PLAN DE SEGURIDAD INFORMÁTICA PARA LA COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CRÉDITO COONFIE SEDE NEIVA

CARLOS ANDRÉS PINTO DÍAZ

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

PLAN DE SEGURIDAD INFORMÁTICA PARA LA COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CRÉDITO COONFIE SEDE NEIVA

CARLOS ANDRÉS PINTO DÍAZ

Trabajo final Seminario de profundización en seguridad informática presentado como requisito para optar al título de INGENIERO DE SISTEMAS

Asesor:
Ing. FERNANDO ROJAS ROJAS

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

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

Neiva, Octubre de 2015

CONTENIDO

pág.

RESUMEN 8

INTRODUCCIÓN 9

1. PLANTEAMIENTO DEL PROBLEMA 10

2. JUSTIFICACIÓN 11

3. OBJETIVOS 12

3.1 OBJETIVO GENERAL 12

3.2 OBJETIVOS ESPECÍFICOS 12

4. ESTADO DEL ARTE 13

4.1 ÁMBITO LOCAL Y REGIONAL 13

4.2 ÁMBITO NACIONAL E INTERNACIONAL 14

5. MARCO TEÓRICO 15

5.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) 15

5.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI 16

6. INGENIERÍA DEL PROYECTO 19

6.1 SITUACIÓN ACTUAL DE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA COOPERATIVA 19

6.2 ESTRUCTURA ORGANIZACIONAL DEL PLAN DE SEGURIDAD INFORMÁTICA 21

6.3 POLÍTICAS DE SEGURIDAD INFORMÁTICA 25

7. CRONOGRAMA DE ACTIVIDADES 27

8. PRESUPUESTO 29

9. CONCLUSIONES 30

REFERENCIAS BIBLIOGRÁFICAS 31

ANEXOS 33

LISTA DE FIGURAS

Pág.

Figura 1. Evolución de ISO 27001 en Colombia 14

Figura 2. Modelo PHVA aplicado a los procesos de SGSI 15

Figura 3. Metodología para el Análisis y Evaluación del Riesgo 17

Figura 4. Organigrama propuesto 24

Figura 5. Estructura organizativa del Comité 25

Figura 6. Actividades 27

Figura 7. Línea de tiempo 28

LISTA DE ANEXOS

Pág.

Anexo A. Manual de Políticas de Seguridad de la Información 19

Anexo B. Política general de seguridad 25

Anexo C. Políticas de acuerdo de intercambios de información 25

Anexo D. Política de control de acceso 25

Anexo E. Política de identificación y autenticación de usuarios 25

Anexo F. Política de gestión de medios removibles 25

Anexo G. Política de protección de los mensajes electrónicos 25

Anexo H. Política de protección de los datos y la privacidad de la información personal 26

Anexo I. Política para el respaldo de la información 26

Anexo J. Política de seguridad de la red 26

Anexo K. Política de uso de Internet 26

RESUMEN

El diseño de una Plan de Seguridad Informática para la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE sede Neiva, se realiza buscando un único objetivo que se enfoca en crear conciencia organizacional en lo que se refiere a la protección de la información, activos 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 tema, partiendo de la base de un diagnóstico de seguridad que mostró varios puntos esenciales de urgente intervención. Aplicando herramientas de recolección de información como observación, entrevistas y encuestas para evaluar el estado actual de la seguridad en las dos oficinas de la Cooperativa ubicadas en la ciudad de Neiva, se establece la falta de prácticas seguras en el área informática y la falta de preocupación por parte de la gerencia de las oficinas para adoptar medidas al respecto.

Finalmente, se diseña una propuesta que, puesta en marcha, le ayudará a la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE sede Neiva a mejorar su protección frente a riesgos propios de su actividad y marcará la ruta para iniciar un proyecto integro y que abarque todos los niveles de seguridad en la cooperativa.

INTRODUCCIÓN

La globalización de los servicios financieros, de la mano de la creciente actualización de la tecnología financiera, están haciendo cada vez más diversas y complejas las actividades de los bancos en términos de seguridad. En otros tiempos la seguridad de la información era fácilmente administrable, solo bastaba con guardarla en un lugar seguro, sin embargo los recientes eventos mundiales en materia de cibercrimen han generado un mayor sentido de urgencia con respecto a la necesidad de tener mayor seguridad. Las empresas pueden haber reforzado las medidas de seguridad, pero nunca se sabe cuándo o cómo pueden estar expuestas. A fin de brindar la más completa protección empresarial, se requiere de un sistema íntegro de seguridad. Es vital implementar un plan de seguridad, al hacerlo de manera proactiva, que indique como sobrevivir a los múltiples escenarios también preparara a las empresas en el manejo de las amenazas inesperadas que podrían afrontar en el futuro.

La mayoría de las empresas han invertido tiempo y dinero en la construcción de una infraestructura para la tecnología de la información que soporte su compañía, sin embargo dicha infraestructura podría resultar ser una gran debilidad si se ve comprometida. Para las organizaciones que funcionan en la era de la informática, las políticas de información bien documentadas que se comunican, comprenden e implementan en toda la empresa, son herramientas esenciales en el entorno actual para minimizar los riesgos y amenazas de seguridad.

Prepararse para múltiples escenarios parece ser la tendencia creciente. En el último informe publicado por la compañía consultora Gartner se estableció que el área de Seguridad Informática tuvo un crecimiento del 5,3% en el año 2014[1], lo que representa ingresos por 21,4 billones de dólares, es por eso que el gasto en seguridad de la información fue de 71,1 billones de dólares en 2014, un incremento del 7,9% con respecto a 2013, siendo el segmento de prevención de pérdida de datos el de más rápido crecimiento (con un 18,9%). De acuerdo a Gartner, el total del gasto en seguridad de la información crecerá un 8,2% en 2015, llegando a 76,9 billones. Es por esto que han nacido estándares para gestionar la seguridad de la información y de los activos de tecnología como la norma ISO 27001, implementar dicha política de seguridad de una manera completa le da valor intrínseco a las empresas, también mejora la credibilidad y reputación de las organizaciones y aumenta la confianza de los accionistas principales, lo que le dará a la empresa una ventaja estratégica.

[1] CIO AMÉRICA LATINA. Mercado de la seguridad informática creció 5,3% en 2014. 2015

1. PLANTEAMIENTO DEL PROBLEMA

Cada vez es más evidente el constante crecimiento de las tecnologías de la información y la sistematización de los procesos en las entidades financieras, y con ellos vienen también nuevos equipos y sistemas, en los que además surgen nuevos riesgos y vulnerabilidades, creados principalmente para alterar y cometer fraudes que pueden comprometer los sistemas de información de cada empresa. A pesar de esto, la mayoría de las entidades no están invirtiendo capital humano ni tecnológico para prevenir el daño o pérdida de su información.

En la actualidad la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE no cuenta en ninguna de sus sedes con medidas para prevenir y mitigar el daño o pérdida de su información confidencial, debido a esto se puede evidenciar que no hay una periodicidad establecida para la generación de copias de seguridad en las estaciones de trabajo y adicionalmente, no cuenta con un registro o control en las entradas y salidas de los equipos de cómputo, causando altos costos para su recuperación en caso de extravío, además, y más importante aún, la pérdida irreversible de la información.

Unido a esto, la falta de un método de clasificación de información dependiendo de su contenido (pública, interna o confidencial) y a raíz de esto, es común observar que el personal que trabaja en la empresa tiene acceso a toda la información sin limitaciones y no toma conciencia de la importancia de su contenido, esto se debe en parte a que los computadores o las aplicaciones de uso frecuente son administrados con contraseñas pero estás son conocidas por el personal que labora en la cooperativa.

Así mismo, la empresa no cuenta con un plan estratégico de infraestructura de tecnología, dando originen a las demoras en el tratamiento de incidentes que puedan presentarse en la organización, peor aún, la empresa no documenta 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.

Teniendo en cuenta las falencias mencionadas anteriormente ¿es factible diseñar un plan de seguridad informática para las oficinas de la sede Neiva de la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE?

2. JUSTIFICACIÓN

En la actualidad, la mayoría de las organizaciones dependen parcialmente de sus sistemas informáticos, esto hace necesario que cada vez se preste mayor atención a la disponibilidad, confidencialidad e integridad de los mismos, garantizando la continua prestación de sus servicios, así como la certeza de tener su información segura y sus sistemas protegidos. Por tal motivo se hace necesario contar con estrategias y medidas de seguridad de la información, para que en un momento dado, se pueda aplicar los correctivos necesarios en caso de un eventual ataque o desastre.

Según el informe Net Losses: Estimatingthe Global Cost of Cybercrime[2], 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[3]; por otra lado, en el informe anual realizado por Kroll Advisory Solutions[4] también se identificó que los empleados son mucho más responsables de la pérdida de información que los hackers. 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%[5].

Con este proyecto se busca realizar un aporte valioso a la cooperativa COONFIE sede Neiva, al diseñar un plan de seguridad informática que sirva como pilar para la implementación de políticas de seguridad fundamentadas en la Norma Técnica Colombiana NTC-ISO/IEC 27001 y la Circular 038 de la Superintendencia Financiera ayudando a mejorar su protección frente a riesgos propios de 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.

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

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un plan de seguridad informática para la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE sede Neiva., tomando como referencia la Norma Técnica Colombiana NTC-ISO/IEC 27001 y la Circular 038 de la Superintendencia Financiera.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los factores de riesgo y vulnerabilidad de la información en COONFIE sede Neiva.

- Diseñar las normas y controles de seguridad de la información para COONFIE sede Neiva.

- Elaborar el Plan de Seguridad Informática para COONFIE sede Neiva.

4. ESTADO DEL ARTE

La seguridad de la información para una organización depende de diferentes factores: el social, relacionado con el grado de circunspección del personal que la manipula; el físico, referente al alojamiento de la información; y el lógico, que se enfoca en la configuración de sus niveles de accesibilidad y disposición. Es así como técnicamente se ha caracterizado que un esquema seguro debe corresponder al ajuste de los niveles de confidencialidad, integridad y disponibilidad de la información, según las directrices OCDE[6]. Las anteriores características se encuentran implícitas 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, constituyendo los denominados Sistemas de Gestión de Seguridad de la Información (SGSI).

4.1 ÁMBITO LOCAL Y REGIONAL

Por medio de entrevistas se identificó que hay varios problemas de protección de la información en algunas organizaciones de la ciudad de Neiva por la ausencia de un SGSI, en otras empresas como SIDA S.A.(*) y MECANICOS ASOCIADOS S.A.S.(**) cuentan con unas normas establecidas para la seguridad de su información pero por falta de capacitación a su personal no se cumplen dejando como reflexión la importancia de sensibilizar a los empleados en relación a la seguridad y a sus responsabilidades en la organización haciéndolos parte activa del proceso.

Por otro lado, entidades como Comfamiliar del Huila(***) se rige por la circular 0023 de la Superintendencia del Subsidio Familiar en donde se da instrucciones para establecer Normas de Control Interno para la Gestión de la Tecnología, al implementar 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, y además, desarrolló 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.

---

[6] OCDE. Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, Julio de 2002.

(*) RODRÍGUEZ, Omar. SIDA S.A.: Sistemas. Neiva, Huila. Observación inédita, 2015.

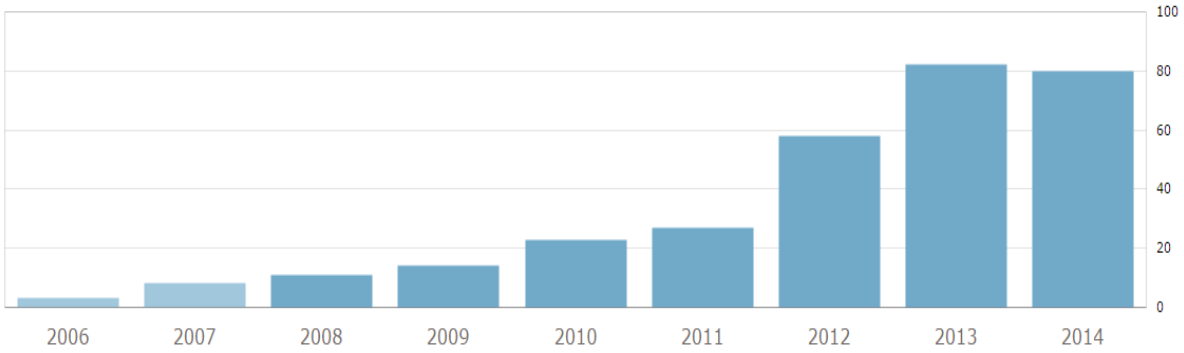
(**)DULCE, Camilo. Mecánicos asociados S.A.S.: Sistemas. Neiva, Huila. Observación inédita, 2015.

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

4.2 ÁMBITO NACIONAL E INTERNACIONAL

Según Chen y Goel[7], recientemente, las empresas están empezando a darse cuenta de que el aumento de la accesibilidad y la productividad, lleva un costo oculto, pues los datos se vuelven más vulnerables a las violaciones de la seguridad. Una prueba de esto es el aumento en un 14% de empresas certificadas en el estándar ISO/IEC 27001 entre los años 2012 y 2013[8]. A nivel mundial 22.293 empresas fueron certificadas en Sistemas de Gestión de Seguridad de la Información[9], de las cuales 82 son colombianas[10]. Sin embargo, la naturaleza confusa y compleja de la seguridad de la información oculta el retorno de la inversión, por lo que las empresas son reacias a invertir en políticas o tecnologías de seguridad. Sin embargo, en Colombia es cada vez más evidente el interés de los empresarios por la seguridad de sus datos, como lo muestra la Figura 1 desde el 2006 hasta el 2011 hubo un incremento paulatino. En el 2006 solo 3 empresas estaban certificadas en nuestro país, y en el año 2011 se contaba con 27 organizaciones certificadas en implementación de un SGSI, pero en los últimos 3 años se ha evidenciado un incremento exponencial dejando en el 2013 el número de 82 empresas certificadas por ISO en el país.

Figura 1. Evolución de ISO 27001 en Colombia



Fuente: ISO Survey

Empresas como UNE y ETEK[11] que cuentan con la certificación en este estándar, han visto beneficios tales como mejora continua en la gestión de la seguridad, reducción de los costos vinculados a los incidentes, el incremento de los niveles de confianza de clientes y partners y el aumento del valor comercial y mejora de la imagen de la organización.

---

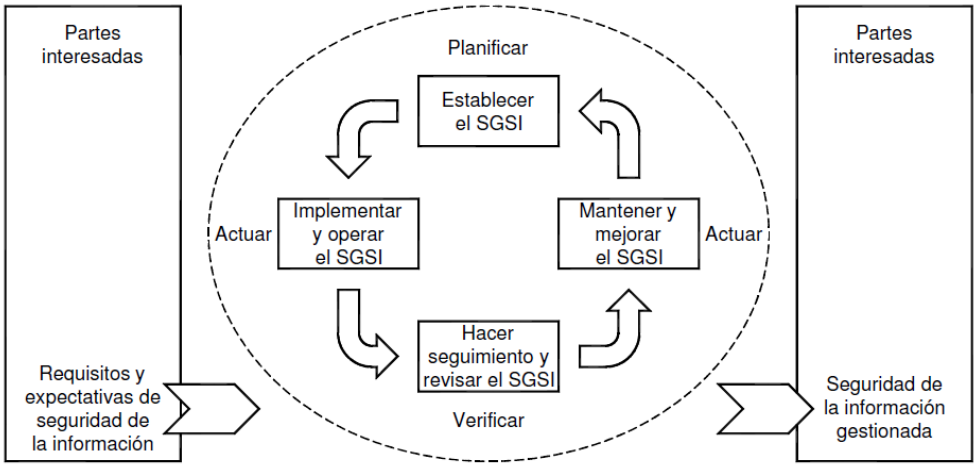
[7] CHEN, Vicki y GOEL, Sanjay. Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process. En: International Journal of Production Economics, Ámsterdam: Elsevier, 2008. p.104 -112.
[8] ISO Org. Evolution of ISO/IEC 27001 certificates in Colombia. En: ISO Survey, 2013.
[9] Ibíd.
[10] Ibíd
[11] PROCESO CERTIFICACIÓN 27001. Empresas certificadas de Colombia. 2013.

5. MARCO TEÓRICO

5.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

ICONTEC [12] , 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 2. Modelo PHVA aplicado a los procesos de SGSI



Fuente NTC-ISO/IEC 27001.

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.

[12] 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.

5.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI[13]

5.2.1 Alcance del SGSI. La planeación para la implementación de un SGSI, es una etapa ineludible, por tanto, definir el alcance para la implementación del sistema en una organización es uno de los primeros aspecto que se debe considerar. Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, se hace necesario determinar qué áreas o dependencias de la organización se desea implantar el SGSI como primera medida y cuales posteriormente. Las primeras áreas que se deben considerar son aquellas que por sus funciones y responsabilidades ayudan en primera instancia a dar cumplimiento a la misión institucional.

5.2.2 Política de Seguridad. Es el primer documento que se debe contemplar debido a que es donde se especifica toda la normativa interna de la organización con el objetivo de que los funcionarios conozcan y cumplan sobre el sistema de gestión de la seguridad de la información (SGSI) implantado, con este documento, también se refleja el compromiso planteado por la dirección. Así mismo contempla todos los aspectos orientados al acceso a la información, utilización de los activos físicos y lógicos de la organización y el comportamiento que debe hacer en caso de que ocurra un incidente de seguridad.

5.2.3 Análisis de riesgos

5.2.3.1 Conceptos básicos. En primer lugar conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

- Amenaza: Es la causa potencial de un daño a un activo.
- Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.
- Impacto: consecuencias de que la amenaza ocurra.

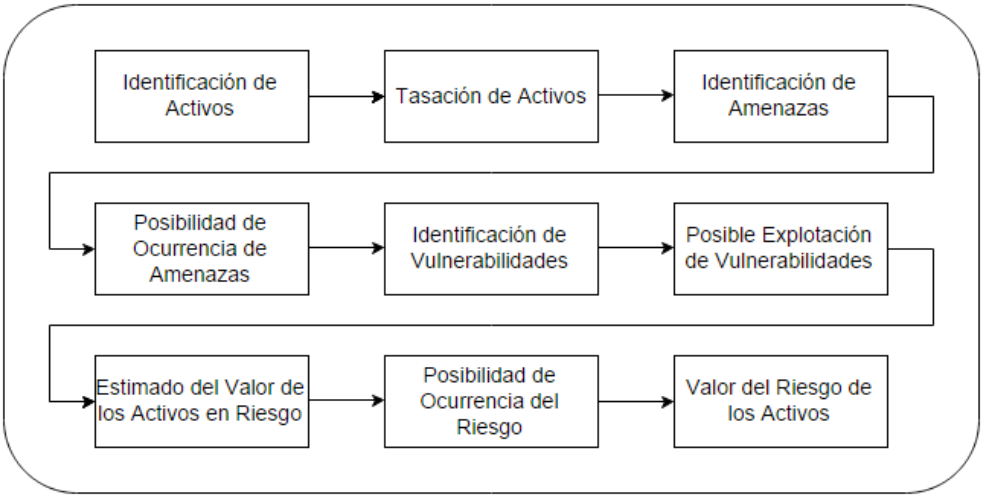
[13] Ibíd., p. 4 – 6.

- Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.
- Salvaguarda: Medida técnica u organizativa que ayuda a paliar el riesgo.
- Riesgo residual: Riesgo remanente tras la aplicación de salvaguardas.

El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos. A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es relativamente sencillo calcular con cuantos recursos se cuenta (económicos, humanos, técnico, etc.) pero no es tan fácil saber a ciencia cierta cuáles son las necesidades de seguridad.

5.2.3.2 Realización del análisis de riesgos. Para realizar un análisis de riesgos se parte del inventario de activos. Si es razonablemente reducido, puede decidirse hacer el análisis sobre todos los activos que contiene. Si el inventario es extenso, es recomendable escoger un grupo relevante y manejable de activos, bien los que tengan más valor, los que se consideren estratégicos o todos aquellos que se considere que se pueden analizar con los recursos disponibles. Se puede tomar cualquier criterio que se estime oportuno para poder abordar el análisis de riesgos en la confianza de que los resultados van a ser útiles. En la Figura 2 se puede observar la metodología del análisis de riesgos. Se valoran las amenazas y las vulnerabilidades que afectan a los activos escogidos para el análisis y el impacto que ocasionaría que alguna de las amenazas realmente ocurriera, sobre la base de su conocimiento y experiencia dentro de la organización.

Figura 3. Metodología para el Análisis y Evaluación del Riesgo



Fuente El autor.

5.2.4 Tratamiento del riesgo. Es una de las actividades que propone la normativa ISO/IEC 27001 en la implementación y operación del SGSI. Este plan, se formula para identificar la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información. La normativa ISO 27001 expresa las acciones que se deben contemplar en el plan de tratamiento de riesgos que son:

- Aplicar los controles apropiados.
- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
- Evitar riesgos.
- Transferir a otras partes los riesgos asociados con el negocio, por ejemplo: aseguradoras, proveedores, etc.

5.2.5 Seleccionar los objetivos de control para el tratamiento de los riesgos. Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos. Esta selección debe tener en cuenta los criterios para la aceptación de riesgos, al igual que los requisitos legales, reglamentarios y contractuales.

5.2.6 Formación, capacitación y toma de conciencia. La organización debe asegurar que todo el personal al que se asigne responsabilidades definidas en el SGSI sea competente para realizar las tareas exigidas, mediante:

- La determinación de las competencias necesarias para el personal que ejecute el trabajo que afecta el SGSI.
- El suministro de formación o realización de otras acciones (por ejemplo, la contratación de personal competente) para satisfacer estas necesidades.
- La evaluación de la eficacia de las acciones emprendidas.
- El mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones

La organización también debe asegurar que todo el personal apropiado tiene conciencia de la pertinencia e importancia de sus actividades de seguridad de la información y cómo ellas contribuyen al logro de los objetivos del SGSI.

6. INGENIERÍA DEL PROYECTO

6.1 SITUACIÓN ACTUAL DE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA COOPERATIVA

Después de realizada la revisión a la Gestión de la Tecnología de Información de la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE se pudo evidenciar que el Plan de Seguridad Informática no ha sido desarrollado. Si bien se observó la existencia de normas que cubren distintos aspectos de la seguridad de la información, se carece en general de una metodología que ayude a la identificación de riesgos y determinación de controles para mitigar los mismos.

Dentro de los distintos aspectos a considerar en la seguridad de la información, se pudo establecer que se carece de Políticas que prevengan y mitiguen los daños que se puedan presentar y de una clasificación de los activos tecnológicos de la cooperativa. Cabe mencionar que se determinó la existencia de controles con respecto a la seguridad física de los activos informáticos de la cooperativa. Sin embargo, estos controles no hacen parte de una definición previa de Políticas a nivel de toda la cooperativa, estos controles son producto de evaluaciones particulares efectuadas por las aéreas involucradas o bajo cuyo ámbito de responsabilidad recae cierto aspecto de la seguridad.

El alcance del proceso de observación y de auditoría comprendió la revisión de las siguientes funciones (Ver Anexo A):

- Administración del área de Tecnología de Información
- Estructura organizacional
- Políticas y procedimientos para administración de los riesgos de TI
- Subcontratación de recursos
- Actividades de desarrollo y mantenimientos de sistemas informáticos
- Seguridad de la información
- Administración de la seguridad de la información
- Aspectos de la seguridad de la información (lógica, personal, física)
- Inventario periódico de activos asociados a TI
- Operaciones computarizadas
- Administración de las operaciones y comunicaciones
- Procedimientos de respaldo
- Planeamiento para la continuidad de negocios

Así mismo, comprende la revisión de los siguientes aspectos:

- Cumplimiento normativo
- Privacidad de la información

- Auditoria de sistemas

La Tabla 1 muestra el grado de cumplimiento en los aspectos relacionados a la adecuación del Plan de Seguridad.

Tabla 1. Diagnostico de Gestión de Seguridad Informática

Ítem	Aspectos Evaluados	Grado de cumplimiento
1	Estructura de la seguridad de la información	
2	Políticas, estándares y procedimientos de seguridad	
2.1	Seguridad lógica	
2.2	Seguridad de Personal	
2.3	Seguridad física	
2.4	Clasificación de seguridad	
3	Administración de las operaciones y comunicaciones	
4	Desarrollo y mantenimiento de sistemas informáticos	
5	Procedimientos de respaldo	
6	Plan de continuidad de negocios	
6.1	Plan para la continuidad de negocios	
6.2	Criterios para el diseño e implementación del Plan de continuidad de negocios	
6.3	Prueba del Plan de continuidad de negocios	
7	Subcontratación	
8	Cumplimiento normativo	
9	Privacidad de la información	
10	Auditoria de sistemas	

Fuente: El autor.

6.2 ESTRUCTURA ORGANIZACIONAL DEL PLAN DE SEGURIDAD INFORMÁTICA

6.2.1 Estructura organizacional actual. En la actualidad, la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE cuenta con un área de sistemas que se encarga de:

- Mantenimiento preventivo y correctivo de los computadores.
- Creación y eliminación de usuarios.
- Verificación y asignación de perfiles en los sistemas de información.
- Control de la red.
- Administración de accesos a las Bases de Datos.
- Administración del Firewall.

Las funciones de diseño y administración de las Políticas y normas de seguridad de información no están definidas dentro de los roles de la organización. Cabe mencionar que el acceso con privilegio administrativo a los computadores está restringido, el área de sistemas define un usuario y una contraseña a cada persona que labora en la cooperativa, sin embargo esta contraseña es conocida por algunos de los empleados y de esta manera se puede acceder a cualquier computador en cualquier momento.

6.2.2 Estructura Organizacional del Plan de Seguridad Informática. El área que quedará encargada de la administración del Plan de seguridad informática debe soportar los objetivos de seguridad de información de la cooperativa. Dentro de sus responsabilidades se encuentra la coordinación de esfuerzos entre el personal de sistemas y los empleados de las demás áreas de la cooperativa, siendo estos últimos los responsables de la información que utilizan. De igual manera, es garante de promover la seguridad de la información en toda la cooperativa. Es importante mencionar que las responsabilidades referentes a la seguridad de la información no son exclusivas del comité de seguridad informática, sino que también existen roles adicionales como lo son los propietarios de la información, los custodios de información y el área de auditoría interna.

- Los propietarios de la información deben verificar la integridad de su información y velar porque esta mantenga la disponibilidad y confidencialidad.
- Los custodios de información deben monitorear el cumplimiento de las actividades encargadas.
- El área de auditoría interna debe monitorear el acatamiento de la política de seguridad y el cumplimiento adecuado de los procesos definidos para mantener la seguridad de la información.

A continuación se presentan los roles y responsabilidades relacionadas a la administración de seguridad de información.

Comité de Seguridad Informática: El área organizacional encargada de la administración de seguridad de información tiene como responsabilidades:

- Establecer y documentar las responsabilidades de la cooperativa en cuanto a seguridad de información.
- Mantener las políticas y normas de seguridad de información de la cooperativa.
- Identificar objetivos de seguridad y estándares de la cooperativa (prevención de virus, uso de herramientas de monitoreo, etc.)
- Definir metodologías y procesos relacionados a la seguridad de la información.
- Comunicar aspectos básicos de seguridad de la información a los empleados de la cooperativa. Esto incluye un programa de concientización para comunicar aspectos básicos de seguridad y de las políticas de la cooperativa.
- Desarrollar controles para las tecnologías que utiliza la cooperativa. Esto incluye el monitoreo de vulnerabilidades documentadas por los proveedores.
- Monitorear el cumplimiento de la política de seguridad de la cooperativa.
- Controlar e investigar incidentes de seguridad o violaciones de seguridad.
- Realizar una evaluación periódica de vulnerabilidades de los sistemas que conforman la red de datos de la cooperativa.
- Evaluar aspectos de seguridad de productos de tecnología, sistemas o aplicaciones utilizados en la cooperativa.
- Verificar que cada activo de información de la cooperativa haya sido asignado a un propietario el cual debe definir los requerimientos de seguridad como políticas de protección, perfiles de acceso, respuesta ante incidentes y sea responsable final del mismo.
- Administrar un programa de clasificación de activos de información, incluyendo la identificación de los propietarios de las aplicaciones y datos.
- Coordinación de todas las funciones relacionadas a seguridad, como seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.
- Administración de accesos a las principales aplicaciones de la cooperativa.
- Controlar aspectos de seguridad en el intercambio de información con entidades externas.
- Monitorear la aplicación de los controles de seguridad física de los principales activos de información.

Propietario de información: Son los gerentes y jefes de las áreas de la cooperativa, los cuales son responsables de la información que se genera y se utiliza en las operaciones de su área. Sus responsabilidades son:

- Asignar los niveles iníciales de clasificación de información.

- Revisión periódica de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos de la cooperativa.
- Determinar los criterios y niveles de acceso a la información.
- Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
- Determinar los requerimientos de copias de respaldo para la información que les pertenece.
- Tomar las acciones adecuadas en caso de violaciones de seguridad.

Custodio de información: Es el responsable de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su administración. Sus responsabilidades son:

- Administrar accesos a nivel de red (sistema operativo).
- Administrar accesos a nivel de bases de datos.
- Administrar los accesos a archivos físicos de información almacenada en medios magnéticos.
- Implementar controles definidos para los sistemas de información.
- Desarrollar procedimientos de autorización y autenticación.
- Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de información que custodia.
- Investigar brechas e incidentes de seguridad.
- Asistir y administrar los procedimientos de Backup, recuperación y plan de continuidad de sistemas.

Auditoría interna: El personal de auditoría interna es responsable de monitorear el cumplimiento de los estándares y guías definidas en las políticas internas. Una estrecha relación del área de auditoría interna con el comité de seguridad informática es crítica para la protección de los activos información. Por lo tanto dentro del plan anual de evaluación del área de auditoría interna se debe incluir la evaluación periódica de los controles de seguridad de información definidos por la cooperativa.

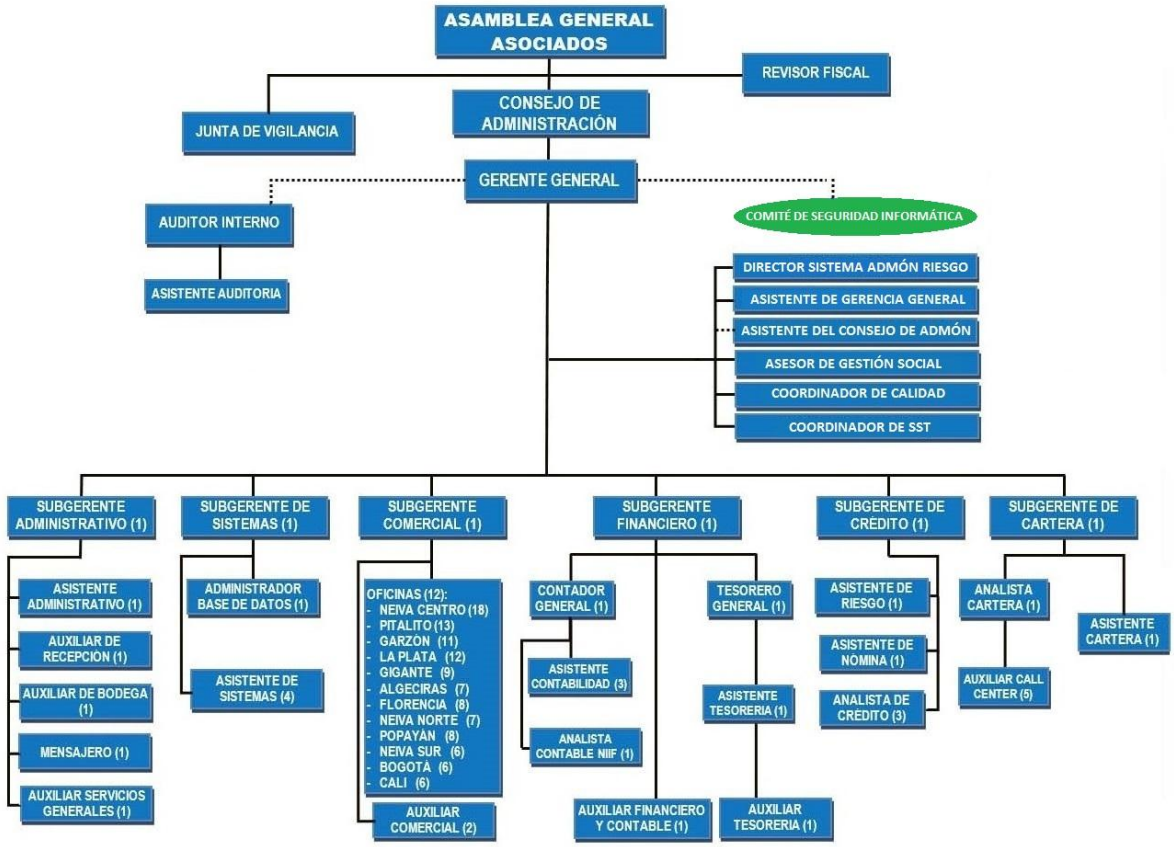
Usuario: Las responsabilidades de los usuarios finales, es decir, aquellas personas que utilizan información de la cooperativa como parte de su trabajo diario están definidas a continuación.

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- Reportar supuestas violaciones de la seguridad de información.
- Asegurarse de ingresar información adecuada a los sistemas.
- Acatar las políticas de seguridad de la cooperativa.

Dadas las características de la estructura organizativa del plan de seguridad informática es conveniente que el comité de seguridad informática sea

independiente al área de sistemas, para esto se propone la estructura organizativa que se puede observa el Figura 4.

Figura 4. Organigrama propuesto

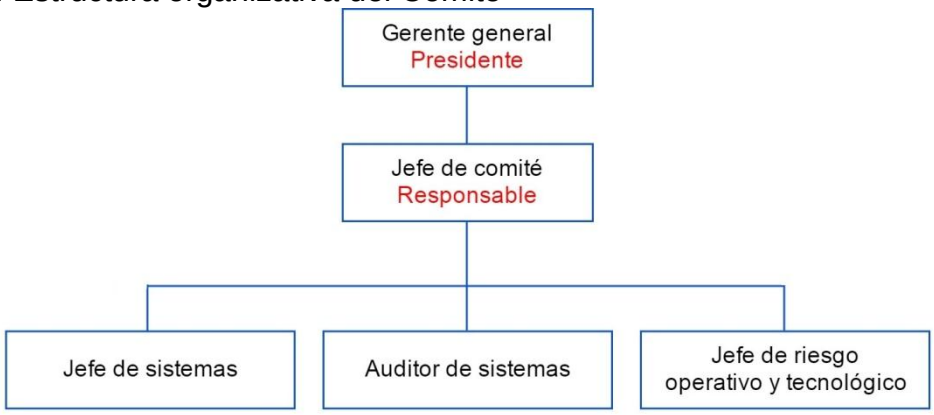


Fuente: El autor.

Este Comité de seguridad informática a su vez estará conformado por los siguientes cargos y como se puede observar en la Figura 5:

- Gerente general
- Jefe de Comité de seguridad informática
- Jefe de sistemas
- Auditor de sistemas
- Jefe de riesgo operativo y tecnológico

Figura 5. Estructura organizativa del Comité



Fuente: El autor.

6.3 POLÍTICAS DE SEGURIDAD INFORMÁTICA

Estas políticas servirán de guía para la implementación de medidas de seguridad que contribuirán a mantener la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales. Dichas políticas de seguridad han sido elaboradas tomando como base los marcos de trabajo de la Norma técnica colombiana NTC-ISO/IEC 27001 y los requerimientos de la Circular 038 de la Superintendencia Financiera de Colombia.

6.3.1 Política general de seguridad (Ver Anexo B). Busca lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales relevantes, asegurando la continuidad operacional de los procesos.

6.3.2 Políticas de Acuerdos de intercambio de información (Ver Anexo C). Define las directrices para proteger el intercambio de información electrónica, con organizaciones externas, y asea electrónica o física; por sistema o manual.

6.3.3 Política de Control de acceso (Ver Anexo D). Establece las definiciones que regulan el acceso a los medios compartidos de información de la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE.

6.3.4 Política de Identificación y autenticación de usuarios (Ver Anexo E). Define los estándares y controles que deben cumplirse para el acceso a los

recursos y sistemas computacionales de la cooperativa, considerando la identificación y autenticación de usuarios que acceden a las plataformas institucionales.

6.3.5 Política de Gestión de los medios removibles (Ver Anexo F). Define las reglas para la protección de datos en diferentes medios de almacenamiento y evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades de negocio.

6.3.6 Política de protección de los mensajes electrónicos (Ver Anexo G). Definir los estándares y controles que deben cumplirse para el acceso y uso de los mensajes electrónicos de la cooperativa.

6.3.7 Política de protección de los datos y la privacidad de la información personal (Ver Anexo H). Definir las directrices para la protección y privacidad de la información personal que se recoja, procese y transmita en la cooperativa.

6.3.8 Política para el respaldo de la información (Ver Anexo I). Establece las directrices de respaldo de información de la cooperativa, para proteger los datos y software en la organización, así como los dispositivos de hardware que la soportan almacena y distribuyen.

6.3.9 Política de seguridad de la red (Ver Anexo J). Define los controles de los niveles de seguridad de la red de comunicaciones de la cooperativa, así como la protección contra servicios conectados no autorizados.

6.3.10 Política de uso de Internet (Ver Anexo K). Establece las normas para regular el uso y navegación de Internet. Además, sensibilizar y formar al personal sobre las amenazas que pueden presentarse a través de Internet.

7. CRONOGRAMA DE ACTIVIDADES

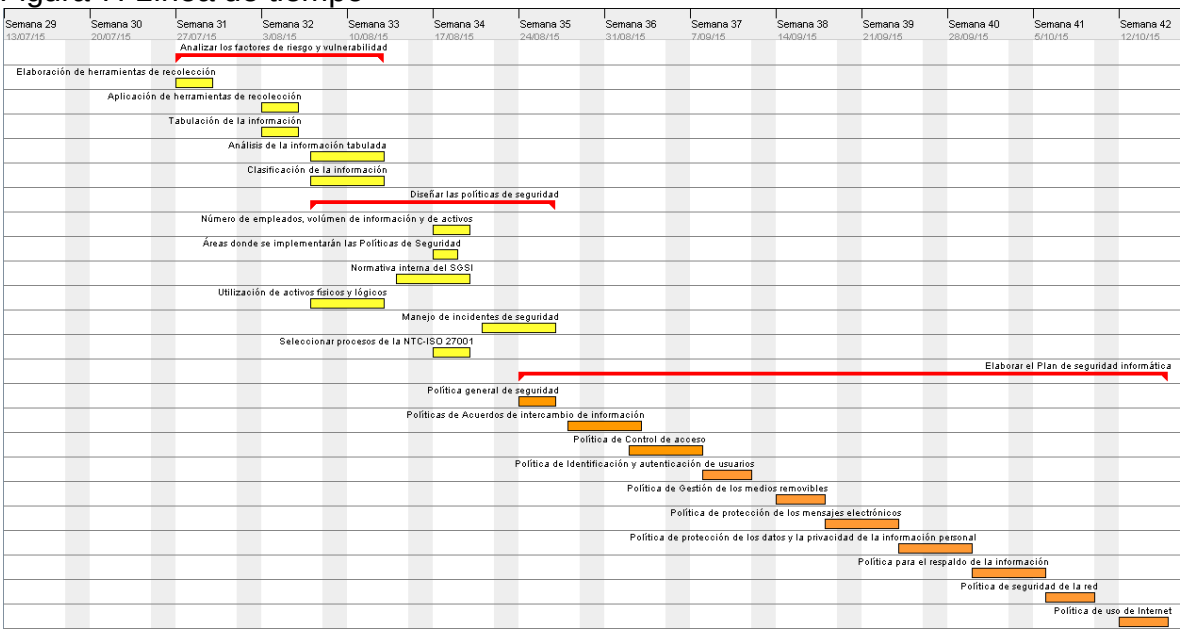
Las Figuras 6 y 7 contienen el cronograma de trabajo para el desarrollo del proyecto, en ellas se describen las actividades a realizar y el tiempo que se dedica a la ejecución de cada una.

Figura 6. Actividades

Nombre	Fecha de inicio	Fecha de fin
Analizar los factores de riesgo y vulnerabilidad	27/07/15	12/08/15
Elaboración de herramientas de recolección	27/07/15	29/07/15
Aplicación de herramientas de recolección	3/08/15	5/08/15
Tabulación de la información	3/08/15	5/08/15
Análisis de la información tabulada	7/08/15	12/08/15
Clasificación de la información	7/08/15	12/08/15
Diseñar las políticas de seguridad	7/08/15	26/08/15
Número de empleados, volúmen de información y de activos	17/08/15	19/08/15
Áreas donde se implementarán las Políticas de Seguridad	17/08/15	18/08/15
Normativa interna del SGSI	14/08/15	19/08/15
Utilización de activos físicos y lógicos	7/08/15	12/08/15
Manejo de incidentes de seguridad	21/08/15	26/08/15
Seleccionar procesos de la NTC-ISO 27001	17/08/15	19/08/15
Elaborar el Plan de seguridad informática	24/08/15	15/10/15
Política general de seguridad	24/08/15	26/08/15
Políticas de Acuerdos de intercambio de información	28/08/15	2/09/15
Política de Control de acceso	2/09/15	7/09/15
Política de Identificación y autenticación de usuarios	8/09/15	11/09/15
Política de Gestión de los medios removibles	14/09/15	17/09/15
Política de protección de los mensajes electrónicos	18/09/15	23/09/15
Política de protección de los datos y la privacidad de la información personal	24/09/15	29/09/15
Política para el respaldo de la información	30/09/15	5/10/15
Política de seguridad de la red	6/10/15	9/10/15
Política de uso de Internet	12/10/15	15/10/15

Fuente: El autor.

Figura 7. Línea de tiempo



Fuente: El autor

8. PRESUPUESTO

Tabla 2. Presupuesto

Tipo	No. Ítem	Descripción	Unidad	Cantidad	Valor Unitario	Valor Total
	2	Análisis de los factores de riesgo y vulnerabilidad	Horas	104	$27.000,00	$2.808.000,00
	3	Diseño de políticas de seguridad	Horas	112	$27.000,00	$3.024.000,00
	4	Elaboración del Plan de Seguridad Informática	Horas	312	$27.000,00	$8.424.000,00
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	1	$1.400.000,00	$1.400.000,00
	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	$16.132.700,00

Fuente: El autor.

9. CONCLUSIONES

Con base en la investigación realizada, es posible determinar que a nivel nacional y regional muchas organizaciones no creen necesario tener una política de seguridad informática definida formalmente, aún así, se considera importante y se ejecutan algunas prácticas tendientes a garantizar la seguridad de la información, pero la falta de procedimientos formales hace que no se tomen medidas definidas en momentos que así lo requieran.

La falta de consideración de estas políticas lleva a que las organizaciones incurran en costos que no estaban definidos en materia de seguridad tanto lógica como físicamente, llevando muchas veces a invertir en elementos innecesarios o adquiridos en momentos inadecuados.

El propósito de establecer estas políticas principalmente es proteger la información y los activos de la organización, tratando de proporcionar confidencialidad, integridad y disponibilidad de los datos, además de las responsabilidades que deben asumir todos y cada uno de los empleados mientras permanezcan en la organización.

REFERENCIAS BIBLIOGRÁFICAS

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

CHEN, Vicki y GOEL, Sanjay. Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process. En: International Journal of Production Economics, Ámsterdam: Elsevier, 2008. p. 104-112.

CIO AMÉRICA LATINA. Mercado de la seguridad informática creció 5,3% en 2014 [en línea]. (23 de Julio de 2015). [Citado el 10 de Octubre de 2015] Disponible en Internet <http://www.cioal.com/2015/07/23/gartner-mercado-de-la-seguridad-informatica-crecio-53-en-2014/>.

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>.

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.

ISO Org. Evolution of ISO/IEC 2700 certificates in Colombia. En: ISO Survey [en línea]. (Diciembre de 2013). [Citado el 20 de Septiembre de 2014] Disponible en Internet <http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=CO#countrypick>.

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>.

PROCESO DE CERTIFICACIÓN 27001. Empresas certificadas en Colombia. En: Proceso de certificación 27001 [en línea]. (Septiembre de 2013). [Citado el 4 de

Agosto de 2015] Disponible en Internet <http://certificacion27001.blogspot.com/2010/09/empresas-certificadas-de-colombia.html>.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular externa 038 de 2009. Bogotá. 2009.

ANEXOS