UNIVERSIDAD NACIONAL PEDRO HENRÍQUEZ UREÑA (UNPHU)

Facultad de Ciencia y Tecnología

Escuela de Ingeniería Industrial

¨Diseño de un Sistema de gestión de seguridad de la información para la empresa Coop-Aspire, basado en la norma ISO 27001¨

Trabajo de Grado presentado por:

Brianda Beatriz Flores Sanchez

Para la obtención del grado de

Ingeniero Industrial.

Asesor:

Ing. Fe Del Carmen Payano

Santo Domingo, D.N.

2017

ÍNDICE

DEDICATORIA

A Dios.

Por haberme guiado hasta este punto y haberme dado salud, fuerza y perseverancia para lograr mis objetivos, gracias por su infinita misericordia y por su amor.

A mi mama María Luisa.

Por sostenerme de la mano en todo mí proceso educativo, por sus consejos, sus valores, por su fuerza, por ayudarme a encontrar una salida siempre, pero más que nada, por su amor.

A mi padre José Manuel.

Por la nobleza que lo caracteriza, por llevarme y traerme, por su amor que siempre me fortalece.

A mi esposo.

Por su apoyo, por su amor, por no cortar mis alas sino por invitarme a volar, por motivarme a superarme, por nuestro bebe.

A mi prima Nery Por iniciar este viaje conmigo en esta universidad y por no dejarme abandonar.

A mis hermanos José Manuel y José Luis, y a mi tía Elizabeth por estar ahí.

Gracias a mis maestros. Por su gran apoyo y motivación para la culminación de mis estudios profesionales especialmente a la Ing. Fe del Carmen Payano por su apoyo ofrecido en este trabajo, por su tiempo compartido y por no dejarme desmayar. A Mónica Pilar por su apoyo, consejos y guía. A mi compañera de siempre María Valerio, que nos apoyamos mutuamente en nuestra formación profesional y que hasta ahora, seguimos siendo amigas. A la

Universidad Nacional Pedro Henríquez Ureña y en especial a la Facultad de Ciencias y tecnología y a la escuela de Ingeniería Industrial por permitirme ser parte de una generación de triunfadores y gente productiva para el país.

INTRODUCCIÓN

Proporcionar una seguridad total a nivel tecnológico para nuestras empresas u organizaciones, es casi imposible en nuestros tiempos, por tanto muchas instituciones acuden a herramientas de control perfectamente flexibles y adaptables a los cambios como es el Sistema de Gestión de Seguridad de la Información. De acuerdo a la aseveración anterior, el propósito de un SGSI es minimizar riesgos haciendo que los mismos sean conocidos y gestionados, a través de documentación, de manera estructurada, sistemática y abierta a los cambios del entorno y la tecnología.

Durante el seminario sobre riesgo operacional, el Ex–Superintendente de Bancos en la Republica Dominicana, Haivanjoe NG Cortiñas, señaló que los eventos que más afectaron a las entidades financieras en el año 2011, fueron los fraudes externos. Las estadísticas arrojan que los fraudes con tarjetas de crédito significaron al menos el 55% del total de pérdidas coligadas a riesgo operacional. [1]

Según investigaciones hechas por la firma "Kaspersky Lab" para Latinoamérica, durante el año 2016, una de cada cinco compañías a nivel mundial fue víctima de un incidente como resultado de un asalto a los sistemas tecnológicos a través de un software malicioso y más del 67% perdió parte de sus datos corporativos, el 33% restante pago el rescate.

En el último trimestre del año 2016 la Superintendencia de Bancos (SIB), registró 103, 438 reclamaciones a los servicios de entidades de intermediación financiera (EIF).

En cuanto al mismo periodo del año 2015 solo se registraron 94,571 y en 2014 se registraron 69,231 casos, las cifras indican que el número de reclamos aumenta de año en año, lo cual resulta alarmante.

Es un hecho que la mayoría de los procesos de negocios, ya están siendo gestionados y automatizados por sistemas informáticos y los mismos a su vez soportan la toma de decisiones y en ocasiones es la misma información y el acceso a ella el principal objetivo del negocio, como es el caso de las instituciones financieras.

El sector financiero, está en la obligación de garantizar la seguridad, protección y privacidad de la información financiera y personal de los usuarios que anidan en sus bases de datos, esto quiere decir, que deben disponer todos sus recursos con el fin de más altos con los más altos niveles y normas en cuanto a seguridad se refiere con el fin de garantizar la debida compilación, y uso de esta información.

Una de las inquietudes permanentes del tipo de organización financiera estudiado en el presente trabajo, es la de garantizar la seguridad de las operaciones que realizan sus clientes, lo cual es cada día más complejo de conseguir, ya que el avance de la tecnología y la apertura de nuevos canales de transacciones generan retos significativos, con el propósito de prevenir los fraudes en general.

Según las observaciones, hay poca atención a la seguridad informática en Coop-Aspire, lo cual ha generado múltiples riesgos que amenazan la seguridad de la información, la salvaguardia y privacidad de los datos, siendo necesario implementar un sistema basado en las amenazas que este alineado con los objetivos generales y necesidades tanto de la institución como de sus involucrados e interesados.

El desafío será entonces diseñar, un Sistema de Gestión de Seguridad de la Información (SGSI) para la Cooperativa de crédito, ahorros y servicios múltiples, teniendo en cuenta como punto de partida la norma ISO 27001 la cual brinda como plataforma un marco metodológico basado en estándares para la seguridad de la Información en cualquier tipo de organización, Esto nos permitirá garantizar una implementación efectiva y asegurar su debida continuación y perfeccionamiento en el tiempo.

Del mismo modo para lograr lo que nos hemos propuesto, utilizaremos ciertas herramientas aprendidas durante el transcurso de la carrera, como son: Diagrama de pescado (Ishikawa) y el ciclo de Deming o PHVA que estaremos detallando más adelante en el marco metodológico del presente trabajo.

PRIMERA PARTE

GENERALIDADES

CAPÍTULO I: GENERALIDADES

1.1 Justificación

Vemos necesario diseñar un procedimiento para la implementación de un Sistema de gestión de la seguridad de la información (SGSI), pues este nos va a permitir localizar, administrar y reducir los riesgos actuales y los posibles riesgos que podrían afectar la seguridad información en la organización, todo esto de manera sistemática, eficiente, documentada y flexible ante los cambios que se produzcan en el entorno, los riesgos y la tecnología.

Para lograr el diseño del SGSI, tomaremos como referencia el grupo de normas ISO 27000 para obtener un sistema esbelto que garantice la disponibilidad, integridad y confidencialidad de la información.

1.2 Motivación

En mis prácticas diarias como colaboradora, pude observar la vulnerabilidad a la cual está expuesta la organización, pude contemplar además a través de los análisis de riesgos, que debido a las mismas vulnerabilidades, en cualquier momento la empresa podría verse afectada.

De modo que en un intento de ayudar a la empresa a evitar el hurto de la información, fraude, falsificación, me vi motivada a proponer el diseño de un sistema que nos podría ayudar a evitar estas cosas.

1.3 Objetivos

1.3.1 Objetivo General

Proponer el diseño de un Sistema de gestión de seguridad de la información para la empresa Coop-Aspire, basado en la ISO 27001.

1.3.2 Objetivos Específicos:

- Elaborar un documento de guía donde se expongan las directrices para la implementación de un Sistema de Gestión de Seguridad de la información.
- Diseñar un sistema para la implementación tomando como referencia el ciclo Planificar, Hacer, Verificar y Actuar (PHVA).
- Sugerir herramientas que faciliten la ejecución de la norma ISO 27001 en un sistema de gestión en Coop-Aspire.

1.4 Alcance del SGSI y Limitaciones

1.4.1 Alcance

El alcance del proyecto abarca el diseño un Sistema de Gestión de Seguridad de la información para la empresa Coop-Aspire, basado en el ciclo PHVA con el propósito de cumplir con la primera fase de la implementación de un SGSI, que atañe a la etapa de planeación.

Para el desarrollo del trabajo de grado utilizaremos como referente la norma NTC-ISOIEC 27001, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, limitándonos solo al diseño y propuesta de el mismo.

En este paso debemos definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Es importante aclarar y definir los límites del SGSI, no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado, por lo cual nos atendremos a hacer los levantamientos limitándonos solo a las oficinas administrativas.

Es importante habilitar un mapa de procesos, y especificar cuáles hará parte del alcance.

Tener claro los involucrados, sus asignaciones y su incidencia en la seguridad de la información, es importante en el momento de definir el alcance, los requisitos legales y contractuales relacionados con la seguridad de la información deben quedar contemplados también dentro del alcance del sistema.

El objetivo de este documento es definir claramente los límites del Sistema de gestión de seguridad de la información (SGSI) en Coop-Aspire.

Este documento se aplica a toda la documentación y actividades dentro del SGSI.

Los usuarios de este documento son los miembros de la dirección de Coop-Aspire, los miembros del equipo del proyecto que implementa el SGSI y los miembros del Consejo de Administración.

La organización necesita definir los límites del SGSI para decidir qué información quiere proteger. Esa información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del SGSI.

El hecho de que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad; esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad será transferida a un tercero que administre esa información.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

- Operaciones

• Cobros

• Contabilidad

• Servicio al cliente

• Evaluación de créditos

- Unidades organizativas

• Informática

- Redes e infraestructura de TI

• Core bancario

• Electricidad

• Comunicaciones con las sucursales

• Telefonía

- Exclusiones del alcance

Los siguientes elementos no están incluidos en el alcance:

• Negocios

• Finanzas

- Operaciones
- Recursos Humanos
- Gerencia
- Operaciones
- Contabilidad
- Análisis & Custodia

Cualquier otro proceso que la organización considere incluir dentro del SGSI es permitido, pero se exhorta que la inclusión del mismo sea con base en un análisis que explique en detalle la importancia de incluir a dicho proceso, hacer un SGSI lo más simple posible es un consejo que se ha tomado en cuenta, más porque se ha empezado desde cero el diseño del Sistema.

1.4.2 Limitaciones

En el presente trabajo de Grado abarcaremos de manera total las etapas de análisis y diseño del SGSI para la empresa Coop-Aspire, basada en la norma NTCISO-IEC 27001, sin embargo las etapas de Implementación revisión, mantenimiento y mejora del Sistema de Gestión solo las tocaremos de manera parcial, permitiéndonos así proponer documentos para su posterior consideración en las subsiguientes etapas.

1.4.3 Entregables:

- Acta Constitutiva del SGSI
- Alcance del SGSI
- Cuadro de evaluación de Riesgos
- Aplicabilidad roles y alcance
- Política de Seguridad de la Información
- Inventario de los activos
- Gestión de incidentes de Seguridad

SEGUNDA PARTE

MARCO TEORICO

CAPITULO II: MARCO TEORICO

A raíz de la importancia que ha tenido la tecnología en los últimos años, estamos en la era de la información, en una época en que la misma ha tomado mayor valor que muchos otros activos de la empresa, por lo cual las organizaciones deben tener como principal objetivo cuidar la disponibilidad y seguridad de sus activos de información, con la finalidad de crear una ventaja competitiva en el mercado. Mientras más tecnología y expansión exista en la organización más riesgos va a correr la información, si no existe protección contra vulnerabilidades y amenazas.

Para evitar lo anteriormente mencionado, es necesario crear un sistema robusto y claro en base a normas que permitan a los usuarios asegurar la seguridad y la disponibilidad de la información que maneja.

2.1 Normas ISO

La International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC), forman el sistema especializado para la normalización mundial. Los organismos miembros de ISO e IEC participan en el desarrollo de las Normas Internacionales por medio de comités técnicos establecidos por la organización respectiva, para atender campos particulares de la actividad técnica[1]. Para fundamentar este trabajo nos enfocaremos en las siguientes normas:

2.1.1 ISO 27001:

Según nuestra consulta[2] "ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Según Academy, Web Consultation: "ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización".

[1] Corletti, A. 2011. Seguridad Por Niveles,
[2] ISO 27001, Online Consultation Center, Academy

También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). ”

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las inspecciones de seguridad que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la ejecución de ISO 27001 estará relacionada con determinar las reglas organizacionales, necesarias para prevenir violaciones de la seguridad.

Como este tipo de proyecto demandará la gestión de múltiples recursos, políticas y procedimientos, etc., ISO 27001 ha especificado cómo mezclar todos estos elementos dentro del SGSI, por lo mismo esta norma será nuestro norte en el presente proyecto.

Por eso, la gestión de la seguridad de la información no se limita a la seguridad de TI (firewall, anti-virus, etc.), sino que también encierra la gestión de procesos, del personal, protección jurídica y física, etc.

2.1.2 ISO 27002:

El día 1 de Julio de 2007, la ISO 17799:2005, cambió de nombre, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005 (Ver Anexo 3). Esta norma es la mejor práctica que da a los responsables los elementos necesarios para gestionar la seguridad de la información, las pautas para estructurar el plan y los objetivos de control, controles necesarios para implementar la seguridad y acciones fundamentales para minimizar los riesgos que la vulneren.[3]

[3] Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

2.1.3 ISO 27005:

Constituye las pautas para la gestión del riesgo en la seguridad de la información. Está diseñada para soportar aplicación favorable de la seguridad de la información basada en un enfoque de gestión de riesgos.

Esta norma respalda el desarrollo de uno de los requerimientos base para la implementación de la ISO 27001:2005 y el cumplimiento de otros como es la "valoración de los riesgos" que incluye el hallazgo, evaluación y mitigación de los riesgos en la seguridad de la información.

"Adicionalmente brinda soporte y conceptos generales que se especifican en la 27001, y está diseñada con el objetivo de facilitar la implementación de la seguridad de la información, con base en el enfoque de gestión de riesgo".[4]

2.1.4 ISO 22301

Norma ISO que establece los requisitos para un sistema de gestión de continuidad de negocio. Tiene su origen en la norma BS 25999.

[4] Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

2.2 Seguridad de la Información

La seguridad de la información es un activo para la empresa, puesto que es un conjunto de datos que genera valor para las organizaciones y por lo mismo mencionado es necesario asegurar su protección.

Como resultado del crecimiento tecnológico y la globalización, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas: puede estar impresa o escrita en un papel, almacenada en magnético, enviada por correo o utilizando medios electrónicos, videos o grabaciones de voz. Sin importar la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debe estar protegida.

Analizando en términos generales las amenazas en los sistemas de información se podrían presentar en diversas formas:

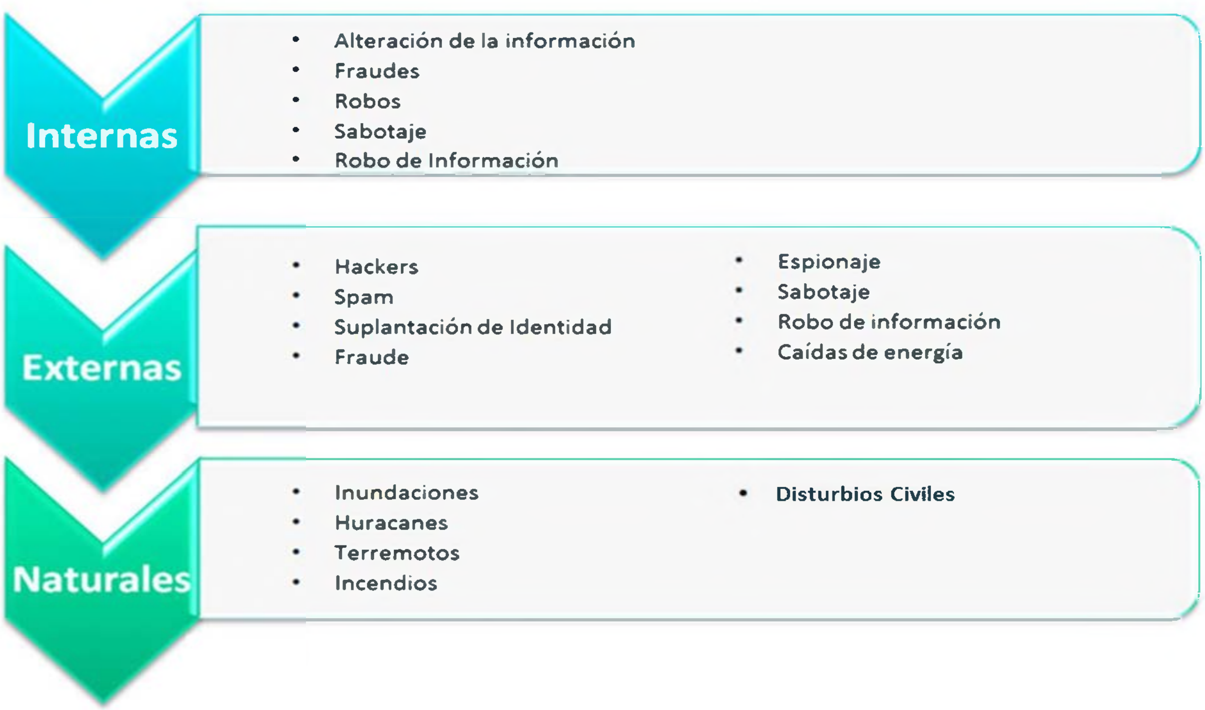


Ilustración 1: Amenazas o Riesgos en un SGSI

Como lo indica la ISO 27002:2005: La seguridad de la información se consigue implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

2.3 Beneficios de un SGSI

Un Sistema de Gestión de Seguridad de la información (0), es la parte de un sistema de gestión global basado directamente en los riesgos para el negocio y los activos del mismo contemplado en la norma ISO 27001, ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información evitando las inversiones mal dirigidas, contrarrestando las amenazas presentes en el entorno y dentro de la misma, implementación de controles proporcionado y de un coste menos elevado.[5]

- Reducir el riesgo de que se produzcan pérdidas de información en las organizaciones (por pérdidas también entendemos robos y corrupciones en la manipulación de la misma).

[5] Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda JD Aguirre Cardona - 2013

- Revisar continuamente los riesgos a los que están expuestos los clientes. Adicionalmente, se hacen controles de manera periódica.
- Establecer una metodología gracias a la cual se puede gestionar la seguridad de la información de forma clara.
- Implementar medidas de seguridad para que los propios clientes puedan acceder a la información.
- Realización de auditorías internas y externas de manera periódica permitiendo la identificación de las vulnerabilidades del Sistema de Gestión de Seguridad de la Información, fomentando de este modo la mejora continua en la organización.
- Diferenciación frente a clientes y socios estratégicos ya que muestra a la misma como un organismo preocupado por la confidencialidad y seguridad de la información que es depositada en la misma.
- Integralidad conjunta con otros Sistemas de Gestión Normalizados tales como ISO 9001, ISO 14001, OHSAS 18001, entre otras. Obligando que la organización esté cumpliendo con la legislación vigente en materia de información personal y propiedad intelectual.
- Reducción de los costes y un mejor funcionamiento de los procesos (derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos)
- Contribuir con la mejora de la motivación del personal, ya que se desempeñan en una organización comprometida y organizada.

2.4 Continuidad del Negocio

Este concepto que siempre ha estado presente en los empresarios más competentes se ha visto afectado por la importancia que ha adquirido la TIC y por la llegada de la Sociedad de la Información. En este nuevo escenario, la información que se maneja se ha destacado como uno de los activos más importantes de las empresas.

Se preocupa por seguir ofreciendo los servicios o productos que genera la empresa después de una contingencia que pueda ser más o menos grave, evitando la paralización de las operaciones.

Por ello, se introduce el concepto de Business Continuity Plan es el proceso que adoptan las empresas para poder recuperarse de alguna eventualidad de una forma rápida y comenzar sus funciones casi de inmediato con los requisitos mínimos establecidos.

Como en el caso anterior de seguridad de la información, los estándares se han preocupado por intentar ofrecer una normativa que pueda ser seguida por toda la empresa que así lo desee para desarrollar un plan que garantice la continuidad del negocio después de una contingencia[6].

2.4.1 Reglamento Del Plan de Emergencia

Para dar cumplimiento a los estándares internacionales, será electo el 10% del personal por cada área para formar las brigadas de emergencia.

[6] Diseño De Un Sistema De Gestión De Seguridad De La Información (SGSI), EAN, P. 21

El comité de emergencia estará compuesto o constituido de la siguiente forma:

a. Un comité central con un representante por cada sucursal

b. Un líder de emergencia a nivel nacional o corporativo.

c. Un líder de brigada por piso (Edificio Principal) y un asistente o sub-brigadista.

d. El representante de las sucursales en el comité central será asimismo el líder de la brigada de la sucursal a la que corresponde.

e. Todo líder de las sucursales tendrá un asistente o sub-brigadista.

f. Todo integrante deberá cumplir con el perfil del brigadista descrito en el reglamento.

g. Todo brigadista llevará puesto siempre un distintivo que lo acredita como brigadista de emergencia y no podrá ser este prestado a otro empleado, ni brigadista.

h. Deberá cumplir con sus funciones y responsabilidades descritas expresamente en este acápite reglamentar.

i. El privilegio de pertenecer a la brigada de emergencia es totalmente voluntario y esto no requiere necesariamente que se tome en consideración para aumento de salarios, ni ningún otro beneficio en lo particular.

j. La brigada tiene una duración de dos años y todo miembro tiene el derecho de elegir y ser elegido.

k. La celebración de elecciones para nuevos líderes será determinada por el encargado de emergencia a nivel corporativo.

l. Al ausentarse los representantes de las sucursales (no pertenecer a la empresa o cualquier otra razón que indique que ya no estará en dicha posición) será reemplazado por el asistente hasta que el líder de emergencia corporativo lo determine.

m. Para pertenecer al comité de emergencia deberá haber recibido todas las capacitaciones requeridas para tales fines (Combate de Incendios, Primeros Auxilios, Evacuación Rescate, etc.).

n. Toda acción o implementación de mejoras para el plan de emergencia, deberá ser primero presentada al Líder de Emergencia y este lo someterá al comité para su aprobación o rechazo según delibere el comité central.

o. Toda actividad que tenga que realizar algún brigadista deberá ser comunicada a su jefe inmediato para mantener la disciplina y respecto del presente reglamento.

2.5 Definición del ciclo PHVA

El ciclo "Planificar-Hacer-Verificar-Actuar" fue desarrollado inicialmente en la década de 1920 por Walter Stewart, y fue popularizado luego por W. Edwards Deming. Por esa razón es frecuentemente conocido como "Ciclo de Deming".

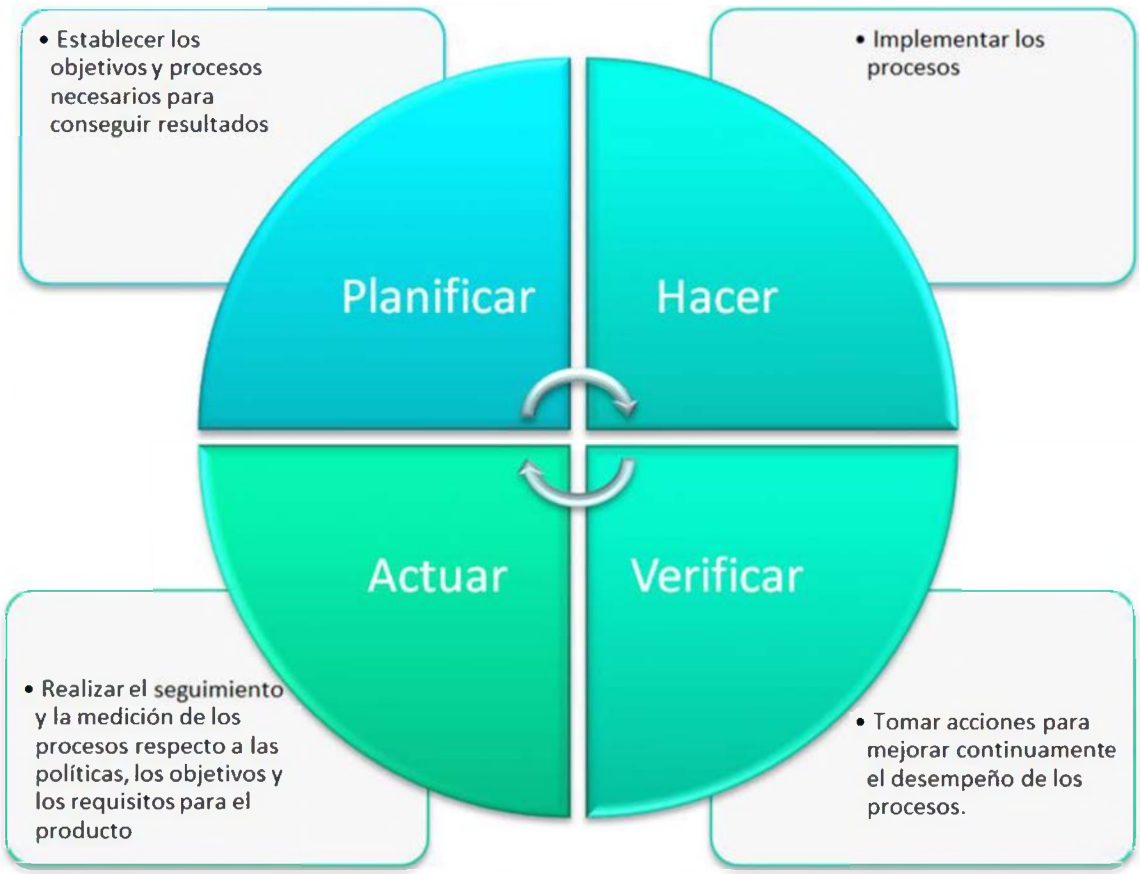
Dentro del contexto de un sistema de gestión de la calidad, el PHVA es un ciclo dinámico que puede desarrollarse dentro de cada proceso de la organización, y en el sistema de procesos como un todo. Está intrínsecamente asociado con la planificación, implementación, control y mejora continua, tanto en la realización del producto como en otros procesos del sistema de gestión de la calidad.

El mantenimiento y la mejora continua del proceso pueden lograrse aplicando el concepto de PHVA en todos los niveles dentro de la organización. Esto aplica por igual a los procesos estratégicos de alto nivel, tales como la planificación de los sistemas de gestión de la calidad o la revisión por la dirección, y a las actividades operacionales simples llevadas a cabo como una parte de los procesos de realización del producto.

La nota en el apartado 0.2 de la Norma ISO 9001:2000 explica que el ciclo de PHVA aplica a los procesos tal como sigue:

- **Planificar:** establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización;
- **Hacer:** implementar los procesos;
- **Verificar:** realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.

- **Actuar:** tomar acciones para mejorar continuamente el desempeño de los procesos.



2.6 Riesgos

Ilustración 2: Ciclo PHVA, Fuente: Autora

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad. [7]

[7] Diseño De Un SGSI, M. Villena, P. 29

HALVORSON (2008, 71) explica tres (3) naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales, según la naturaleza de los procesos que he definido en el capítulo 2:

- Los riesgos estratégicos son los que están más relacionados con la seguridad de la información; sin embargo, se encuentran más alineados a los riesgos de ámbito económico y de reputación de la organización, ya que se desprende de decisiones estratégicas que han sido o serán tomadas en la organización.
- Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.
- Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).
- Es importante conocer cuáles son las causas para que se cometan los delitos:

Mayor Riesgo:

- Beneficio personal
- Síndrome de Robín Hood
- Odio a la organización
- Mentalidad turbada

- Equivocación de ego
- Deshonestidad del departamento
- Problemas financieros de algún individuo
- Fácil modo de desfalco

Menor Riesgo

- Beneficio de la organización
- Jugando a jugar

2.7 Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología

Esta ley tiene como objetivo la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o moral, en los términos previstos en la misma.

2.8 Estado de la norma

El número de certificaciones ha aumentado considerablemente en los últimos años como demostración de la relevancia que tiene la protección de la información para el desarrollo de las actividades de las organizaciones y para mantener y desarrollar el tejido industrial de los diferentes países y en todo el mundo.

Existe información regular aportada por ISO en el documento ISO Survey[8] donde se informa de manera detallada y a año vencido (p.ej. la publicación del año 2015 refleja los totales para el año anterior completo a fecha 31 de diciembre) del resultado en el número de certificaciones acreditadas con referencia a las regiones, países, sectores industriales de mayor implantación, entre otros, tanto para ISO/IEC 27001 como para otros sistemas de gestión (ISO/IEC 9001, ISO 14001, ISO 22000, ISO 50001, entre otros).[9]

Del Informe antes mencionado de la ISO pudimos observar que el número de certificados ISO/IEC 27001 a nivel mundial a finales del año 2015 asciende a 27.536 lo que representa un 20% de crecimiento en relación al año anterior (Ver Anexo 4).

2.8.1 Estado de la norma en República Dominicana.

Según las últimas estadísticas disponibles, en el país existen una gran cantidad de organizaciones que actualmente están certificadas algunas del sector servicios y otras del sector industrial. Entre las que podemos mencionar:

Agencias del Gobierno Dominicano.

- **Banco Central de La República Dominicana.**

http://www.bancentral.gov.do/notas_bc/2012/05/30/56/valdez-albizu-informa-banco-central-obtiene-certificacion-iso-27001-

[8] Ver anexos
[9] http://www.iso27000.es/certificacion.html

- **Superintendencia de Salud y Riesgos Laborales.**

http://www.diariolibre.com/noticias/2012/08/14/i347832_sisalril-logra-norma-seguridad-informacin.html

Existe una tercera organización que aunque no es gubernamental está asociada al sector salud y la seguridad social:

- **Unipago**

La empresa procesadora de la base de datos del Sistema Dominicano de Seguridad Social.

http://www.elcaribe.com.do/2012/10/31/unipago-10-anos-dando-apoyo-seguridad-social#sthash.CvXBMISR.dpuf

Otra entidad que exhibe esta certificación es:

- **Editora LJ**

http://jleditora.com.do/certificacion-iso-270012005/

- **Cevaldom Depósito Centralizado de Valores (CEVALDOM)**

Cevaldom, informa que el mes de diciembre de 2016 obtuvo la certificación que avala el cumplimiento por su parte del estándar ISO/IEC 27001: 2013 sobre Sistemas de Gestión de Seguridad de la Información.

El referido certificado es válido para el siguiente alcance: El sistema de gestión de seguridad de la información del servicio de liquidación de las operaciones pactadas en el mercado de valores de la República Dominicana, así como también de sus procesos de soporte de gestión tecnológica y de gestión humana, de acuerdo a la versión 1.1 de la declaración de aplicabilidad.

http://www.bvrd.com.do/noticias/cevaldom-obtiene-certificacion-iso-27001

- **EQA**

European Quality Assurance, es una entidad de Certificación internacional.

http://www.eqa.com.do/servicios/calidad/tecnologia-de-la-informacion/iso27001/

- **Sistema Único de Beneficiarios (Siuben).**

http://www.siuben.gob.do/2016/04/12/vicepresidenta-recibe-certificaciones-iso-obtuvo-el-siuben/

Actualmente diferentes entidades del gobierno dominicano se encuentran iniciando los trabajos elaboración de términos de referencia de selección de consultores.

En el presente nuestro país se cuenta con tan solo dos Auditores Principales en ISO 27001 y unos cuatro Implementadores Principales en ISO/IEC 27001.

Con frecuencia para este tipo de funciones el personal de trabajo es captado y contratado de otros países para realizar estas auditorías.

2.9 Historia de la empresa

La Cooperativa de Ahorro, Crédito y Servicios Múltiples ASPIRE, INC (Coop-Aspire) es una organización que tiene su génesis en la búsqueda de nuevos horizontes para que hombres y mujeres emprendedores desplieguen su potencial creativo y productivo, a favor de ellos, de sus familias y del entorno comunitario en el que viven. Su nacimiento mismo se enmarca en la decisión de los miembros de la Asociación para Inversión y Empleos, Inc. (ASPIRE), de reinventar modelos institucionales de servicios comunitarios incluyentes, sostenibles en el tiempo y con un impacto positivo en la vida de los participantes. De esa manera se intenta ir más allá de los límites estrictos de los servicios micro financieros, avanzando hacia la adopción plena de los principios y filosofía del cooperativismo.

Su llamado consiste en crear oportunidades para que miles de dominicanos y dominicanas se inserten en la vida productiva con niveles crecientes de dignidad.

Coop-Aspire fue incorporada, mediante el decreto No. 61-13 de fecha 28 de Febrero 2013. Inició sus operaciones formalmente, el 1ero. De Julio 2013.

En consonancia con las razones que le dieron origen, sus servicios siguen enfocados de manera prioritaria a propietarios y propietarias de micro y pequeñas empresas, Concilios e iglesias de profesión cristianas, centros educativos privados y empleados de instituciones públicas y privadas. Ofrecemos servicios en las principales zonas del país, en la zona norte: Villa Altagracia, Monseñor Nouel, La Vega y Santiago; en la zona este: San Pedro de Macorís y en el municipio de Consuelo; en la Zona Sur, en San Cristóbal y el Municipio de Haina; y en la Zona Metropolitana en: Los Alcarrizos, Herrera, Villa Mella, Sabana Perdida, Los Frailes, Los Minas, Villa Consuelo y en el Ensanche Piantini.

Coop-Aspire es parte de la Asociación de Instituciones Rurales de Ahorro y Créditos, Inc. (AIRAC) y del Consejo Nacional de Cooperativas, (CONACOOP).

2.9.1 Misión

Facilitar el empoderamiento de personas emprendedoras en su proceso de Transformación integral. Se dará cumplimiento a esta misión:

- Proveyendo servicios micro financieros, con sentido de responsabilidad y justicia.
- Capacitando a personas con el potencial de desarrollar micro y pequeñas empresas, desde una perspectiva integral.
- Gestionando los recursos de manera responsable y transparente.
- Acompañando a nuestros clientes en su proceso de transformación, sin generar Dependencia.
- Cultivando los principios del cooperativismo en la inserción de nuestros socios a la vida productiva.

2.9.2 Visión

Ser una referencia nacional en la prestación de servicios Financieros que enriquezcan integralmente la vida de nuestros asociados, de manera progresiva y sostenible.

2.10 Planteamiento del problema

Luego de analizar la plataforma informática del departamento de TI de la empresa Coop-Aspire, hemos visualizado el exponencial crecimiento desde su creación como Cooperativa en 2013 con 15, 919 Socios, en 2014 34,173 Socios y en 2015 57,632 (Ver Anexo 2). Esto ha provocado que los controles a nivel de Seguridad de la Información resulten inadecuados para garantizar la disponibilidad, integridad y confidencialidad de la información de los socios, y que crezcan considerablemente las amenazas que afectarían en el futuro lo que nos indica que es necesario que sean revisados y mejorados.

Con el crecimiento antes mencionado también ha proliferado el almacenamiento de datos, el uso de la tecnología, el mantenimiento, transmisión y recuperación de información, y con ellos la cantidad de amenazas que podrían surgir y afectar la disponibilidad, privacidad, auditabilidad y la veracidad de la información, lo mismo podría causar graves pérdidas tanto financieras como de tiempo para la empresa.

La falta de un Sistema de Seguridad de la Información que respalde la gestión de los riesgos, la poca concienciación, apropiación y conocimiento en cuanto a los mismos, no se le ha dado la importancia necesaria a la información y su protección, lo cual no produce las acciones necesarias para la protección de la información como recurso valioso para la empresa.

Este panorama, también nos deja entrever que se desconoce la diferencia entre seguridad de la información y seguridad informática.

La organización necesita mejoras en el sistema de información para la gestión de riesgos de seguridad, pues el que hay en existencia no permite ver el panorama actual de la seguridad, en cuanto a usuarios (o socios), procesos y tecnología, e implica entre otros aspectos, que no existe la participación activa de toda la organización con relación a la definición de procedimientos adecuados y a la planeación e identificación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

Hemos observado que la institución no posee un plan de contingencia, el cual garantiza la continuidad de las funciones de la organización ante cualquier incidente sea material o personal.

A

Activo de Información: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa. La información, como activo corporativo, puede existir de muchas formas:

- Impresa
- Almacenada electrónicamente
- Transmitida por medios electrónicos
- Mostrada en videos

- Suministrada en una conversación
- Conocimiento de las personas
- Alcance de la auditoría: Extensión y límites de una auditoría.

Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

Análisis de Riesgos: Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

C

Compromiso de la Dirección: (Inglés: Management Commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Conformidad: cumplimiento de un requisito

Continuidad del negocio: Se preocupa por seguir ofreciendo los servicios o productos que genera la empresa después de una contingencia que pueda ser más o menos grave, el concepto de BCP (Business Continuity Plan) que puede definirse como el proceso que las empresas definen para poder recuperarse de una situación de contingencia lo antes posible y empezar a funcionar con unas condiciones mínimas aceptables.[10]

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Core bancario: Core bancario (en inglés, core banking) se define como el negocio desarrollado por una institución bancaria con sus clientes minoristas y pequeñas empresas. Muchos bancos tratan a los clientes minoristas como a sus clientes de "Core bancario", y tienen una línea de negocios separada para gestionar las pequeñas empresas. Las grandes empresas son administradas a través de la División de Banca Corporativa de la institución. "Core bancario", básicamente, se refiere a las operaciones de depósito y de préstamos de dinero.[11]

Cortafuegos: Cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer

[10] (IGLESIAS, 2009)
[11] https://es.wikipedia.org/wiki/Core_bancario

su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.[12]

D

Declaración de aplicabilidad: (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001 (Ver Anexo 3).

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes.

Desastre: (Inglés: Disasters). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

E

Efectividad: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

[12] ICETEX, Manual de políticas de seguridad de la información

Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados.

Estándar: Un estándar es una publicación que recoge el trabajo en común de los comités de fabricantes, usuario, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.[13]

Evaluación de riesgos: (Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

I

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

Integridad: La información de Coop-Aspire debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras.

[13] Norma ISO27001

ISO: La Organización Internacional de Normalización (ISO), es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países, uno por cada país. La ISO es una organización no gubernamental, establecida en 1947 cuya misión es promover el desarrollo de la estandarización y las actividades relacionadas, con el 2 fin de facilitar el intercambio de servicios y bienes y promover la cooperación en la esfera de lo con intelectual, científico, tecnológico y económico. Todos los trabajos realizados por la ISO resultan en acuerdos internacionales, los cuales son publicados como Estándares Internacionales.[14]

M

Macro-Proceso: Agrupación de procesos de similares características y naturaleza, cuyo ámbito institucional es de muy alto nivel y refleja la forma como se organiza la Cooperativa.

Mapa de procesos: El mapa de procesos proporciona una perspectiva global-local, obligando a “posicionar” cada proceso respecto a la cadena de valor. Al mismo tiempo, relaciona el propósito de la organización con los procesos que lo gestionan, utilizándose también como herramienta de consenso y aprendizaje.

[14] https://www.ecured.cu/ISO

N

No conformidad: El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real.

NTP: Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

P

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Plan de continuidad del negocio: (Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Proceso: (Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

R

Ramsomware: Es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados.

Riesgo: Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la información en los activos de una empresa.

S

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 buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Seguridad informática: Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

S.G.S.I: Sistema de Gestión de Seguridad de la Información.[15] (Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y

[15] ROBIN J. SALCEDO B. ISAGXXX, P. 7, 2014

unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y la mejora continua.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el Coop-Aspire o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.[16]

---

[16] MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, ICETEX, PEuropa, C. d. (2001). Convenio sobre la Ciberdelincuencia. 3.

ICETEX. (2014). Manual de Politicas de seguridad de la informacion.

IGLESIAS, L. M. (2009). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). *UNIVERSIDAD REY JUAN CARLOS*, 6.

pmg-ssi. (7 de marzo de 2014). Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: http://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

SIB. (2016). Especialista afirma mayor riesgo de ataques cibernéticos están en filtración de datos personales. *Superintendencia de Bancos* .

Verizon. (2010- 2012). *Data Breach Investigations Report.*

Servidor de base de datos: Provee servicios de base de datos a otros programas u otras computadoras, son aquellas computadoras dedicadas a ejecutar y prestar servicios.

La base de datos maneja grandes cantidades de información que deben estar seguras, tiene un sistema de gestión de base de datos que proporciona una herramienta de apoyo a la toma de decisiones y así se tiene una información actualizada y consistente.[17]

V

Vulnerabilidad: (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas

.8

[17] Tesis Auditoria de seguridad informática, C. Cadme D. Duque, 2011, P. 30

TERCERA PARTE

MARCO METODOLOGICO

CAPITULO III: MARCO METODOLOGICO

3.1 Metodología para la implementación del SGSI en Coop-Aspire

La principal visión que debe tener una empresa que busque establecer un SGSI es un enfoque por procesos, la norma ISO 27001 aconseja la adopción del ciclo Planear – Hacer – Verificar – Actuar (PHVA), para la descripción de los procesos relacionados en el SGSI, a pesar de que no es parte del alcance del presente trabajo de grado el trazar una metodología para las organizaciones de cómo lograr un enfoque por procesos, haremos unas recomendaciones generales que ayudaran al lector a concretar los procesos que intervendrán en el SGSI.

Trabajaremos con el ciclo PHVA para pautar una metodología general para la ejecución de lo que establece la norma ISO 27001 para el sector financiero, en la cual enumeraremos cada una de las etapas para la implementación del SGSI.

3.1.1 Ciclo PHVA para el SGSI

Según el marco metodológico de este Trabajo de Grado trabajaremos en la metodología PHVA de la norma ISO 27001 de los SGSI, la siguiente figura describe la metodología que usaremos dentro de cada fase del ciclo.

Esta figura contiene un resumen de la metodología sugerida, en la misma se enumeran los entregables en cada etapa del ciclo, esto ayuda al lector a desarrollar herramientas necesarias con el fin de cumplir los requerimientos exigidos por la norma 27001. Las mismas herramientas, las estaremos evidenciando en los anexos.

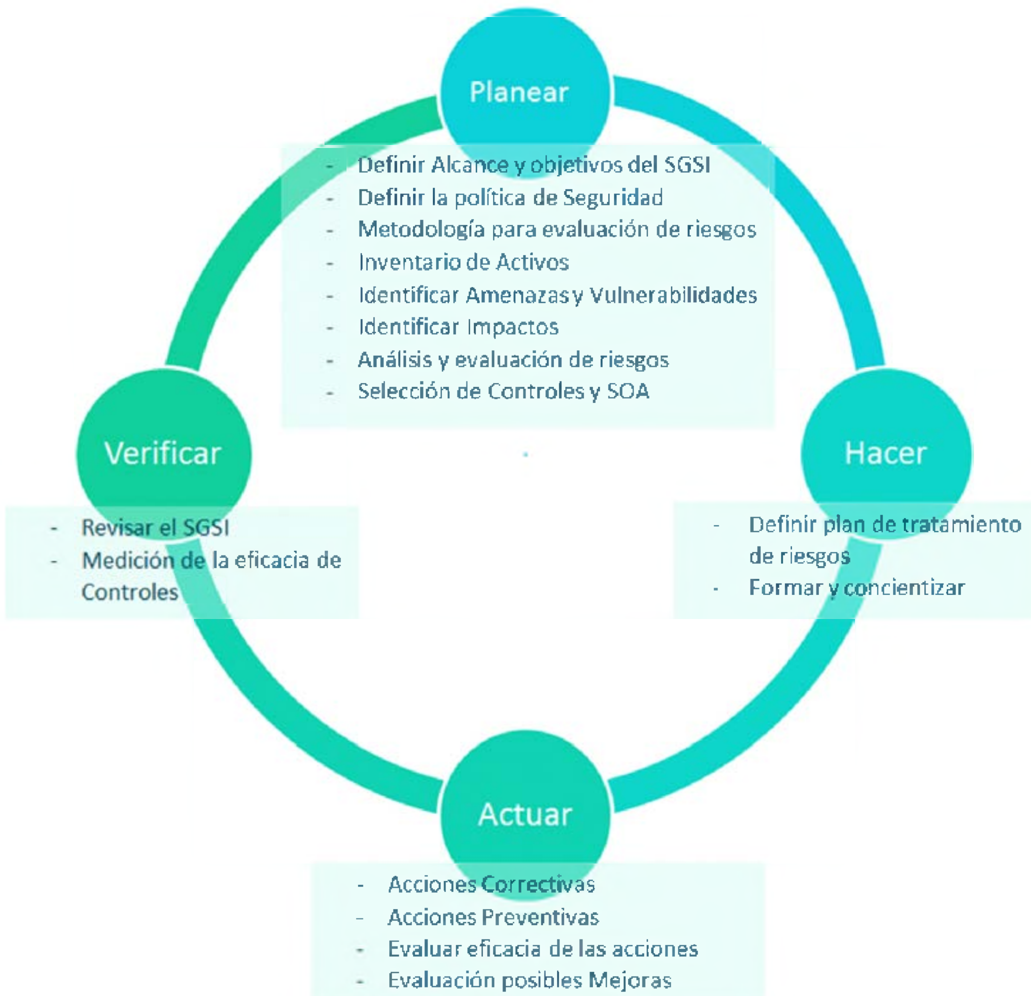


Ilustración 3, Entregables del ciclo PHVA. Fuente ISO 27001.es, Modificado por la Autora

3.2 Método de estudio

Para este proyecto usaremos varios métodos de investigación:

- Descriptiva: Con el fin de estudiar las realidades de nuestro caso de estudio a partir de herramientas como el estudio de exploración, de campo y de desarrollo, a partir de lo mismo recolectaremos datos para sacar conclusiones a partir de un análisis detallado.
- Interactiva: En este proyecto modificaremos el sistema que existe con el fin de aplicar sobre el mismo un sistema especialmente diseñado

3.3 Diseño de la investigación

En la presente investigación se han de utilizar dos fuentes de información: La norma técnica ISO 27001, datos históricos de la institución, entre otras fuentes que se citaran en el presente documento.

- Ishikawa
- Identificación de los Riesgos
- Implementación de ciclo de Deming (PHVA)

3.4 Fases del trabajo de grado

Según lo que propone la norma ISO 27001 se ha tomado en cuenta las siguientes fases para el logro de objetivos del presente trabajo de grado:

CUARTA PARTE

DESARROLLO DE LA TESIS

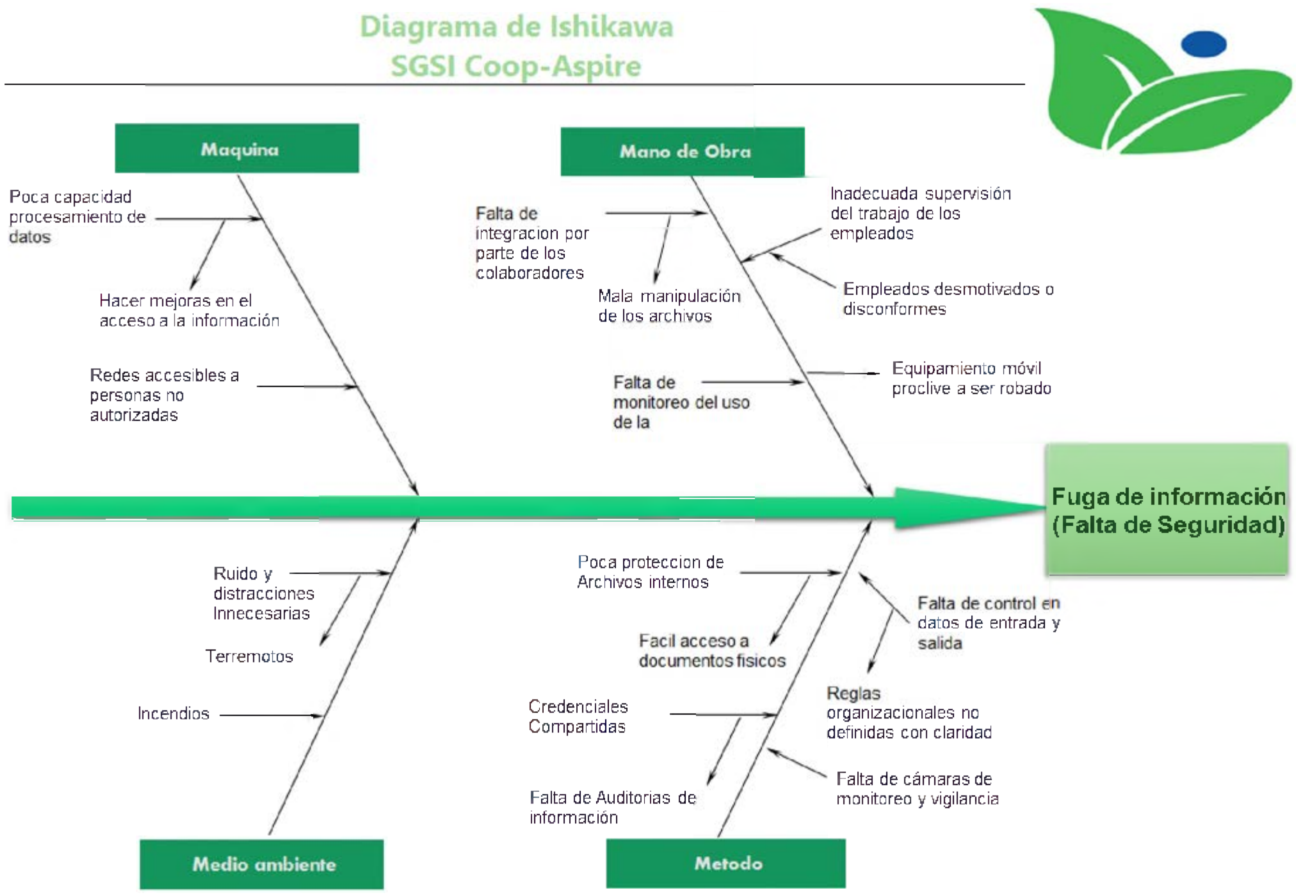
CAPITULO IV: DESARROLLO DE LA TESIS

4.1 Situación Actual

Según el historial de la empresa se han observado situaciones de robo de la información, falta de controles en temas de las claves lo que permite que se fugue información a través de los empleados y sirviendo como intermediarios para el robo de información sensible de nuestro sistema bancario.

Debido estos problemas se ha contemplado implementar un SGSI, hemos realizado un diagnóstico de la situación actual de la empresa en relación a la norma, de manera que podamos obtener una idea de que tan apegada o dispersa se encuentra la empresa, y así aprovechar los mecanismos ya establecidos y usarlos a nuestro favor en la implementación del SGSI.

El siguiente diagrama de pescado Ilustra los factores que generan el problema:



Los documentos no están bien organizados, y los formularios que competen a cada manual no están debidamente mencionados en la parte correspondiente, tampoco los formularios están Codificados.

Existe una fuerte resistencia al cambio, se necesitaría apoyo de la dirección general y cambio de la cultura organizacional.

Como mencionamos en el marco metodológico de nuestro trabajo de grado trabajaremos en base a la metodología PHVA, la cual desarrollaremos en este capítulo.

Esta metodología sugiere un enfoque en procesos. Las probabilidades de éxito son sumamente altas, y es por esto que se aplica en la mayoría de procesos y en la política y objetivos del sistema.

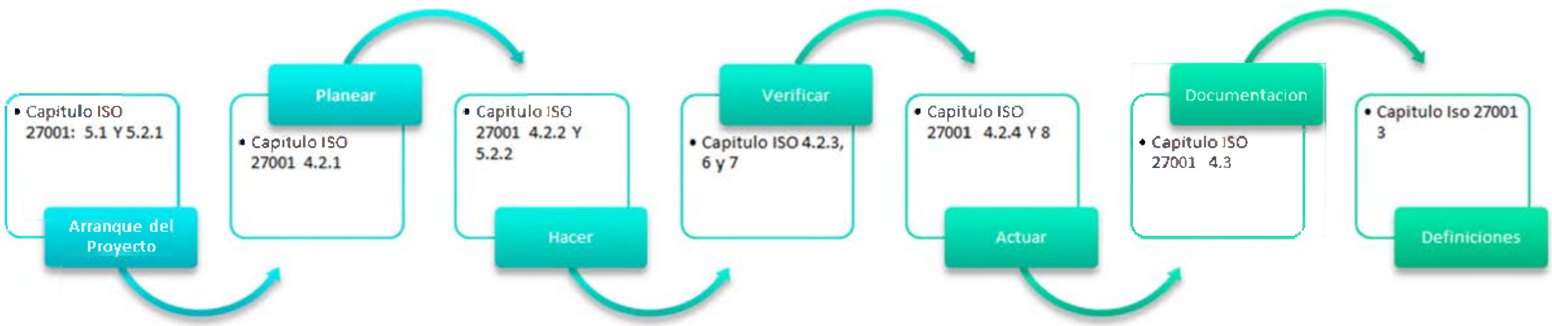


Ilustración 4. Relación de la metodología, con la norma 27001

4.1.1 Identificación de los procesos clave de la empresa

Como hemos mencionado antes, el estándar ISO 27001 promueve la adopción de un enfoque por procesos en cada fase del SGSI, de modo que se aplique un sistema de procesos dentro de la organización a partir de la identificación y gestión sistemática de estas actividades y la interacción entre ellas.

De esta manera que para fines del presente trabajo de Grado hemos organizado las actividades de la empresa en procesos, definimos como proceso a Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas, transformándose a menudo la salida de un proceso en la entrada de otro proceso.

Como fin ilustrativo definiré la naturaleza de los procesos en tres categorías:

- **Estratégicos:** Normalmente no se relacionan directamente con el Cliente, sin embargo las operaciones y la evolución de la organización de ven afectadas en el tiempo por los mismos.
    a) Dirección General
    b) Control Interno
- **Operativos:** Son la razón de ser de la organización. De modo que se representa por la prestación del servicio y aporta valor añadido al socio, estos procesos deben tener como enfoque principal satisfacer las necesidades y expectativas de los socios, También son llamados procesos Core.
    a) Mercadeo
    b) Negocios
    c) Operaciones
- **Soporte:** Estos procesos facilitan la realización de las actividades que forman parte de los procesos operativos y generan valor al cliente interno de la organización.
    a) Gestión de finanzas
    b) Gestión de Recursos humanos
    c) Asesoría Jurídica
    d) Documentación
    e) Gestión de Tecnologías de Información

Es importante habilitar un mapa de procesos, con el fin de ilustrar y especificar las que harán parte del alcance.

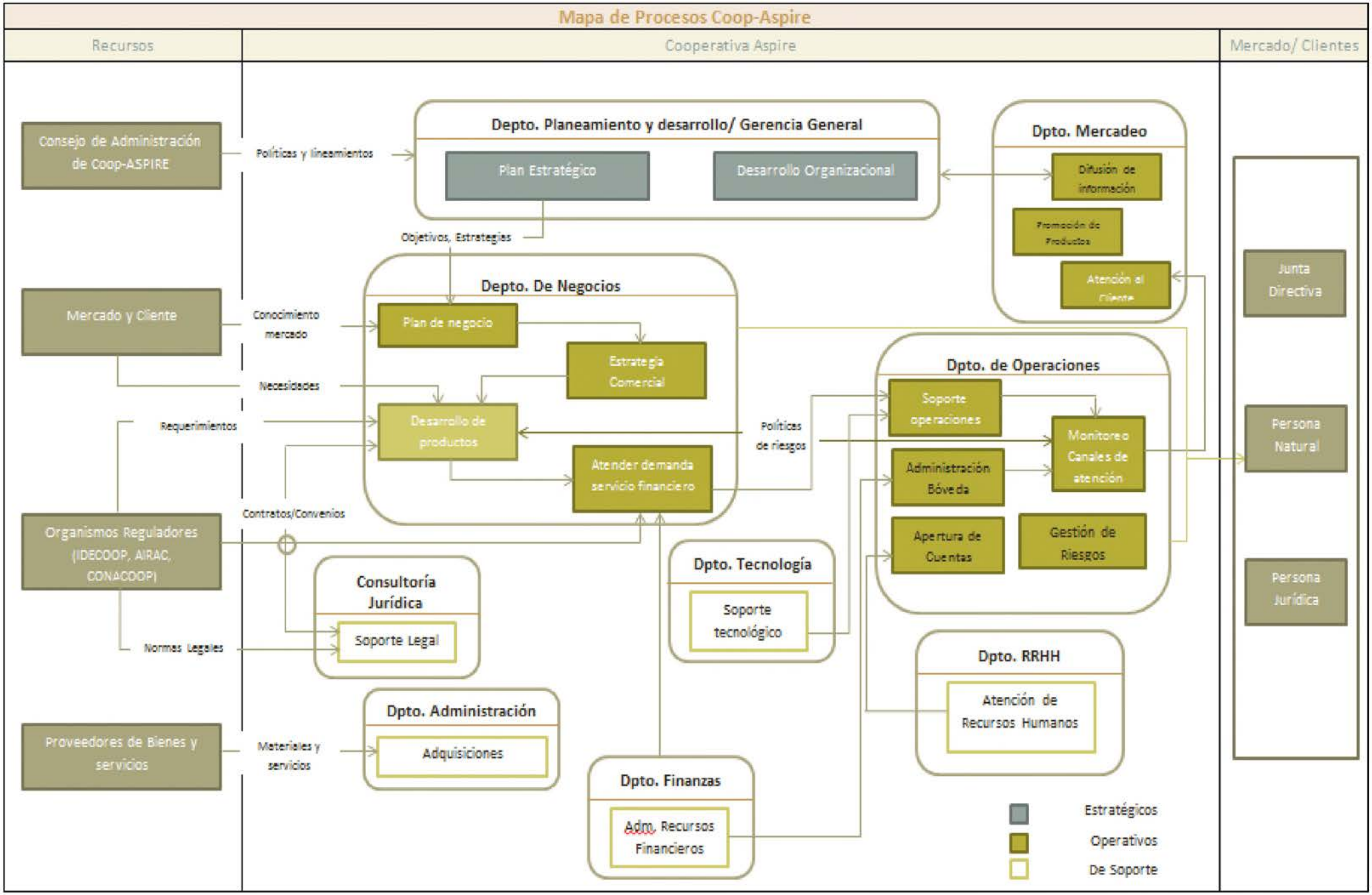


Ilustración 5: Procesos estratégicos, operativos y de soporte de Coop-Aspire. Fuente: Autora

4.2 Solución Propuesta

La manera más viable de proteger la información (activo importante de la empresa) es una gestión eficiente de los riesgos que derivan de los problemas mencionados en la sección 2.10 del presente capitulo. De esta manera podremos identificar aquellos riesgos que exponen más a la organización y así enfocar nuestros esfuerzos en los mismos, considerando el caso de Coop-Aspire que es una institución financiera que maneja información sensible de cada socio de manera que es de suma prioridad mantener protegida dicha información.

Dada esa premisa, el presente trabajo de grado aglomera toda la información imprescindible usada como diseño para la implementación de un sistema de Gestión de seguridad de la información, basado en ISO 27001, el cual se asegurara de garantizar la protección de la información de la organización.

4.3 Autodiagnóstico

Antes de iniciar hemos elaborado un autodiagnóstico de la etapa en la cual se encuentra la empresa en cuestiones de seguridad de la información (Ver Anexos: Autodiagnóstico SGSI), en este cuestionario participaron las áreas de operaciones, tecnología de la información y control interno, de manera que estos controles están destinados a proteger las operaciones de la empresa y de igual forma la información de la misma.

A través del Gap 2 del autoanálisis del SGSI, se diagnosticó el nivel de la organización en cuanto a cumplimiento de objetivos de control establecidos en el Anexo A de la norma ISO/IEC 27001, esto nos permitió ver que controles se podían establecer para asegurar la información y su integridad.

Según lo observado, el cumplimiento de la organización según el autodiagnóstico referido es de **21%**

Se evidencia que la implementación de este sistema, requerirá un gran esfuerzo puesto que hay muchos de los controles que se sugieren, que no se ponen en práctica para lograr un SGSI robusto y eficiente.

4.4 Planificación

4.4.1 Compromiso de la dirección

La junta directiva de Coop-Aspire debe aprobar este proyecto comprometiéndose con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI.[18]

[18] SGSI, ISO 27001, P. 11

La dirección proporcionará los recursos necesarios para establecer, implementar, operar, brindar seguimiento, revisar, mantener y mejorar un SGSI; asegurar que los procedimientos de seguridad de la información brinden apoyo a los requisitos del negocio; identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales; mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados; llevar a cabo revisiones cuando sea necesario y mejorar la eficacia del SGSI[19].

4.5 Planear

En la etapa de planeación se define el alcance del sistema dentro de la organización y las políticas y lineamientos sobre los que se desarrollará, se presentan herramientas para la identificación, análisis y evaluación de riesgos, según el impacto de cada uno y el tipo de información que se afectaría, de igual forma es objetivo de esta etapa definir la forma de tratamiento de los riesgos identificados.[20]

Como fines ilustrativos en el presente documento proponemos una idea de cómo debe estar estructurado el documento del Alcance, ver anexos.

[19] Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001, P. 26
[20] ISO/IEC 27001:2005, P. 12

4.5.1 Política del SGSI

ISO 27001 establece una política para el SGSI la cual establece los objetivos de una organización (pmg-ssi, 2014) dicha política corresponde a toda la empresa y lo divulgará el responsable de seguridad. La Gerencia General de la organización aprobará la Política y Objetivos de Seguridad.

La empresa debe tener un compromiso de implementar y mejorar continuamente el SGSI de modo que la política contenga programas para el mantenimiento y crecimiento del mismo como por ejemplo: Actividades de capacitación y concientización para el personal de la empresa, Revisión anual de lo que fuera el objetivo del SGSI, Revisión Continua del Plan de Continuidad del Negocio[21], respeto por las políticas y procedimientos relacionados con el SGSI.

El responsable del SGSI será el encargado de mantener la política del SGSI y a su vez será el mentor y guía de los colaboradores de la empresa en materia de la seguridad de la información.

[21] Ver Anexo 7: Plan de continuidad de negocios

En el presente trabajo de Grado propondremos una política seguridad basada en la norma ISO 27001 y definida por la misión, visión y valores de la organización protegiéndose de esta manera la información que maneja la empresa logrando preservar los cuatro pilares del SGSI:

Ilustración 6: Los 4 pilares de un SGSI

- **Confidencialidad:** Solo el personal de la empresa que tiene la autorización de acceder a la información puede hacerlo. Por lo tanto la misma no puede ser difundida pública, sino que debe ser preservada. Este es uno de los pilares que motiva a las organizaciones a proteger su información.
- **Integridad[22]:** Cuando una información se mantiene intacta desde su origen de destino, es decir cuando no la han copiado, restaurado, modificado o borrado, cuando. Un ataque a la integridad de la información se puede presentar en archivos planos de bases de datos, información documental, registros de datos, etc.

Uno de los mecanismos más utilizados para asegurar la integridad de la información es a través de la firma digital. Casanovas Inés (2009) afirma: “la firma digital permite garantizar la identidad del autor y la integridad de un documento digital a partir del concepto tradicional de la firma manuscrita en papel. Técnicamente es un conjunto de datos único, asociado al documento y al firmante, que no tiene por objetivo la confidencialidad sino asegurar la autoría y que no ha sufrido alteraciones” (p.204).

[22]http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html

- **Disponibilidad:** La información existente en cualquier forma digital o software, debe estar disponible para ser procesada y para ser usada para el correcto funcionamiento de los procesos de la empresa, clientes y colaboradores sin ser interrumpidos. Un claro ejemplo de agravio a este pilar, se ilustra cuando se ha eliminado un cable disponible en el cuarto de servidores de la empresa, no se autoriza el servicio a una página web, mal funcionamiento del sistema, virus y software malicioso, entre otros. Estos ataques pueden ser controlados a través de cortafuegos, así como el diseño de planes de continuidad de negocio para mantener la disponibilidad de los servicios a pesar de inconvenientes que puedan ocurrir en la empresa.
- **Autenticidad:** Este fundamento se desprende de la información genuina que al ser encontrada se pudiera reproducir a pesar de que la información sea idéntica, la fuente no es la original, como podría ocurrir con el plagio de un documento.

La política del SGSI debe tener en cuenta el marco legal de la seguridad de la información:

- **Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología:** La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley.

La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.[23]

- **El Convenio sobre la Ciberdelincuencia del Consejo de Europa, del 23 de noviembre del 2001:** Convenio para prevenir actos que pongan en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas[24], redes y datos para luchar eficazmente en contra de dichos delitos.
- **Ley General de Telecomunicaciones No. 153-98 – Indotel:** Esta ley constituye el marco regulatorio básico que se ha de aplicar en todo el territorio nacional, para regular la instalación, mantenimiento y operación de redes, la prestación de servicios y la provisión de equipos de telecomunicaciones.
- **Ley No. 20-00 sobre Propiedad Industrial:** Contribuye con la transferencia y difusión de la tecnología, en beneficio recíproco de los productores y de los usuarios de conocimientos tecnológicos a bien de favorecer el bienestar social y económico del país.[25]

[23] Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. El congreso nacional de la República. SECCIÓN I
[24] CONVENIO. SOBRE LA CIBERDELINCUENCIA. Budapest, 23.XI.2001, P. 3
[25] Ley No. 20-00 sobre Propiedad Industrial. El Congreso nacional de la Republica

Parte importante de la implementación de un SGSI es la propagación de la política, de este modo nos aseguramos que cada nivel de la organización tome decisiones alineadas a los objetivos del sistema, de esta manera a demás se tendrá un compromiso integral por parte de los colaboradores.

La política también debe considerar establecer el método de estimación, tratamiento y clasificación de riesgos (Para ver la propuesta de tratamiento de riesgos, dirigirse a los anexos) que afectan la seguridad de la información:

- Identificar los riesgos.
- Hacer el análisis de riesgos,
- Puntualizar los objetivos de los controles,
- Establecer los controles necesarios para tratamiento de los riesgos.
- Plantear iniciativas para el tratamiento de los riesgos.

4.6 Hacer

Continuando con el ciclo de Deming (PHVA), el paso que se desarrollaremos en este apartado es Hacer, para iniciar debemos haber definido un plan de riesgos (Véase el anexo), según se establecido en la sección anterior, además de seleccionar los controles y el plan de tratamiento de riesgo para atenuar la incidencia de los mismos. El propósito de la implementación del plan de tratamiento de riesgos es lograr los objetivos que nos trazamos en la etapa de Planear.

Como hemos dicho anteriormente, para desarrollar esta etapa se tomará como referencia la norma ISO 27001:2005 ya que la misma nos dicta las pautas para el desarrollo, mejora y mantenimiento de la gestión de la Seguridad de la Información de la Cooperativa.

A continuación se deberán iniciar las labores de concientización del personal en cuanto a lo que será el SGSI y los cambios que se producirán producto del mismo. En ese sentido recomiendo crear los manuales de normas, procedimientos e instrucciones que permitan monitorear las operaciones del SGSI.

Según lo desarrollado la etapa hacer contempla:

- Definir el plan de tratamiento de riesgos
- Implementar el plan de tratamiento de riesgos
- Implementar controles
- Formación y concientización de los colaboradores.

Como se ha mencionado, solo hemos mencionado esta etapa para fines didácticos, de modo que se propondrán ciertos documentos sin incluir la implementación de las mismas.

4.6.1 Análisis de Riesgos

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por Departamento de Riesgo, la identificación de amenazas y vulnerabilidades la realizan los propietarios de los activos, mientras que la evaluación de consecuencias y probabilidad es realizada por los propietarios de los riesgos.

QUINTA PARTE

ISO 27002 - CONTROLES DE SEGURIDAD

CAPITULO V: ISO 27002 - CONTROLES DE SEGURIDAD

5.1 Políticas Seguridad:

El propósito de esta Política es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información. Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI), según se define en el Documento del Alcance del SGSI. Los usuarios de este documento son todos los empleados de Coop-Aspire, como también terceros externos a la organización.

Los objetivos generales para el sistema de gestión de seguridad de la información son los siguientes:

- Crear una mejor imagen de mercado
- Reducir el daño ocasionado por potenciales incidentes estando en líneas con la estrategia comerciales de la Organización.

La Gerencia General y la Gerencia de Operaciones son responsables de revisar estos objetivos generales del SGSI y de establecer nuevos. Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por la Gerencia de Informática, la Gerencia de Contabilidad, la Gerencia de Operaciones, la Gerencia de Negocios, la Gerencia Administrativa, y la Gerencia de Capacitación y son aprobados por Auditoría. Coop-Aspire medirá el cumplimiento de todos los objetivos. La Gerencia General y la Gerencia de Operaciones son responsables de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos una vez al año y el Departamento de Operaciones analizará y evaluará los resultados y los reportará la Gerencia General como material para la revisión por parte del Consejo de Vigilancia.

SEXTA PARTE

CONCLUSION

CAPITULO VI: CONCLUSION

Como conclusión podríamos decir que las nuevas Tecnologías de la Información han evolucionado espectacularmente en los últimos años, debido especialmente a la importancia de estas en el sector productivo, teniendo gran impacto en las organizaciones y en este caso de este importante reglón del sector empresarial como son las empresas del entorno financiero.

Con el presente trabajo de grado pretendíamos diseñar un Sistema de Seguridad de la Información para la Cooperativa de ahorros créditos y servicios Múltiples Aspire (Coop-Aspire), bajo la norma ISO 27001.

Como consecuencia del uso de las diferentes herramientas propuestas en dicha norma se pudo diagnosticar los avances en cuanto a cómo proceder para la implementación del sistema en la misma.

A continuación detallamos las conclusiones:

• Consideramos que la capacidad de la infraestructura informática está comprometida debido al crecimiento rápido de la población de la empresa, lo cual se evidencia en el cuadro de tratamiento de riesgos, esto hace necesario un esfuerzo por cumplir con los controles propuestos en el mismo.

• Según el autodiagnóstico de SGSI realizado (Antes de la implementación de este diseño), la institución solo cumple con un 28%, de modo que se hace necesario un esfuerzo por parte de los involucrados, para cumplir con los controles formulados en el presente trabajo (Como se proponen en la política de seguridad de la información, y en el cuadro de tratamiento de riesgos)

• Según los riesgos observados y el comportamiento de la empresa, se deben observar el plan de acción en cuanto a la protección de la información compartida con terceros, puesto que la mala manipulación de la misma podría afectar gravemente a la entidad. Consideramos de suma necesidad implementar mecanismos de criptografía a fin de proteger la información.

• Se debe poner en marcha cuanto antes los planes de contingencia, con el fin de poder responder ante cualquier catástrofe que pudiera afectar la seguridad de la información de la empresa.

• Es importante dar seguimiento al cumplimiento de la política de seguridad propuesta en el presente trabajo, así como la actualización constante de la misma.

• Es necesario hacer un plan de capacitación en cuanto a la seguridad de la información, a fin de crear una cultura de seguridad en los empleados internos y externos.

• Se recomienda crear un mecanismo de control de acceso a la red wifi de la empresa, con el fin de solo permitir la conexión a equipos autorizados.

• Se observó la falta de una política de controles de uso de los activos de información y unidades de procesamiento de información, lo que genera que los usuarios desconozcan sus responsabilidades y consecuencia de sus acciones.

BIBLIOGRAFÍA

BIBLIOGRAFIA

1. Corletti, A. 2011. Seguridad por Niveles,
2. Data Breach Investigations Report, 2010- 2012, P. 16
3. Diseño de un SGSI, M. Villena, P. 29
4. Diseño de un Sistema de Gestión De Seguridad de la Información (SGSI), EAN, P. 21
5. Diseño de una metodología para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001, P. 26
6. Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial la ofrenda JD Aguirre Cardona - 2013
7. Europa, C. d. (2001). Convenio sobre la Ciberdelincuencia. 3.
8. ISO 27001, Online Consultation Center, Academy
9. ISO/IEC 27001:2005, P. 12
10. Ley No. 20-00 sobre Propiedad Industrial. El Congreso Nacional de la Republica
11. Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. El Congreso Nacional de la República. SECCIÓN I CONVENIO. SOBRE LA CIBERDELINCUENCIA. Budapest, 23.XI.2001, P. 3
12. Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.
13. SGSI, ISO 27001, P. 11
14. Superintendencia de Bancos de la República Dominicana, Informe del Sistema Financiero, Enero – junio 2012
15. Toro, M. 2011. Plan de Seguridad de la Información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

Europa, C. d. (2001). Convenio sobre la Ciberdelincuencia. 3.

ICETEX. (2014). Manual de Politicas de seguridad de la informacion.

IGLESIAS, L. M. (2009). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). *UNIVERSIDAD REY JUAN CARLOS*, 6.

pmg-ssi. (7 de marzo de 2014). Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: http://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

SIB. (2016). Especialista afirma mayor riesgo de ataques cibernéticos están en filtración de datos personales. *Superintendencia de Bancos* .

Verizon. (2010- 2012). *Data Breach Investigations Report.*

ANEXOS

Anexo 1 - Norma NTC-ISO-IEC 27001

Estadísticas de la cooperativa

Datos Estadísticos	Dic-14	Dic-15	Crecimiento 2014-2015
Cantidad de socios	34,173	57,632	69%
Monto en activos	RD$767,953,508	RD$1,101,024,033	43%
Socios con Crédito	24,033	32,763	36%
Monto Colocado	RD$720,586,876	RD$1,067,559,232	48%
Monto en Cartera	RD$610,535,661	RD$916,448,880	50%
Porcentaje en mora	3.53	2.79	-21%
% Riesgo > 30 Días	3.60	3.40	-5%
Cuentas de Ahorros	31,871	56508	77%
Balance de Ahorros	RD$37,294,480	RD$70,175,148	88%
Cantidad de Depósitos a Plazos	524	922	76%
Cantidad de Aportaciones	31,871	56553	77%
Balance en Aportaciones	RD$63,917,100	RD$204,335,205	220%
Personas Impactadas por Capacitaciones	4,082	13,062	220%
Sucursales	15	19	27%
Cantidad De empleados	210	299	42%
Oficiales de Negocios	73	133	82%

Tabla 1: Crecimiento de la Cooperativa hasta el momento de la investigación

Controles y Dominios de la norma ISO 27001

ISO 27001:2005 (11 dominios; 133 controles)		ISO 27001:2013 (14 dominios; 113 controles)	
A.5	Política de seguridad.	A.5	Política de seguridad.
A.6	Organización de la seguridad de la información.	A.6	Organización de la seguridad de la información.
A.7	Gestión de activos.	A.7	Seguridad de los RRHH.
A.8	Seguridad de los RRHH.	A.8	Gestión de activos.
A.9	Seguridad física y del ambiente.	A.9	Control de accesos.
A.10	Gestión de comunicaciones y operaciones.	A.10	Criptografía.
A.11	Control de acceso.	A.11	Seguridad física y ambiental.
A.12	Adquisición, desarrollo y mantenimiento de sistemas de información.	A.12	Seguridad en las operaciones.
A.13	Gestión de incidentes de seguridad de la información.	A.13	Transferencia de información.
A.14	Gestión de la continuidad del negocio.	A.14	Adquisición de sistemas, desarrollo y mantenimiento.
A.15	Cumplimiento.	A.15	Relación con proveedores.
		A.16	Gestión de los incidentes de seguridad.
		A.17	Continuidad del negocio.
		A.18	Cumplimiento con requerimientos legales y contractuales.

Requisito Normativo	Porcentaje de cumplimiento
4. Sistema de Gestión de seguridad de la Información	**11%**
4.1 Requisitos Generales	10%
4.2 Establecimiento y Gestión del SGSI	15%
4.3 Requisitos de la documentación	40%
5. Responsabilidad de la Dirección	**24%**
5.1 Compromiso de la dirección	20%
5.2 Gestión de los recursos	28%
6. Auditorías internas del SGSI	**5%**
7. Revisión por la dirección del SGSI	**7%**
7.1 Generalidades	10%
7.2 Elementos de entrada para la revisión	0%
7.3 Resultados de la Revisión	10%
8. Mejora del SGSI	**10%**
8.1 Mejora continua	10%
8.2 Acción Correctiva	10%
8.3 Acción Preventiva	10%
Porcentaje de Cumplimiento General	**12.2%**

Tabla 2: Evaluación basada en ISO 27001

Anexo 2 - Acta constitutiva - Cronograma

Anexo 3 - Política de seguridad de la información

Anexo 4 - ISO SURVEY

EVALUACIÓN

Brianda Beatriz Flores Sánchez
Sustentante

Ing. Fe Del Carmen Payano Vásquez
Consejera

Ing. Nelbry María Zapata
Miembro del jurado

Ing. José Enrique Ramirez
Miembro del jurado

Jhonathan Matos
Miembro del jurado

Ing. Jorge Encarnación Montero
Director Escuela Ingeniería Industrial

Calificación Numérica ______

Calificación Alfabética ______

Fecha: ______ / ______ / ______