigos maliciosos presentados en el último año a nivel latinoamericano sobre el que se respalda la necesidad de la implementación del CSIRT.

2.1.1.2 Antecedentes Nacionales. Yesid Alberto Tibaquira Cortes, en su proyecto de especialización en seguridad informática con título Metodología de Gestión de Incidentes de Seguridad de la Información y Gestión de Riesgos Para la Plataforma SIEM de una Entidad Financiera Basada en la Norma ISO/IEC 27035 e ISO/IEC 27005 para la UNAD, Bogotá D.C**.** Donde define un modelo de gestión de incidentes de seguridad de la información y de gestión de riesgos sobre estos incidentes, que son detectados o derivados de la implementación y operación de una herramienta SIEM (Correlacionador de Eventos de Seguridad). La definición de los modelos de gestión se realizó bajo las normas ISO 27035 para incidentes de seguridad y 27005 para la gestión de riesgos.

2.2 **Marco conceptual**

2.2.1 Ataque. Según la norma NTC-ISO/IEC 27000 se define como: "Tentativa de destruir, exponer, alterar, inhabilitar, robar, o acceder sin autorización o hacer uso no autorizado de un activo". (ICONTEC, 2017, p.1**).** Este puede ser realizado por un individuo o un grupo de

individuos, los cuales se organizan para causar daños aprovechando alguna vulnerabilidad, estos ataques por lo general van dirigidos hacia las empresas y puede ser con el objetivo de obtener lucro económico, espionaje, reputación, entre otros.

2.2.2 Evento de seguridad de la información. Como se describe en la norma NTC-ISO/IEC 27001: **"**Ocurrencia identificada de un estado del sistema, servicio o la red indicando un posible incumplimiento a la Política de seguridad de la información o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la información". (ICONTEC, 2013, p.3**)**

2.2.3 Incidente de seguridad de la información. Según la norma NTC-ISO/IEC 27001:"Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de negocio y amenazar la seguridad de la información". (ICONTEC, 2013, p.3**).** Estos incidentes pueden ser deliberados o accidentales, ya que son causados por un error o por causa de un ataque, los cuales pueden traer consecuencias tales como modificación o divulgación de información sensible, hurto o robo.

2.2.4 Gestión de incidentes de seguridad de la información. Según la norma NTC-ISO/IEC 27000: "Procesos para detectar, informar, evaluar, responder y aprender de incidentes de seguridad de la información". (ICONTEC, 2017, p.6**)** Para la gestión adecuada de estos incidentes se debería establecer responsabilidades y procedimientos, aplicar un proceso de mejora continua, realizar una adecuada recolección de evidencias, realizar revisiones pasados los incidentes, diligenciar los respectivos informes, todos los empleados deben informar cualquier incidente de seguridad a tiempo y se debe dar a conocer los resultados post-incidente.

2.2.5 ISIRT – ERISI. (Information Security Incident Response Team – Equipo de Respuesta a Incidentes de Seguridad de la Información), en el compendio de sistema de gestión de la seguridad de la información se define como: **"**equipo de miembros de la organización, que son de confianza y tienen las habilidades adecuadas para manejar los incidentes de seguridad de la información durante su ciclo de vida. En ocasiones este equipo puede ser complementado por expertos externos" (ICONTEC, 2009, p.3**)**, este equipo puede ser virtual o permanente, ya que los integrantes pueden tener otras ocupaciones y ser convocados en el momento de presentarse los incidentes de seguridad o tener presencia permanente en una oficina de la organización.

2.2.6 Riesgo residual. Según la norma NTC-ISO/IEC 27001: "Riesgo que queda después de tratamiento del riesgo" (ICONTEC, 2013, p.3**)**.

2.2.7 NAP. Es un punto de conexión nacional de las redes de las empresas que proveen el servicio de acceso de Internet en Colombia, con el cual se logra que el tráfico de Internet que tiene origen y destino en nuestro país, utilice solamente canales locales o nacionales. NAP COLOMBIA permite el uso eficiente de la red de telecomunicaciones de nuestro país, produce una mejora significativa en el servicio de las empresas que integran el NAP y reduce los costos por el uso de los enlaces internacionales. (NAP Colombia, s/f)

2.2.8 Análisis Forense digital. "Conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial" (López Miguel, 2007, p. 5). Este análisis se realiza con el objetivo de extraer información importante de cualquier medio de almacenamiento magnético intentando buscar un patrón e información que puede estar oculta y dificulta su recuperación, todo esto se realiza con herramientas aprobadas,

ya que por el hecho de ser información sensible, podría ser utilizada como evidencia ante los entes correspondientes.

2.2.9 Vulnerabilidad. Es la debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas y como resultado puede sufrir cualquier tipo de daño, ya que no se tienen todas las capacidades para hacer frente al peligro y tampoco de recuperarse, puede presentarse por cierto grado de aislamiento, presiones, la falta de preparación, entre otros.

2.2.10 Gestión del riesgo. Según la norma NTC-ISO/IEC 27001: "Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo". (ICONTEC, 2013, p.3**).**

2.2.11 Auditoria. Es principalmente, estudiar y analizar toda la documentación y sistemas de información relativos a una empresa, institución u organismo, esta auditoría ayuda a determinar si la información que ofrece la entidad u área objeto de estudio esta correlacionada con la situación real de la misma, y para determinar si sus sistemas de información son los correctos para el funcionamiento de la misma y la consecución de sus objetivos. (Erazo y Moran, 2015)

2.3 Marco contextual

La caja de compensación familiar de Norte de Santander, COMFANORTE es una corporación de carácter privado, sin ánimo de lucro, que cumple funciones de seguridad social, con personería jurídica, otorgada por el ministerio de justicia mediante resolución N° 2894 de octubre de 1957. La sede principal de COMFANORTE está ubicada en la ciudad de Cúcuta

COMFANORTE es una entidad de redistribución económica y naturaleza solidaria, creada para mejorar la calidad de vida de las familias de los trabajadores de Norte de Santander, mediante la gestión y entrega, en subsidios y servicios, recibiendo el 4% de los aportes de

seguridad social que pagan los empleadores sobre el salario de sus trabajadores permanentes a cargo.

El objetivo de la caja de compensación familiar es ayudar a los empleados del departamento de Norte de Santander en su desarrollo humano, familiar, laboral y social y contribuir a mejorar la calidad de vida de la comunidad en general. Entre los beneficios que entrega la caja de compensación se pueden encontrar: salud, educación, recreación, cultura, turismo, deporte, vivienda, crédito y microcrédito.

2.4 **Marco teórico**

La Seguridad de la Información, de acuerdo a la norma ISO 27000:20146, se define como la preservación de la confidencialidad, integridad y disponibilidad y tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada.

El aumento de la implementación de herramientas de seguridad informática ha crecido con la misma rapidez que las diferentes técnicas de ataque informático. Sin embargo, el tener la mejor herramienta, no asegura una protección 100% segura de la información en la corporación, siempre habrá un riesgo residual que de materializarse puede afectar la continuidad del negocio y afectara clientes y proveedores en la prestación de los servicios.

La norma GTC-ISO/IEC-27035:2012, denominada Gestión de incidentes de Seguridad de la información fue publicada en el año de 2011 por la ISO e implementada por ICONTEC en el año 2012, Provee un enfoque estructurado y planificado donde específica los lineamientos para una efectiva gestión de incidentes de seguridad.

En un Sistema de Gestión de Seguridad de la Información (SGSI) la implementación de políticas y controles no garantizan una total protección de la información y de los sistemas que la

procesan, se encuentra un riesgo residual, el cual se puede materializar por la existencia de alguna vulnerabilidad por pequeña que sea y donde los controles implementados son inefectivos. Para estos tipos de casos, es necesario implementar un sistema de administración de aquellos incidentes de seguridad que puedan hacer realidad este riesgo residual y que garantice una rápida respuesta y control eficaz. La norma GTC-ISO/IEC-27035, se encuentra organizada en 5 fases (ICONTEC, 2012):

Planear y Preparar: En esta fase se planea y se define la política de gestión de incidentes de seguridad, alineada a la política de seguridad de la información y de análisis de riesgos, además de concientizar a la gerencia. Se debe definir un equipo de respuesta a incidentes de seguridad de la información.

Detección y Reporte: Es la detección y el registro o reporte del incidente, donde se realiza la recolección asociada al incidente. Es la primera fase del proceso operacional de la gestión.

Evaluación y Decisión: Es la evaluación de la información recolectada y un análisis para validar si el evento reportado es un incidente de seguridad.

Respuesta: Respuesta al incidente de seguridad, con el análisis forense si fue necesario realizarlo, dependiendo de la decisión tomada en la fase de Evaluación y Decisión, y la respectiva entrega del reporte a las personas involucradas.

Lecciones Aprendidas: Se identifican las lecciones aprendidas del incidente de seguridad y la mejora del proceso o del SGSI. De ser necesario validar el proceso de gestión de incidentes para implementar mejoras, debido a la lección aprendida del resultado del incidente de seguridad.

Para la conformación del ISIRT se opta por aplicar el procedimiento publicado por la Agencia Europea de seguridad en la redes y de la información ENISA Como crear un CSIRT paso a paso, el cual propone la estrategia de creación desde varias perspectivas (ENISA, 2006):

Ventajas de tener un CSIRT

Descripción de los diferentes tipos de CSIRT

Servicios posibles de un CSIRT

Análisis del grupo de clientes atendidos y declaración de servicios

Desarrollar un plan comercial

Definir Estructura orgánica

Uso y equipamiento de la oficina

Búsqueda de colaboración con otros CSIRT

2.5 **Marco legal**

En esta sección se presenta brevemente el marco normativo nacional a lo relacionado con el objeto de estudio:

2.5.1 Circular Externa Superintendencia de Industria y comercio 02 del 3 de noviembre de 2015. Por la cual la Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el registro nacional de bases de datos a partir del 9 de noviembre de 2015. (Consejo Nacional de Política Económica y Social CONPES 3854, 2016, p. 78)

2.5.2 Decreto 1074 de 2015. (Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo) Por medio del cual se expide el Decreto único reglamentario del sector de comercio, industria y turismo, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Compilación de los Decretos 2364 de 2012 Firma electrónica y 333 Habeas data de 2014, entre otros. (CONPES 3854, 2016, p. 77)

2.5.3 Ley 1273 de 2009. En el cual se modifica el Código Penal se "crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." (Congreso de Colombia, 2009). La ley 1273 de 2009 añade dos nuevos capítulos al Código Penal Colombiano: el primero referente a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y el segundo referente a los atentados informáticos y otras infracciones.

2.5.4 Decreto 4485 de 2009. Se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g):

> Establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder.

2.5.5 Ley 87 de 1993. Artículo 2, ítem f) "Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos". (Congreso de Colombia, 1993).

Capítulo 3. Diseño Metodológico

3.1 Tipo de investigación

Para el desarrollo del presente proyecto, se llevará a cabo una investigación descriptiva con enfoque cuantitativo, puesto que permitirá de modo sistemático definir, clasificar, catalogar o caracterizar el objeto de estudio. En esta fase se diseñaran los diferentes instrumentos seleccionados de recolección de información, se aplicaran, tabularan y procederá al análisis de la información necesaria para el cumplimiento de los objetivos. Con la aplicación de este método de investigación se pretende obtener un diagnóstico situacional de una caja de compensación familiar en el departamento de Norte de Santander.

Adicionalmente se utilizará el ciclo PHVA de mejora continua que se basa en 4 fases: planear, hacer, verificar y actuar adoptado por la familia de normas de la Organización Internacional de Normalización (ISO International Organization for Standardization).

3.2 Población y Muestra

La población objeto de estudio está conformada por los responsables de los 16 procesos existentes en la caja de compensación familiar de Norte de Santander, COMFANORTE, los 2 coordinadores del área de gestión tecnológica y el coordinador de control interno.

Tabla 1.

Población objeto de estudio

Proceso	Cargo
Planeación	Responsable del proceso Coordinador de Control Interno
Gestión Comercial y Mercadeo	Responsable del proceso
Subsidio	Responsable del proceso
Recreación	Responsable del proceso
Vivienda y Crédito Social	Responsable del proceso
Educación	Responsable del proceso
Salud	Responsable del proceso

Gestión Social	Responsable del proceso
Gestión Humana	Responsable del proceso
Gestión jurídica	Responsable del proceso
Gestión Administrativa	Responsable del proceso
Gestión Contable	Responsable del proceso
Gestión Financiera	Responsable del proceso
Gestión Tecnológica	Responsable del proceso Responsable del proceso Coordinador de sistemas de información Coordinador de Infraestructura tecnológica
Gestión de Auditorias	Responsable del proceso

Fuente. Estructuras Caja de Compensación Familiar

Para el desarrollo del proyecto de investigación se trabajará con el 100% de la población es decir 19 personas.

3.3 **Técnicas de recolección de la información**

Para la ejecución del estudio de investigación una vez definido el enfoque, se seleccionara el instrumento adecuado, con el fin de aplicarlo y preparar los objetos de estudio para ser analizados como lo enumera Fernández y Baptista (2003) la recopilación de datos radica en:

> Una vez que seleccionamos el diseño de investigación apropiado y la muestra adecuada... la siguiente etapa consiste en recolectar los datos pertinentes sobre las variables...u objetos involucrados en la investigación. Recolectar los datos implica tres actividades estrechamente vinculadas entre sí: 1.Seleccionar un instrumento o método de recolección entre los disponibles en el área de estudio en el cual se inserte nuestra investigación o desarrollar uno. Este instrumento debe ser válido y confiable, de lo contrario no podemos basarnos en sus resultados.2.Aplicar ese instrumento o método para recolectar datos. Es decir, obtener las observaciones, registros o mediciones de variables...u objetos que son de interés para nuestro estudio. 3. Preparar observaciones, registros y mediciones obtenidas para que se analicen correctamente. (Bisquerra, 2009 p. 149)

Las técnicas e instrumentos de recolección de información que se utilizarán son la entrevista, encuesta, lista de chequeo y revisión documental.

3.3.1 Fuentes primarias. Las fuentes primarias en el presente proyecto son entrevistas y encuestas a funcionarios de la caja de compensación familiar, observación directa y revisión de

información documentada en la organización pertinente al trabajo de investigación y normas ISO/IEC.

3.3.2 Fuentes secundarias. Para el presente proyecto se consultaran fuentes secundarias como revistas especializadas, artículos y trabajos de investigación del objeto de estudio.

3.4 Análisis de datos

3.4.1 Seguimiento metodológico

3.4.1.1 Objetivo específico N° 1. Diagnosticar el estado actual de respuesta a incidentes de la caja de compensación familiar de Norte de Santander, COMFANORTE. Se realizará a través de una auditoria pasiva utilizando como criterio la norma ISO/IEC 27035. Para alcanzar el objetivo propuesto se plantea el desarrollo de las siguientes actividades: a) Recopilar información organizacional de la corporación (misión, visión, objetivos, estructura orgánica, procesos, etc.) b) Diseñar plan de auditoria e instrumentos para recolección de información del tratamiento de incidentes en la caja de compensación. c) Aplicar Instrumentos, d) Análisis y evaluación de la información recolectada, e). Generar informe de auditoría.

***3.4.1.2 Objetivo Especifico N° 2. Realizar el análisis de riesgos y clasificación de incidentes de seguridad para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE*.** Para el logro del objetivo propuesto se definieron una serie de actividades: a) Identificar los riesgos para la seguridad de la información en la corporación, b) Estimación de los riesgos de seguridad de la información en la caja de compensación, c)Evaluación de los riesgos y d)Clasificación de incidentes de seguridad.

3.4.1.3 Objetivo Especifico N° 3. Documentar plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE. Teniendo como referencia la norma ISO/IEC 27035. Para alcanzar el objetivo propuesto se implementaron las siguientes actividades: a) Identificar alcance y objetivos del plan de incidentes y b). Crear plan de respuesta a incidentes de seguridad de la información basada en la norma ISO/IEC 27035.

Capítulo 4. Presentación de Resultados

Tabla 2

Objetivos propuestos y actividades a desarrollar

Objetivo	Actividades
Diagnosticar el estado actual de respuesta a incidentes de la caja de compensación familiar de Norte de Santander, COMFANORTE. Se realizará a través de una auditoria pasiva utilizando como criterio la norma ISO/IEC 27035	1. Recopilar información organizacional de la corporación (misión, visión, objetivos, estructura orgánica, procesos, etc.) 2. Diseñar programa de auditoria e instrumentos para recolección de información del tratamiento de incidentes en la caja de compensación. 3. Aplicar Instrumentos, 4. Análisis y evaluación de la información recolectada 5. Generar informe de auditoria
Realizar el análisis de riesgos y clasificación de incidentes de seguridad para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE	1. Identificar los riesgos para la seguridad de la información en la corporación 2. Estimación de los riesgos de seguridad de la información en la caja de compensación 3. Clasificación de incidentes de seguridad
Documentar plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE, teniendo como referencia la norma ISO/IEC 27035	1. Identificar alcance y objetivos del plan de incidentes **2.** Crear plan de respuesta a incidentes de seguridad de la información basada en la norma ISO/IEC 27035

Nota. La tabla muestra la relación entre los objetivos propuestos para el proyecto y las actividades a desarrollar.

Fuente. Autores del proyecto

4.1. Diagnosticar el estado actual de respuesta a incidentes de la caja de compensación familiar de Norte de Santander, COMFANORTE.

4.1.1 Caja de Compensación Familiar del Norte de Santander Comfanorte. La Caja de Compensación Familiar del Norte de Santander COMFANORTE, es una corporación de carácter privado, sin ánimo de lucro, que cumple funciones de seguridad social, con personería jurídica, otorgada por el Ministerio de Justicia mediante la Resolución No 2894 de octubre 18 de 1957.

Siendo su objeto social propender por el alivio de la carga económica que representa el sostenimiento de la familia como núcleo básico de la sociedad, a través de la capacitación y generación de recursos que destina a contribuir a la superación de las necesidades de los trabajadores de menores ingresos dentro del marco de la ley. (Comfanorte, sf)

La Caja tiene por objeto el recaudo de los aportes y el pago del subsidio familiar como prestación social pagadera en dinero, especie y servicios a los trabajadores de medianos y menores ingresos, en proporción al número de personas a cargo, y cuyo objetivo fundamental consiste en el alivio de las cargas económicas que representan el sostenimiento de la familia como núcleo básico de la sociedad. . (Comfanorte, sf)

4.1.2 Modelo del negocio. El desarrollo de modelo del negocio es la representación de diferentes elementos de un negocio que permite entender fácilmente su propósito, los productos o servicios que presta, objetivos estratégicos, entre otros como lo afirma Osterwalder (2004):

> El modelo del negocio es una herramienta conceptual que, mediante un conjunto de elementos y sus relaciones, permite expresar la lógica mediante la cual una compañía intenta ganar dinero generando y ofreciendo valor a uno o varios segmentos de clientes, la arquitectura de la firma, su red de aliados para crear, mercadear y entregar este valor. (p.15)

El modelo del negocio de la Caja de Compensación Familiar permite representar de forma abstracta su funcionamiento y todos los elementos necesarios para lograr los objetivos estratégicos, proporcionando un mayor conocimiento y claridad de la corporación.

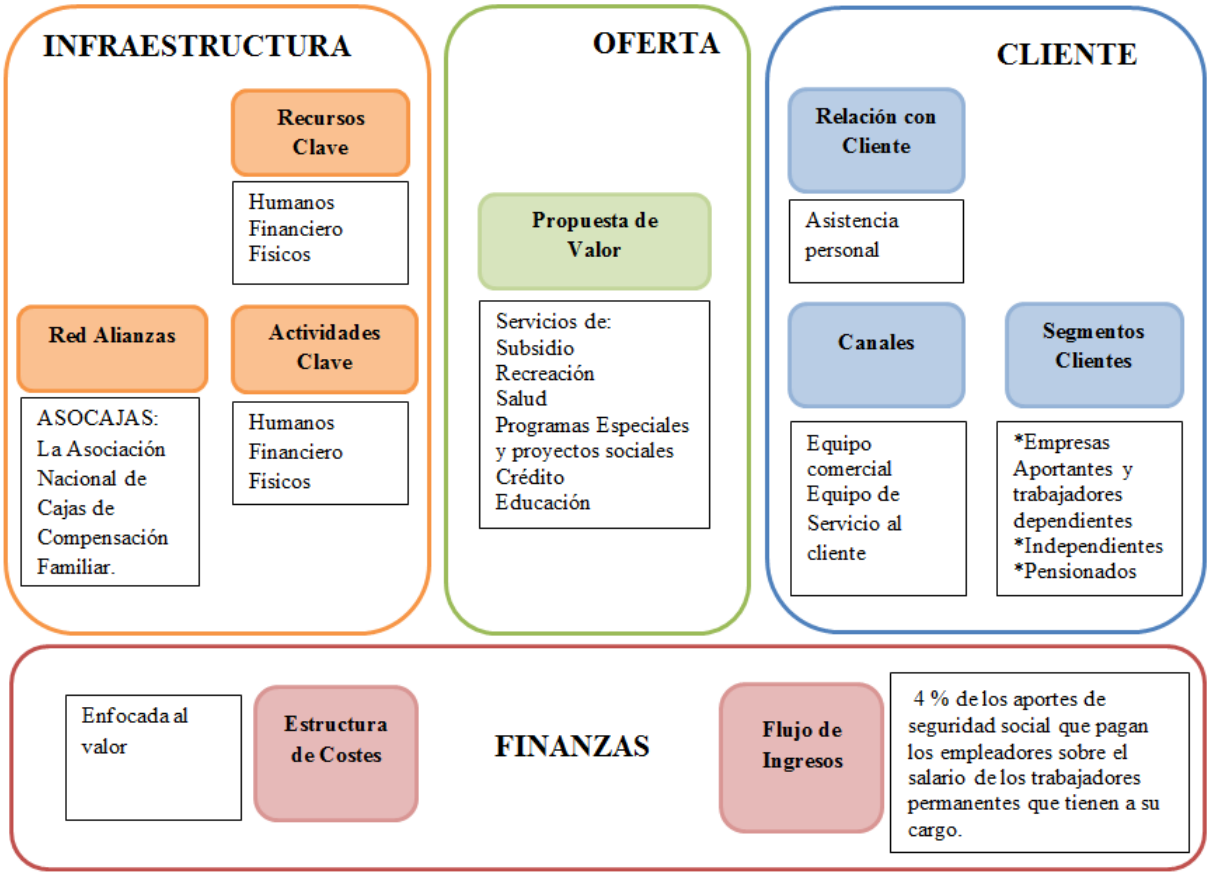


Figura 1. Modelo del Negocio

Fuente. Autores del proyecto

4.1.3 Modelo de objetivos. La caja de compensación familiar del Norte de Santander describe su objetivo general en la misión y la Visión de la corporación.

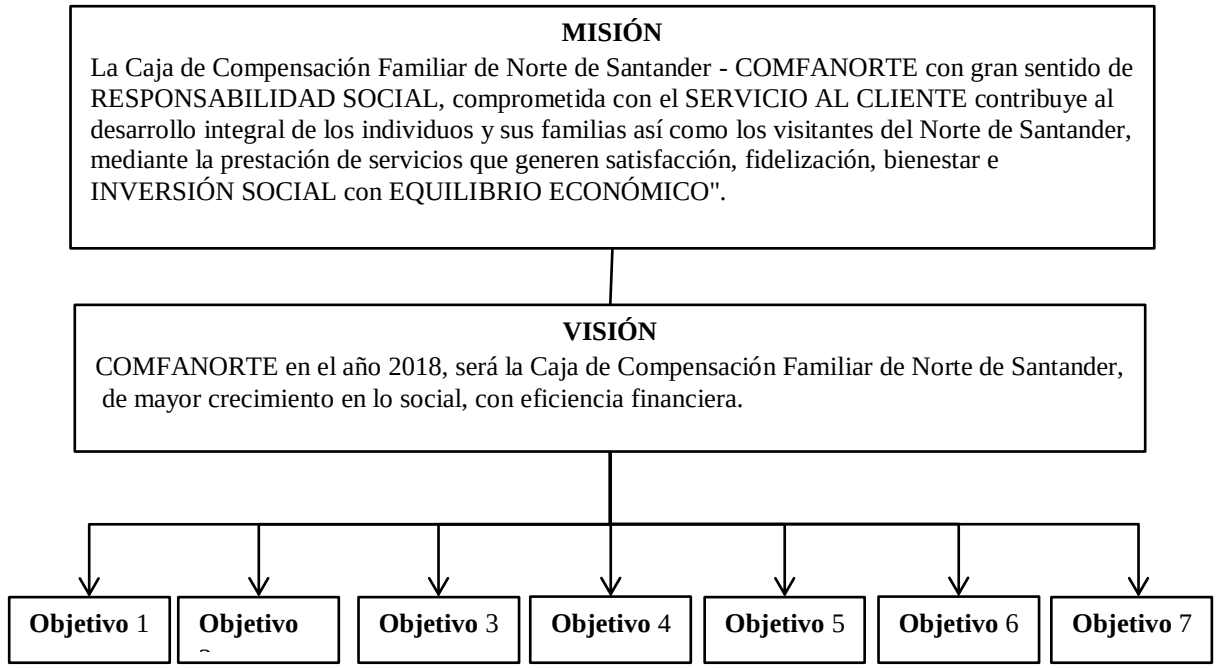


Figura 2. Misión, Visión y objetivos.

Fuente. Direccionamiento estratégico de Comfanorte (2014-2018)

Los objetivos definidos en la planificación estratégica de Comfanorte según lo descrito en el diagrama son:

1. Construir la iniciativa de Responsabilidad Social alineado al pacto global de la caja.
2. Beneficiar a mayor población afiliada a través de la prestación de programas y servicios de la Caja.
3. Eficiencia en la administración de recursos
4. Bienestar del Afiliado, su familia y demás Partes Interesadas.
5. Estructurar el Sistema Integral de Gestión: Calidad, Seguridad y Salud en el Trabajo, Medio Ambiente y Seguridad del Paciente.
6. Alinear la infraestructura física y tecnológica como respaldo a la prestación de servicios.

7. Cultura organizacional en la gestión integral por procesos.

4.1.4 Estructura Orgánica. La estructura general de la caja fue aprobada por el consejo directivo mediante acta 1021 del 21 de febrero de 2017.

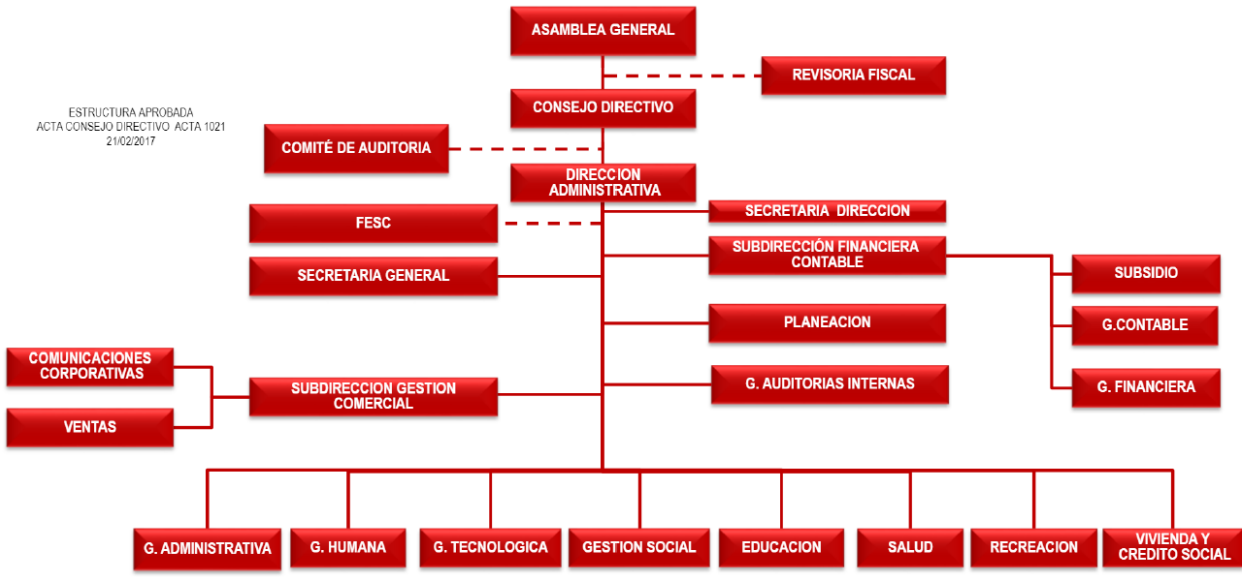


Figura 3. Estructura orgánica de la caja de compensación.

Fuente. Direccionamiento Estratégico – Planeación estratégica Comfanorte.

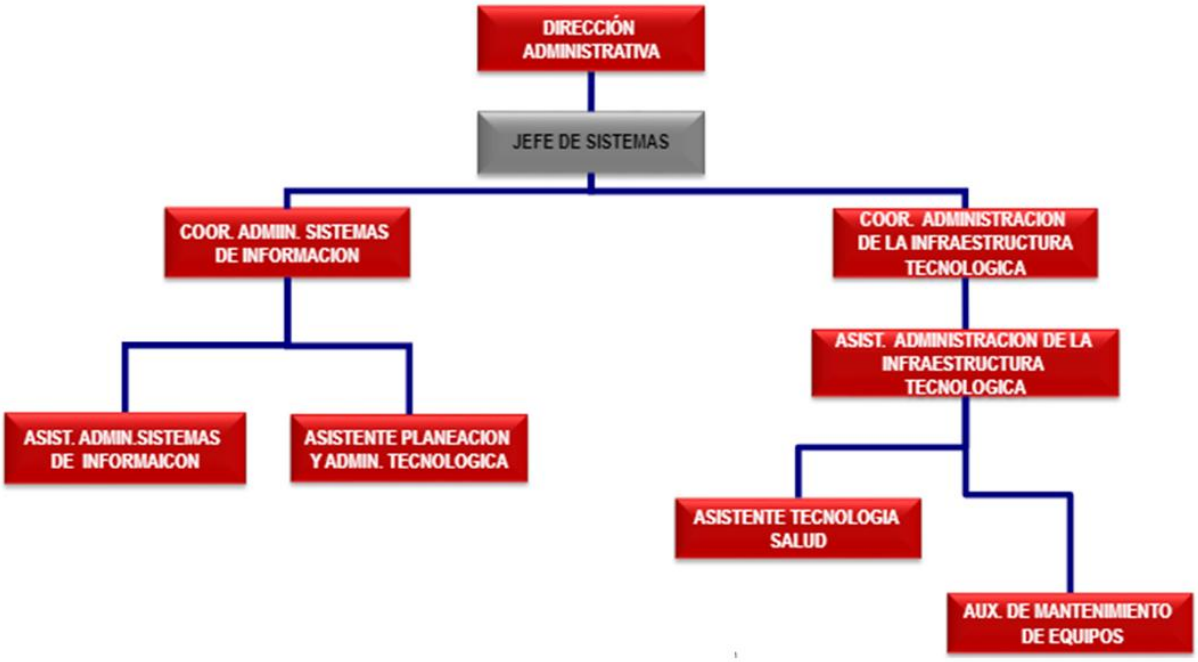


Figura 4. Estructura Orgánica del proceso Gestión Tecnológica

Fuente. Procedimiento - Estructura Gestión Tecnológica. GH-id-Pr-15

4.1.5 Modelo de procesos de negocios. En este modelo se representó el hacer de la caja de compensación describiendo las actividades que permiten lograr los objetivos específicos descritos. De conformidad con el direccionamiento estratégico 2014 - 2018 de la corporación, COMFANORTE presta los siguientes servicios:

- Subsidio: cuota monetaria, subsidio en especie, subsidio de vivienda, subsidio por la muerte de una Persona a cargo del afiliado, servicio público de empleo.

- Recreación: servicio de alojamiento en sus sedes vacacionales, turismo social, eventos deportivos, eventos recreativos, Ecoparque, alquiler de instalaciones para conferencias, seminarios, congresos, alimentos y bebidas.

Salud: IPS: Clínica Metropolitana IPS.

Programas especiales y proyectos sociales: Dirigidos a la población más vulnerable; atención a la infancia, beneficios para personas entre 60 y 85 años, jornada complementaria para niños escolarizados entre 5 y 15 años, asistencia a niños discapacitados y Adulto Mayor.

Crédito: Préstamos de libre inversión que comprende diferentes destinos o modalidades: turismo, educación, vivienda, compra de cartera, adelanto de subsidio, entre otros.

Educación: Jardín Infantil, Colegio Comfanorte, Instituto Técnico Laboral y Empresarial, Fundación de Estudios Superiores FESC.

4.1.5.1 ***Diagrama de procesos:*** Se realizó revisión a la documentación proporcionada por La Caja de Compensación Familiar, definida en el sistema de gestión 2017 en el cual se definen los principales procesos, sus actividades, procedimientos e instrucciones de trabajo.

En la figura 5 se representa cómo funciona la cadena de valor corporativa y la interacción de los procesos. En la parte superior se observan los procesos Gerenciales de Planeación y Gestión Comercial -Mercadeo que interactúan entre si y dan línea para el trabajo desarrollado en los procesos fundamentales que se observan en el centro de la cadena que son los diferentes servicios que presta la corporación. En la parte inferior se encuentran los procesos de apoyo, los cuales brindan las herramientas necesarias (gestión Humana, gestión Jurídica, gestión administrativa, gestión contable, gestión financiera, gestión tecnológica) para una prestación de los servicios de forma eficiente.

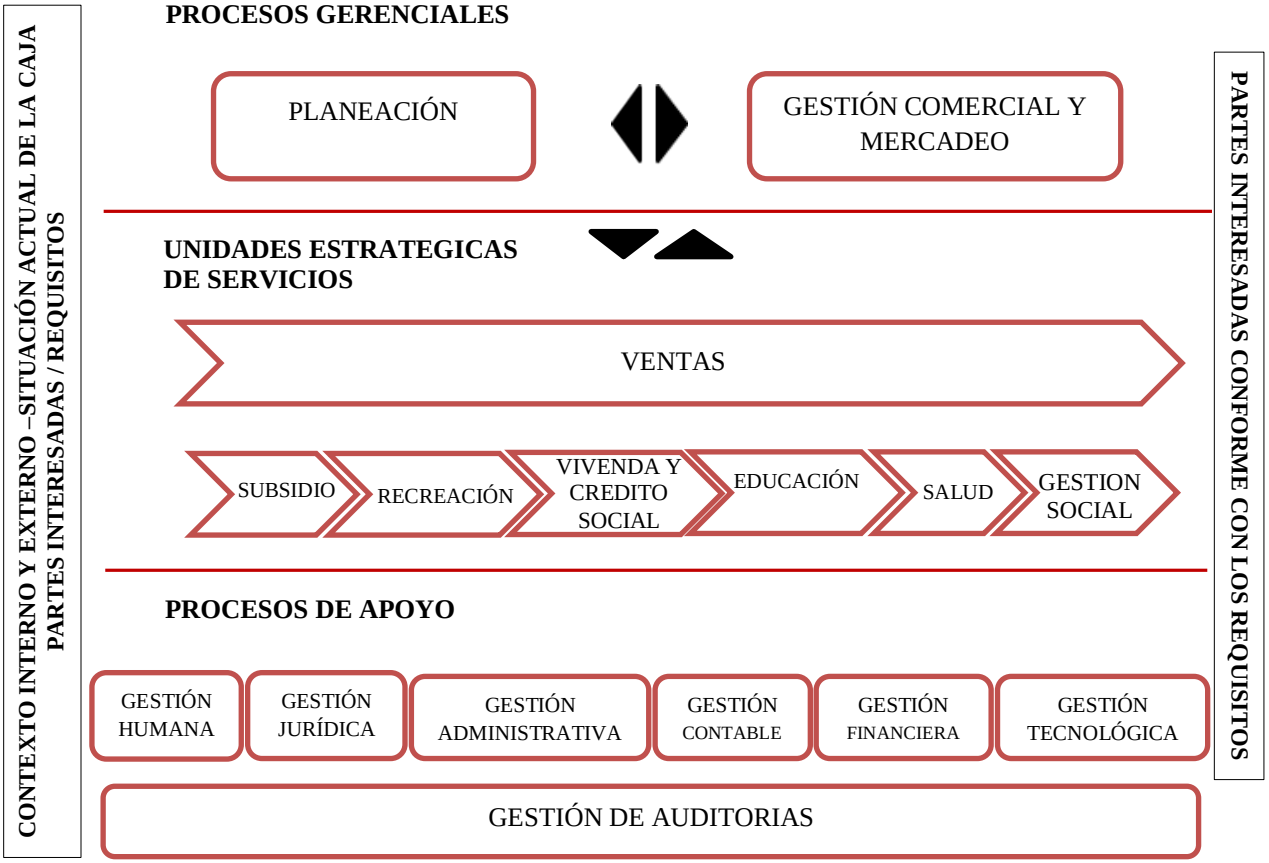


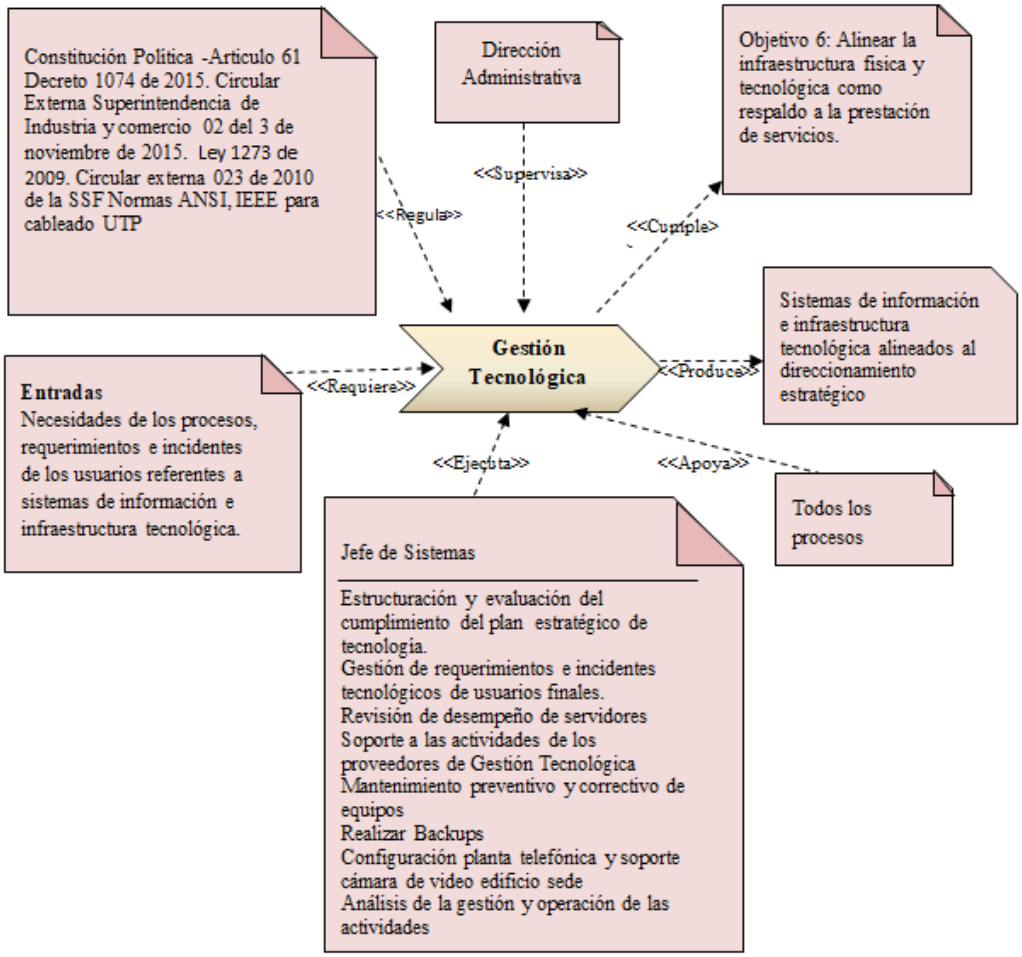
Figura 5. Cadena de valor corporativa

Fuente. Autores del proyecto

Entre los procesos de apoyo se encuentra el proceso de Gestión tecnológica que es el encargado de la gestión de incidentes de la seguridad de la información dentro de la caja de Compensación Familiar.

4.1.5.2 Diagrama de descripción de procesos. Se realizó el diagrama del proceso que tiene establecido dentro de sus funciones la respuesta a incidentes de seguridad de la información, el proceso de apoyo de Gestión tecnológica el cual tiene definido como objetivo Gestionar oportunamente, eficientemente, eficazmente y confiablemente el desempeño de la infraestructura

tecnológica y los sistemas de información alineados al direccionamiento estratégico y en cumplimiento de los requisitos legales vigentes.



SSF: Superintendencia de subsidio Familiar

Figura 6. Proceso Gestión Tecnológica

Fuente. Autores del proyecto

El proceso de Gestión tecnológica está compuesto por dos subprocesos que permiten desempeñar las funciones definidas por la corporación: administración de sistemas de información y administración de Infraestructura Tecnológica.

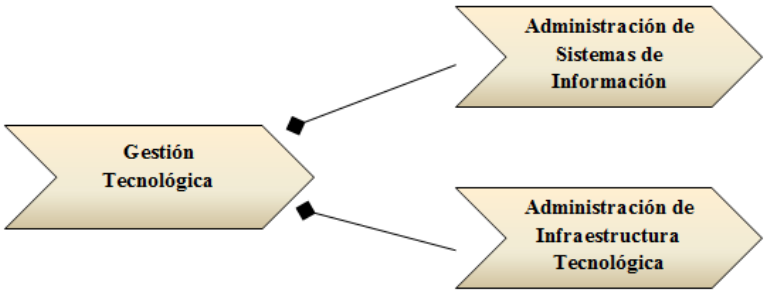


Figura 7. Gestión Tecnológica y sus Subprocesos

Fuente. Autores del proyecto

Administración Sistemas de Información. Gestionar oportunamente, eficientemente, eficazmente y confiablemente el desempeño de los sistemas de información alineados al direccionamiento estratégico. Inicia desde la estructuración del Plan estratégico de sistemas de información hasta generación de los informes de gestión respectivos del subproceso.

Administración Infraestructura Tecnológica. Gestionar oportunamente, eficientemente, eficazmente y confiablemente el desempeño de la Infraestructura tecnológica alineados al direccionamiento estratégico. Inicia desde la estructuración del Plan estratégico de infraestructura tecnológica hasta generación de los informes de gestión respectivos del subproceso.

4.1.6 Auditoría de Sistemas

4.1.6.1 Objetivo. Evaluar el estado actual de la gestión de incidentes de seguridad de la información en la Caja de Compensación Familiar del Norte de Santander.

4.1.6.2 Alcance de la auditoria: Detección, reporte, evaluación, respuesta y gestión a incidentes de seguridad de la información, detección, evaluación y gestión de las vulnerabilidades de la seguridad de la información y resultado de la gestión de incidentes y vulnerabilidades de seguridad de la información.

4.1.6.3 Programa de auditoría. De acuerdo a los resultados obtenidos en la recolección de información que permitió conocer la estructura de la corporación y entendimiento del negocio, se realizó el programa de auditoría donde se incluyen las actividades a desarrollar, fechas y recurso humano necesario para cumplir con el alcance de la auditoria. (Apéndice A).

4.1.6.4 ***Ejecución de la auditoria***. Entre los instrumentos aplicados esta la entrevista al jefe de sistemas, encuesta a los funcionarios del proceso de gestión tecnológica y a jefes de procesos y lista de chequeo para verificar el cumplimiento de buenas prácticas en la respuesta a incidentes de seguridad según la norma GTC ISO/IEC 27035.

Entrevista. De los resultado de la entrevista y de la observación directa se determinó que aunque no se han desarrollado las diferentes etapas que se proponen en la norma ISO 27035 la caja de compensación cuenta con canales para reportar los diferentes incidentes (mesa de servicios, línea interna de telefonía y línea celular), con el soporte de una empresa externa de seguridad informática y un grupo de 6 ingenieros de sistemas y un técnico que pertenecen al proceso de gestión tecnológica; adicionalmente existe un procedimiento documentado para resolver los incidentes presentados en el uso de herramientas tecnológicas. (Apéndice B)

Encuestas. Se aplicaron dos cuestionarios uno a los 7 integrantes del proceso de gestión tecnológica (Apéndice C, D) y el otro a los jefes de procesos de la caja de compensación familiar con base en la norma ISO 27035: 2012. (Apéndice E, F)

Lista de chequeo (Apéndice G)

Pruebas de auditoria. Una vez aplicados los instrumentos de recolección de información que nos proporcionaron datos valiosos para conocer el estado de la gestión de incidentes en la

Caja de Compensación Familiar de Norte de Santander se realizaron pruebas para corroborar la información obtenida. (Apéndice H)

4.1.6.5 ***Informe de auditoría.*** Una vez realizada la auditoria pasiva en la Caja de Compensación Familiar de Norte de Santander evaluando aspectos de acuerdo a la norma GTC ISO/IEC 27035 se evidenció la inexistencia de una política y plan de gestión de incidentes de seguridad de la información, respecto al equipo de respuesta a incidentes que tiene la corporación actualmente se observó que aunque está bien estructurado no hay claridad en la responsabilidades asumidas frente a un incidente, asimismo se evidenció la ausencia de definición de tiempos de respuesta debido a que no se ha realizado la clasificación de incidentes de seguridad. Del mismo modo se comprobó el desconocimiento del manejo de incidentes de seguridad por parte de los funcionarios de la corporación a causa de que no se dan instrucciones ni formación en toma de conciencia de gestión de incidentes y de seguridad informática.

Del mismo modo se recomienda a la corporación para mantener la continuidad en la prestación de los servicios a sus afiliados establecer la gestión de incidentes de seguridad de la información basada en buenas prácticas lo que le permitirá controlar cualquier incidente de seguridad que se presente. (Apéndice K)

4.2 **Realizar el análisis de riesgos y clasificación de incidentes de seguridad para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE**.

Así como se puede observar en la figura 8 el proceso de gestión del riesgo en seguridad de la información tiene varias fases, para el desarrollo de este proyecto solo se contempla llegar al análisis del riesgo.

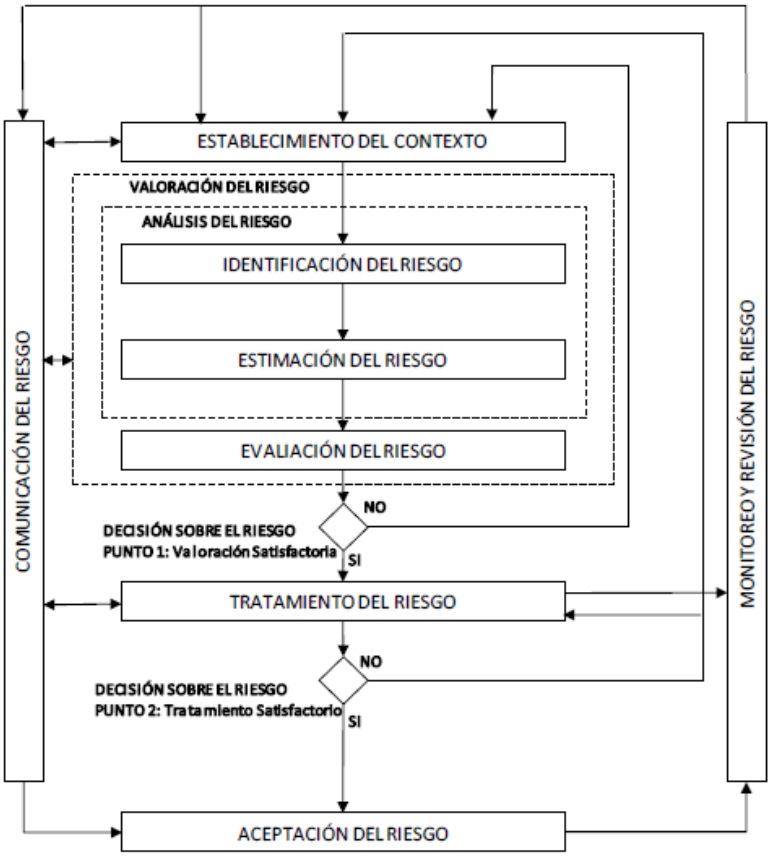


Figura 8. Proceso para la administración del riesgo en seguridad de la información.

Fuente. Tomada de la guía de Gestión de Riesgos. (Mintic pág. 11)

4.2.1 Fase 1 Establecimiento del contexto. En numeral 4.1 se describen las principales características de la caja de compensación familiar, procesos definidos y servicios que presta, igualmente para el subproceso de Gestión Tecnológica de la Caja se sus funciones, procedimientos, infraestructura, personal y servicios que soporta. A continuación se presenta la definición del contexto en función de las características de la caja de compensación familiar, utilizando la matriz DOFA

DOFA	
DEBILIDADES	**AMENAZAS**
• Debilidad en las notificaciones a la población afiliada. • Falta de capacitación • El enfoque está más hacia la rentabilidad social y no hacia el desempeño • No todos los procesos cuentan con tecnología ajustada • Es insuficiente la renovación del portafolio de servicios. • El equipo de fuerza de ventas es insuficiente	• Desconocimiento por parte de los afiliados de los beneficios que ofrece la entidad • Deficiente oferta de software aplicado a las cajas • Bajo crecimiento de nuevas empresas y aumento en la tasa de desempleo en la región • Diversidad de entes de control que vigilan el actuar de las actividades de las Caja de Compensación Familiar y complejidad en la identificación de las competencias de los entes de control.
FORTALEZAS	**OPORTUNIDADES**
• Seguimiento continuo a indicadores de gestión • Experiencia y conocimiento de los procesos • Empresa con alto reconocimiento en el sector. • La Caja cuenta con buenas relaciones en el departamento a través de su participación en programas sociales.	• Grupos interdisciplinarios de las diferentes cajas de Compensación. (Mesa de trabajo de subsidio familiar a través de ASOCAJAS) • Implementar un mejor canal transaccional • para los afiliados y permitir la virtualización • de documentos para acreditar subsidio • familiar • Posibilidad de establecer alianzas estratégicas y convenios de desarrollo con instituciones nacionales e internacionales.

Figura 9. Establecimiento del contexto a través de la matriz DOFA

Fuente. Autores del proyecto.

4.2.2 Fase 2. Análisis de riesgos. El ministerio de Tecnologías de la información y las Comunicaciones (MINTIC, 2016) basado en la norma ISO27005 establece las siguientes etapas para la generación del análisis de riesgos a) identificación de activos, b)identificación de las

amenazas, c) Identificación de los controles d)Identificación de vulnerabilidades. Estas fases permiten recolectar información para la Identificación del Riesgo.

4.2.2.1 Identificación de activos. Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La información representa un activo de gran valor para las organizaciones y en la caja de compensación se puede encontrar de forma física o digital. A continuación se realizará el análisis de los activos el cual incluye organizar, agrupar, identificar su propietario y custodio, y por ultimo contemplar el impacto de cada activo con el fin de minimizar los riesgos a los que estos se enfrentan.

Tabla 3

Identificación de Activos

Tipo de Activo	Activo	Propietario	Custodio
Información	Caracterización de Gestión Tecnologica	Gestión Tecnologica	Gestión Tecnologica
	Procedimientos operativos	Gestión Tecnologica	Gestión Tecnologica
	Manuales de usuario	Gestión Tecnologica	Gestión Tecnologica
	Plan de seguridad de la información	Gestión Tecnologica	Gestión Tecnologica
	Base de datos de subsidio Informix	Gestión Tecnologica	Gestión Tecnologica
	Base de datos del sistema finaciero y administrativo Sql Server	Gestión Tecnologica	Gestión Tecnologica
	Base de datos del sistema de gestión de calidad Sql Server	Gestión Tecnologica	Gestión Tecnologica
	Base de datos Nomina Sql Server	Gestión Tecnologica	Gestión Tecnologica
	Formularios y documentos de afiliación fisicos	Gestion Documental	Gestion Documental
	Licencias de Software	Gestión Tecnologica	Gestión Tecnologica
Software	Sistemas de información de Subsidios (cubre la mayoria de los procesos misionales)	Gestión Tecnologica	Coordinador de administracion de sistemas de información
	Sistema de información financiero y administrativo Seven	Gestión Tecnologica	Asistente de administracion de Infraestructura tecnologica

Tipo de Activo	Activo	Propietario	Custodio
	Software de nomina y gestion humana KACTUS-HCM	Gestión Tecnologica	Asistente de administracion de Infraestructura tecnologica
	Mesa de servicios Discovery	Gestión Tecnologica	Gestión Tecnologica
	Kawak Herramienta para la administración y el mantenimiento del sistema de gestión de calidad.	Gestión Tecnologica	Asistente de administracion de sistemas de información
	Antivirus Kaspersky	Gestión Tecnologica	Asistente de administracion de Infraestructura tecnologica
	Cliente de correo electrónico corporativo IBM Lotus Notes	Gestión Tecnologica	Asistente de administracion de sistemas de información
	Firewall	Gestión Tecnologica	Coordinador de administración de Infraestructura Tecnologica
	Proxy	Gestión Tecnologica	Coordinador de administración de Infraestructura Tecnologica
Hardware	Equipos portatiles	Gestión Tecnologica	Gestión Tecnologica
	Equipos de Escritorio	Gestión Tecnologica	Gestión Tecnologica
	Servidores (NAS, de base de datos, de reportes, de aplicaciones, , de virtualizacion)	Gestión Tecnologica	Coordinador de administración de Infraestructura Tecnologica
	Discos Duros Externos	Gestión Tecnologica	Coordinador de administración de Infraestructura Tecnologica
	UPS	Subproceso de administración de Infraestructura Tecnologica	Coordinador de administración de Infraestructura Tecnologica
	Impresoras	Gestión Tecnologica	Gestión Tecnologica
	Rack	Subproceso de administración de Infraestructura	Coordinador de administración de Infraestructura
	Switch	Subproceso de administración de Infraestructura	Coordinador de administración de Infraestructura
	Router	Subproceso de administración de Infraestructura	Coordinador de administración de Infraestructura
Personas	Jefe de sistemas	Gestión Tecnologica	Jefe de sistemas
	Coordinador de administracion Infraestructura Tecnologica	Subproceso de administración de Infraestructura Tecnologica	Coordinador de administracion Infraestructura Tecnologica
	Coordinador de administracion Sistemas de Información	Subproceso de administración de Sistemas de Información	Coordinador de administracion Sistemas de Información

Tipo de Activo	Activo	Propietario	Custodio
	Asistentes de Sistemas de Información (3)	Subproceso de administración de Sistemas de Información	Asistentes de Sistemas de Información
	Asistente de Infraestructura Tecnologica	Subproceso de administración de Infraestructura Tecnologica	Asistentes de Sistemas de Información
	Auxiliar de Infraestructura Tecnologica	Subproceso de administración de Infraestructura Tecnologica	Auxiliar de Infraestructura Tecnologica
Servicios	Directorios compartidos	Gestión Tecnologica	Gestión Tecnologica
	Pagina Web de la caja de compensación	Gestión Tecnologica	Gestión Tecnologica
	Red de Datos MPLS Multiprotocol Label Switch para conectarse con las sedes en los municipios.	Gestión Tecnologica	Gestión Tecnologica
	VPN Virtual Private Network conectarse con asopagos	Gestión Tecnologica	Gestión Tecnologica
	Red LAN	Gestión Tecnologica	Gestión Tecnologica

Fuente. Autores del proyecto

Para realizar la clasificación de los activos de información según el valor general del activo en la corporación se aplicaron los criterios y niveles de clasificación de la Guía para la Gestión y Clasificación de Activos de Información del MINTIC. En la tabla 4 se establecen los criterios para realizar la clasificación de los activos de información basados en la confidencialidad, integridad y disponibilidad de la información y en la tabla 5 se explica los niveles de clasificación para el activo.

Tabla 4

Criterios de Clasificación.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Información pública reservada	Alta (a)	Alta (1)
Información pública clasificada	Media (m)	Media (2)
Información pública	Baja (b)	Baja (3)
No clasificada	No clasificada	No clasificada

Fuente. Guía de Gestión del Riesgo MINTIC

Tabla 5

Niveles de Clasificación. Guía de Gestión del Riesgo MINTIC

ALTA (A)	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA (M)	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA (B)	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente. Guía de Gestión del Riesgo MINTIC

Tabla 6

Impacto de los Activos de información

Nota: C: Confidencialidad I: Integridad D: Disponibilidad

Tipo de Activo	Activo	C	D	I	Valor Activo
Información	Caracterización de Gestión Tecnológica	**M**	**B**	**M**	**M**
	Procedimientos operativos	**M**	**B**	**M**	**M**
	Manuales de usuario	**M**	**B**	**M**	**M**
	Plan de seguridad de la información	**M**	**A**	**M**	**M**
	Base de datos de subsidio Informix	**A**	**A**	**A**	**A**
	Base de datos del sistema financiero y administrativo Sql Server	**A**	**M**	**A**	**A**
	Base de datos del sistema de gestión de calidad Sql Server	**A**	**B**	**A**	**A**

Tipo de Activo	Activo	C	D	I	Valor Activo
	Base de datos Nomina Sql Server	A	M	A	A
	Formularios y documentos de afiliación físicos	A	A	B	A
	Copias de Seguridad	M	A	A	A
	Licencias de Software	M	M	B	M
Software	Sistemas de información de Subsidios (cubre la mayoría de los procesos misionales)	A	A	A	A
	Sistema de información financiero y administrativo Seven	M	M	A	M
	Software de nómina y gestión humana KACTUS-HCM	B	M	A	M
	Mesa de servicios Discovery	B	A	M	M
	Kawak Herramienta para la administración y el mantenimiento del sistema de gestión de calidad.	B	M	M	M
	Antivirus Kaspersky	B	A	A	M
	Correo electrónico corporativo IBM Lotus Notes	M	A	M	M
	Firewall	A	A	M	A
	Proxy	A	A	M	A
Hardware	Equipos portátiles	M	A	B	M
	Equipos de Escritorio	M	A	B	M
	Servidores (NAS, de base de datos, de reportes, de aplicaciones, de virtualización)	A	A	A	A
	Discos Duros Externos	M	B	B	M
	UPS	M	A	M	M
	Impresoras	M	M	B	M
	Rack	A	A	M	A
	Switch	A	A	M	A
	Router	A	A	M	A
Servicios	Directorios compartidos	M	M	B	M
	Página Web de la caja de compensación	B	A	M	M
	Red de Datos MPLS Multiprotocol Label Switch para conectarse con las sedes en los municipios.	M	A	M	M
	VPN Virtual Private Network conectarse con Asopagos	M	A	A	A
	Red LAN	A	A	A	A
Personas	Jefe de sistemas	B	A	M	M
	Coordinador de administración Infraestructura Tecnológica	B	A	M	M
	Coordinador de administración Sistemas de Información	B	A	M	M
	Asistentes de Sistemas de Información (3)	B	A	M	M
	Asistente de Infraestructura Tecnológica	B	A	M	M
	Auxiliar de Infraestructura Tecnológica	B	A	B	M

Fuente. Autores del proyecto

4.2.2.2 Identificación de las amenazas. Las amenazas pueden causar alteración o perdida de los activos de información, Rios (2017) afirma “la amenaza puede ser externa, causada por situaciones de origen humano o natural, que puede afectar a personas, cosas o sistemas

involucrados (agua, información, electricidad, etc) y por lo general no se puede impedir que esten presentes o existan" (p, 437).

Tabla 7

Identificación de Amenzas

Tipo	**Amenaza**	**Origen**
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Falla Eléctrica	A, D, E
	Destrucción del equipo o medios	A, D, E
Eventos naturales	Fenómenos sísmicos	E
	Fenómenos climáticos	E
Perdida de los servicios esenciales	Fallas en el suministro de aire acondicionado	A, D
	Perdida de suministro de Energía	A, D, E
	Falla en equipo de Telecomunicaciones	D, E
Compromiso de la información	Hurto de medios o documentos	D
	Espionaje remoto	D
	Hurto de equipo	D
	Recuperación de medios reciclados	D
	Perdida de datos	A, D
Fallas técnicas	Fallas de equipo	A, D
	Mal funcionamiento de equipo	A,D
	Saturación del sistema de información	A, D
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falsificado o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	A, D
	Abuso de Derechos	A, D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D

Nota. D= Deliberadas, A= Accidentales, E= Ambientales

Fuente. Autores del proyecto

4.2.2.3 Identificación de controles. La identificación de controles existentes se realizó a través de observación directa, revisando las caracterizaciones y procedimientos del proceso de Gestión Tecnológica, entrevistas al personal de Infraestructura Tecnológica y a usuarios.

Tabla 8

Identificación de Controles

Tipo	**Controles existentes**	**Observación**
Daño físico	Sistema contra Incendios	En caso que se presente un incendio en el Datacenter se cuenta con detectores de humo los cuales activan una alarma sonora y activan el sistema contra incendios.
	Extintores	Existen 3 extintores en la oficina de gestión tecnológica
	Aire de precisión en Datacenter Aire acondicionado en la oficina	En el Datacenter se cuentas con dos aires de precisión e utilizados para asegurar, las condiciones de operación y 2 aires acondicionados 2 en la oficina de Gestión Tecnológica.
	Copias de seguridad	Se realizan copias de seguridad con diferentes periodicidad (cada hora, diaria, semanal) que se almacenan en diferentes medios (discos externos, servidor de almacenamiento NAS).
Eventos Naturales	Fenómenos Sísmicos	Se realizan semestralmente simulacros para saber actuar en caso de un fenómeno sísmico.
Perdida de los servicios esenciales	Mantenimientos y revisiones periódicas	A los aires acondicionados se realizan revisiones mensuales y mantenimiento cada 5 meses
	UPS y planta de emergencia	Se cuenta con 3 UPS (sistemas de alimentación interrumpida) y una planta de emergencia
	Switch de borde redundante	Cuenta con Switch de borde redundante con tecnologías HP
	Canales de internet redundantes	Servicios de internet con dos canales redundantes para dar respaldo de conexión, en caso que el internet de la sede principal falle.
Compromiso de la información	Cámaras de seguridad	Se cuenta con un sistema de cámaras de vigilancia ubicado en puntos estratégicos, incluyendo la oficina de Tecnología y el Datacenter
	Sistema de identificación Biométrica para ingresar al Datacenter	Sistema de identificación biométrica de huella dactilar para controlar el acceso al Datacenter.
	Alarma	Alarma general para controlar el acceso a

Tipo	Controles existentes	Observación
		personal no autorizado durante las horas en que la oficina de tecnología este cerrada.
	Cantonera	Dispositivo de control de acceso en la puerta de la oficina de tecnología, únicamente se accede a la oficina con permiso de algún miembro del proceso. Aunque los funcionarios de gestión tecnológica no pueden ver quien está solicitando acceso a la oficina ya que la solicitud se realiza a través de un timbre y no hay una cámara instalada en el área de la puerta para verificar y por lo general dan acceso.
	Firewall	Es el encargado de administrar todas las conexiones entrantes y salientes de internet, con reglados para acceso a las direcciones IP asignadas por cada VLAN de acuerdo al proceso y rol del usuario.
Fallas técnicas	Antivirus	Se cuenta con la consola de administración de Kaspersky donde están todos los equipos y servidores de la corporación Antivirus Kaspersky instalados en todos los equipos de la caja de compensación.
	Personal	El proceso de gestión tecnológica cuenta con personal capacitado para dar soporte a los diferentes procesos.
	Mantenimientos Preventivos	Se realiza mantenimientos preventivos a cada equipo de la corporación dos veces al año según el cronograma GT-Ai-Fo-2
Acciones no autorizadas	Controlador de dominio	El controlador de dominio tiene un repositorio centralizado de contraseñas, que están enlazados a los nombres de usuarios. Garantiza o denega a los usuario el acceso a recursos compartidos o a otra máquina de la red. Es el primer nivel de seguridad.
	Autenticación de usuarios para los diferentes sistemas de información	Para los sistemas de información se asigna un usuario y contraseña por cada sistema que requiera acceder de acuerdo al cargo del usuario (roles y perfiles).
Compromiso de las funciones	VLAN Red de área local virtual	Segmentación de la red por medio de Vlans y el acceso y configuración se realiza por el administrador de red.
	Plan de seguridad	Documento donde se establece Controles de acceso Uso y caducidad de contraseñas Navegación y uso del correo electrónico Entre otros.
	Cláusula de confidencialidad	Antes de entrar a trabajar, la persona que empieza las tareas para las que se contrató, firma un acuerdo de confidencialidad y no divulgación con el fin de evitar fugas de información.

Tipo	Controles existentes	Observación
	Cancelación de privilegios de accesos	Cuando una persona es dada de baja de su puesto de trabajo, se le revocan todos los privilegios de acceso. (controlador de dominio, sistemas de información)

Fuente. Autores del proyecto

4.2.2.4 Identificación de vulnerabilidades. Una vez se haya realizdo el inventario de activos, identificación de amenazas y el listado de controles existentes se prosigue identificando las vulnerabilidades. Las vulnerabilidades son la debilidad de seguridad de los activos que si logran ser aprovechadas por amenazas puede traer como consecuencia daño o alteración de los activos.

Tabla 9

Identificación de vulnerabilidades

Tipo de Amenaza	Amenaza	Vulnerabilidad
Daño físico	Fuego	Desconocimiento del procedimiento de emergencia ante un incendio. Desconocimiento en la utilización de extintores
	Agua	Posibilidad de filtración de agua por rotura de un tubo de agua.
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal externo
	Espionaje	Ausencia de auditorías intrusivas para detectar debilidades en la seguridad.
	Hurto de equipo	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.
	Perdida de datos	Las copias de seguridad se guardan en el mismo edificio, donde se encuentra el Datacenter.
Fallas técnicas		
	Saturación del sistema de información	No se realiza afinamiento a las bases de datos periódicamente.

Tipo de Amenaza	Amenaza	Vulnerabilidad
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información
Acciones no autorizadas	Uso no autorizado d	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de prevención de intrusos.
	Copia fraudulenta del software	
	Uso de software falsificado o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos	
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	No existe documentación de la configuración de los servidores en caso que estos fallen.
	Error en el uso	Entrenamiento insuficiente en seguridad FA de conocimiento acerca del plan de seguridad de la información GT-Ai-Pr-3
	Negación de acciones	
		Contraseñas visibles a otros usuarios.
	Abuso de Derechos	Falta de conciencia acerca de la seguridad
		Ausencia de procedimiento formal para el registro y retiro de usuarios del dominio y de los sistemas de información

Fuente. Autores del proyecto

Identificación de las consecuencias. Se presentan las consecuencias o impactos detectados en los servicios que ofrece el proceso de Gestión tecnológica, que pueden ser causadas por las vulnerabilidades encontradas, ver tabla 10.

Tabla 10

Identificación de las consecuencias

Tipo de Amenaza	Amenaza	Vulnerabilidad	Consecuencia	Descripción
Daño físico	Fuego	Desconocimiento del procedimiento de emergencia ante un	Perdida de información y daño en los equipos que se alojan en las oficinas	En caso de incendio existiría pérdida de tiempo valioso por

Tipo de Amenaza	Amenaza	Vulnerabilidad	Consecuencia	Descripción
		incendio. Desconocimiento en la utilización de extintores	de gestión tecnológica en caso de producirse un incendio.	desconocimiento de cómo actuar ante esta situación lo que aumentaría la perdida de información y daño material en los equipos. Afectaría la disponibilidad de la información.
	Agua	Posibilidad de filtración de agua por rotura de un tubo de agua.	Daño en lo equipos de los funcionarios de tecnología.	Serian afectados los equipos de los funcionarios de tecnología que dan respuesta a los diferentes incidentes lo que aumentaría los tiempos de respuesta a los usuarios de los servicios TIC.
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal.	Hurto o pérdida de activos, (información, discos, memorias, portátiles, etc.)	Facilidad de sacar de las instalaciones de la caja activos (equipos portátiles, información, etc.).
	Espionaje	Ausencia de auditorías intrusivas para detectar debilidades en la seguridad.	Desconocimiento de debilidades de seguridad de la información y falta de controles para estas debilidades.	
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.	Fuga de información sensible.	Actualmente no se realiza borrado seguro de los datos contenidos en los dispositivos de almacenamiento lo que permite la recuperación de la información por personal externo a la corporación.
	Perdida de datos	Las copias de seguridad se guardan en el mismo edificio, donde se encuentra el Datacenter.	Perdida de la disponibilidad de la información	En caso que la pérdida de datos sea por catástrofe (incendio, inundación, etc.) no se podrán recuperar los datos porque la copia de seguridad también será destruida.
Fallas técnicas	Saturación del sistema de información	No se realiza afinamiento a las bases de datos periódicamente.	Afectación al rendimiento de las bases de datos, procesos más lentos.	No hay una programación periódica ni procedimientos definidos para realizar afinamiento a las diferentes bases de datos lo que puede ocasionar bajo rendimiento de los sistemas de información

Tipo de Amenaza	Amenaza	Vulnerabilidad	Consecuencia	Descripción
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información	Pérdidas de los archivos de configuración y/o desarrollo	No documenta los cambios que se realizan a los sistemas de información, en caso de
Acciones no autorizadas	Uso no autorizado	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de prevención de intrusos.	Desconocimiento si se realizan ingresos no autorizados	En el caso que haya intrusos no se detectarían.
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	No existe documentación de la configuración de los servidores en caso que estos fallen.	Dependencia para configuración inicial de un servidor	Para configurar inicialmente los servidores se depende de unos de los funcionarios de tecnología
	Error en el uso	Entrenamiento insuficiente en seguridad Falta de conocimiento acerca del plan de seguridad de la información GT-Ai-Pr-3	Desconocimiento en la aplicación de buenas prácticas de seguridad de la información	No se aplican las normas establecidas por los usuarios en el plan de seguridad de la información.
	Abuso de Derechos	Ausencia de procedimiento formal para el registro y retiro de usuarios del dominio y de los sistemas de información	Posibilidad de error al asignar permisos de usuario	Realizan erradamente el procedimiento para el registro y retiro de usuarios por los usuarios líderes en los sistemas de información

Fuente. Autores del proyecto

4.2.3 Fase 3. Estimación del riesgo. La estimación del riesgo puede ser cuantitativa, cualitativa o una combinación de las dos. Para el presente proyecto se realizó cuantitativa, a través de la cual se obtiene un valor para identificar el nivel del riesgo.

4.2.3.1 Valoración de las consecuencias. Para la Caja de Compensación familiar es de vital importancia mantener la operatividad en todos los servicios que presta, y de presentarse alguna falla en sus activos y procesos causaría un gran impacto afectando la imagen de la corporación. La valoración para cada grupo de activo se presenta en las tablas descritas nivel del riesgo utilizando los siguientes criterios de valoración de impacto según el Tiempo que el servicio se encuentra sin funcionamiento y la pérdida de confidencialidad integridad y/o disponibilidad de los activos.

En la tabla 11 se establecen escalas de tiempo sin funcionamiento de un servicio asignando un valor de 1 a 4.

Tabla 11

Impacto de acuerdo al tiempo sin funcionamiento del servicio

Valor	Grado de Impacto	Descripción
1	Bajo	Tiempo de caída mínimo de 1 a 29 minutos
2	Medio	Tiempo de caída mínimo de 30 a 59 minutos
3	Grave	Tiempo de caída del servicio alto de 60 minutos a 89 minutos
4	Muy Grave	Tiempo de caída muy alto de más de 90 minutos

Fuente. Autores del proyecto

En la tabla 12 Se establecen los criterios para valorar el impacto desde el punto de vista que pueda presentarse una pérdida de confidencialidad, integridad y disponibilidad de los activos de información.

Tabla 12.

Impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo

Valor	Grado de Impacto	Descripción
1	Bajo	Pérdida de confidencialidad, integridad y disponibilidad del activo mínimo.
2	Medio	Pérdida de confidencialidad, integridad y disponibilidad del activo moderado
3	Grave	Pérdida de confidencialidad, integridad y disponibilidad del activo grave
4	Muy Grave	Pérdida de confidencialidad, integridad y disponibilidad del activo muy grave.

Fuente. Autores del proyecto

4.2.3.2 Valoración de los incidentes. Consiste en valorar la probabilidad de ocurrencia de alguna amenaza. En la tabla 13 se establecen los criterios de probabilidad de ocurrencia de una amenaza.

Tabla 13.

Probabilidad de ocurrencia de una amenaza

Valor	Grado de Impacto	Descripción
1	Poco Probable	Amenaza cuya probabilidad de explotar vulnerabilidades es poco probable
2	Probable	Amenaza que con poca frecuencia explotan vulnerabilidades
3	Muy Probable	Amenaza que frecuentemente explotan vulnerabilidades
4	Altamente Probable	Amenaza que en la mayoría de los casos explotan vulnerabilidades

Fuente. Autores del proyecto

4.2.3.3 Nivel de estimación del riesgo. Para realizar la estimación del riesgo se han definido los valores para probabilidad de ocurrencia de una amenaza y los impactos de acuerdo al tiempo sin funcionamiento del servicio y el impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo.

Después de hacer la valoración de los criterios probabilidad de ocurrencia de una amenaza, impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo e impacto de acuerdo al tiempo sin funcionamiento del servicio se procede hallar el nivel del riesgo según la tabla 14, teniendo en cuenta que:

$$Nivel\ del\ riesgo = PA * \text{Impacto CID} * \text{Impacto FS}$$

Dónde:

PA= probabilidad de ocurrencia de amenaza

Impacto CID= impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo.

Impacto FS= impacto de acuerdo al tiempo sin funcionamiento del servicio

Tabla 14

Nivel de Riesgo

Valor	Grado de Impacto	Descripción
1 – 4	Bajo	El nivel del riesgo es bajo, cuando el tiempo sin funcionamiento del servicio es mínimo la perdida de integridad, disponibilidad y confidencialidad es mínima y tiene pocas probabilidades de la ocurrencia de una amenaza
6- 12	Moderado	El nivel del riesgo es moderado, cuando el tiempo sin funcionamiento del servicio y la perdida de integridad, disponibilidad y confidencialidad es medio y con ciertas probabilidades de la ocurrencia de una amenaza
16-27	Alto	El nivel del riesgo es alto, cuando el tiempo sin funcionamiento del servicio es grave la perdida de integridad, disponibilidad y confidencialidad es alta y con altas probabilidades de la ocurrencia de una amenaza
32-64	Muy Alto	El nivel del riesgo es muy alto, cuando el tiempo sin funcionamiento del servicio es muy alta la perdida de integridad, disponibilidad y confidencialidad es considerable y con altísimas probabilidades de la ocurrencia de una amenaza

Fuente. Autores del proyecto

Seguidamente se presenta la valoración del riesgo para cada tipo de activo Información, Software, Hardware, Servicios y Personas.

Tabla 15.

Valoración del riesgo del activo Información

Nota: PA= probabilidad de ocurrencia de amenaza, Impacto CID= impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo, Impacto FS= impacto de acuerdo al tiempo sin funcionamiento del servicio

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
Daño físico	Fuego	Desconocimiento del	Perdida de	1	4	4	16

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
		procedimiento de emergencia ante un incendio. Desconocimiento en la utilización de extintores	información y daño en los equipos que se alojan en las oficinas de gestión tecnológica en caso de producirse un incendio.				
	Agua	Posibilidad de filtración de agua por rotura de un tubo de agua.	Daño en lo equipos de los funcionarios de tecnología.	2	4	2	32
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal.	Hurto o pérdida de activos, (información, discos, memorias, portátiles, etc.)	2	4	2	16
	Espionaje	Ausencia de auditorías intrusivas para detectar debilidades en la seguridad.	Desconocimiento de debilidades de seguridad de la información y falta de controles para estas debilidades.	1	4	4	16
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.	Fuga de información sensible.	1	4	4	16
	Perdida de datos	Las copias de seguridad se guardan en el mismo edificio, donde se encuentra el Datacenter.	Perdida de la disponibilidad de la información	1	4	4	16
	Saturación del sistema de información	No se realiza afinamiento a las bases de datos periódicamente.	Afectación al rendimiento de las bases de datos, procesos más lentos.	2	2	3	12
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información	Pérdidas de los archivos de configuración y/o desarrollo	2	2	2	8

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
Acciones no autorizadas	Uso no autorizado	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de prevención de intrusos.	Desconocimiento si se realizan ingresos no autorizados, perdida de confidencialidad, integridad y disponibilidad de la información	2	4	4	32

Fuente. Autores del proyecto

En la tabla 15 valoración del riesgo del tipo de activo Información, se puede evidenciar que se cuenta con riesgos altos en las amenazas por agua y acciones no autorizadas.

Tabla 16.

Valoración del riesgo del activo software

Nota: PA= probabilidad de ocurrencia de amenaza, Impacto CID= impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo, Impacto FS= impacto de acuerdo al tiempo sin funcionamiento del servicio

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel de Riesgo
Daño físico	Fuego	Desconocimiento del procedimiento de emergencia ante un incendio. Desconocimiento en la utilización de extintores	Perdida de información y daño en los equipos que se alojan en las oficinas de gestión tecnológica en caso de producirse un incendio.	1	4	3	12
	Agua	Posibilidad de filtración de agua por rotura de un tubo de agua.	Daño en lo equipos de los funcionarios de tecnología.	1	4	3	12

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel de Riesgo
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal.	Hurto o pérdida de activos, (información, discos, memorias, portátiles, etc.)	2	3	3	18
	Espionaje	Ausencia de auditorías intrusivas para detectar debilidades en la seguridad.	Desconocimiento de debilidades de seguridad de la información y falta de controles para estas debilidades.	2	2	4	16
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.	Fuga de información sensible.	1	2	2	4
	Perdida de datos	Las copias de seguridad se guardan en el mismo edificio, donde se encuentra el Datacenter.	Perdida de la disponibilidad de la información	2	3	3	18
Fallas técnicas	Saturación del sistema de información	No se realiza afinamiento a las bases de datos periódicamente.	Afectación al rendimiento de las bases de datos, procesos más lentos.	2	4	4	32
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información	Pérdidas de los archivos de configuración y/o desarrollo	2	2	1	4
Acciones no autorizadas	Uso no autorizado	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de prevención de intrusos.	Desconocimiento si se realizan ingresos no autorizados, perdida de confidencialidad, integridad y disponibilidad de la información	3	3	4	36

Fuente. Autores del proyecto

En la tabla 16 valoración del riesgo del tipo de activo Software, se puede evidenciar que se cuenta con riesgos altos en las amenazas por saturación del sistema de información y uso no autorizado.

Tabla 17.

Valoración del riesgo del activo hardware

Nota: PA= probabilidad de ocurrencia de amenaza, Impacto CID= impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo, Impacto FS= impacto de acuerdo al tiempo sin funcionamiento del servicio

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
Daño físico	Fuego	Desconocimiento del procedimiento de emergencia ante un incendio. Desconocimiento en la utilización de extintores	Perdida de información y daño en los equipos que se alojan en las oficinas de gestión tecnológica en caso de producirse un incendio.	1	4	4	16
	Agua	Posibilidad de filtración de agua por rotura de un tubo de agua.	Daño en lo equipos de los funcionarios de tecnología.	2	4	4	32
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal.	Hurto o pérdida de activos, (información, discos, memorias, portátiles, etc.)	2	3	4	24
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.	Fuga de información sensible.	2	1	3	6
	Perdida de datos	Las copias de seguridad se guardan en el mismo edificio, donde se encuentra el Datacenter.	Perdida de la disponibilidad de la información	1	4	4	16

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
	Saturación del sistema de información	No se realiza afinamiento a las bases de datos periódicamente.	Afectación al rendimiento de las bases de datos, procesos más lentos.	2	3	3	18
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información	Pérdidas de los archivos de configuración y/o desarrollo	2	2	2	8
Acciones no autorizadas	Uso no autorizado	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de prevención de intrusos.	Desconocimiento si se realizan ingresos no autorizados, perdida de confidencialidad, integridad y disponibilidad de la información	2	3	3	18

Fuente. Autores del proyecto

En la tabla 17 valoración del riesgo del tipo de activo Hardware, se puede evidenciar que se cuenta con riesgos altos en la amenaza por agua.

Tabla 18.

Valoración del riesgo del activo Servicios

Nota: PA= probabilidad de ocurrencia de amenaza, Impacto CID= impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo, Impacto FS= impacto de acuerdo al tiempo sin funcionamiento del servicio

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
Daño físico	Fuego	Desconocimiento del procedimiento de emergencia ante un incendio.	Perdida de información y daño en los equipos que se alojan en las	1	4	4	16

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
		Desconocimiento en la utilización de extintores	oficinas de gestión tecnológica en caso de producirse un incendio.				
	Agua	Posibilidad de filtración de agua por rotura de un tubo de agua.	Daño en lo equipos de los funcionarios de tecnología.	2	2	2	8
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal.	Hurto o pérdida de activos, (información, discos, memorias, portátiles, etc.)	2	1	2	4
	Espionaje	Ausencia de auditorías intrusivas para detectar debilidades en la seguridad.	Desconocimiento de debilidades de seguridad de la información y falta de controles para estas debilidades.	1	2	4	8
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.	Fuga de información sensible.	1	2	4	8
	Perdida de datos	Las copias de seguridad se guardan en el mismo edificio, donde se encuentra el Datacenter.	Perdida de la disponibilidad de la información	1	3	3	9
	Saturación del sistema de información	No se realiza afinamiento a las bases de datos periódicamente.	Afectación al rendimiento de las bases de datos, procesos más lentos.	2	2	3	12
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información	Pérdidas de los archivos de configuración y/o desarrollo	2	2	2	8
Acciones no autorizadas	Uso no autorizado	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de	Desconocimiento si se realizan ingresos no autorizados, perdida de	2	2	4	16

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
		prevención de intrusos.	confidencialidad, integridad y disponibilidad de la información				

Fuente. Autores del proyecto

En la tabla 18 valoración del riesgo del tipo de activo Servicios, se puede evidenciar que no se cuenta con riesgos altos.

Tabla 19.

Valoración del riesgo del activo personas

Nota: PA= probabilidad de ocurrencia de amenaza, Impacto CID= impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo, Impacto FS= impacto de acuerdo al tiempo sin funcionamiento del servicio

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
Daño físico	Fuego	Desconocimiento del procedimiento de emergencia ante un incendio. Desconocimiento en la utilización de extintores	Perdida de información y daño en los equipos que se alojan en las oficinas de gestión tecnológica en caso de producirse un incendio.	2	3	3	18
Compromiso de la información	Hurto de medios o documentos	Trabajo no supervisado del personal.	Hurto o pérdida de activos, (información, discos, memorias, portátiles, etc.)	2	2	3	12
	Espionaje	Ausencia de auditorías intrusivas para detectar debilidades en la	Desconocimiento de debilidades de seguridad de la	2	2	1	4

Tipo de Amenaza	Amenaza	Vulnerabilidad	Impacto	PA	Impacto FS	Impacto CID	Nivel Riesgo
		seguridad.	información y falta de controles para estas debilidades.				
	Recuperación de medios reciclados	No existe un procedimiento formal para dar de baja a dispositivos con información sensible.	Fuga de información sensible.	2	3	1	6
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de control de cambios eficaz a los sistemas de información	Pérdidas de los archivos de configuración y/o desarrollo	2	1	2	4
Acciones no autorizadas	Uso no autorizado	No se cuenta con un IDS Sistema de detección de intrusos ni IPS Sistema de prevención de intrusos.	Desconocimiento si se realizan ingresos no autorizados, perdida de confidencialidad, integridad y disponibilidad de la información	2	2	1	32
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	No existe documentación de la configuración de los servidores en caso que estos fallen.	Dependencia para configuración inicial de un servidor	2	3	2	12
	Error en el uso	Entrenamiento insuficiente en seguridad Falta de conocimiento acerca del plan de seguridad de la información GT-Ai-Pr-3	Desconocimiento en la aplicación de buenas prácticas de seguridad de la información	2	3	3	18
	Abuso de Derechos	Ausencia de procedimiento formal para el registro y retiro de usuarios del dominio y de los sistemas de información	Posibilidad de error al asignar permisos de usuario	2	2	2	8

Fuente. Autores del proyecto

En la tabla 19 valoración del riesgo del tipo de activo Personas, se puede evidenciar que se cuenta con riesgos altos en la amenaza por uso no autorizado.

4.2.4 Clasificación y categorización de incidentes. El enfoque propuesto en la norma 27035, considera las amenazas como factores de categorización, de acuerdo al anexo C de la norma se extraen los siguientes tipos de incidentes de seguridad de la información:

Tabla 20

Categorización de Incidentes

CATEGORÍA	TIPOS DE INCIDENTES
Incidente de daño físico	• Incendio • Ambiente no apto (contaminación, polvo) • Robo de equipos • Perdida de equipos
Incidente de fallas de infraestructura	• Fallas en alimentación eléctrica • Fallas en aires acondicionados • Fallas en las redes de cableado estructurado
Incidente de falla técnica	• Falla del hardware • Saturación capacidad de los sistemas
Incidente de malware	• Virus informáticos • Gusanos de red • Troyanos • Botnet (Robots que se ejecutan de manera autónoma) • Página web con código malicioso
Incidente de ataque técnico	• Escaneo de redes • Vulnerabilidades en sistemas de información • Interferencia • Denegación de servicio
Incidente de violación de reglas	• Violación de los derechos de autor • Uso de recursos para propósitos no autorizados (páginas no autorizadas, correo no autorizado)
Incidente puesta en riesgo de la información	• Phishing • Robo de datos • Borrado de datos • Alteración de datos • Espionaje • Chuzar teléfonos
Incidentes relacionados con	• Contenido ilegal (pornografía, fraude)

CATEGORÍA	TIPOS DE INCIDENTES
contenidos peligrosos	• Contenido malicioso (bromas pesadas, acoso)

Fuente**.** Norma GTC ISO/IEC 27035.

La clasificación de los incidentes de seguridad de la información se realizó en base al anexo C de la norma GTC ISO/IEC 27035, clasificando los incidentes de seguridad en cuatro clases como se puede apreciar en la tabla 21

Tabla 21

Clasificación De Incidentes

CLASIFICACIÓN	DESCRIPCIÓN DE FACTORES
Muy grave (Clase IV)	a. Actúa sobre sistemas de información especialmente importantes b. Da como resultado pérdidas para el negocio especialmente graves c. Conduce a un impacto social especialmente importante
Grave (Clase III)	a. Actúa sobre sistemas de información especialmente importantes o sistemas de información importantes b. Da como resultado perdidas graves para el negocio c. Conduce a un impacto social importante
Menos Grave (Clase II)	a. Actúa sobre sistemas de información importantes o sistemas de información comunes b. Da como resultado pérdidas considerables para el negocio c. Conduce a un impacto social considerable
Mínima (Clase I)	a. Actúa sobre sistemas de información importantes comunes b. Da como resultado perdidas menores para el negocio o ninguna perdida c. Conduce a impactos sociales menores o a ningún impacto social

Fuente. Norma GTC ISO/IEC 27035.

4.2.4.1 Evaluación de los incidentes. El punto de contacto evalúa la información del incidente reportado, define su alcance inicial y registra la información del incidente de seguridad. A continuación se presenta la tabla 22 de identificación de severidad del incidente donde se evalúa las categorías de incidentes vs clases de severidad:

Tabla 22

Categorías De Incidentes Vs Clases De Severidad

CATEGORIA DE INCIDENTES	**CLASE DE SEVERIDAD**			
	MINIMA	**MENOS GRAVE**	**GRAVE**	**MUY GRAVE**
Incidente de daño físico	1 equipo afectado	10 equipos afectados	50 equipos afectados	100 a más equipos afectados
Incidente de fallas de infraestructura	1 equipo afectado	10 equipos afectados	50 equipos afectados	100 a más equipos afectados
Incidente de falla técnica	1 equipo afectado	10 equipos afectados	50 equipos afectados	100 a más equipos afectados
Incidente de malware	1 equipo afectado	10 equipos afectados	50 equipos afectados	100 a más equipos afectados
Incidente de ataque técnico	1 equipo afectado	10 equipos afectados	50 equipos afectados	100 a más equipos afectados
Incidente de violación de reglas	1 caso detectado	10 casos detectados	50 casos detectados	100 a más casos detectados
Incidente puesta en riesgo de la información	1 caso detectado	10 casos detectados	50 casos detectados	100 a más casos detectados
Incidentes relacionados con contenidos peligrosos	1 caso detectado	10 casos detectados	50 casos detectados	100 a más casos detectados

Fuente. Norma GTC ISO/IEC 27035.

A continuación se presenta la escala de impacto del incidente y el tiempo de respuesta estimado de acuerdo a la severidad:

Tabla 23

Tiempos de respuesta según severidad del incidente

CLASE DE SEVERIDAD	TIEMPO DE RESPUESTA
Mínima	48 Horas
Menos grave	24 Horas
Grave	8 Horas
Muy grave	Inmediato

Fuente. Norma GTC ISO/IEC 27035.

4.3 Documentar plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander, COMFANORTE, teniendo como referencia la norma ISO/IEC 27035.

4.3.1 Alcance del plan de respuesta a incidentes. En el plan de respuesta a incidentes se diseñó una propuesta de la normativa mediante la cual se hará el manejo de incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander alineada principalmente a la norma ISO/IEC 27035. Los documentos resultantes del proceso de generar el plan de respuesta a incidentes y que se desarrollaron específicamente en los próximos apartados son:

- Política de gestión de incidentes de seguridad de la información

- Plan de respuesta a incidentes de seguridad de la información
- Plan de establecimiento del equipo de respuesta a incidentes de seguridad de la información
- Escala de clasificación de eventos e incidentes de seguridad de la conformación

4.3.2 Política de gestión de incidentes de seguridad de la información. Según la organización Internacional de Estandarización (ISO, 2013) en la norma GTC-ISO/IEC 27035:

> Una organización debería documentar su política para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información como un documento autónomo. El tamaño, estructura y naturaleza del negocio de una organización y el alcance de su programa de gestión de incidentes son factores para determinar que opción adoptar. (p. 13).

De acuerdo al proceso previo de diagnóstico realizado mediante la auditoría pasiva se logró establecer el estado del arte de la gestión de incidentes y por consiguiente es posible construir una política acorde a las necesidades de la organización. En Apéndice L se presenta la propuesta de la política de gestión de incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander Comfanorte.

4.3.3 Plan de respuesta a incidentes de seguridad de la información. El plan de respuesta a incidente permite guiar a la corporación en caso de presentarse un incidente de seguridad de la información. La organización internacional de estandarización ISO (2013) en la norma GTC ISO/IEC 27035 afirma que:

> El objetivo del esquema de gestión de incidentes de seguridad de la información es brindar documentación detallada que describa las actividades y procedimientos para tratar eventos e incidentes de seguridad de la información, y comunicar estos eventos, incidentes y vulnerabilidades (p. 17)

En el Apéndice M se presenta la propuesta del plan de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander COMFANORTE.

4.3.4 Propuesta para el establecimiento del equipo de respuesta a incidentes de seguridad de la información. El equipo de respuesta a incidentes de seguridad de la información debe estar conformado por un grupo de expertos multidisciplinarios que le permita tomar decisiones en las diferentes áreas (financiera, recurso humano, administrativa, tecnológica, etc.), La organización internacional de estandarización en la norma GTC ISO/IEC 27035 afirma que:

> El objetivo de establecer el ISIRT es proveer a la organización con una capacidad adecuada para evaluar, responder a los incidentes de seguridad de la información, aprender de ellos y brindar la coordinación, gestión, retroalimentación y comunicación necesarias (p. 24)

En el Apéndice N se expone la propuesta para el establecimiento del equipo de respuesta a incidentes de seguridad de la información para la Caja de Compensación Familiar de Norte de Santander "COMFANORTE"

4.3.5 Clasificación de incidentes de seguridad de la información del Departamento de Gestión Tecnológica. La organización internacional de estandarización (ISO, 2013) afirma que: "Los incidentes de seguridad de la información pueden ser causados por acciones humanas deliberadas o accidentales y también por medios técnicos o físicos". (p. 64). La clasificación de incidentes se presentó en el desarrollo del objetivo 2 del proyecto.

Capítulo 5: Conclusiones

La auditoría pasiva que se realizó permitió conocer el negocio de las cajas de compensación familiar y proporciono información sobre el estado en que se encuentra la corporación referente a la gestión de incidentes de acuerdo a la norma ISO 27035.

El análisis de riesgo desarrollado basado en la guía de gestión de riesgos del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, permitió identificar y clasificar lo activos de información, las amenazas para los mismos y etiquetarlos con un nivel de importancia según su confidencialidad, integridad y disponibilidad. Así mismo suministró la base para realizar la clasificación y categorización de incidentes

Teniendo como base las normas ISO 27035:2012 se logra construir la base para para el establecimiento del esquema de gestión de incidentes de seguridad de la información que consiste en la política y el plan propuesto a la corporación, es importante resaltar los beneficios de implementar este esquema dentro de un estándar debido a que guía el proceso, define cada una de las actividades del proceso y permite alcanzar los resultados de manera eficiente.

Referencias

Mendoza, M. (2015). ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? *Welivesecurity, (20150518).* Recuperado de https://www.welivesecurity.com/la-es/2015/05/18/

Georgia, K. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRT´s). Pensilvania: Universidad Carnegie Mellon.

Cuadros, A., y Velásquez, G. (2011). Análisis, Rediseño e Implementación de los procesos, basados en ITIL, para el área de gestión y soporte técnico de la unidad de tecnología de información y comunicaciones de la escuela politécnica del ejército. Sangolquí.

NAP Colombia, Preguntas Frecuentes. Recuperado de http://nap.co/html/faq.php

López, M (2007). *Análisis Forense Digital* (Segunda edición). Recuperado de https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, (2012) Norma Técnica Colombiana GTC-ISO/IEC 27035. (2012).

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, (2017) Norma Técnica Colombiana GTC-ISO/IEC 27000. (2017).

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, (2013) Norma Técnica Colombiana GTC-ISO/IEC 27001. (2013).

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, (2009) Compendio sistema de gestión de la seguridad de la información (SGSI). (2009).

Congreso de Colombia (2009), *Ley 1273 de 2009*. Recuperado de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf,20159

Consejo Nacional De Política Económica Y Social República De Colombia, CONPES. (2016), *Política Nacional de Seguridad Digital.* Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Congreso de Colombia (1993), *Ley 87 de 1993*. Recuperado de https://www.mintic.gov.co/portal/604/articles-3697_documento.pdf

Bisquerra, R. y otros (2009), *Metodología de la investigación educativa*, (2 edición) Editorial La Muralla S.A Recuperado de https://books.google.com.co/books?isbn=8471337487.

Erazo A., y Moran C., Políticas de seguridad para el área de sistemas del instituto Colombiano de Bienestar Familiar Regional Nariño. Pasto: I. U CESMAG

Caja de Compensación Familiar de Norte de Santander (2014-2018), *Direccionamiento Estratégico* 2014-2018.

Osterwalder, A. (2004). The Business Model Ontology: a Proposition in a Design Science.

Approach. Disertación doctoral. Lausana: École des Hautes Études Comerciales del 'Université de Lausanne.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (2016). *Guía De Gestión De Riesgos* versión 3.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (2016). *Guía para la Gestión y Clasificación de Activos de Información*.

Apéndices

Apéndice A. Programa de auditoria

PROGRAMA DE AUDITORIA						
Fase	**Descripción**	**Actividad**	**Cantidad Personas**	**Periodo**		**Días**
				Inicio	**Fin**	
Planeación de la Auditoría	En esta fase se realiza la recolección de la información y elaboración de instrumentos.	• Solicitud y análisis de la de la información organizacional: estructura orgánica, misión, visión, objetivos y direccionamiento estratégico para el conocimiento de la corporación.	3	24/08/17	31/08/17	6
		• Visita preliminar para observar el estado del área de Gestión Tecnológica.	2	01/09/16	01/09/16	1
		• Elaboración de herramientas de recopilación de información.	3	04/09/17	09/09/17	5
Ejecución de auditoría	En esta fase se realiza la aplicación de los instrumentos y se realizan la pruebas detectadas	• Reunión de apertura de la auditoría con el jefe y coordinadores del proceso de Gestión Tecnológica.	1	11/09/17	11/09/17	1
		• Entrevista al Jefe de Gestión Tecnológica	1	11/09/17	11/09/17	1
		• Aplicación del cuestionario al personal del proceso.	1	12/09/17	12/09/17	1
		• Aplicación del cuestionario 2 a los jefes de procesos	2	14/09/17	14/09/17	1
		• Aplicación de la lista de chequeo.	1	19/09/17	19/09/17	1
		• Realización de pruebas	3	18/09/17	22/09/17	
		• Identificación y elaboración de los documentos de desviaciones detectadas y situaciones encontradas.	2	25/09/17	28/09/17	2
Informe de Auditoría	Elaboración del Informa de Auditoría	• Elaboración del Informe	3	04/10/17	05/10/17	1

Apéndice B. Entrevista para medir el estado de la gestión de incidentes de la seguridad de la información al interior del proceso de Gestión Tecnológica, aplicada al jefe de Sistemas.

ENTREVISTA

Nombre del encuestado: _____
Fecha: ____/____/_____ **Hora de Inicio**: __:__ **Hora Final**: __:__

1. Como se encuentran identificados los activos al interior del proceso y de la corporación.
2. Han sido clasificados estos activos con el fin de brindarle la protección adecuada a cada uno de ellos
3. Que tan frecuente se presentan incidentes de seguridad de la información
4. Cuando se presentan incidentes de seguridad cual es el nivel de compromiso y apoyo de la dirección
5. La corporación asigna presupuesto para atender incidentes de seguridad de la información
6. La corporación cuenta con personal capacitado para atender un incidente de seguridad de la información
7. Existe algún responsable de la gestión de incidentes de seguridad
8. Con que herramientas y servicios cuentan los funcionarios para reportar los incidentes de seguridad de la información
9. Existe un equipo de respuesta a incidentes de seguridad de la información (ISIRT) constituido, para operar en caso de la ocurrencia de un incidente de seguridad
10. La corporación recibe soporte de entidades externas para atender incidentes de seguridad
11. Existe documentación que indique los pasos a seguir en el caso ocurrencia de cualquier incidente de seguridad de la información
12. Se monitorea periódicamente los sistemas informáticos con el fin de evaluar el nivel de seguridad
13. Existen personas trabajando los diversos temas de seguridad dentro del proceso o la corporación
14. Existe algún programa de formación para enseñar a los empleados a actuar en caso de un incidente de seguridad de la información

Apéndice C. Encuesta para medir el estado de la gestión de incidentes de la seguridad de la información al interior del Departamento de Gestión Tecnológica.

ENCUESTA 1

Nombre del encuestado: _____

Fecha: ____/____/_____ **Hora de Inicio**: __:__ **Hora Final**: __:__

Objetivo: recopilar información correspondiente a la respuesta dada a los incidentes de seguridad de la información.

Marque la opción que crea correcta:

1. ¿Con que frecuencia se presentan incidentes de seguridad de la información?
   - Muy frecuentemente
   - Frecuentemente
   - Poco Frecuente
   - Nunca

2. ¿Con que frecuencia se capacita a los empleados en el modo de actuar el caso de presentarse un incidente de seguridad de la información?

   - Muy frecuentemente
   - Frecuentemente
   - Poco Frecuente
   - Nunca

3. ¿Está documentado en detalle las responsabilidades de cada integrante del proceso de gestión tecnológica frente a la respuesta de incidentes?

   - Si
   - No

4. ¿Existe un punto de contacto donde se pueda reportar un incidente en caso de presentarse?

   - Si
   - No

5. ¿Señale los medios por los cuales se realiza con más frecuencia la detección de incidentes de seguridad?

   - Antivirus
   - Seguimiento de Redes

- Notificación de terceros
- Otros

6. Es acertado el diagnóstico y la respectiva solución en caso de presentarse un incidente de seguridad de la información

- Muy acertado
- Acertado
- Poco acertado
- Desacertado

7. ¿Se realiza seguimiento del incidente de seguridad de la información hasta su respectiva solución?

- Si
- No

8. ¿Se mantiene interacción con otras entidades para recibir apoyo en caso de presentarse un incidente de seguridad?

- Frecuentemente
- Muy poco frecuente
- Nunca
-

9. Existe un grupo de personas expertas dentro de la corporación encargadas de solucionar los incidentes de seguridad de la información

- Si
- No

10. Califique el estado actual de la gestión de incidentes de seguridad de la información

- Excelente
- Buena
- Regular
- Deficiente

Apéndice D. Resultado de la encuesta para medir el estado de la gestión de incidentes de la seguridad de la información al interior del Departamento de Gestión Tecnológica.

1. Frecuencia de incidentes de seguridad de la información

Tabla 1.

Frecuencia de incidentes de seguridad de la información

Respuesta	**Cantidad**
Muy frecuentemente	0
Frecuentemente	5
Poco Frecuente	2
Nunca	0
Total	7

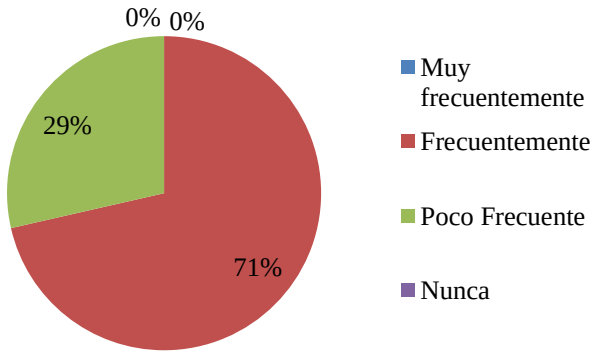


Figura 1. Frecuencia de incidentes de seguridad de la información

2. Frecuencia de capacitación a los empleados en incidentes de seguridad

Tabla 2.

Frecuencia de capacitación a los empleados en incidentes de seguridad

Respuesta	Cantidad
Muy frecuentemente	0
Frecuentemente	0
Poco Frecuente	7
Nunca	0
Total	7

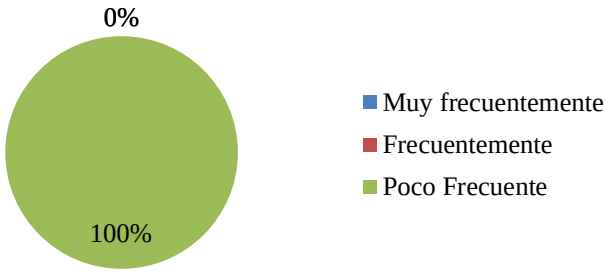


Figura 2. Frecuencia se capacitación a los empleados en incidentes de seguridad

3. Documentación de responsabilidades frente a respuesta a incidentes de seguridad

Tabla 3.

Documentación de responsabilidades frente a respuesta a incidentes de seguridad

Respuesta	Cantidad
SI	0
NO	7
Total	7

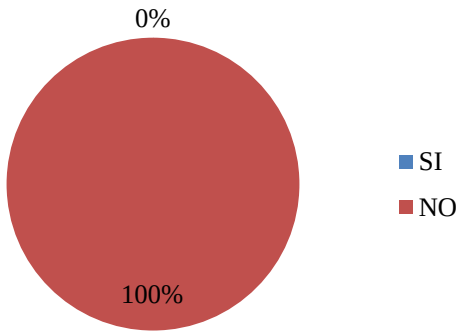


Figura 3. Documentación de responsabilidades frente a respuesta a incidentes de seguridad

4. Existencia de punto de contacto para reportar un incidente

Tabla 4.

Existencia de punto de contacto para reportar un incidente

Respuesta	**Cantidad**
SI	7
NO	0
Total	7

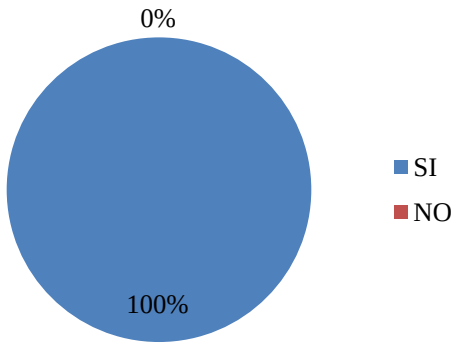


Figura 4. Existencia de punto de contacto para reportar un incidente

5. Medios para la detección de incidentes de seguridad

Tabla 5.

Medios para la detección de incidentes de seguridad

Respuesta	**Cantidad**
Antivirus	2
Seguimiento de Redes	1
Notificación de terceros	4
Otros	0
Total	7

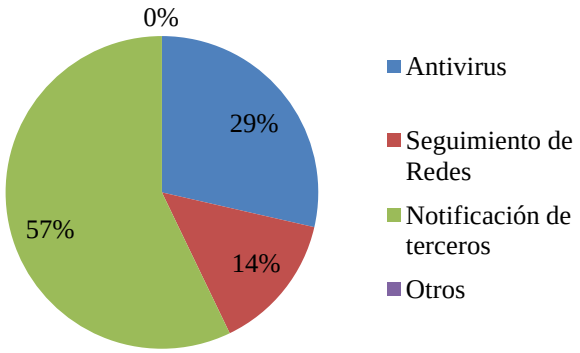


Figura 5. Medios para la detección de incidentes de seguridad

6. Diagnóstico acertado de incidentes de seguridad de la información

Tabla 6.

Diagnóstico acertado de incidentes de seguridad de la información

Respuesta	**Cantidad**
Muy acertado	0
Acertado	5
Poco acertado	2
Desacertado	0
Total	7

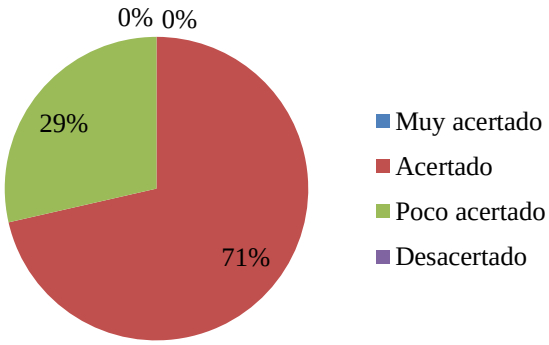


Figura 6. Diagnóstico acertado de incidentes de seguridad de la información

7. Seguimiento del incidente de seguridad de la información

Tabla 7.

Seguimiento del incidente de seguridad de la información

Respuesta	**Cantidad**
SI	7
NO	0
Total	7

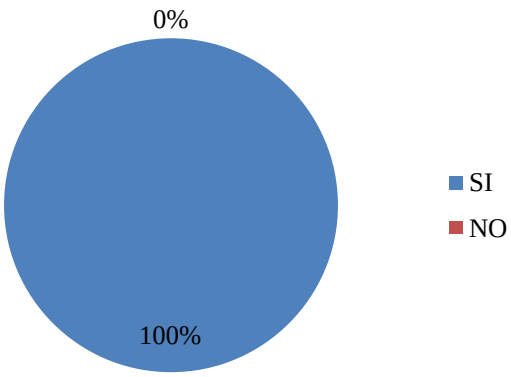


Figura 7. Seguimiento del incidente de seguridad de la información

8. Interacción con entidades en caso de un incidente de seguridad

Tabla 8.

Interacción con entidades en caso de un incidente de seguridad

Respuesta	**Cantidad**
Muy frecuentemente	0
Frecuentemente	7
Poco Frecuente	0
Nunca	0
Total	7

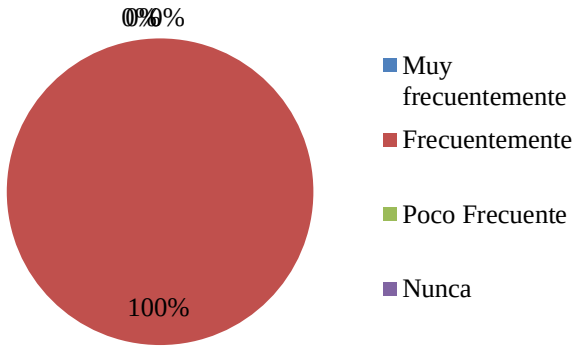


Figura 8. Interacción con entidades en caso de un incidente de seguridad

9. Expertos dentro de la corporación en incidentes de seguridad de la información

Tabla 9.

Expertos dentro de la corporación en incidentes de seguridad de la información

Respuesta	Cantidad
SI	0
NO	7
Total	7

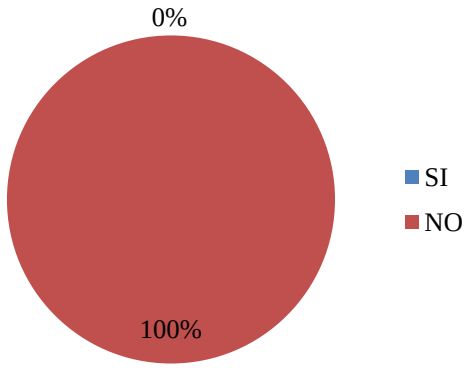


Figura 9. Expertos dentro de la corporación en incidentes de seguridad de la información

10. Calificación del estado de la gestión de incidentes de seguridad

Tabla 10.

Calificación del estado de la gestión de incidentes de seguridad

Respuesta	**Cantidad**
Excelente	1
Buena	3
Regular	3
Deficiente	0
Total	7

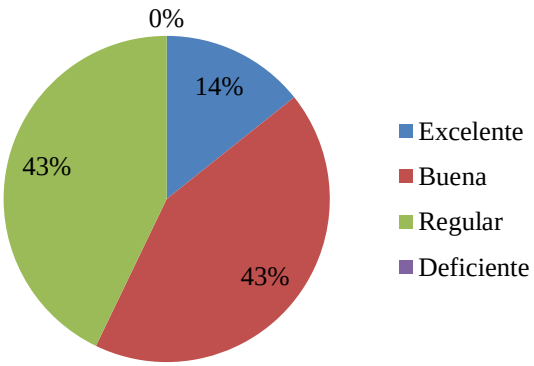


Figura 10. Calificación del estado de la gestión de incidentes de seguridad

Apéndice E. Encuesta para medir el estado de la gestión de incidentes de la seguridad de la información a los jefes de procesos

ENCUESTA 2

Nombre del encuestado: _____
Fecha: ____/____/_____ **Hora de Inicio**: __:__ **Hora Final**: __:__

Objetivo: recopilar información correspondiente al conocimiento de los incidentes de seguridad de la información en los procesos de la corporación.

Marque la opción que crea correcta:

1. Ha recibido capacitación referente a seguridad de la información
   - Muy frecuente
   - Frecuente
   - Poco Frecuente
   - Nunca

2. Ha recibido capacitación, tiene acceso al manual de usuario para la utilización de la mesa de ayuda
   - Si
   - No

3. Sabe cómo reportar incidentes de seguridad de la información y cuáles son los medios habilitados para reportarlos
   - Si
   - No

4. Conoce la diferencia entre incidente y evento de seguridad de la información
   - Si
   - No

5. Maneja medidas básicas de seguridad como no prestar sus claves, cerrar su sesión al momento de dejar las estaciones de trabajo, proteger con clave los archivos importantes, etc.

   - Muy frecuente
   - Frecuente
   - Poco Frecuente
   - Nunca

6. Con que frecuencia se le han presentado incidentes de seguridad virus, robo de datos, contenido malicioso

   - Muy frecuente
   - Frecuente
   - Poco Frecuente
   - Nunca

7. En caso de que se le hayan presentado incidentes como virus, robo de datos, contenido malicioso, califique la solución dada por el proceso de gestión tecnológica

- Excelente
- Buena
- Regular
- Deficiente
- No Aplica

Apéndice F. Encuesta para medir el estado de la gestión de incidentes de la seguridad de la información a los jefes de procesos

1. Capacitación referente a seguridad de la información

Tabla 1.

Capacitación referente a seguridad de la información

Respuesta	Cantidad
Muy frecuente	0
Frecuente	0
Poco Frecuente	5
Nunca	11
Total	16

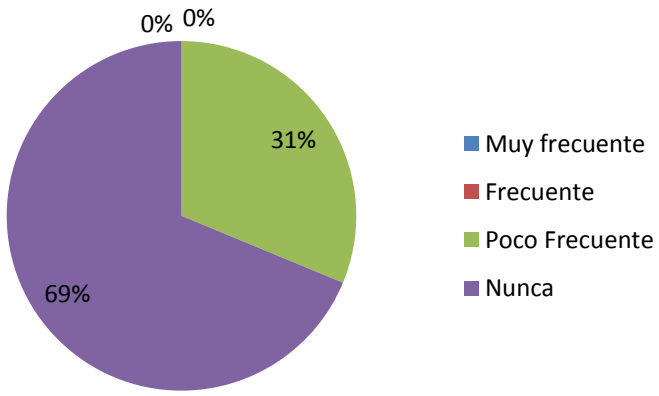


Figura 1. Capacitación referente a seguridad de la información

2. Capacitación y acceso al manual de usuario de la mesa de ayuda

Tabla 2.

Capacitación y acceso al manual de usuario de la mesa de ayuda

Respuesta	Cantidad
SI	14
NO	2
Total	16

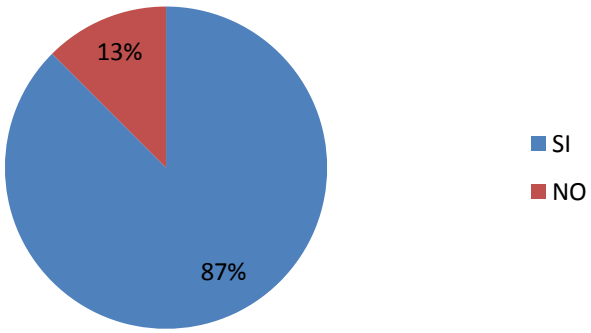


Figura 2. Capacitación y acceso al manual de usuario de la mesa de ayuda

3. Sabe cómo reportar incidentes de seguridad y a que proceso

Tabla 3.

Cómo reportar incidentes de seguridad y a que proceso

Respuesta	Cantidad
SI	12
NO	4
Total	16

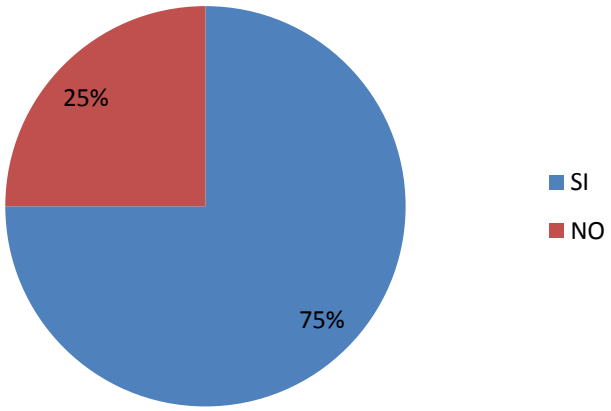


Figura 3. Cómo reportar incidentes de seguridad y a que proceso

4. Diferencia entre incidente y evento de seguridad de la información

Tabla 4.

Diferencia entre incidente y evento de seguridad de la información

Respuesta	Cantidad
SI	0
NO	16
Total	16

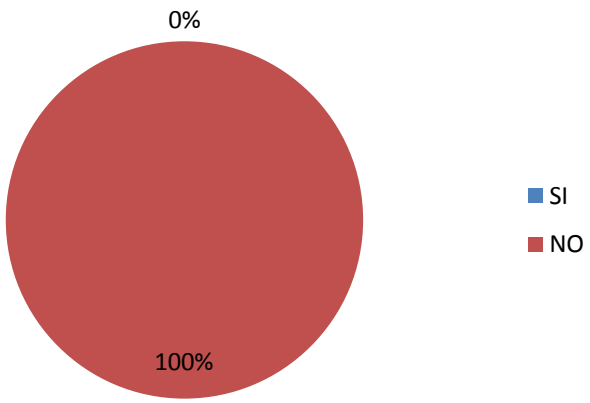


Figura 4. Diferencia entre incidente y evento de seguridad de la información

5. Medidas de seguridad (no prestar sus claves, cerrar su sesión, etc.).

Tabla 5.

Medidas de seguridad (no prestar sus claves, cerrar su sesión, etc.)

Respuesta	Cantidad
Muy frecuente	0
Frecuente	2
Poco Frecuente	8
Nunca	6
Total	16

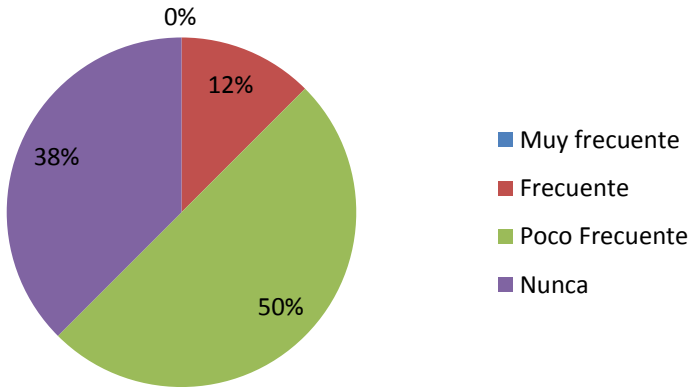


Figura 5. Medidas de seguridad (no prestar sus claves, cerrar su sesión, etc.)

6. Frecuencia de ocurrencia de incidentes de seguridad

Tabla 6.

Frecuencia de ocurrencia de incidentes de seguridad

Respuesta	**Cantidad**
Muy frecuente	0
Frecuente	4
Poco Frecuente	8
Nunca	4
Total	16

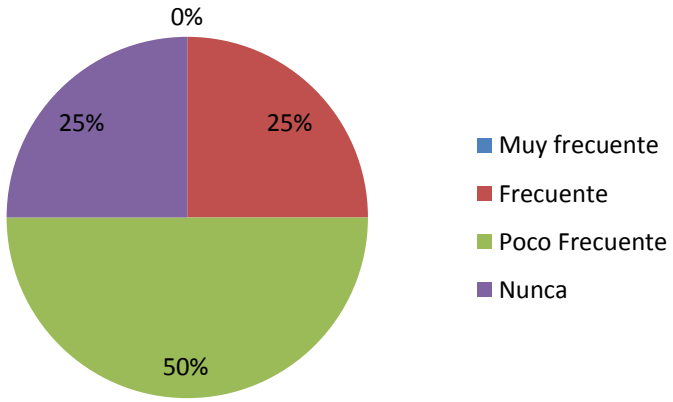


Figura 6. Frecuencia de ocurrencia de incidentes de seguridad

7. Calificación de la solución dada por el proceso de gestión tecnológica

Tabla 7.

Calificación de la solución dada por el proceso de gestión tecnológica

Respuesta	**Cantidad**
Excelente	1
Buena	5
Regular	5
Deficiente	1
No Aplica	4
Total	7

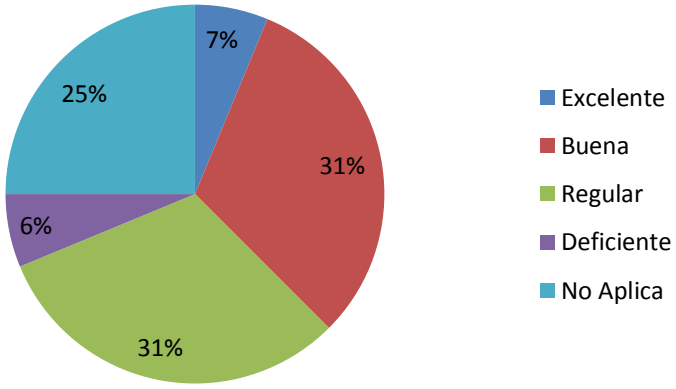


Figura 8. Calificación de la solución dada por el proceso de gestión tecnológica

Apéndice G. Lista de chequeo para medir el estado de la gestión de incidentes de la seguridad de la información al interior del Departamento de Gestión Tecnológica.

LISTA DE CHEQUEO

NOMBRE DE LA EMPRESA	COMFANORTE
PROCESO AUDITADO	Gestión Tecnológica
AUDITOR	Sergio Rubio Dayana González José Chacón

ITEM	CALIFICAR EL GRADO DE CUMPLIMIENTO	EXCELENTE	CUMPLE	MINIMO	NO CUMPLE
1	Existencia de una política de gestión de incidentes de seguridad de la información				✓
2	Existencia de una escala de clasificación de Eventos e incidentes de seguridad de la información				✓
3	Se tienen identificados los riesgos de seguridad de la información		✓		
4	Se realizan auditorías internas a la seguridad de la información		✓		
5	Existencia de formatos de eventos e incidentes de seguridad de la información			✓	
6	Almacenamiento de evidencia de incidentes de seguridad				✓
7	Existencia del registro de las actividades realizadas durante incidentes de seguridad de la información para análisis posterior			✓	

Apéndice H. Pruebas realizadas.

PRUEBA No 1 **CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE**	
PRUEBA	Auditorías internas de Seguridad de la información
OBJETIVO	Verificar la ejecución de auditorías de seguridad de la información
TECNICA EMPLEADA	Revisión documental
TIPO DE PRUEBA	Cumplimiento
PROCEDIMIENTO A EMPLEAR	1. Solicitar relación de auditorías internas al proceso de Gestión Tecnológica. 2. Revisar el alcance de las auditorías realizadas para verificar que se incluya la seguridad de la información.
RECURSOS	Lista de chequeo, auditorías internas al proceso
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Se evidencia la inclusión en el alcance de las auditorías internas, la seguridad de la información.
SITUACION DE RIESGO QUE GENERA	
RECOMENDACIONES DE AUDITORIA	Realizar al menos una auditoria anual con el objetivo principal de evaluar el nivel de seguridad de la información en la corporación
FECHA	19/09/2017
ELABORADA POR	Sergio David Rubio Dayana González José Chacón

PRUEBA No 2 **CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE**	
PRUEBA	Política de gestión de incidentes de seguridad de la información
OBJETIVO	Verificar el existencia del documento de política de gestión de incidentes de seguridad de la información
TECNICA EMPLEADA	Revisión documental
TIPO DE PRUEBA	Cumplimiento
PROCEDIMIENTO A EMPLEAR	1. Solicitar documento con de la política de gestión de incidentes de seguridad 2. Revisar que el documento cumpla con los criterios establecidos por la norma GTC-ISO/IEC 27035
RECURSOS	Documento de política de gestión de incidentes de seguridad de la información, lista de chequeo.
RESULTADOS DE LA PRUEBA	
HALLAZGOS	No se evidencia la existencia de un documento de

	política de gestión de incidentes de seguridad de la información.
SITUACION DE RIESGO QUE GENERA	Desconocimiento de un protocolo y desorden al momento de abordar un incidente de seguridad de la información.
RECOMENDACIONES DE AUDITORIA	Documentar y dar a conocer la política de gestión de incidentes de seguridad de la información
FECHA	20/09/2017
ELABORADA POR	Sergio David Rubio Dayana González José Chacón

PRUEBA No 3 **CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE**	
PRUEBA	Existencia de una escala de clasificación de Eventos e incidentes de seguridad de la información
OBJETIVO	Verificar la Existencia de una escala de clasificación de Eventos e incidentes de seguridad
TECNICA	Revisión documental
TIPO DE PRUEBA	Cumplimiento
PROCEDIMIENTO A EMPLEAR	1. Solicitar la escala de clasificación de Eventos e incidentes de seguridad 2. Revisar que el documento cumpla con los criterios establecidos por la norma GTC-ISO/IEC 27035
RECURSOS	Documento escala de clasificación de Eventos e incidentes de seguridad, lista de chequeo
RESULTADOS DE LA PRUEBA	
HALLAZGOS	No se evidencia la existencia de un documento de escala de clasificación de incidentes.
SITUACION DE RIESGO QUE GENERA	Incrementa el tiempo de respuesta al no tener claro el tipo de incidente y el procedimiento para abordarlo
RECOMENDACIONES DE AUDITORIA	Implementar documento de clasificación de eventos e incidentes de seguridad
FECHA	21/09/2017
ELABORADA POR	Sergio David Rubio Dayana González José Chacón

PRUEBA No 4 **CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE**	
PRUEBA	Existencia de un equipo de respuesta incidentes de seguridad de la información
OBJETIVO	Verificar la Existencia de un equipo de respuesta a incidentes de seguridad
TECNICA	Entrevista, encuesta y revisión documental
TIPO DE PRUEBA	Cumplimiento
PROCEDIMIENTO A EMPLEAR	1. Indagar sobre la existencia de un equipo de repuesta a incidentes

	2. Solicitar documento donde se establecen responsabilidades, con la información detallada. 3. Revisar que el documento cumpla con los criterios establecidos por la norma GTC-ISO/IEC 27035
RECURSOS	Documento Establecimiento de un equipo de respuesta a incidentes de seguridad de la información, cuestionario
RESULTADOS DE LA PRUEBA	
HALLAZGOS	No se evidencia la existencia de un documento de establecimiento de un equipo de respuesta a incidentes de seguridad.
SITUACION DE RIESGO QUE GENERA	Se presenta incertidumbre al momento de abordar un incidente al no tener claro quien se encargará de este.
RECOMENDACIONES DE AUDITORIA	Establecer y documentar la conformación de un equipo de respuesta a incidentes de seguridad de la información definiendo en detalle las responsabilidades de cada
FECHA	20/09/2017
ELABORADA POR	Sergio David Rubio Dayana González José Chacón

PRUEBA No 5 **CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE**	
PRUEBA	Canales para reportar eventos o incidentes de seguridad de la información
OBJETIVO	Verificar la Existencia de canales que permitan reportar eventos o incidentes de seguridad.
TECNICA	Entrevista, encuesta, Inspección
TIPO DE PRUEBA	Cumplimiento
PROCEDIMIENTO A EMPLEAR	1. Indagar sobre los canales para reportar eventos o incidentes de seguridad en la corporación 2. Evidenciar el funcionamiento y uso de esta aplicación
RECURSOS	Software para mesa de ayuda
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Se evidencia la existencia del software para mesa de ayuda Discovery, línea de telefonía interna y línea de celular.
SITUACION DE RIESGO QUE GENERA	
RECOMENDACIONES DE AUDITORIA	
FECHA	22/09/2017
ELABORADA POR	Sergio David Rubio Dayana González José Chacón

PRUEBA No 6 CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE	
PRUEBA	Conocimiento sobre seguridad de la información
OBJETIVO	Verificar la realización de capacitaciones de seguridad de la información a los funcionarios de la corporación.
TECNICA	Entrevista, encuesta
TIPO DE PRUEBA	Cumplimiento
PROCEDIMIENTO A EMPLEAR	1. Indagar sobre el desarrollo de capacitaciones de seguridad de la información 2. Solicitar las capacitaciones realizadas en el año 2016 y 2017.
RECURSOS	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Se evidencia que no se han realizado capacitaciones de seguridad de la información en los últimos dos años.
SITUACION DE RIESGO QUE GENERA	Vulnerabilidad en el recurso humano para seguridad de la información de la corporación Tratamiento errado de los incidentes de seguridad de la información
RECOMENDACIONES DE AUDITORIA	Solicitar al subproceso de gestión del conocimiento incluir en el programa de capacitación del personal de la caja, temas de seguridad de la información y tratamiento de eventos e incidentes de seguridad.
FECHA	21/09/2017
ELABORADA POR	Sergio David Rubio Dayana González José Chacón

Apéndice I. Situaciones Encontradas

Empresa	**Área Auditada**	**DIA**	**MES**	**AÑO**
Comfanorte	**Gestión Tecnológica**	26	09	2017

Ref.	**Situación**	**Causas**	**Solución**	**Fecha Sol.**	**Responsable**
1	Aunque se realizan auditorias que incluyen seguridad de la información no se realiza una auditoria que evalué el nivel de seguridad de la información en la corporación	No se prioriza dentro del plan de auditoría interna la ejecución de este tipo de auditorías.	Realizar al menos una auditoria anual con el objetivo principal de evaluar el nivel de seguridad de la información	Se establecerá en el comité de auditoria	Auditor Interno
2	No se evidencia la existencia de la política de gestión de incidentes de seguridad de la información.	Desconocimiento de la importancia de buenas prácticas en la gestión de incidentes	Documentar y dar a conocer la política de gestión de incidentes de seguridad de la información	Se establecerá en la reunión de grupo primario	Jefe de sistemas
3	Inexistencia de un documento de escala de clasificación de incidentes	Desconocimiento de buenas prácticas en la gestión de incidentes	Implementar documento de clasificación de eventos e incidentes de seguridad	Se establecerá en la reunión de grupo primario	Coordinador de administración de infraestructura tecnológica
4	Aun cuando existe un equipo de respuesta a incidentes no se evidencia la existencia de un documento donde se establezca el equipo y las responsabilidades de cada miembro.	Falta de claridad en las responsabilidades asumidas por cada integrante	Establecer y documentar la conformación de un equipo de respuesta a incidentes de seguridad de la información ISIRT, definiendo en detalle las responsabilidades de cada cargo.	Se establecerá en la reunión de grupo primario	Jefe de sistemas
5	Falta de capacitación de seguridad de la información en los últimos dos años	Falta de gestión del proceso de tecnología para incluir en el programa de capacitación de gestión del conocimiento temas referentes a la seguridad de la información	Solicitar al proceso de gestión de conocimiento incluir en el programa de capacitación del personal de la corporación, temas de seguridad de la información y tratamientos de eventos e incidentes de seguridad	Se establecerá en la reunión de grupo primario	Jefe de sistemas

Apéndice J. Situaciones Relevantes

Empresa Área Auditada	Fecha	Día	Mes	Año
COMFANORTE		27	10	2017

Ref.	Situaciones	Causas	Solución
2	No se evidencia la existencia de la política de gestión de incidentes de seguridad de la información.	Desconocimiento de la importancia de buenas prácticas en la gestión de incidentes	Documentar y dar a conocer la política de gestión de incidentes de seguridad de la información
3	Inexistencia de un documento de escala de clasificación de incidentes	Desconocimiento de buenas prácticas en la gestión de incidentes	Implementar documento de clasificación de eventos e incidentes de seguridad
4	Aun cuando existe un equipo de respuesta a incidentes no se evidencia la existencia de un documento donde se establezca el equipo y las responsabilidades de cada miembro.	Falta de claridad en las responsabilidades asumidas por cada integrante	Establecer y documentar la conformación de un equipo de respuesta a incidentes de seguridad de la información ISIRT, definiendo en detalle las responsabilidades de cada cargo.
5	Falta de capacitación de seguridad de la información en los últimos dos años	Falta de gestión del proceso de tecnología para incluir en el programa de capacitación de gestión del conocimiento temas referentes a la seguridad de la información	Solicitar al proceso de gestión de conocimiento incluir en el programa de capacitación del personal de la corporación, temas de seguridad de la información y tratamientos de eventos e incidentes de seguridad

Apendice K. Informe de Auditoría

Cúcuta, 6 octubre de 2017

COMFANORTE

Informe auditoria

De acuerdo a su respuesta positiva de realizar la auditoría pasiva con fines académicos utilizando como criterio la norma GTC-ISO/IEC 27035 y con el fin de evaluar la gestión de incidentes de seguridad de la información, me permito remitir el dictamen de la auditoría.

Organizados de mayor a menor relevancia se presentan los resultados obtenidos durante la auditoría: respecto a los requerimientos de documentación según la norma GTC ISO/IEC-27035, se evidenció la inexistencia de una política y plan de gestión de incidentes de seguridad de la información, respecto al equipo de respuesta a incidentes que tiene la corporación actualmente se observó que aunque está bien estructurado no hay claridad en la responsabilidades asumidas frente a un incidente, asimismo se evidenció la ausencia de definición de tiempos de respuesta debido a que no se ha realizado la clasificación de incidentes de seguridad. Del mismo modo se comprobó el desconocimiento del manejo de incidentes de seguridad por parte de los funcionarios de la corporación a causa de que no se dan instrucciones ni formación en toma de conciencia de gestión de incidentes y de seguridad informática.

De acuerdo a las pruebas realizadas, la información recolectada y los criterios de evaluación de la seguridad de la información es preciso indicar que para mantener la continuidad en la prestación de los servicios a sus afiliados la corporación debe establecer la gestión de incidentes de seguridad de la información basado en buenas prácticas lo que le permitirá controlar cualquier incidente de seguridad que se presente.

Atentamente,

Auditores,

Sergio David Rubio
María Dayana González
José Fabián Chacón

Apéndice L. Política de Gestión de Incidentes de seguridad de la información propuesto

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA LA CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE	Código: GT- Ai- Pl-2 Versión: 1.0 Tipo: Política Implementación: 15/12/2017

1. Declaración de compromiso de la alta dirección

La completa satisfacción de nuestros afiliados constituye para nuestra corporación el objetivo esencial. Conviene comprender sus necesidades presentes y futuras y esforzarse en estar más arriba de sus expectativas. Esta es la razón por la que la caja de compensación debe colaborar en la aplicación de la política de gestión de incidentes de seguridad descrita en el manual con el fin de mejorar continuamente su nivel de resultados y se garantice la continuidad del negocio.

La Caja de Compensación Familiar de Norte de Santander "COMFANORTE" se compromete a prestar todo el apoyo así como los recursos humanos y materiales necesarios para el cumplimiento de esta política y nombra al responsable _____ representante de la dirección para desarrollar, aplicar, mantener, mejorar y comprobar sus procesos y concientizar al personal.

Para dar cumplimiento a la anterior declaración de compromiso, la gerencia declara lo siguiente:

- Incentivar la creación del Equipo de Respuesta a Incidentes de Seguridad de la Información.

- Apoyar los procesos de implantación, gestión y comunicaciones entre procesos, departamentos y/o funcionarios tanto internos como externos, derivados de la aplicación de la política de gestión de incidentes de seguridad de la información.
- Participar activamente en los procesos de adopción de nuevos estándares para garantizar la gestión de incidentes de seguridad de la información.

2. Objetivos del esquema de gestión de incidentes de seguridad

La corporación debe garantizar la continuidad del negocio, los servicios ofrecidos no deben interrumpirse para garantizar la satisfacción del cliente, por eso se elabora el esquema de gestión de incidentes para dar respuesta rápida a aquellos riesgos residuales.

Los objetivos de la política de gestión de incidentes de seguridad de la información, son los siguientes:

- Responder a los eventos e incidentes de seguridad de la información.
- Escalar adecuadamente los eventos e incidentes de seguridad de la información.
- Registrar adecuadamente la información relacionada con el incidente.
- Establecer procedimientos para el reporte y tratamiento de incidentes de seguridad de la información.
- Crear una base de conocimiento de incidentes de seguridad y procedimientos aplicados para su solución.

3. Definición de Incidentes de Seguridad de la Información

- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4. Clasificación de incidentes de seguridad de la información

Los tipos de incidentes que son contemplados pueden agruparse dentro de la siguiente clasificación, según su tipo y como se presentan.

Incidente de daño físico. La pérdida de seguridad de la información es causada por acciones físicas accidentales o deliberadas. Son parte de esta categoría:

- Incendio
- Ambiente no apto (contaminación, polvo)
- Robo de equipos
- Perdida de equipos

Incidente de fallas de infraestructura. La pérdida de seguridad de la información es causada por fallas de los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información. Son parte de esta categoría:

- Fallas en alimentación eléctrica
- Fallas en aires acondicionados
- Fallas en las redes de cableado estructurado

Incidente de falla técnica. La pérdida de seguridad de la información es causada por fallas en los sistemas de información o problemas humanos no intencionales. Son parte de esta categoría:

- Falla del hardware
- Saturación capacidad de los sistemas

Incidente de malware. La pérdida de seguridad de la información es causada por programas maliciosos creados y divulgados en forma deliberada. Son parte de esta categoría:

- Virus informáticos
- Gusanos de red
- Troyanos
- Botnet (Robots que se ejecutan de manera autónoma)
- Página web con código malicioso

Incidente de ataque técnico. La pérdida de seguridad de la información es causada por el ataque a sistemas de información, a través de redes u otros medios técnicos aprovechando vulnerabilidades en redes, protocolos, programas, entre otros. Son parte de esta categoría:

- Escaneo de redes
- Vulnerabilidades en sistemas de información
- Interferencia
- Denegación de servicio

Incidente de violación de reglas. La pérdida de seguridad de la información es causada por la violación de las reglas de manera intencional o deliberada

- Violación de los derechos de autor
- Uso de recursos para propósitos no autorizados (páginas no autorizadas, correo no autorizado)

Incidente puesta en riesgo de la información. La pérdida de seguridad de la información es causada al poner en riesgo de forma accidental o deliberada la seguridad de la información. Son parte de esta categoría:

- Phishing
- Robo de datos
- Borrado de datos
- Alteración de datos
- Espionaje
- Chuzar teléfonos

Incidentes relacionados con contenidos peligrosos. La pérdida de seguridad de la información es causada por la propagación de contenido indeseable a través de redes de información

- Contenido ilegal (pornografía, fraude)
- Contenido malicioso (bromas pesadas, acoso)

5. Tratamiento un evento o incidente de seguridad

Al presentarse un evento o incidente de seguridad se debe reportar en el menor tiempo posible al punto de contacto mesa de servicios Discovery, el asistente de gestión tecnológica procederá a confirmar si es un evento o incidente y si es un evento lo escala al funcionario correspondiente de gestión tecnológica, en caso contrario de acuerdo al tipo de incidente, se encarga de escalarlo al equipo de respuesta evaluativa que es el primero en abordar el incidente, en el caso de poder resolverlo este realiza todo el proceso para dar solución caso opuesto lo debe escalar al equipo de respuesta experto.

Todo este procedimiento debe estar apoyado en los formatos Reporte de evento de seguridad de la información y Reporte de incidente de seguridad de la información según sea el caso, con el fin de poder llevar el control, seguimiento y trazabilidad del evento o incidente. Toda la evidencia recolectada debe preservarse de manera segura en caso que se requiera para emprender acciones legales o disciplinarias internas.

6. Visión general del equipo de respuesta a incidentes ISIRT

El equipo de respuesta a incidentes de seguridad de la información (ISIRT) será el encargado de actuar al ser confirmado un incidente de seguridad para lo cual se deben delimitar sus responsabilidades y alcance ya que en ciertos momentos se deberán tomar decisiones en tiempo real, para la atención de un incidente el ISIRT trabajará con tres equipos, los cuales son:

Equipo de Respuesta Evaluativa

Una vez registrado en la mesa de servicios Discovery el incidente de seguridad se debe desplegar el personal requerido de acuerdo a la magnitud y a los lugares afectados para realizar la evaluación del tipo de incidente y el impacto, de ser posible la solución por el equipo evaluador lo realiza el mismo, de lo contrario se debe escalar al siguiente equipo.

Equipo Respuesta Experto Interno

De acuerdo al tipo de incidente y el impacto se busca en el formato Información de contacto de personal ISIRT el personal interno más idóneo para ser contactado, estas deben estar capacitadas en el manejo del incidente y en la metodología a seguir: roles definidos, manejo de formatos, escalabilidad del incidente.

Equipo Respuesta Experto Externo

En caso de que el incidente no pueda ser controlado por el equipo de respuesta interno, se debe escalar al equipo externo con los datos de contacto registrados en el formato Información de

contacto de proveedores, que en coordinación con el grupo interno deben tomar todas las medidas necesarias para que el incidente pueda ser solucionado.

Elaborada por	Revisada por	Aprobada por
Sergio David Rubio Dayana González José Chacón	Sergio David Rubio Dayana González José Chacón	

Apéndice M. Plan de respuesta a incidentes propuesto

PLAN DE RESPUESTA A INCIDENTES PARA LA CAJA DE COMPENSACIÓN FAMILIAR DE NORTE DE SANTANDER COMFANORTE	Código: GT-Ai- Pla-2 Versión: 1.0 Tipo: Plan Implementación:15/12/2017

La necesidad de mantener la continuidad del negocio y no perder la confianza de clientes y proveedores, conlleva a la organización a establecer un conjunto de procedimientos para controlar cualquier incidente de seguridad que se presente.

La información contenida en el presente plan debe ser de acceso restringido y solo disponible para aquellas personas pertenecientes al ISIRT, ya que cualquier conocimiento que pueda tener algún agente externo puede aportar información y hacer más difícil la detección del origen del incidente y su posterior solución.

1. Visión General

De acuerdo a los requerimientos de la norma ISO/IEC 27035 la organización debe usar este plan de respuesta a incidentes para:

- Responder a eventos e incidentes de seguridad de la información
- Determinar si los eventos de seguridad de la información llegan a ser incidentes de seguridad de seguridad de la información
- Gestionar incidentes de seguridad de la información hasta su conclusión
- Responder a vulnerabilidades de seguridad de la información

- Identificar las lecciones aprendidas y cualquier mejora al esquema y/o seguridad en general que se requiera
- Hacer las mejoras identificadas

Este plan operará en mayor o menor escala al momento de detectarse un incidente de seguridad, todos procesos de la organización deben estar involucrados en la gestión de incidentes ya que es de vital importancia realizar una detección temprana para evitar el aumento de la magnitud del incidente.

2. Objetivos

El plan de gestión de incidentes ha sido desarrollado para cumplir con los siguientes objetivos:

- Proporcionar un enfoque organizado y consolidado para la gestión de la respuesta inicial y las actividades de recuperación después de un incidente o interrupción del negocio no planificado, evitando la confusión y reducir la exposición a errores.
- Proporcionar una respuesta rápida y adecuada a los incidentes no deseados, reduciendo así los impactos resultantes de las interrupciones del negocio a corto plazo.
- Notificar la adecuada gestión, al personal operativo, los clientes y las organizaciones pertinentes los hechos del incidente.
- Recuperar las operaciones empresariales esenciales en el momento oportuno, incrementar la capacidad de la corporación para recuperarse de una pérdida perjudicial

3. Categorización de incidentes

Como parte fundamental del plan es necesario saber los tipos de incidentes y categorizarlos, para luego clasificarlos de acuerdo a su severidad así una categoría de incidente de seguridad puede tener diferentes clases de severidad. En el documento clasificación de los incidentes de seguridad de la información se presentan la clasificación y categorización de incidentes y las clases de severidad.

4. Establecimiento del ISIRT

El objetivo de establecer el ISIRT es proveer a la organización con una capacidad adecuada para evaluar, responder a los incidentes de seguridad de la información, aprender de ellos y brindar la coordinación, gestión, retroalimentación y comunicación necesarias.

En el documento establecimiento del ISIRT se presenta la estrategia general de planificación y creación del equipo de respuesta a incidentes de seguridad de la información.

5. Actividades de los equipos del proceso de gestión de incidentes de seguridad de la información

Como se estableció en el documento establecimiento del ISIRT en el organigrama se encuentran varios equipos multidisciplinares virtuales, ningún equipo está conformado sino hasta cuando se presenta un incidente, puede no haber la necesidad de conformar todos los equipos, a continuación se presentan las actividades que deben realizar cada uno de estos equipos.

5.1 Actividades del oficial de seguridad del equipo de gestión de incidentes

- Los integrantes de los equipos deben en todo momento atender las recomendaciones del equipo de seguridad que es el encargado de velar por la integridad de los funcionarios, este equipo debe ser consultado en caso de limitaciones de acceso, en caso de requerir equipo especial de protección.
- Por ser este integrante del proceso de gestión humana como coordinador de subproceso seguridad y salud en el trabajo se debe regir por la política de seguridad y salud en el trabajo.
- En caso de presentarse afectación a la integridad física de algún funcionario debe desplegar el esquema de administración de los primeros auxilios, garantizar las medidas de vida y seguridad según sea necesario.
- Coordinarse con los demás equipos del proceso, cualquier actividad a realizar debe respetar la cadena de mando y debe ser informada al jefe de Gestión de incidentes.
- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

5.2 Actividades del responsable de información pública del equipo de gestión de incidentes

- Toda la información solicitada por entidades externas debe ser revisada por este equipo.
- Es el directamente implicado en la preparación de comunicados para los medios (prensa, televisión), instituciones gubernamentales y público en general.
- Toda información a divulgar pertinente al incidente de seguridad debe ser autorizada por la dirección administrativa.

- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

5.3 Actividades del responsable de enlace del equipo de gestión de incidentes

- Cualquier institución externa que se involucre en la solución del incidente debe entrar en comunicación previa con el responsable de enlace.
- Las entidades externas deben entrar en coordinación con los demás equipos, trabajo que debe realizar el responsable del enlace, estas entidades pueden ser la policía, entidades de seguridad de la información externas, entre otras.
- Cualquier acción a realizar se debe reportar al coordinador de Gestión de incidentes.
- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

5.4 Actividades del responsable del equipo de planeación

- Es el equipo encargado de llevar el control de los recursos asignados al incidente tales como manuales, mapas, planos, dispositivos tecnológicos, entre otros.
- El equipo responsable debe estar pendiente de las necesidades de los diferentes equipos, debe estar en estado de alerta ya que cualquier retraso es vital y causaría aumento de la criticidad del incidente.
- Mantener el inventario de los recursos para poder hacer la recuperación una vez sea solucionado el incidente, se debe almacenar la responsabilidad y estado de los recursos entregados.

- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

5.5 Actividades del responsable del equipo de logística

- Proporcionar todos los servicios de apoyo durante el incidente tales como instalaciones, refrigerios, recursos necesarios para eventos.
- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

5.6 Actividades del responsable del equipo de operaciones

- Este es el equipo de más carga laboral durante el incidente, ya que se encarga de la parte operativa de solución del incidente, este se divide en tres grupos:
  - Equipo de respuesta evaluativa
  - Equipo de respuesta experto interno
  - Equipo de respuesta experto externo
- Es el responsable de establecer toda la estrategia de respuesta al incidente
- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

5.7 Actividades del responsable del equipo de finanzas

- Es el encargado de llevar el control de los costos asociados al incidente y de realizar el informe de gastos.

- En este se incluye la negociación de los diferentes contratos requeridos.
- Solo se utilizan los recursos requeridos para el incidente concreto.
- La asignación de recursos debe ser flexible, esto no quiere decir que sea ilimitada, pero no se puede dejar pasar mucho tiempo para dar solución a un incidente porque aumentaría los costos del mismo.
- Las actividades realizadas durante la gestión del incidente se deben reportar en el respectivo informe post incidente.

6. Gestión y respuesta a incidentes

Al momento de afrontar un incidente de seguridad de la información es muy importante tener claro los pasos a seguir para evitar perder tiempo que sería valioso, la personas implicadas en el proceso deben saber a dónde recurrir y el procedimiento adecuado a realizar, las siguientes actividades están enmarcadas en los equipos pertenecientes al nivel de operaciones.

6.1 Como identificar y tratar un incidente de seguridad de la información

- En primera instancia se recibe una solicitud por cualquiera de los medios permitidos a la mesa de ayuda, telefónico, email, o se rastrea por medio de dispositivos de monitoreo, antivirus, reportes de incidentes de foros o proveedores, robo de activos de información, se debe diligenciar el formato de reporte de evento de seguridad.
- La mesa de ayuda clasifica la solicitud, y verifica si se trata de un incidente de seguridad u otro tipo de evento, de confirmarse el incidente el funcionario asistente de Gestión de

incidentes debe registrar la información del formato “Reporte de incidentes de seguridad de la información” y escala al Equipo de Respuesta Evaluativa.

- El asistente debe consultar en el “Formato de información de contacto de personal ISIRT” donde se encuentra la información de contacto de los integrantes de los equipos de gestión de incidentes y convocar al personal necesario para realizar la operación.
- El Equipo de Respuesta Evaluativa investiga el incidente utilizando la base de datos de incidentes ocurridos, en caso de encontrarse el incidente en la base de datos este equipo procede a aplicar el procedimiento de solución y tramitar el formato “Reporte de incidentes de seguridad de la información” para dar por solucionado el incidente, en caso contrario se debe escalar el incidente al Equipo Respuesta Experto Interno.
- Se debe convocar el equipo Respuesta Experto Interno el cual procede a verificar en las fuentes, fabricantes, foros, proveedores y realiza los demás procedimientos necesarios para eliminar o mitigar el incidente, en caso de dar solución al incidente se debe alimentar la base de datos de incidentes y tramitar el formato “Reporte de incidentes de seguridad de la información” para dar por solucionado el incidente, en caso contrario se debe escalar al equipo hibrido entre el equipo Respuesta Experto Interno y externo.
- De llegar a este paso los equipos de Respuesta Experto Interno y externo deben aunar esfuerzos y el incidente o conjunto de estos debe reportarse en estado crítico y realizar todo el procedimiento requerido para solucionarlo, esto incluye solicitar apoyo de otros ISIRT o personal externo requerido, anexo al tratamiento del incidente se debe reportar periódicamente a la dirección administrativa el estado del proceso, al momento de dar solución al incidente se debe alimentar la base de datos de incidentes y tramitar el formato “Reporte de incidentes de seguridad de la información” para dar por solucionado el incidente.

- Se necesita realizar la revisión final al proceso después de confirmada la solución del incidente para dar el parte definitivo y poder informar el restablecimiento de las operaciones al 100%.

7. Consideraciones adicionales:

- Los procedimientos de análisis forense, manejo de custodia, tratar correctamente los aspectos legales, restaurar el sistema, tener copias de seguridad, entre otros que pudieran surgir durante el proceso de gestión de los incidentes se pueden realizar por cualquiera de los equipos de respuesta en caso de ser necesario.
- Es importante documentar todo el proceso de gestión de incidentes encontrados, creando una base de datos que contenga eventos e incidentes de seguridad de la información gestionados por los equipos de respuesta a incidentes de seguridad y generar una retroalimentación para facilitar y evitar que se vuelvan a presentar en un futuro aplicando una metodología de mejoramiento continuo que permita optimizar el proceso.
- Los equipos de respuesta a incidentes no tienen tamaño fijo, dependiendo del tipo de incidente y la magnitud del mismo se puede requerir adherir al equipo personal de otros procesos de la corporación.
- Los equipos de respuesta a incidentes en caso de la ocurrencia de un incidente y de acuerdo a los procedimientos establecidos puede desconectar equipos de red, equipo de mesa, portátiles o cualquier dispositivo corporativo que sea motivo de investigación.
- Todos los empleados deben conocer la existencia del proceso de gestión de incidentes y colaborar en caso de ser necesario en esclarecer el incidente.

8. Actividades Generales de los Equipos de respuesta a Incidentes

Todos los equipos de respuestas a incidentes deben cumplir con la siguiente lista de actividades como parte del proceso de gestión del incidente.

8.1 Antes de la ocurrencia de un incidente

- Revisión de la información del contacto de los integrantes, que sea verídica y que se encuentre al día, se debe realizar verificación periódica, realizar llamadas de verificación.
- Se debe mantener a los integrantes en constante formación en temas de seguridad de la información, de esta manera se garantiza que el personal se encuentra capacitado en nuevos temas de seguridad.
- El personal del proceso de Gestión de incidentes debe conocer la infraestructura de la corporación y los cambios realizados, al momento de la ocurrencia del incidente se debe interactuar con los funcionarios y conocer la cadena de mando.

8.2 Durante un incidente

- Los integrantes de los equipos de respuesta deben Informar al coordinador del proceso de Gestión de Incidentes sobre el estado actual la situación del incidente, ya que este es el responsable de mantener informados a los demás procesos.
- Los integrantes de los equipos de respuesta deben saber obedecer órdenes de su jefe directo y realizar todas las tareas de trabajo que le sean asignadas.

- Los equipos deben registrar todas las actividades realizadas para dar solución al incidente, tanto en los formatos físicos establecidos, como en la base de datos de incidentes.
- Los equipos deben tener el criterio para determinar si un incidente se debe escalar a otro equipo de respuesta, de esto depende muchas veces la rapidez en que es resuelto.

8.3 Después de la ocurrencia del incidente

- Los equipos de respuesta a incidentes deben entregar toda la documentación relacionada con el caso a su jefe inmediato y reportar las entradas a la base de datos de incidentes para agregar el nuevo incidente con su solución o retroalimentar el existente.
- Los equipos de respuesta deben participar en actividades de depuración y/o recuperación post incidente y las investigaciones posteriores a la acción de incidencia, con el objetivo de limpiar cualquier rastro.
- Los equipos de respuesta pueden hacer recomendaciones para cambios y mejoras a los procesos de seguridad de la información o cualquier otro proceso que consideren debe mejorar para evitar que se repita el mismo incidente.
- Los equipos de respuesta deben en caso de ser necesario realizar todas las actividades de investigación para detectar el origen del incidente, este proceso puede seguir aun cuando se dé por finalizado y podría tener implicaciones legales.
- El proceso de Gestión de incidentes debe realizar la respectiva reunión de cierre donde se realiza la retroalimentación y evaluación del trabajo realizado.

9. Formatos

Para poder controlar las actividades realizadas antes durante y después de la ocurrencia de un incidente se debe tener un control adecuado de la información que se genera en cada uno de los procedimientos realizados, la mejor forma de realizarlo es documentar la información lo más clara y completa posible, a continuación se presentan los formatos propuestos para llevar la trazabilidad de eventos e incidentes de seguridad de la información.

9.1 Formato de información de contacto de personal ISIRT

El siguiente formato es utilizado para registrar la información de cada uno de los miembros del ISIRT, esta debe estar los más actualizada posible y tener varias copias tanto físicas como digitales.

INFORMACIÓN DE CONTACTO DE PERSONAL ISIRT					
Nombre	**Cargo**	**Proceso**	**Teléfono Oficina**	**Teléfono Celular**	**Teléfono Casa**

9.2 Formato de información de contacto de proveedores

El siguiente formato es utilizado para registrar la información de cada uno de los posibles proveedores de servicios en caso de un incidente, puede contener información de contacto de especialistas en seguridad de la información, análisis forense, entre otros.

INFORMACIÓN DE CONTACTO DE PROVEEDORES					
Nombre entidad	**Nombre persona contacto**	**Tema especialista**	**Teléfono Oficina**	**Teléfono Celular**	**Numero Fax**

9.3 Formato de reporte de evento de seguridad de la información

El siguiente formato se diligencia al momento de reportar un evento de seguridad de la información, la persona debe tener muy claras las fechas.

REPORTE DE EVENTO DE SEGURIDAD DE LA INFORMACIÓN	
Fecha Actual:	**Página 1 de 1**
Numero de Evento:	Eventos Relacionados:
DETALLES DE LA PERSONA QUE REPORTA	
Nombre:	Dirección:
Sede:	Proceso:
Teléfono:	Email:
DESCRIPCIÓN DE EVENTO DE SEGURIDAD DE LA INFORMACIÓN	
Descripción del Evento: • Que Ocurrió • Como Ocurrió • Porque Ocurrió • Activos Afectados • Anomalías Detectadas	
DETALLES DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN	
Fecha y Hora de Ocurrencia del Evento:	
Fecha y Hora de Detección del Evento:	
Fecha y Hora de Reporte del Evento:	

9.4 Formato de reporte de incidentes de seguridad de la información

En este formato se registra de manera detallada la información del incidente desde el momento en que se reporta hasta las conclusiones finales posteriores a la solución del mismo.

REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
Fecha Actual:		**Página 1 de 3**
Numero de Incidente:	Incidentes Relacionados:	
DETALLES DEL MIEMBRO DEL PUNTO DE CONTACTO		
Nombre:	Dirección:	
Sede:	Proceso:	
Teléfono:	Email:	
DETALLES DEL MIEMBRO DEL PUNTO DEL ISIRT		
Nombre:	Dirección:	
Sede:	Proceso:	
Teléfono:	Email:	
DESCRIPCIÓN DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
Descripción del Incidente: • Que Ocurrió • Como Ocurrió • Porque Ocurrió • Activos Afectados • Impactos para el Negocio • Anomalías Detectadas		
DETALLES DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
Fecha y Hora de Ocurrencia del Incidente:		
Fecha y Hora de Detección del Incidente:		
Fecha y Hora de Reporte del Incidente:		
Incidente Finalizado: (Marque la respuesta adecuada)	SI	NO
En caso afirmativo, Especifique cuanto duró el incidente		

REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	
	Página 2 de 3
CATEGORÍA DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	
Seleccione el tipo de incidente Daño físico _____ Ataque técnico _____ Fallas de infraestructura _____ Violación de reglas _____ Falla técnica _____ Puesta en riesgo de la información _____ Malware _____ Contenidos Peligrosos _____	
DETALLES DE LA CLASIFICACIÓN DEL INCIDENTE	
Escriba la clasificación del incidente:	
ACTIVOS AFECTADOS	
Información/Datos	
Hardware	
Software	
Comunicaciones	
Documentación	
Otros	
EFECTO DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	
Violación de la confidencialidad: ____	
Violación de la integridad:____	
Violación de la disponibilidad:____	
RESOLUCIÓN DEL INCIDENTE	
Fecha inicio investigación del incidente:	
Nombre investigadores del incidente:	
Fecha finalización del incidente:	
Fecha finalización investigación del incidente:	
SI EL INCIDENTE FUE CAUSADO POR PERSONAS	
Persona:_____ Organización establecida legal:_____ Grupo Organizado___ No hay Autor:___	
DESCRIPCIÓN DEL AUTOR:	
MOTIVACION REAL O PERCIBIDA:	

REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	
	Página 3 de 3
ACCIONES PARA RESOLVER INCIDENTE	
Acciones tomadas para resolver el incidente:	
Acciones planificadas para resolver el incidente:	
Acciones pendientes:	
CONCLUSION	
Conclusión del incidente:	
INDIVIDUOS INTERNOS	
Líder del ISIRT:_____ Líder de Sistemas de Información:_____ Otros:	
INDIVIDUOS EXTERNOS	
Organizaciones externas participantes:	

Apéndice N. Propuesta para el establecimiento del equipo de respuesta a incidentes de seguridad de la información.

ESTABLECIMIENTO DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 1.0 Tipo: Propuesta Implementación: 15/12/2017

El equipo de respuesta a incidentes de seguridad de la información ISIRT para la caja de compensación familiar COMFANORTE servirá a una población de 400 empleados. La institución tiene su propio proceso de Gestión Tecnológica cuenta con el colegio ubicado en el municipio de Los Patios, Ecoparque y sedes en Ocaña, Tibú, Pamplona y el Fundación de estudios superiores FESC.

Las Tecnologías de la información son muy importantes en la organización, pues soportan muchos procesos vitales para el trabajo diario, entre los cuales se tienen mensajería interna, sistemas de información, toda la infraestructura de red y cableado estructurado.
La organización trabaja en horarios de oficina y dispone de una red propia y de una conexión redundante a Internet por medio de dos proveedores de servicios de Internet diferentes.

1. Clasificación del ISIRT

El ISIRT que se establecerá en COMFANORTE es un ISIRT Interno ya que solo prestará sus servicios de respuesta a incidentes de seguridad a todos los procesos de la corporación. También apoyará y coordinara las diferentes sedes de la caja de compensación en el tratamiento de los incidentes relacionados con la seguridad de la información.

2. Servicios prestados por el ISIRT

De acuerdo a las características de Comfanorte los servicios que prestará son los siguientes:

Servicios reactivos

- Alertas y advertencias
- Tratamiento de incidentes
- Análisis de incidentes
- Apoyo a la respuesta a incidentes
- Coordinación de la respuesta a incidentes

Servicios proactivos

- Comunicados
- Evaluaciones o auditorías intrusivas de la seguridad
- Configuración y mantenimiento de la seguridad
- Servicios de detección de intrusos
- Difusión de información relacionada con la seguridad

3. Declaración de servicios

Los servicios que prestará el equipo de respuesta a incidentes de la organización, se plantea la siguiente declaración de servicios:

<< El ISIRT de la caja de compensación familiar COMFANORTE ofrece comunicados, evaluaciones y mantenimientos de la seguridad, detección de intrusiones y difusión de información relacionada con la seguridad de la información, así como tratamiento, análisis, apoyo y coordinación de la respuesta a incidentes de seguridad cuando se produzcan. >>

4. Definición del plan comercial

Modelo financiero. La corporación cuenta con el proceso de Gestión Tecnológica que funciona en horario 7 am a 12 m y de 2 pm a 6 pm de lunes a viernes, por lo que se decide prestar un servicio completo en dicho horario. Los costos de los servicios prestados por el ISIRT ya sea por personal externo o interno estarán a cargo de la caja de compensación.

Modelo organizativo. La organización a la que pertenece el ISIRT es una organización mediana, por lo que se elige el modelo incrustado ya que se va a hacer uso del proceso de Gestión Tecnológica ya existente.

En horario de oficina, el asistente de gestión de incidentes se encargará de los servicios básicos (distribución de avisos de seguridad, tratamiento, análisis, apoyo y coordinación de la respuesta a incidentes de seguridad).

Habrá un equipo central del ISIRT con tres miembros a tiempo completo y una empresa que presta servicios de seguridad de informática a la corporación, además en caso de ser

necesario el jefe del proceso de Gestión Tecnológica podría ceder recursos adecuados previa solicitud del ISIRT.

Personal. El coordinador del ISIRT debe tener experiencia en seguridad informática, mitigación de ataques y en el ámbito de la gestión de crisis. Los otros dos miembros del equipo son especialistas en seguridad informática. Los miembros del equipo procedentes del departamento de TI que intervienen a tiempo parcial son especialistas infraestructura de la empresa.

5. Uso Equipamiento de la oficina

La caja de compensación con 60 años de experiencia y más de 400 empleados cuenta con la infraestructura adecuada para acoger el ISIRT. Debe proveer la oficina muy cercana al área de gestión tecnológica donde se coordinará el accionar del equipo en caso de presentarse un incidente de seguridad de la información. Se debe proveer al equipo una caja fuerte donde se ubique todo el material sensible y líneas telefónicas fijas y móviles.

Se debe mantener la lista de correo electrónico de cada uno de los integrantes del equipo, información de contacto en copias digitales y una copia en físico dentro de la caja fuerte.

6. Buscar cooperación

Se realiza la búsqueda de equipos de respuesta a incidentes de seguridad de la información en el país, entre los que se tienen:

- Grupo de respuesta a emergencias cibernéticas de Colombia COLCERT
- Equipo de respuesta a incidentes informáticos CSIRT-PONAL
- Proyecto AMPARO donde se encuentra documentación y cursos.

7. Formar al personal

El ISIRT debe capacitar en seguridad de la información y gestión de incidentes a todo su personal técnico asociado a la seguridad de la corporación. Adicionalmente se deben incluir en el plan de capacitación de todos los funcionarios formación en manejo de incidentes.

8. Estructura organizacional del ISIRT

El equipo de respuesta a incidentes debe tener una estructura para garantizar la ejecución organizada de los procesos y evitar retrasos en la solución del incidente, la estructura propuesta se basa en el sistema de comando de incidentes (SCI), que permite el manejo efectivo y eficiente de los incidentes integrando una combinación de instalaciones, equipo, personal, procedimientos y comunicaciones que operan dentro de estructura organizacional común. La estructura del ISIRT planteada es la siguiente:

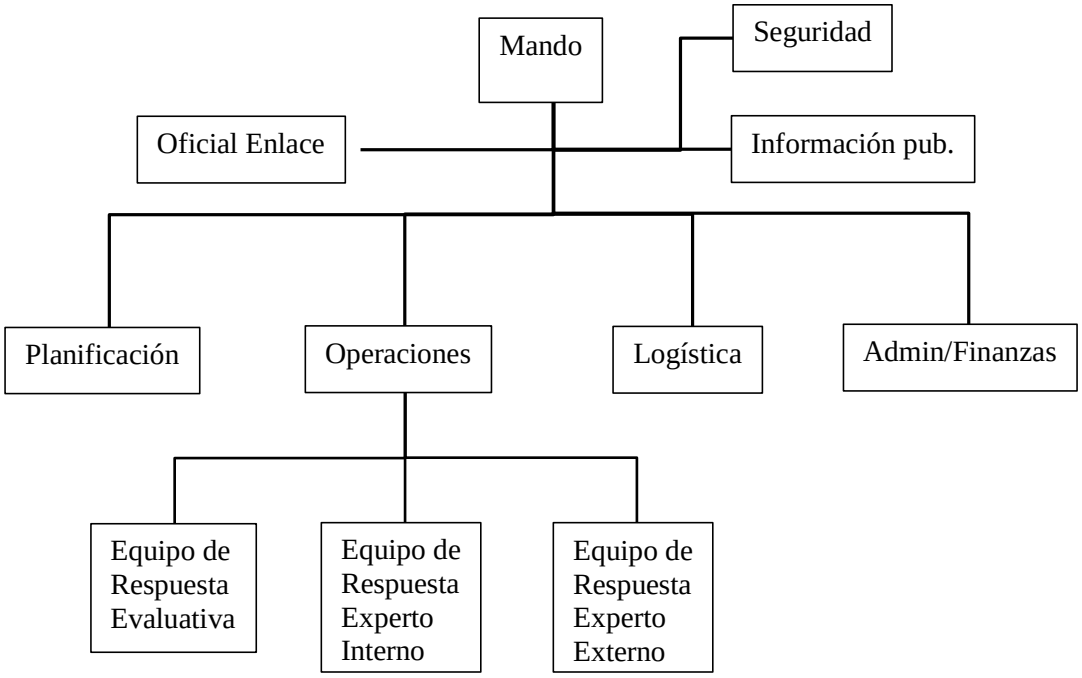


Figura. Estructura del ISIRT

Todos los equipos planteados en el organigrama a excepción del mando son equipos virtuales, solo se concentran en caso de la ocurrencia de un incidente, puede haber casos de no ser necesaria la instalación de algunos equipos, todo depende de la naturaleza del incidente. De acuerdo al organigrama anterior se plantean las responsabilidades asignadas a cada uno de los equipos:

Seguridad

- Proceso: Gestión humana
- Subproceso: Sistema de seguridad y salud en el trabajo
- Responsable: Equipo de seguridad

Información Pública

- Proceso: Gestión comercial y mercadeo
- Subproceso: Subproceso comunicaciones
- Responsable: Responsable de comunicaciones

Oficial Enlace

- Proceso: Gestión administrativa
- Subproceso: Gestión de la infraestructura
- Responsable: Coordinador de infraestructura

Planificación

- Proceso: Gestión administrativa
- Subproceso: Gestión de la infraestructura
- Responsable: Coordinador de infraestructura

Operaciones

- Proceso: Gestión Tecnológica
- Subproceso: Gestión de Incidentes
- Responsable: Responsable de Gestión de incidentes

Logística

- Proceso: Gestión administrativa
- Subproceso: Gestión de la infraestructura

- Responsable: Coordinador de infraestructura

Administración / Finanzas

- Proceso: Gestión financiera
- Subproceso: Presupuesto
- Responsable: Subdirector financiero

Las tareas asignadas a cada uno de los equipo de gestión de incidentes planteados en el organigrama se describen en el documento plan de respuesta a incidentes de seguridad de la información. (Apéndice M)