MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA FUNDAMENTADAS EN LA CIRCULAR 023 DE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR PARA CAJAS DE COMPENSACIÓN FAMILIAR

LUIS ALFREDO GONZALEZ RAMIREZ
JANETH PAOLA MEDINA MEDINA
MAGDA LORENA VIVAS MEDINA

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍAS
PROGRAMA INGENIERÍA DE SISTEMAS
NEIVA
2015

MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA FUNDAMENTADAS EN LA CIRCULAR 023 DE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR PARA CAJAS DE COMPENSACIÓN FAMILIAR

LUIS ALFREDO GONZALEZ RAMIREZ
JANETH PAOLA MEDINA MEDINA
MAGDA LORENA VIVAS MEDINA

Trabajo de grado presentado como requisito para optar al título de INGENIERO DE SISTEMAS

Asesor:
Ing. FERLEY MEDINA

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍAS
PROGRAMA INGENIERÍA DE SISTEMAS
NEIVA
2015

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

Neiva, Abril de 2015

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

RESUMEN

El diseño de una Política de Seguridad de la Información como base para las Cajas de Compensación Familiar, se realiza buscando un objetivo único y principal que se enfoca en crear conciencia organizacional, en lo referente a la protección de la información y de los datos.

La etapa inicial del proyecto se centra en la búsqueda de fuentes que permitan darle la importancia y la relevancia a este importante tema, partiendo de la base de un diagnóstico en seguridad que mostró varios puntos fundamentales de urgente intervención. Aplicando herramientas de recolección de información como observación, entrevistas y encuestas para evaluar el estado actual de la seguridad en algunas Cajas de Compensación Familiar, se establece y se confirma la falta de prácticas seguras en el área informática y la falta de preocupación por parte de la alta gerencia de las organizaciones para adoptar medidas al respecto.

Finalmente, se diseña una propuesta que, puesta en marcha, le ayudará a las Cajas de Compensación Familiar a mejorar su protección frente a riesgos inherentes a su actividad y marcará la ruta para iniciar un proyecto estructurado y que abarque todos los niveles de seguridad en la organización.

INTRODUCCIÓN

En la actualidad el mundo está cada vez más globalizado, y sigue integrándose día tras día, por tal razón, exige por parte de las organizaciones un mayor y mejor acceso a la información, esto con el objetivo de mejorar sus relaciones con clientes, proveedores y empleados. Las tecnologías de la información han abierto una serie de posibilidades para las empresas, dándoles nuevas oportunidades dentro de sus mercados y haciéndolas más competitivas.

Frente a estos nuevos cambios tecnológicos, también aparecen los riesgos y la necesidad de contar con una plataforma informática segura. Una forma de enfrentar los problemas de seguridad de la información que se presentan en la actualidad, es que las empresas entiendan lo importante que es proteger su sistema de información de los intrusos, usuarios o daños fortuitos que pongan en peligro el desempeño informático de la organización.

A la velocidad con que ocurren los cambios, sobretodo en el área tecnológica, hace difícil la planeación estratégica, que permita asegurar el capital intelectual representado por la información dentro de una empresa. Por lo que se hace necesario integrar las estrategias de negocio con las estrategias tecnológicas en materia informática, lo que traerá como consecuencia un diseño e implementación de políticas de seguridad que se ajusten a la organización.

La seguridad de la información, involucra la protección de los activos de la información, para lo cual es necesario identificar las situaciones de riesgo que se puedan determinar, cuáles de estos activos son vulnerables ante las amenazas, tanto internas, como externas a la empresa. Tomando en cuenta que entre los objetivos de la seguridad de la información, se encuentran el acceso, confiabilidad e integridad de la información, es necesario determinar qué herramientas o controles pueden ayudar, reducir y a monitorear los riesgos detectados en las plataformas informáticas empresariales. Entre este tipo de controles se cuentan las políticas o normas de seguridad para el manejo de la información tales como, la circular externa No. 023 del 2010numeral 5.4 de la Superintendencia del subsidio familiar.

1. PLANTEAMIENTO DEL PROBLEMA

Con el constante crecimiento de las tecnologías de la información, se va extendiendo también la aparición de nuevas aplicaciones, nuevos avances técnicos y mejoramiento en la funcionalidad de los mismos; por tanto y de forma paralela a estos, surgen nuevos riesgos, vulnerabilidades, virus y software malicioso circulando en la red, diseñados para alterar y/o cometer fraudes que pueden comprometer los sistemas de información de cada organización.

A pesar de esto, las organizaciones no invierten capital humano ni económico para prevenir el daño o pérdida de su información confidencial, a raíz de esto, es común observar que el personal que trabaja en las organizaciones tienen acceso a toda la información sin restricciones y no toman conciencia de la delicadeza de su contenido, esto se debe en parte a que en la mayoría de veces los computadores o las aplicaciones de uso frecuente son administrados sin contraseñas, y cuando lo hacen, son repetitivas y/o conocidas por más de un empleado.

Así mismo, no cuentan con un plan estratégico e infraestructura de tecnología, dando originen a las demoras en el tratamiento de incidentes que puedan presentarse en la organización, peor aún, las empresas no documentan los acontecimientos tecnológicos que ocurren en sus instalaciones y de esta manera no se puede llevar un seguimiento a las acciones preventivas y/o correctivas que se tomen, impidiendo el control adecuado.

Adicionalmente, la mayoría de las empresas no cuentan con un registro y/o control en las entradas y salidas de los equipos, causando de esta manera altos costos para su recuperación, además, y más importante aún, la pérdida irreversible de la información. Unido a esto, no hay una periodicidad establecida para la generación de copias de seguridad en las estaciones de trabajo, porque no se tiene en cuenta el gran flujo de información que se maneja en las Cajas de compensación familiar, ligado a esto, se evidencia la ausencia de un método de clasificación de esta información dependiendo de su contenido (pública, interna o confidencial), y mucho menos, establecen políticas para la reutilización de medios tecnológicos.

2. JUSTIFICACIÓN

Se debe tener en cuenta que en la actualidad, la información juega un papel muy importante y es considerado el activo más valioso en todas las organizaciones, lo cual ha generado que se le dé mayor atención a la disponibilidad, confidencialidad e integridad de los sistemas informáticos para así garantizar una fluidez de información segura y sistemas protegidos. Por lo tanto, se hace necesario contar con estrategias y procedimientos a la hora de implementar un sistema de seguridad de la información, para así garantizar el correcto funcionamiento de los sistemas y al momento de un posible ataque o desastre natural que traiga consigo perdida de información o sistemas informáticos, saber cómo actuar para mitigar el problema tomando los correctivos apropiados.

Según el informe Net Losses: Estimating the Global Cost of Cybercrime[1], del Centro de Estudios Estratégicos Internacionales (CSIS), Internet genera ingresos anuales que oscilan entre 2 y 3 billones de dólares. Sin embargo, recientes estudios han relevado que el robo de información sigue siendo la segunda forma más común de fraude, en el año 2013 una de cada cinco compañías presentaron pérdidas equivalentes a los 550 millones de dólares[2]; también se identificó que los empleados son mucho más responsables de la pérdida de información que los hackers[3]. Donde haya una pérdida, el 35% de las veces el problema es la acción ilegal de un empleado, más del doble de la tasa a la que se responsabiliza a los hackers externos en un 17% (porcentajes a nivel mundial), en Colombia la tasa de incidencia de robos de información por parte del personal de la organización es del 23%[4].

Con este proyecto se busca realizar un aporte valioso a las Cajas de Compensación Familiar, al diseñar una propuesta que sirva como base para la implementación de políticas de seguridad establecidas en la Circular 023 del 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar ayudando a mejorar su protección frente a riesgos inherentes a su actividad y creará conciencia organizacional en lo que se refiere a la seguridad de los datos y las implicaciones que conllevaría la no aplicación de las medidas diseñadas para tal fin.

[1] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. 2014. p. 8.
[2] KPMG. Encuesta de fraude en Colombia 2013. Bogotá D.C. 2013. p. 33.
[3] KROLL ADVISORY SOLUTIONS. Informe global sobre fraude. 2013. p. 6.
[4] KPMG. Encuesta de fraude en Colombia 2013. Bogotá D.C. 2013. p. 33.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un modelo de Políticas de Seguridad de la información para las Cajas de Compensación Familiar del departamento del Huila, tomando como referencia la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar los factores de riesgo y vulnerabilidad de la información mediante herramientas de recolección de información.

- Diseñar las Políticas de Seguridad de acuerdo a la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar necesarias para el control de la seguridad informática, a través del análisis, clasificación y monitoreo de los riesgos que afectan la infraestructura tecnológica de las Cajas de Compensación Familiar.

- Elaborar el modelo de Seguridad Tecnológica basado en la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar.

4. ESTADO DEL ARTE

La seguridad de la información para cualquier organización depende de factores como el grado de discreción del personal que manipula la información, el alojamiento de ésta y la configuración de sus niveles de accesibilidad y disposición. Es así como se ha determinado técnicamente que un esquema seguro debe corresponder al ajuste de los niveles de confidencialidad, integridad y disponibilidad de la información según los principios establecidos en las Directrices OCDE[5]. Las anteriores características se encuentran incluidas en la información, por lo que las organizaciones deben complementar el ciclo de seguridad con la constitución de políticas efectivas para que la información fluya dentro de procesos bien estructurados, formando los nombrados Sistemas de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo.

4.1 ÁMBITO LOCAL Y REGIONAL

Por medio de entrevistas vía telefónica y encuestas realizadas a empleados se identificó que entidades como Comfamiliar del Huila que se rige por la Circular 023 de 2010 de la Superintendencia del Subsidio Familiar en donde se da instrucciones para establecer Normas de Control Interno para la Gestión de la Tecnología, están en proceso de implementación con un porcentaje del 56% (*) de avance, a medida que se implementaron las pautas pertinentes para la seguridad de la información se manifestó conformidad en el cumplimiento de los requisitos legales ya que permitió demostrar a las autoridades competentes que la entidad trabaja de acuerdo a todas las leyes y normativas aplicables, desarrollando además una adecuada gestión de los riesgos que permite obtener un mejor conocimiento de los sistemas de información, sus problemas y los medios de protección, garantizando también una mejor disponibilidad de los materiales y datos necesarios.

[5] OCDE. Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, Julio de 2002.
(*)BELTRAN ROMERO, Jaime. Comfamiliar del Huila: Auditoría Interna. Neiva, Huila. Observación inédita, 2015.

4.2 ÁMBITO NACIONAL E INTERNACIONAL

Cada vez es más notoria en las empresas colombianas la pérdida de la información por el hecho de no saber administrar adecuadamente sus recursos tecnológicos, es por esa razón que la Superintendencia del Subsidio Familiar decidió tomar acciones preventivas en las Cajas de compensación de todo el país diseñando la Circular 023 de 2010. Sin embargo, solo en los grandes departamentos del país como Cundinamarca, Antioquia y Valle del cauca, en cajas de compensación como Colsubsidio, Cafam, Comfenalco y Compensarse encuentran en un porcentaje alto de avance en la implementación de dicha Circular con un porcentaje promedio del 85% (**), en donde se han dado beneficios tales como una mejora continua en la gestión de la seguridad y garantía de continuidad, reducción de los costos vinculados a los incidentes, incremento de los niveles de confianza de clientes y aumento del valor comercial y mejora de la imagen de la organización.

A nivel mundial, en países como Chile, las denominadas Cajas de Asignación Familiar son supervisadas por la Superintendencia de Seguridad Social, este ente gubernamental ha establecido una Normativa para el Sistema de Control Interno para las Mutualidades de Empleadores en la Circular 2892 del 17 de diciembre de 2012, en donde el Sistema de Control Interno tiene como finalidad verificar el cumplimiento de aspectos como la Gestión de la Mutualidad, transacciones realizadas con autorización correspondiente, contabilidad, entre otros, en el área de tecnología de información, la circular es puntual en los numerales 3.3.2, 3.3.4, 3.3.5 y 3.3.8[6] en donde se exige la seguridad de los sistemas de información, acceso restringido a los recursos, activos y registros, niveles definidos de autorización y el registro oportuno y adecuado de las transacciones y operaciones.

(**)BELTRAN ROMERO, Jaime. Comfamiliar del Huila: Auditoría Interna. Neiva, Huila. Observación inédita, 2015.

[6]SUPERINTENDENCIA DE SEGURIDAD SOCIAL. Circular 2892: Norma sobre sistema de control interno para las mutualidades de empleadores de la ley n° 16.744. Chile, 17 de diciembre de 2012.

5. MARCO CONCEPTUAL

5.1 CAJAS DE COMPENSACIÓN FAMILIAR

Son entidades privadas, sin ánimo de lucro, de redistribución económica y naturaleza solidaria, creadas para mejorar la calidad de vida de las familias de los trabajadores colombianos, mediante la gestión y entrega, en subsidios y servicios, de parte de los aportes de seguridad social que hacen los empleadores[7].

5.1.1 En Colombia. La primera vez que apareció el Subsidio Familiar en Colombia como prestación nueva y con este nombre, fue el 22 de febrero de 1949 en una convención colectiva entre la Empresa Ferrocarril de Antioquia y sus trabajadores, se estableció un subsidio de 3 pesos mensuales por cada hijo menor de 15 años. El 30 de junio de 1954 se firmó el acta de constitución de la primera caja de subsidio familiar por compensación en el país con el Nombre de Caja de Compensación Familiar de Antioquia, COMFAMA, la cual empezó a funcionar el 30 de agosto del mismo año (1954). Por decreto legislativo No. 118 de 1957 se extendió al país con carácter obligatorio, tres años más tarde. El Concepto en Colombia era totalmente novedoso, pues si bien correspondía a las tradicionales asignaciones familiares que se conocían ya en otros países, nuestros dirigentes empresariales optaron por anticiparse al estado y aplicarle la dinámica propia de la iniciativa privada, a una institución de Seguridad Social que hoy sin lugar a dudas muestra inequívocos beneficios[8].

Las cajas de compensación familiar son vigiladas por la Superintendencia del Subsidio Familiar, esta es una Entidad estatal del orden nacional cuya razón de ser, es garantizar mediante sus funciones de inspección, vigilancia y control, el eficaz funcionamiento de las Cajas de Compensación Familiar. Garantiza, de acuerdo acorde con la Ley y las normas vigentes, la ampliación de la cobertura del Sistema de Subsidio Familiar y la calidad de los servicios que prestan las Cajas de compensación, en especial a la población de medianos y bajos ingresos, en aplicación de los principios de universalidad y solidaridad - las 43 Cajas de Compensación Familiar que operan en Colombia son consideradas instrumentos de compensación y redistribución eficientes, que orientan los aportes de los empleadores (más de 364.000 empresas afiliadas), hacia las familias de los trabajadores con ingresos bajos y medios[9].

[7]COMFENALCO ANTIOQUIA. ¿Qué son las Cajas de Compensación? En: Comfenalco Antioquia, 2011.
[8]BUSINESSCOL. Cajas de Compensación Familiar en Colombia. En: BusinessCol, 2013.
[9]COMFAMA. Lo que debes saber sobre las Cajas de Compensación en Colombia. En: Comfama, 2012.

5.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información. La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas[10].

5.2.1 Propiedades de la Información.

5.2.1.1 Confidencialidad. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO)[11] en la norma ISO/IEC 27002 como garantizar que la información es accesible sólo para aquellos autorizados a tener acceso y es una de las piedras angulares de la seguridad de la información. La confidencialidad es uno de los objetivos de diseño de muchos criptosistemas, hecha posible en la práctica gracias a las técnicas de criptografía moderna.

5.2.1.2 Integridad. Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información[12].

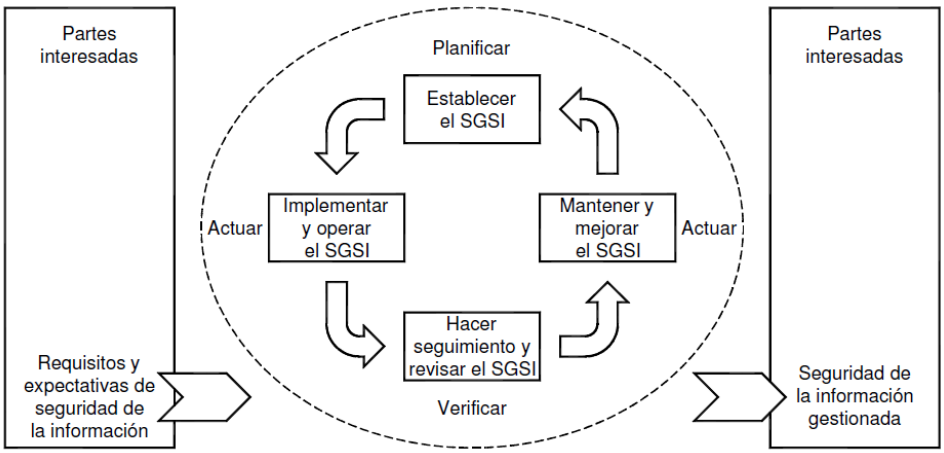
[10] GÓMEZ, Álvaro. Enciclopedia de la Seguridad Informática. 2007.
[11] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información: Generalidades. NTC-ISO 27001. Bogotá D.C.: El Instituto, 2013
[12] GÓMEZ, Álvaro. Enciclopedia de la Seguridad Informática. 2007.

5.2.1.3 Disponibilidad. Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, mediante el uso de clústeres o arreglos de discos[13].

5.3 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

ICONTEC [14] , expresa que un Sistema de Gestión de la Seguridad de la Información, es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.

Figura 1. Modelo PHVA aplicado a los procesos de SGSI



Fuente NTC-ISO/IEC 27001.

[13]GÓMEZ, Álvaro. Enciclopedia de la Seguridad Informática. 2007.
[14] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información: Generalidades. NTC-ISO 27001. Bogotá D.C.: El Instituto, 2013. p. I – II.

El modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA) que se puede apreciar en la Figura 1, se aplica para estructurar todos los procesos del SGSI. La Figura 1 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas.

5.4 CIRCULAR 023 DE 2010 DE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

Esta circular busca fortalecer los sistemas de control interno de las Cajas de Compensación Familiar, enfocada hacia una evaluación continua de su eficiencia y eficacia razonable, requiriendo de las Cajas una estructuración formal mediante la implementación y sostenimiento de un Sistema de Control Interno del Subsidio Familiar (SCISF) o su adecuación, de tal manera que dicho Sistema contribuya al logro de sus objetivos y fortalezca la apropiada administración de los riesgos a los cuales se ven expuestas las Cajas de Compensación Familiar en el desarrollo de su actividad para lograr condiciones de seguridad, transparencia y eficacia razonables[15].

Las reglas, parámetros generales y requisitos mínimos que se plantean en la Circular, deben ser implementados o ajustados por las Cajas de Compensación Familiar, de acuerdo con el tamaño de la respectiva organización, la naturaleza de sus actividades y la complejidad de sus operaciones, teniendo en cuenta la relación coste/beneficio.

5.4.1 Objetivos de la Circular.

- Mejorar la eficiencia y eficacia en las operaciones de las Cajas de Compensación Familiar.
- Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de las Cajas de Compensación Familiar.
- Orientar a los Organismos de Dirección, Administración y Jefaturas de las Cajas de Compensación Familiar en el cumplimiento de los deberes que les corresponde según la normatividad vigente, precisando el alcance de la responsabilidad en materia de control interno de los distintos órganos sociales.
- Fomentar tanto la autorregulación como el autocontrol, dado que sin perjuicio de la responsabilidad que corresponde a los administradores, todos los integrantes de la organización deben evaluar y controlar su propio trabajo.

[15]SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR. Circular externa 023 de 2010. Bogotá. 2010.

5.4.2 Elementos del SCISF. El SCISF debe abarcar todas las áreas de la Caja de Compensación Familiar, aplicando para cada una de ellas los objetivos, principios, elementos y actividades de control. Información, comunicación y otros fundamentos del sistema de control interno.

5.4.2.1 Normas de Control Interno para la Gestión de la Tecnología. La tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de servicios de las Cajas de Compensación Familiar en condiciones de seguridad, calidad y efectividad, para ello es necesario velar que el diseño del SCISF para la gestión de la tecnología responda a las políticas, necesidades y expectativas de la Caja, así como a las exigencias normativas, siendo necesario establecer igualmente mecanismos de evaluación y mejoramiento continuo para lograr los objetivos institucionales; contando con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir los siguientes aspectos:

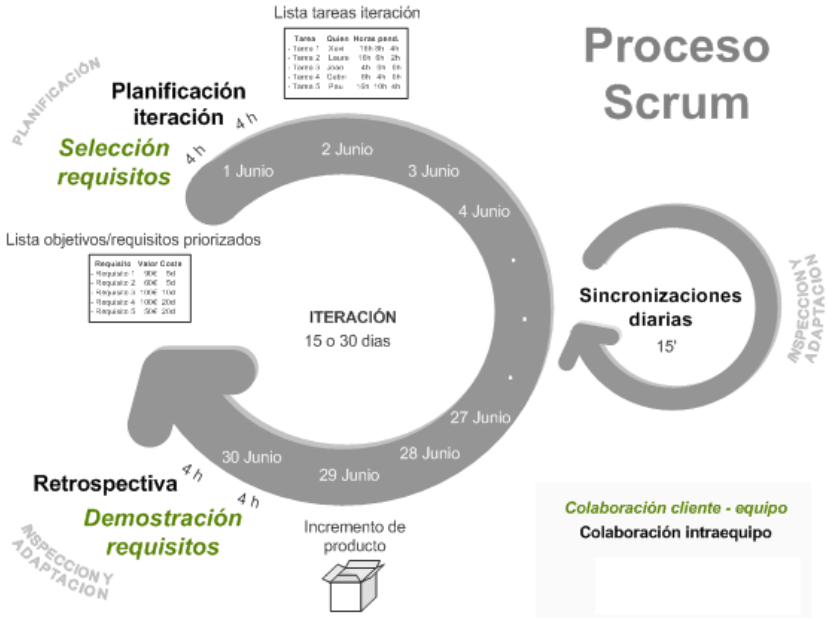
i. Plan estratégico e infraestructura de tecnología
ii. Relaciones con proveedores
iii. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico
iv. Administración de proyectos de sistemas
v. Administración de la calidad
vi. Adquisición de tecnología
vii. Adquisición y mantenimiento de software de aplicación
viii. Instalación y acreditación de sistemas
ix. Administración de cambios
x. Administración de servicios con terceros
xi. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica
xii. Continuidad de la Caja
xiii. Seguridad de los sistemas
xiv. Educación y entrenamiento de usuarios
xv. Administración de instalaciones
xvi. Administración de operaciones de tecnología
xvii. Documentación

6. METODOLOGÍA

La metodología utilizada para el desarrollo del proyecto fue un ciclo de desarrollo iterativo e incremental de tipo Scrum. Las principales razones de su uso son que las características del proyecto permiten desarrollar una base funcional mínima y sobre ella ir incrementando las funcionalidades o modificando el comportamiento o apariencia de las ya implementadas, entregas frecuentes y continuas de las políticas terminadas, de forma que puede disponer de una funcionalidad básica en un tiempo mínimo y a partir de ahí un incremento y mejora continua del sistema, y la previsible inestabilidad de los requisitos ya que es posible que el sistema incorpore más funcionalidades de las inicialmente identificadas y también es posible que durante la ejecución del proyecto se altere el orden en el que se desean recibir las políticas.

6.1. PROCESO

Figura 2. Proceso Scrum



Fuente: http://Proyectosagiles.org

El proceso parte de la lista de objetivos/requisitos (Product Backlog) priorizada del producto, que actúa como plan del proyecto. Seguidamente se realiza la lista de tareas (Sprint Backlog) que el equipo elabora en la reunión de planificación de la iteración como plan para completar los objetivos/requisitos seleccionados para la iteración y que se compromete a demostrar al cliente al finalizar la iteración, en forma de incremento de producto preparado para ser entregado.

6.2. LISTA DE OBJETIVOS / REQUISITOS PRIORIZADA (PRODUCT BACKLOG)

Tabla 1. Product Backlog

Product Backlog	Prioridad	Estimación de Esfuerzo (Persona/Hora)
Antecedentes del proyecto	1	124
Analizar los factores de riesgo y vulnerabilidad de la información.	2	60
Diseñar las Políticas de Seguridad de acuerdo a la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar.	3	62
Elaborar el modelo de Seguridad Tecnológica basado en la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar.	4	174

Fuente: El autor

6.3. LISTA DE ITERACIONES (SPRINT BACKLOG)

Tabla 2. Sprint Backlog

Product Backlog	Sprint Backlog	Tarea del Sprint	Responsable	Estimación de Esfuerzo (Horas/Persona)
Antecedentes del proyecto	Planteamiento del problema	Describir el problema	Janeth Paola Medina	4
		Determinar el espacio donde ocurre el problema	Magda Vivas	2
		Determinar los sujetos que intervienen en el problema	Luis Alfredo González	2
	Justificación	Necesidad de realizar el proyecto (conveniencia)	Magda Vivas	6
		Beneficios de realizar el proyecto	Janeth Paola Medina	4
	Objetivos	Definir la meta del proyecto	Janeth Paola Medina	4
		Determinar las tareas a realizar para la ejecución del proyecto	Magda Vivas	6
	Estado del arte	Investigar sobre sistemas de gestión de seguridad informática en cajas de compensación en el Huila	Luis Alfredo González	8

Product Backlog	Sprint Backlog	Tarea del Sprint	Responsable	Estimación de Esfuerzo (Horas/Persona)
Antecedentes del proyecto	Estado del arte	Investigar sobre sistemas de gestión de seguridad informática en cajas de compensación en Colombia	Luis Alfredo González	12
		Investigar sobre sistemas de gestión de seguridad informática en cajas de compensación a nivel internacional	Magda Vivas	16
	Marco conceptual	Definir qué son las cajas de compensación, cómo y para qué nacieron en Colombia	Janeth Paola Medina	8
		Definir que es seguridad de la información y cuáles son sus características	Luis Alfredo González	10
		Definir que es un sistema de gestión de seguridad de la información	Magda Vivas	8
		Definir que es la Circular 023 de la superintendencia del subsidio familiar y cuáles son sus objetivos	Luis Alfredo González	12
	Metodología	Establecer un cronograma de desarrollo de las actividades	Janeth Paola Medina	12
		Establecer el presupuesto de desarrollo del proyecto	Magda Vivas	10
Analizar los factores de riesgo y vulnerabilidad de la información.	Recolección de información	Elaboración de herramientas de recolección de información (encuesta y entrevista) para empleados de Comfamiliar Huila.	Janeth Paola Medina	10
		Aplicación de las herramientas de recolección de información a los empleados de Comfamiliar Huila.	Luis Alfredo González	8
	Interpretación de información recolectada	Tabulación de la información recolectada.	Magda Vivas	12
		Análisis de la información tabulada.	Janeth Paola Medina	16
		Clasificación de los factores de riesgo y vulnerabilidad de la información recolectada.	Luis Alfredo González	14

Product Backlog	Sprint Backlog	Tarea del Sprint	Responsable	Estimación de Esfuerzo (Horas/Persona)
Diseñar las Políticas de Seguridad de acuerdo a la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar.	Definir el alcance de las NCIGT.	Determinar número de empleados, volumen de información, de activos físicos y lógicos	Luis Alfredo González	6
		Determinar en qué áreas de la caja de compensación se va a implementar el sistema de gestión	Luis Alfredo González	4
	Elaborar la política general de seguridad.	Normativa interna del sistema de gestión de seguridad de la información	Janeth Paola Medina	14
		Utilización de los activos físicos y lógicos	Magda Vivas	16
		Manejo de incidentes de seguridad.	Janeth Paola Medina	12
		Seleccionar los procesos a elaborar de la Circular 023 de 2010 de la Superintendencia del subsidio familiar.	Luis Alfredo González	10
Elaborar el modelo de Seguridad Tecnológica basado en la Circular 023 de 2010 numeral 5.4 de la Superintendencia del Subsidio Familiar.	Elaborar el proceso de Seguridad física y del Entorno.	Áreas de acceso restringido	Janeth Paola Medina	10
		Normas de seguridad para el acceso físico a las áreas restringidas	Magda Vivas	16
		Protección y ubicación de equipos y redes	Luis Alfredo González	12
		Seguridad de equipos móviles	Magda Vivas	10
	Elaborar el proceso de Gestión de Comunicaciones y Operaciones.	Protección contra código malicioso	Janeth Paola Medina	14
		Gestión de copias de respaldo	Luis Alfredo González	16
		Gestión de seguridad de redes	Janeth Paola Medina	12
		Intercambio de información confidencial	Magda Vivas	14
		Monitoreo	Luis Alfredo González	10
	Elaborar el proceso de Control de Acceso Lógico.	Gestión de acceso de usuarios	Janeth Paola Medina	16
		Gestión de privilegios	Magda Vivas	12
		Manejo de contraseñas	Janeth Paola Medina	10
		Responsabilidades de los usuarios	Luis Alfredo González	8
		Controles de seguridad en los servicios de red	Magda Vivas	14

Fuente: El autor

6.4. ITERACIONES

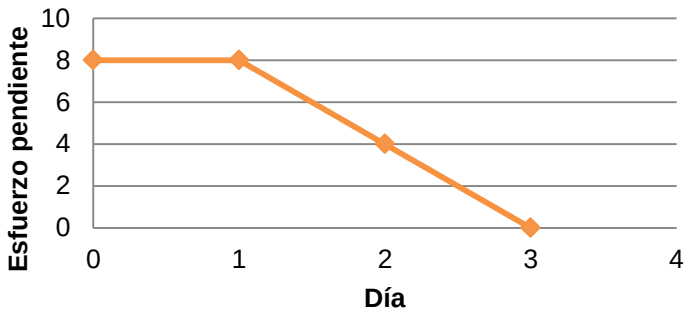
6.4.1 Planteamiento del problema

Tabla 3. Sprint 1

Sprint 1: Planteamiento del problema.			Valor estimado por día				
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5
Describir el problema	Janeth Paola Medina	4	4	2	0	0	
Determinar el espacio donde ocurre el problema	Magda Vivas	2	2	2	0	0	
Determinar los sujetos que intervienen en el problema	Luis Alfredo González	2	2	0	0	0	

Fuente: El autor

Gráfica1. Avance del Sprint 1



Fuente: El autor.

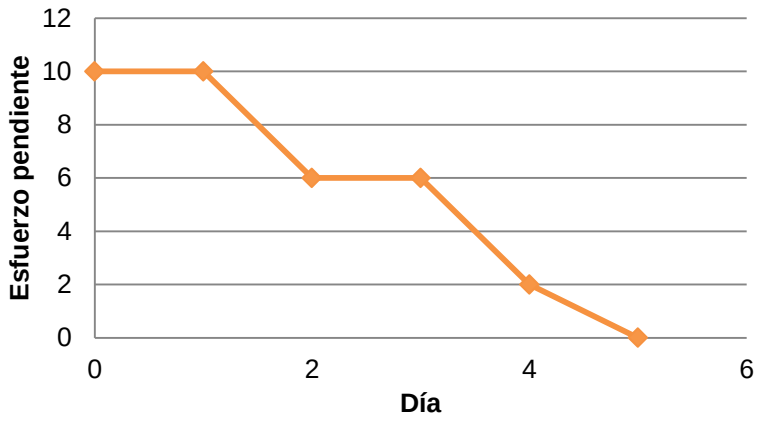
6.4.2 Justificación

Tabla 4. Sprint 2

Sprint 2: Justificación.			Valor Estimado por día					
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6
Necesidad de realizar el proyecto (conveniencia)	Magda Vivas	6	6	4	4	2	0	0
Beneficios de realizar el proyecto	Janeth Paola Medina	4	4	2	2	0	0	0

Fuente: El autor.

Gráfica 2. Avance del Sprint 2



Fuente: El autor.

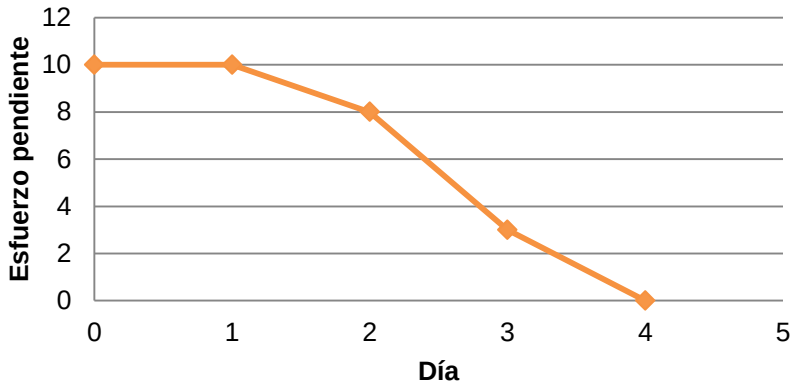
6.4.3 Objetivos

Tabla 5. Sprint 3

Sprint 3: Objetivos.			Valor estimado por día						
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7
Definir la meta del proyecto	Janeth Paola Medina	4	4	4	2	0	0	0	
Determinar las tareas a realizar para la ejecución del proyecto	Magda Vivas	6	6	4	1	0	0	0	

Fuente: El autor

Gráfica3. Avance del Sprint 3



Fuente: El autor

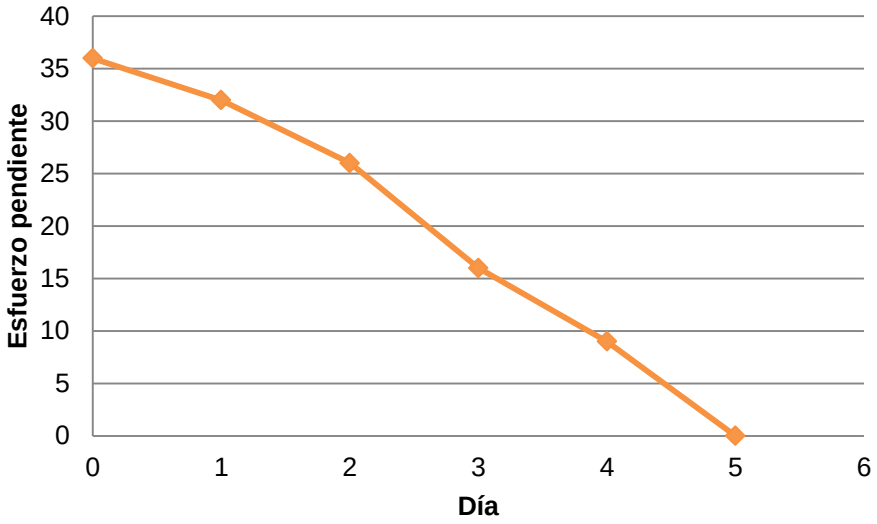
6.4.4 Estado del Arte

Tabla 6. Sprint 4

Sprint 4: Estado del arte.			Valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Investigar sobre sistemas de gestión de seguridad informática en cajas de compensación en el Huila	Luis Alfredo González	8	8	8	6	4	1	0			
Investigar sobre sistemas de gestión de seguridad informática en cajas de compensación en Colombia	Luis Alfredo González	12	10	8	5	3	1	0			
Investigar sobre sistemas de gestión de seguridad informática en cajas de compensación a nivel internacional	Magda Vivas	16	14	10	5	2	0	0			

Fuente: El autor.

Gráfica4. Avance del Sprint 4



Fuente: El autor.

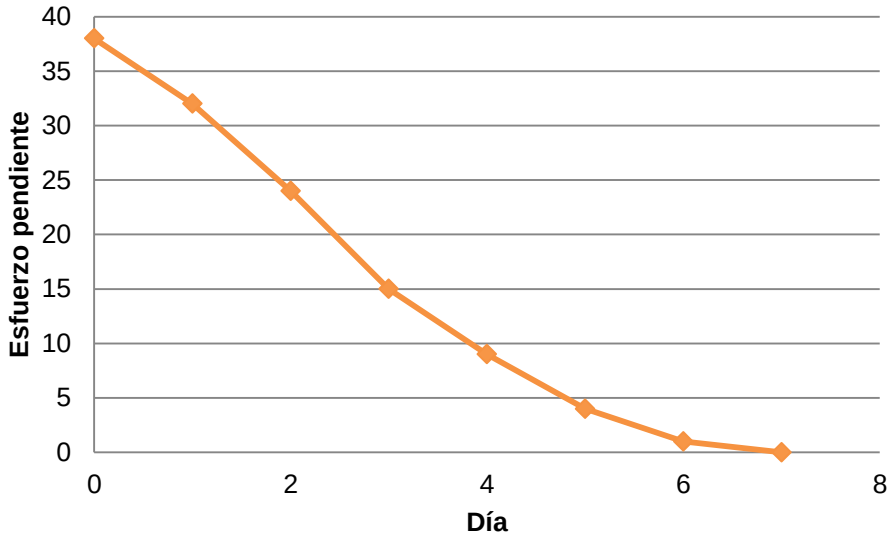
6.4.5 Marco conceptual

Tabla 7. Sprint 5

Sprint 5: Marco conceptual.			Valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Definir qué son las cajas de compensación, cómo y para qué nacieron en Colombia	Janeth Paola Medina	8	8	8	5	3	3	1	0		
Definir que es seguridad de la información y cuáles son sus características	Luis Alfredo González	10	8	6	6	4	1	0	0		
Definir que es un sistema de gestión de seguridad de la información	Magda Vivas	8	6	3	0	0	0	0	0		
Definir que es la Circular 023 de la superintendencia del subsidio familiar y cuáles son sus objetivos	Luis Alfredo González	12	10	7	4	2	0	0	0		

Fuente: El autor.

Gráfica5. Avance del Sprint 5



Fuente: El autor.

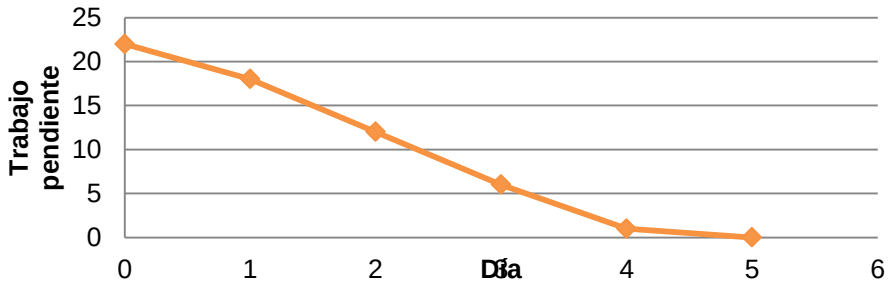
6.4.6 Metodología

Tabla 8. Sprint 6

Sprint 6: Metodología.			Valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Establecer un cronograma de desarrollo de las actividades	Janeth Paola Medina	12	10	8	4	1	0				
Establecer el presupuesto de desarrollo del proyecto	Magda Vivas	10	8	4	2	0	0				

Fuente: El autor

Gráfica6. Avance del Sprint 6



Fuente: El autor

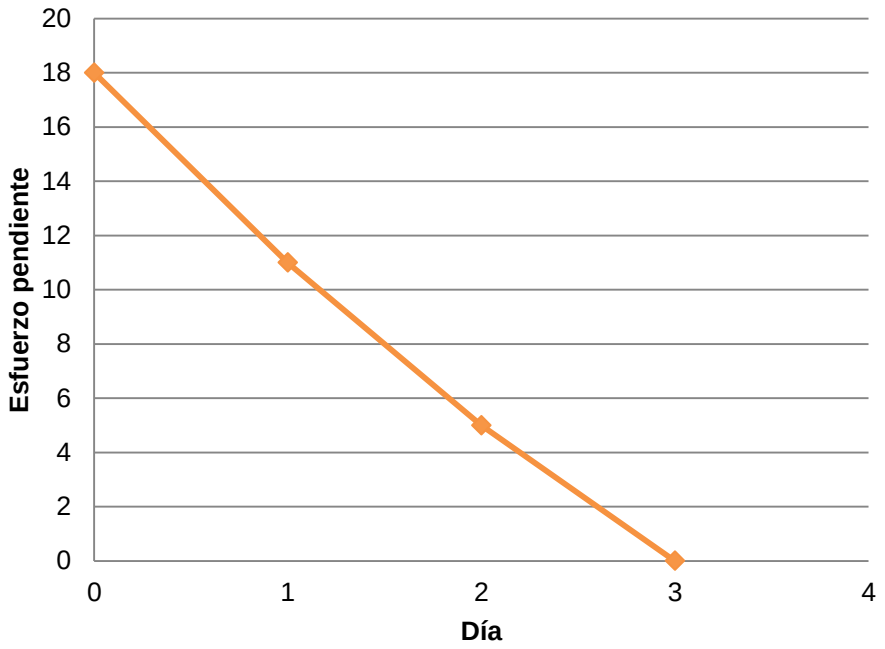
6.4.7 Recolección de información

Tabla 9. Sprint 7

Sprint 7: Recolección de información.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Elaboración de herramientas de recolección de información (encuesta y entrevista) para empleados de Comfamiliar Huila.	Janeth Paola Medina	10	6	2	0						
Aplicación de las herramientas de recolección de información a los empleados de Comfamiliar Huila.	Luis Alfredo González	8	5	3	0						

Fuente: El autor

Gráfica 7. Avance del Sprint 7



Fuente: El autor.

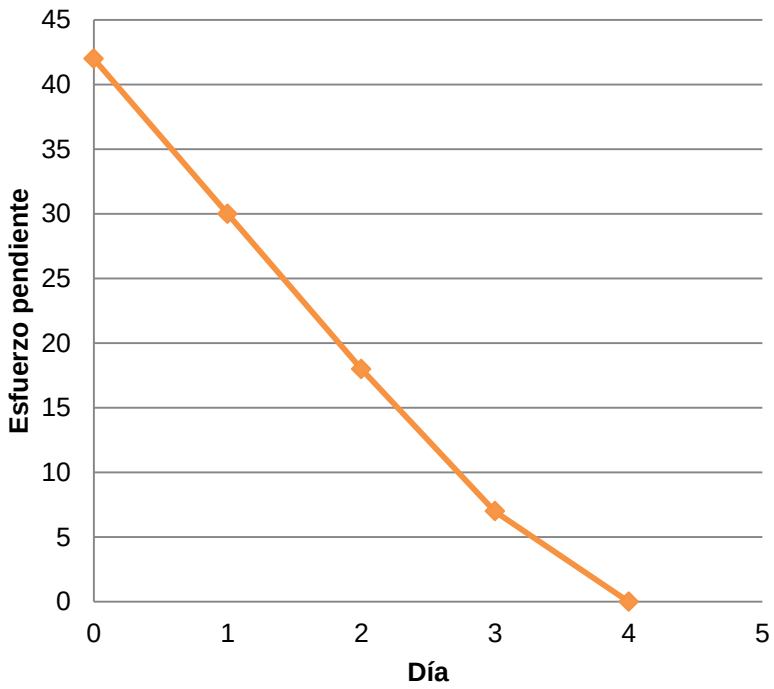
6.4.8 Interpretación de información recolectada

Tabla 10. Sprint 8

Sprint 8: Interpretación de información recolectada.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Tabulación de la información recolectada.	Magda Vivas	12	8	4	0	0					
Análisis de la información tabulada.	Janeth Paola Medina	16	12	8	4	0					
Clasificación de los factores de riesgo y vulnerabilidad de la información recolectada.	Luis Alfredo González	14	10	6	3	0					

Fuente: El autor.

Gráfica 8. Avance del Sprint 8.



Fuente: El autor.

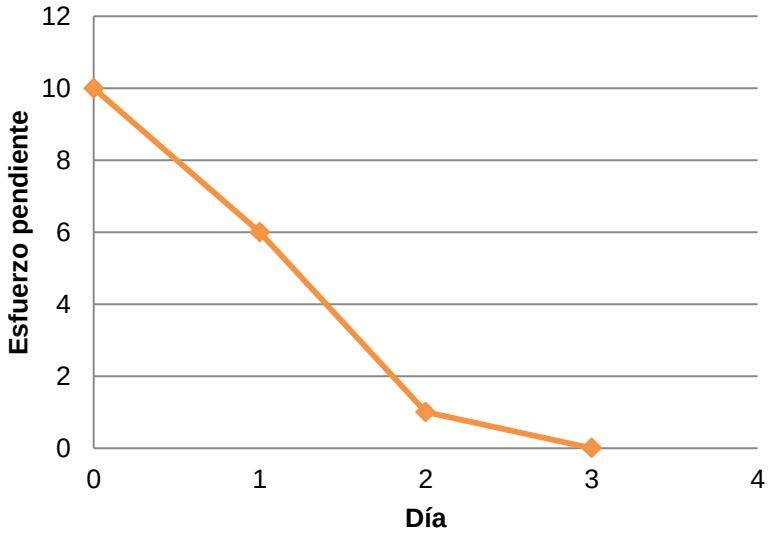
6.4.9 Definir el alcance de las NCIGT

Tabla 11. Sprint 9

Sprint 9: Definir el alcance de las NCIGT.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Determinar número de empleados, volumen de información, de activos físicos y lógicos	Luis Alfredo González	6	4	1	0						
Determinar en qué áreas de la caja de compensación se va a implementar el sistema de gestión	Luis Alfredo González	4	2	0	0						

Fuente: El autor.

Gráfica 9. Avance del Sprint 9



Fuente: El autor.

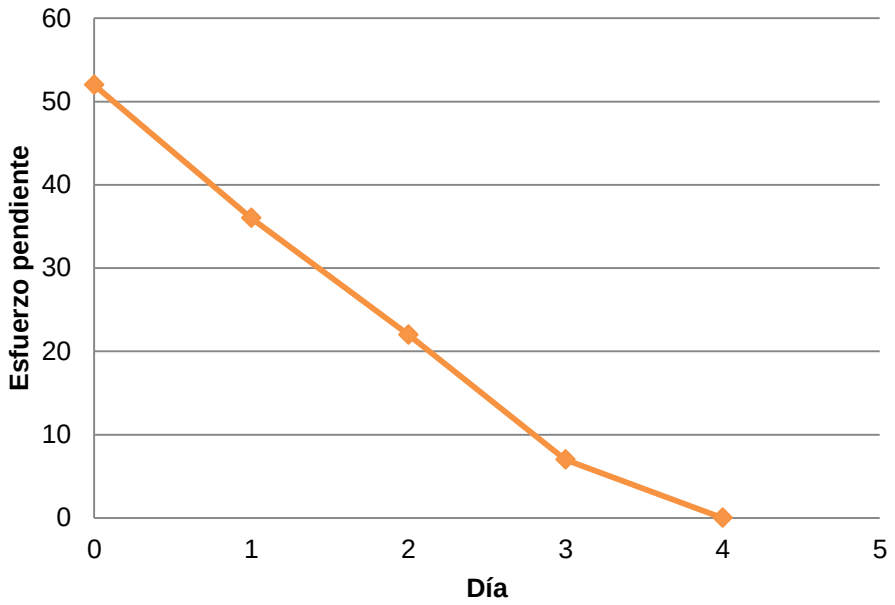
6.4.10 Elaborar la política general de seguridad

Tabla 12. Sprint 10.

Sprint 10: Elaborar la política general de seguridad.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Normativa interna del sistema de gestión de seguridad de la información	Janeth Paola Medina	14	10	7	3	0					
Utilización de los activos físicos y lógicos	Magda Vivas	16	12	7	3	0					
Manejo de incidentes de seguridad.	Janeth Paola Medina	12	8	5	1	0					
Seleccionar los procesos a elaborar de la Circular 023 de 2010 de la Superintendencia del subsidio familiar.	Luis Alfredo González	10	6	3	0	0					

Fuente: El autor.

Gráfica 10. Avance del Sprint 10.



Fuente: El autor.

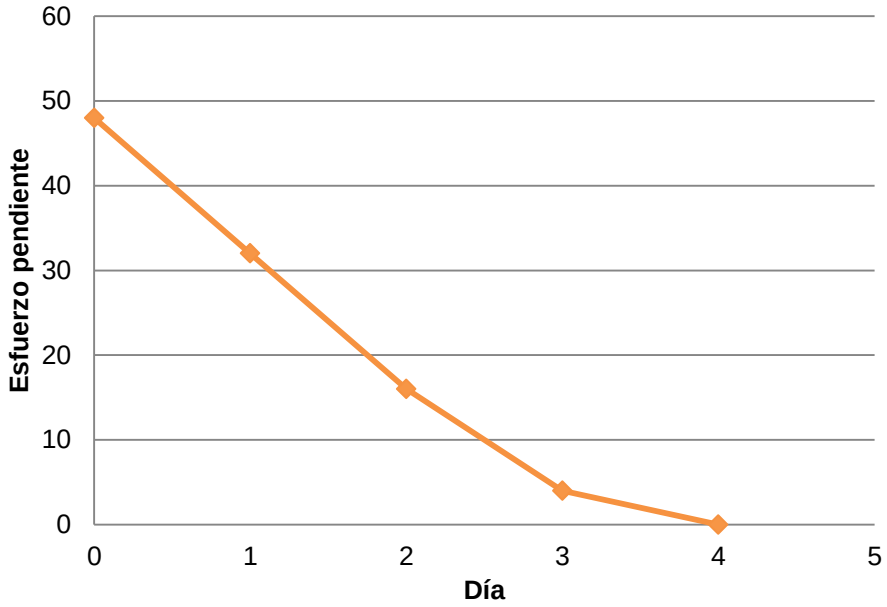
6.4.11 Elaborar el proceso de Seguridad física y del Entorno

Tabla 13. Sprint 11.

Sprint 11: Elaborar el proceso de Seguridad física y del Entorno.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Áreas de acceso restringido	Janeth Paola Medina	10	6	2	0	0					
Normas de seguridad para el acceso físico a las áreas restringidas	Magda Vivas	16	12	8	4	0					
Protección y ubicación de equipos y redes	Luis Alfredo González	12	8	3	0	0					
Seguridad de equipos móviles	Magda Vivas	10	6	3	0	0					

Fuente: El autor

Gráfica 11. Avance del Sprint 11.



Fuente: El autor

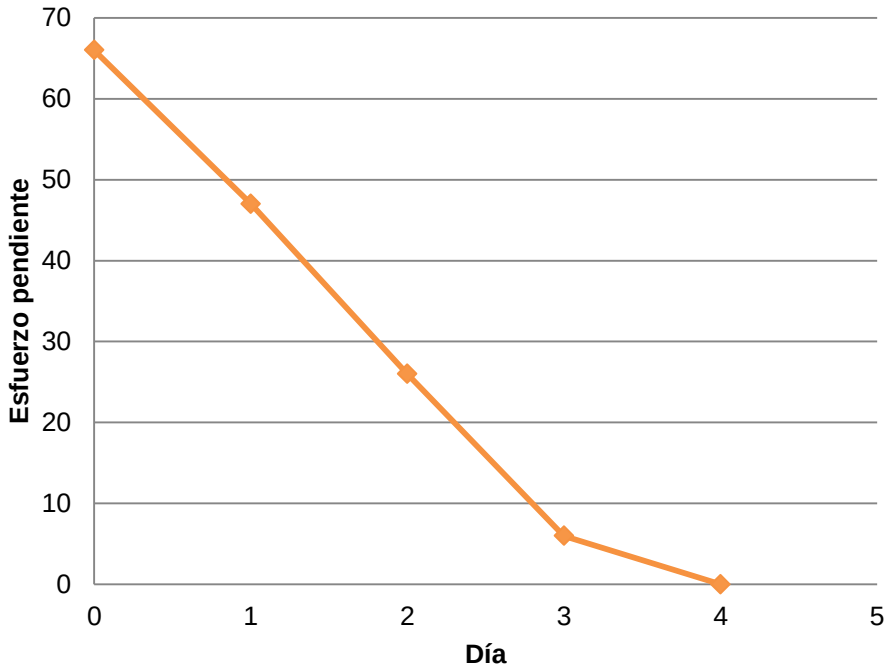
6.4.12 Elaborar el proceso de Gestión de Comunicaciones y Operaciones

Tabla 14. Sprint 12.

Sprint 12: Elaborar el proceso de Gestión de Comunicaciones y Operaciones.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Protección contra código malicioso	Janeth Paola Medina	14	10	5	1	0					
Gestión de copias de respaldo	Luis Alfredo González	16	12	7	3	0					
Gestión de seguridad de redes	Janeth Paola Medina	12	8	5	0	0					
Intercambio de información confidencial	Magda Vivas	14	10	7	2	0					
Monitoreo	Luis Alfredo González	10	7	2	0	0					

Fuente: El autor.

Gráfica 12. Avance del Sprint 12.



Fuente: El autor.

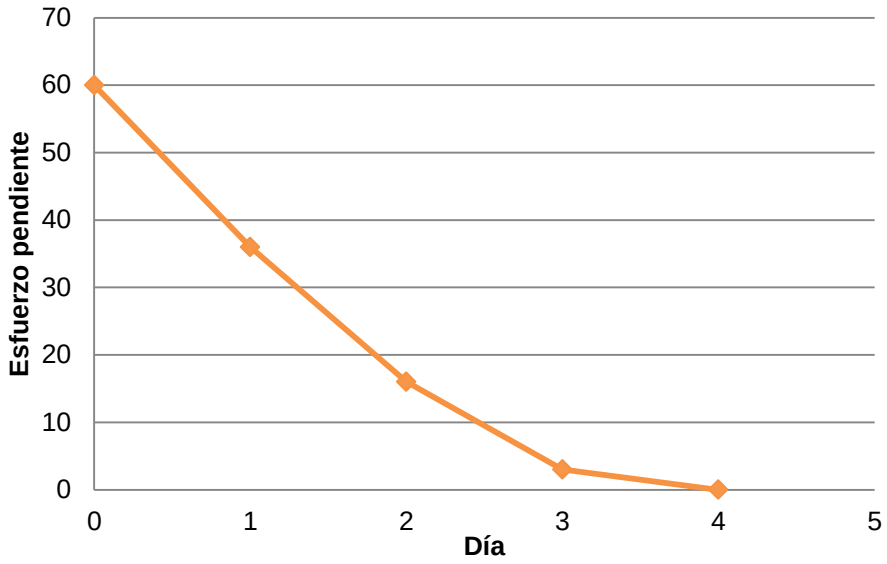
6.4.13 Elaborar el proceso de Control de Acceso lógico

Tabla 15. Sprint 13.

Sprint 13: Elaborar el proceso de Control de Acceso Lógico.			Nuevo valor estimado por día								
Tarea del Sprint	Responsable	Estimación de Esfuerzo	1	2	3	4	5	6	7	8	9
Gestión de acceso de usuarios	Janeth Paola Medina	16	10	6	2	0					
Gestión de privilegios	Magda Vivas	12	7	2	0	0					
Manejo de contraseñas	Janeth Paola Medina	10	5	2	0	0					
Responsabilidades de los usuarios	Luis Alfredo González	8	4	0	0	0					
Controles de seguridad en los servicios de red	Magda Vivas	14	10	6	1	0					

Fuente: El autor

Gráfica 13. Avance del Sprint 13.



Fuente: El autor.

7. CRONOGRAMA DE ACTIVIDADES

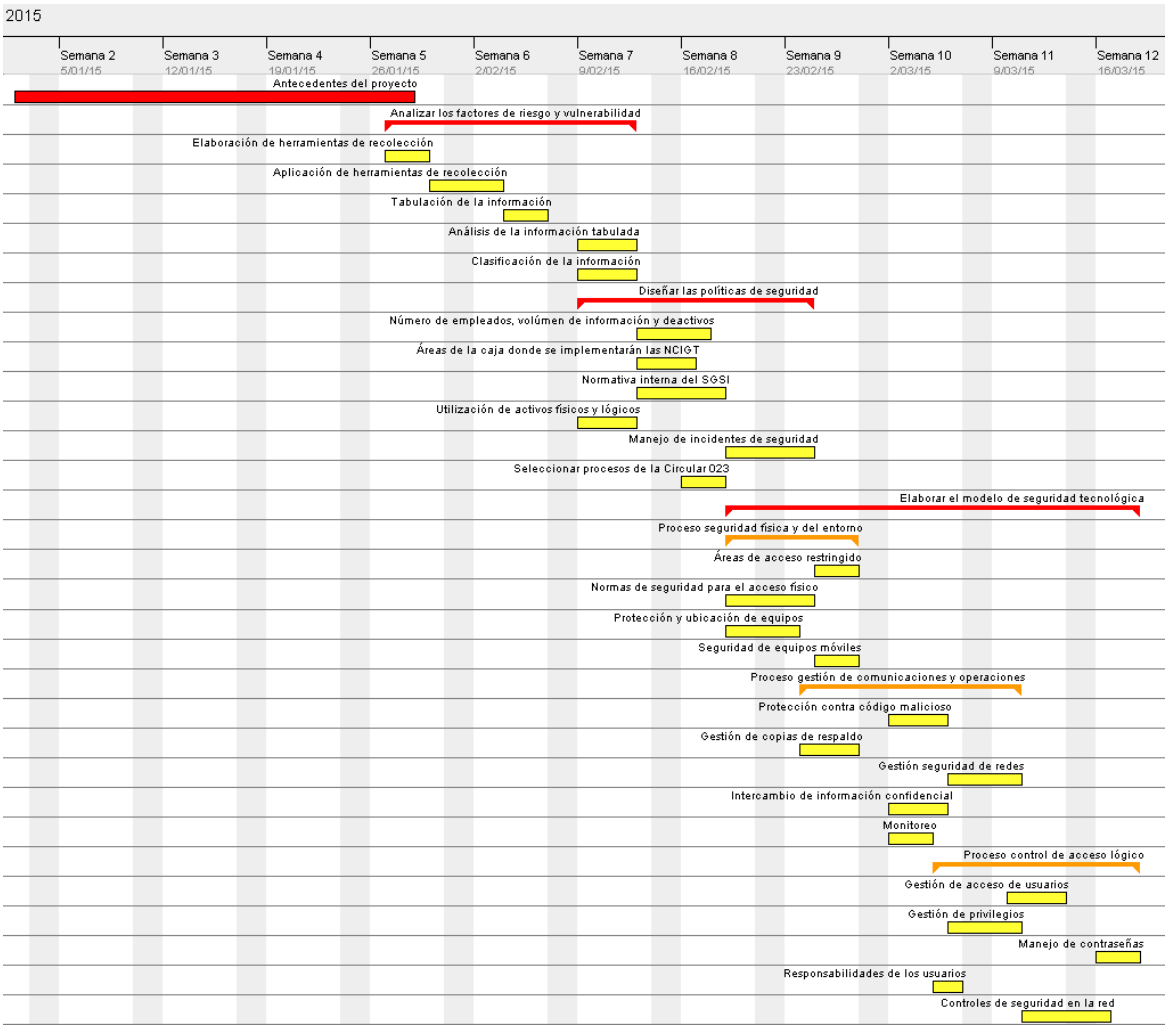
Las Figuras 3 y 4 contienen el cronograma de trabajo para el desarrollo del proyecto, en ellas se describen las actividades a realizar y el tiempo que se dedica a la ejecución de cada una.

Figura 3. Actividades

Nombre	Fecha de inicio	Fecha de fin
Antecedentes del proyecto	2/01/15	28/01/15
Analizar los factores de riesgo y vulnerabilidad	27/01/15	12/02/15
Elaboración de herramientas de recolección	27/01/15	29/01/15
Aplicación de herramientas de recolección	30/01/15	3/02/15
Tabulación de la información	4/02/15	6/02/15
Análisis de la información tabulada	9/02/15	12/02/15
Clasificación de la información	9/02/15	12/02/15
Diseñar las políticas de seguridad	9/02/15	24/02/15
Número de empleados, volúmen de información y deactivos	13/02/15	17/02/15
Áreas de la caja donde se implementarán las NCIGT	13/02/15	16/02/15
Normativa interna del SGSI	13/02/15	18/02/15
Utilización de activos físicos y lógicos	9/02/15	12/02/15
Manejo de incidentes de seguridad	19/02/15	24/02/15
Seleccionar procesos de la Circular 023	16/02/15	18/02/15
Elaborar el modelo de seguridad tecnológica	19/02/15	18/03/15
Proceso seguridad física y del entorno	19/02/15	27/02/15
Áreas de acceso restringido	25/02/15	27/02/15
Normas de seguridad para el acceso físico	19/02/15	24/02/15
Protección y ubicación de equipos	19/02/15	23/02/15
Seguridad de equipos móviles	25/02/15	27/02/15
Proceso gestión de comunicaciones y operaciones	24/02/15	10/03/15
Protección contra código malicioso	2/03/15	5/03/15
Gestión de copias de respaldo	24/02/15	27/02/15
Gestión seguridad de redes	6/03/15	10/03/15
Intercambio de información confidencial	2/03/15	5/03/15
Monitoreo	2/03/15	4/03/15
Proceso control de acceso lógico	5/03/15	18/03/15
Gestión de acceso de usuarios	10/03/15	13/03/15
Gestión de privilegios	6/03/15	10/03/15
Manejo de contraseñas	16/03/15	18/03/15
Responsabilidades de los usuarios	5/03/15	6/03/15
Controles de seguridad en la red	11/03/15	16/03/15

Fuente: El autor

Figura 4. Línea de tiempo



Fuente: El autor

El desarrollo del proyecto tuvo una duración de 420 horas, las cuales se dividieron en cuatro etapas.

7.1 ANTECEDENTES DE PROYECTO

Tiene una duración de 124 horas y en ella se presentan todos los aspectos que sirvieron como referencia para la elaboración del proyecto, uno de ellos es la problemática que se evidencia en las cajas de compensación familiar por el uso inadecuado de la información y cómo beneficiará a la entidad el implementar un sistema que le permita gestionar la seguridad en la infraestructura tecnológica.

7.2 ANÁLISIS DE LOS FACTORES DE RIESGO Y VULNERABILIDAD

Cuenta con una intensidad horaria de 60 horas, aquí se realizaron las encuestas para determinar el nivel de seguridad de la caja de compensación familiar, estos resultados sirvieron como base para seleccionar los aspectos de seguridad tecnológica más relevantes establecidos en el numeral 5.4 de la Circular 023 de 2010 de la Superintendencia del subsidio familiar.

7.3 DISEÑO DE POLÍTICAS DE SEGURIDAD

Tiene una duración de 62 horas, en esta etapa se elaboró la **Política general de seguridad (Ver Anexo A)**en donde se establece el alcance que tendrá el sistema de seguridad tecnológica en la caja de compensación, los objetivos de este sistema, así mismo da a conocer los responsables y sus funciones al velar por el cumplimiento del sistema, y por último las principales normas que debe cumplir el personal de la Caja de compensación familiar.

7.4 ELABORACIÓN DEL MODELO DE POLÍTICAS DE SEGURIDAD TECNOLÓGICA

Cuenta con una duración de 174 horas, aquí se elaboraron los procesos que conforman el sistema de gestión de seguridad de la información.

- **Seguridad física y del entorno (Ver Anexo B):**Se definen las áreas de acceso restringido y las normas de seguridad al ingresar a dichas áreas. Así mismo se plantean los procedimientos en cuanto a la protección y ubicación de los equipos y redes, seguridad de los equipos móviles y el suministro de equipos de soporte energéticos.

- **Gestión de comunicaciones y operaciones (Ver Anexo C):**Se precisan los controles contra código malicioso, cómo se deben gestionar las copias de respaldo y las redes, de qué manera se debe efectuar el intercambio de información confidencial y el monitoreo de la utilización de la infraestructura tecnológica de la caja de compensación familiar.

- **Control de acceso lógico (Ver Anexo D):**Como su nombre lo indica en este proceso se plantean los procedimientos que se deben efectuar para el acceso lógico a la infraestructura tecnológica de la caja de compensación, se establecen el acceso de los usuarios, cómo deben ser sus nombres y contraseñas de usuarios para el acceso a los aplicativos y sistemas de información, los privilegios de cada tipo de usuario y los controles de seguridad en los servicios de la red.

8. PRESUPUESTO

Tabla 1. Presupuesto

PRESUPUESTO						
Tipo	**No. Ítem**	**Descripción**	**Unidad**	**Cantidad**	**Valor Unitario**	**Valor Total**
Talento Humano	1	Antecedentes del proyecto	Horas	124	$27.000,00	$3.348.000,00
	2	Análisis de los factores de riesgo y vulnerabilidad	Horas	60	$27.000,00	$1.620.000,00
	3	Diseño de políticas de seguridad	Horas	62	$27.000,00	$1.674.000,00
	4	Elaboración de modelo de políticas de seguridad informática	Horas	174	$27.000,00	$4.698.000,00
Recursos Técnicos	6	Norma NTC-ISO/IEC 27001	Docum.	1	$45.000,00	$45.000,00
	7	Computador Portátil (Lenovo Intel Core i5 3.20GHZ, 8 GB RAM, DD 500 GB)	Unidad	3	$1.400.000,00	$4.200.000,00
	8	Impresora Multifuncional Epson L210 C11CC59201	Unidad	1	$409.900,00	$409.900,00
	9	Papel x Resma	Unidad	2	$10.900,00	$21.800,00
					Total Gastos	**$16.016.700,00**

Fuente El autor.

9. CONCLUSIONES

Se elaboró un modelo de Políticas de Seguridad de la Información fundamentado en los requerimientos establecidos en el Numeral 5.4 de la Circular 023 de 2010 de la Superintendencia del Subsidio Familiar, que apoyará a las Cajas de Compensación Familiar del departamento del Huila que deseen implementarlo para mejorar su protección frente a riesgos inherentes a su actividad marcando la ruta para iniciar un proyecto estructurado que abarque todos los niveles de seguridad en la organización.

Después de una visión general de esta metodología, quedó claro que Scrum es muy útil para el desarrollo de proyectos, en particular para aquellos en constante cambio y con una necesidad de revisión constante por parte del cliente; esta metódica de trabajo promueve la innovación, motivación y compromiso del equipo que forma parte del proyecto, por lo que los profesionales encuentran un ámbito propicio para desarrollar sus capacidades.

Por último, se logró fortalecer el componente de Control para todas las Unidades de Negocio enfatizándose en la Gestión de Riesgos de todos los Procesos y Procedimientos, mitigando situaciones de Riesgo, Inseguridad y/o Peligro que son inherentes a la actividad del proceso de Tecnologías de la Información de la Organización por ende el Resultado de la Evaluación de Controles realizada por cada uno, fue más Objetiva al momento de proporcionar un tratamiento para los Riesgos Tecnológicos de toda la Empresa.

REFERENCIAS BILIOGRÁFICAS

BUSINESSCOL. Cajas de Compensación Familiar en Colombia. En: BusinessCol [en línea]. (Diciembre de 2013). [Citado el 18 de Febrero de 2015] Disponible en Internet < http://www.businesscol.com/empresarial/sistemfin/cajascomp.htm>.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. 2014. p. 8.

COMFAMA. Lo que debes saber sobre las Cajas de Compensación en Colombia. En: Comfama [en línea]. (Diciembre de 2012). [Citado el 18 de Febrero de 2015] Disponible en Internet <http://www.comfama.com/contenidos/noticarteleras/20121203/38099.asp?id_Not=38099>.

COMFENALCO ANTIOQUIA. ¿Qué son las Cajas de Compensación? En: Comfenalco [en línea]. (Diciembre de 2011). [Citado el 18 de Febrero de 2015] Disponible en Internet <http://www.comfenalcoantioquia.com/Default.aspx?tabid=238&id=161>.

OCDE. Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. En: OECD [en línea]. (Julio de 2002). [Citado el 18 de Febrero de 2015] Disponible en <http://www.oecd.org/sti/ieconomy/34912912.pdf>.

GÓMEZ, Álvaro. Enciclopedia de la Seguridad Informática. Ra-Ma EDITORIAL, 2011.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información: Generalidades. NTC-ISO 27001. Bogotá D.C.: El Instituto, 2013. p. I–II.

--------.--------.Establecimiento y gestión del SGSI. NTC.ISO 27001. Bogotá D.C.: El Instituto, 2013. p. 4–6.

Organización Internacional de Estandarización. Evolution of ISO/IEC 2700 certificates in Colombia. En: ISO Survey [en línea]. (Diciembre de 2013). [Citado el 18 de Febrero de 2015] Disponible en Internet <http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=CO#countrypick>.

KPMG. Encuesta de fraude en Colombia 2013 [en línea]. (4 de Septiembre de 2013). [Citado el 20 de Septiembre de 2014] Disponible en Internet

<http://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf>.

KROLL ADVISORY SOLUTIONS. Informe global sobre fraude [en línea].(23 de Noviembre 2013). [Citado el 20 de Septiembre de 2014]Disponible en Internet<http://fraud.kroll.com/wp-content/uploads/Reporte%20de%20Fraude%20Kroll%202013-2013%20Espanol%20-%20WEB.pdf>.

SUPERINTENDENCIA DE SEGURIDAD SOCIAL. Circular 2892: Norma sobre sistema de control interno para las mutualidades de empleadores de la ley n° 16.744. Chile, 17 de diciembre de 2012.

SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR. Circular externa 023 de 2010. Bogotá. 2010.

ANEXOS