UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

ÁREA DE SISTEMAS INFORMÁTICOS

Trabajo de fin de carrera titulado:

"DISEÑO Y CREACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMATIVA ISO 27000 PARA LA COOPERATIVA CONSTRUCCIÓN, COMERCIO Y PRODUCCIÓN."

Realizado por:

JEAN PIERRE RODRÍGUEZ GUERRA

Director del proyecto:

ING. VERÓNICA RODRÍGUEZ, MBA.

Como requisito para la obtención del título de:

INGENIERO EN SISTEMAS EN DISEÑO Y MULTIMEDIA

QUITO, JUNIO 2016

DECLARACIÓN JURAMENTADA

Yo, JEAN PIERRE RODRÍGUEZ GUERRA, con cédula de identidad #171816489-0, declaro bajo juramento que el trabajo aquí desarrollado es de mi propia autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, se cede los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Jean Pierre Rodríguez Guerra

C.C.: 171816489-8

DECLARATORIA

El presente trabajo de investigación titulado:

“DISEÑO Y CREACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMATIVA ISO 27000 PARA LA COOPERATIVA CONSTRUCCIÓN, COMERCIO Y PRODUCCIÓN.”

Realizado por:

JEAN PIERRE RODRÍGUEZ GUERRA

Como requisito para la obtención del título de:

INGENIERO EN SISTEMAS EN DISEÑO Y MULTIMEDIA

Ha sido dirigido por el docente:

ING. VERÓNICA RODRÍGUEZ, MBA.

Quien considera que constituye un trabajo original de su autor

ING. VERÓNICA RODRÍGUEZ, MBA.

DIRECTOR

PROFESOR INFORMANTE

Los profesores informantes:

ING. JUAN SEBASTIÁN GRIJALVA, MSc.

Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el tribunal del examinador

ING. JUAN SEBASTIÁN GRIJALVA, MSc.

Quito, Mayo del 2016

PROFESOR INFORMANTE

Los profesores informantes:

ING. DANIEL RIPALDA, MSc.

Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el tribunal del examinador

ING. DANIEL RIPALDA, MSc.

Quito, Mayo del 2016

DEDICATORIA

Dedico el presente trabajo a mis padres, quienes han dado todo para formar hijos responsables, honestos y útiles a la sociedad, a mis hermanos, las más fuertes y admirables figuras en mi vida y a mi dulce Mamina quien me enseñó que el amor trasciende cualquier plano existencial.

AGRADECIMIENTO

Primeramente a Dios, por permitirme tener la vida que con altos y bajos, es perfecta.

A mi familia, por su incondicional apoyo y cariño, no importa el tiempo que pase, siempre podremos contar los unos con los otros.

A mis queridos amigos, la familia que uno escoge y me han sabido acompañar en cada éxito, cada fracaso, cada alegría e incluso cada lágrima.

A la Ing. Verónica Rodríguez, no solo por formar buenos profesionales sino también seres humanos preocupados de vivir adecuadamente la vida. Quien me enseñó a darle lugar a cada sentimiento y por encima de todo 100% respeto.

Al Ing. Juan Sebastián Grijalva, quien supo apostar a sus alumnos, motivar y ser más que un magnífico profesor, un modelo profesional a seguir y un amigo que nos ayuda a comprender cada vez más la vida.

Finalmente a todas las personas que conocí en esta etapa de mi vida, quienes… buenas o malas ayudaron a formar la persona y el profesional que hoy soy.

ÍNDICE GENERAL DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

Debido al avance tecnológico que se dio en los últimos años, la información se convirtió en el bien más valioso para todas las instituciones que busquen un crecimiento económico o laboral, ya que con ella se pueden realizar desde mercadeo hasta grandes movimientos financieros, en los cuales se tiene presente que el producto que se comercializa es el dinero y el movimiento no consentido del mismo tiene severas consecuencias en quien lo maneja. La Cooperativa de ahorro y crédito Construcción, Comercio y Producción - COOPCCP es un ente financiero bajo el control de la Superintendencia Económica Popular y Solidaria - SEPS que cuenta con 14 sucursales a nivel nacional y el matriz ubicado en la ciudad de Quito, en la cual se realizó un análisis que evidenció que no existe un manejo apropiado de la información lo que crea complicaciones en el cumplimiento de las actividades que se realizan dentro de todas las áreas que la componen. Todos estos problemas repercuten directamente en la dificultad para tener un crecimiento representativo en todos sus años de funcionamiento, por lo tanto se vio la necesidad de crear una política de seguridad de la información que ayude a cumplir con los objetivos organizacionales, administrativos y técnicos que consten en cada planificación anual. Se hizo el levantamiento de procesos, trabajo conjunto con cada líder de proceso para poder formular un ERM y de esta manera identificar de una forma específica las necesidades que tiene la empresa en función del criterio profesional de los encargados de cada área, extrayendo así un diccionario de controles que fue la base fundamental para escribir la política de seguridad

Palabras clave: Política de Seguridad, SGSI, empresas de alto riesgo, entidades bancarias, seguridad de la información.

ABSTRACT

Due to technological advances that occurred in recent years, information became the most valuable for all institutions seeking economic or job growth well, because with it can be made from marketing to large financial movements, in which It bearing in mind that the product sold is money and no consent thereof has severe consequences on who handles movement. The credit union Construction, Trade and Production - COOPCCP is a financial entity under the control of the Popular and Solidarity Economic Superintendency - SEPS has 14 branches nationwide and matrix located in the city of Quito, in which an analysis that showed that there is no proper information management which creates complications in implementing the activities undertaken within all areas that compose it was made. All these problems directly affect the difficulty to have a representative growth in all its years of operation, therefore he saw the need to create a security policy information to help meet organizational, administrative and technical objectives stating in each annual planning. the lifting process was done, working together with each leader process to develop an ERM and thus identify a specific way the needs that the company based on the professional judgment of those responsible for each area, thereby extracting a dictionary controls that was the fundamental basis for writing security policy

Key words: Security policy, ISMS, high-risk companies, bank entities, information security.

CAPÍTULO I

INTRODUCCIÓN

1.1 EL PROBLEMA DE INVESTIGACIÓN

1.1.1 Planteamiento del Problema

La seguridad informática es un campo de estudio muy extenso, el cual se centra en entender cuáles son las vulnerabilidades y riesgos que tiene una entidad en relación al tipo de información que maneja. Los datos son afectados de diferentes maneras y por muchos factores, referentes directamente a los aspectos de confidencialidad, integridad, disponibilidad y manejo de éstos. Actualmente los delitos informáticos no están muy bien definidos ni estructurados, motivo por el cual las empresas no pueden medir con exactitud cuál es el riesgo inherente que tienen al no aplicar una correcta política de seguridad, por lo que la información se hace fácilmente vulnerable y los datos que consten como clasificados pueden estar abiertos al público o expuestos a una amenaza.

La falta de controles de accesos a la plataforma web, el manejo no autorizado de la base de datos, y el mal uso de ciertas herramientas en la intranet como “ISOTOOLS”, archivos compartidos e incluso el core bancario, son solo algunos de los muchos problemas derivados de no tener una política de seguridad debidamente aplicada dentro de la entidad financiera Cooperativa de ahorro y crédito Construcción, Comercio y Producción - COOPCCP.

Actualmente la seguridad se encuentra bajo el área de TI. No tienen un control sobre los usuarios de la red y no se cuenta con una administración de permisos adecuada.

En la política de seguridad existente no se contempla la separación del personal de la actividad laboral, por lo tanto, los empleados que alguna vez pertenecieron a la empresa mantienen el acceso virtual con los permisos otorgados cuando formaban parte de la COOPCCP.

Un control indebido de las plataformas web causa una vulnerabilidad fuerte a la empresa y al software denominado "Core Bancario", el cual se encuentra limitado en su crecimiento, debido a que no se tiene creado el diccionario de datos y la estructura de la BDD está mal definida. Existen también un gran número de problemáticas derivadas de las mencionadas anteriormente que de una u otra manera interfieren o dificultan en el crecimiento de la entidad financiera.

Hablando de la realidad Ecuatoriana, actualmente existen controles, normativas y estándares vigentes que prometen el crecimiento integral de una empresa, siempre y cuando los mismos sean aplicados a través de un estudio, lastimosamente este jamás es el mismo para ninguna organización aun así compartan la misma línea de negocios. La Superintendencia de Economía Popular y Solidaria - SEPS, tiene recomendaciones, estructuras de cumplimiento e incluso buenas prácticas para el funcionamiento de las cooperativas de ahorro y crédito. Para el caso particular de la COOPCCP la aplicación de un SGSI y el uso de un manual de seguridad de la información es necesario para su avalúo y correcta funcionalidad.

1.1.2 Objetivos

1.1.2.1 Objetivo general

Desarrollar un manual de políticas de seguridad de la información aplicando los controles de la ISO 27002 para la Cooperativa de ahorro y crédito Construcción, Comercio y Producción.

1.1.2.2 Objetivos específicos

- Crear un análisis integral de la COOPCCP mediante el levantamiento de procesos e información a través de reuniones con personal específico de cada área para conocer el estado de la empresa y contar con toda la información requerida para desarrollar las diferentes etapas del proyecto.

- Desarrollo de un ERM, basado en las normas ISO27000 alineado a las necesidades de la COOPCCP analizadas en el levantamiento de procesos para identificar de manera específica las posibles faltas de seguridad y denominar los procesos críticos.

- Creación de un diccionario de controles aplicado a la realidad de la COOPCCP en base del análisis del levantamiento de procesos, alineado a la norma internacional ISO27000-27002 para la identificación de los controles que contiene la política de seguridad con su debida justificación.

- Desarrollo de la nueva política de seguridad de la información para la COOPCCP en base a los levantamientos de información , el ERM y diccionario de controles para mejorar los

procesos, procedimientos y el manejo de información aplicando medidas preventivas y correctivas.

1.1.3 Justificación

A pesar del gran esfuerzo que se hace para mantener al día en servicios y sistemas financieros a una organización tan importante como la COOPCCP, al momento de revisar el manejo de la información, se encuentra que no se tiene aplicada una política de seguridad, solamente cuentan con algunos controles físicos y protocolos para el funcionamiento de la misma, pero no constituyen como tal una medida real de protección de datos, debido a que los accesos a la información pueden estar vulnerables por cualquier tipo de conexión ya sea interna o externa a la COOPCCP.

Bajo este contexto, se considera necesario el desarrollo de una política de seguridad de la información (SGSI) con estándares internacionales que contribuyan a la solución del problema y a la naturaleza de funcionamiento de la institución, definidas a base de su situación actual.

El contar con una política de seguridad de la información aportará con mejoras significativas en muchos ámbitos como: laboral, productivo, ambiente de trabajo, etc. Los problemas de seguridad serían mínimos y se podrá contar con un correcto monitoreo en la parte de infraestructura, una solución rápida a las solicitudes de otras áreas y mantendrá la información segura. La capacitación del personal es parte del proceso de cambio, dentro del mismo se van tipificando la manera de proceder para tener un crecimiento en las distintas áreas organizacionales de la COOPCCP, todo esto se traduce como diferentes tipos de

ganancias para la empresa como tiempo de acción, respuestas rápidas, un fuerte control de datos y administración, etc.

El logro más importante es realizar los cambios pertinentes dentro de la COOPCCP y al mismo tiempo mantener segura la información para no comprometer sus operaciones ni el correcto desarrollo de funciones en las diferentes áreas, que entran en un proceso de adaptación, cambio y mejora continua, bajo de la dirección de una política de seguridad bien desarrollada. Con la cual podrán no solo funcionar de manera independiente sino que también dar soporte a otras áreas con las que trabaje de manera más directa, no solo en este proceso de cambio sino en cualquiera que se pueda dar a partir de la implementación de la nueva política de seguridad de la información.

1.1.4 Alcance

El presente proyecto se alinea a las diferentes actividades que se desarrollan en la COOPCCP como son:

- **Levantamiento de información inicial:** Este proceso consistió en realizar reuniones iniciales dentro de la COOPCCP para extraer información específica requerida para obtener un punto de partida y conocimiento puntual del manejo de todos los dispositivos utilizados, protocolos, administración del software de desarrollo interno, bases de datos, proveedores de servicios y formas de administración de accesos y credenciales. Se elaboró un análisis de documentos existentes como informes de auditorías, acuerdos de nivel de servicios, libro de registros en la manipulación del Core bancario y toda la documentación relevante para el desarrollo del proyecto, este

proceso se realizó mediante entrevistas al personal especializado dentro de la COOPCCP en los temas mencionados.

- **Levantamiento de procesos:** Para el desarrollo de esta actividad fue necesario planificar una reunión con una persona de cada área organizacional de la COOPCCP denominados "líderes de procesos", el trabajo con estas personas consistió en llevar a cabo un diálogo a manera de entrevista que se divide en 4 partes: Introducción al área, comparativa de procesos levantados VS procesos realizados en el día a día, funcionamiento con otras áreas, conclusiones y recomendaciones. Los líderes de procesos aportaron con su opinión y experiencia en el campo, lo que define la importancia a opinión profesional de los procedimientos que se llevan a cabo.

- **Definición de procesos críticos:** Se determinó la criticidad de los procesos en base del levantamiento previamente realizado, esto con el fin de clasificar los puntos en los que se hace énfasis al momento de diseñar el diccionario de controles, esto se realizó mediante un proceso analítico de la información obtenida, tomando como puntos de referencia las entrevistas de los líderes de procesos, el trabajo previo levantado por la COOPCCP y el punto de vista del director del proyecto.

- **Análisis de riesgos basado en ISO27000:** Para poder realizar con éxito este paso fue necesario contar con la información levantada previamente hasta este punto, este trabajo tuvo arista principal la cuantificación de los resultados obtenidos de los levantamientos de procesos e información, una vez realizado, se puedo definir mediante una matriz el nivel de criticidad de la empresa, basada en el criterio técnico de las personas pertenecientes a cada área, este trabajo no es exclusivo de seguridad de

la información sino que también va orientado a todo riesgo inherente dentro de la COOPCCP.

- **Definición del diccionario de controles:** En este paso se tomó todo el material recolectado para poder justificar el uso de los diferentes controles encontrados en la ISO27002 codificado en una matriz que indica el tipo de control que se utiliza, el área al que va dirigido, la justificación y su correcta aplicación. En el diccionario de controles se pueden repetir algunos que estén ubicados en distintas áreas de acuerdo a la cantidad de personal que trabaje de manera dedicada.

- **Creación de la nueva política de seguridad:** Se desarrolla en base al ERM tras obtener los resultados cuantificados en la matriz usable de riesgos, se continúa con la estructuración de la política, en la que constan los libros en las que se va a dividir acorde al tipo de información que manejen, a la sensibilidad de los datos y grados de importancia que se pudo extraer de los análisis anteriores a éste. Escribir la política de seguridad como tal es un proceso que se lleva a cabo como punto final del proyecto en el que se concatena toda la información obtenida hasta este punto, para la creación de la política de seguridad se contó con la aprobación de los encargados de cada área.

- **Mapeo de eventos encontrados con otras normas alineadas a la línea de negocios:** Este paso consta como un valor agregado a lo planteado al inicio del proyecto y requirió de un acercamiento del estado de la empresa tras aplicar a un mínimo del 90% lo que dice la nueva política de seguridad, el cual se encuentra distribuido en un matriz que muestra el evento o problemática, cuál es el punto según la ISO27000 que cubre ese evento y el mapeo que existe con otras normas de interés para la COOPCCP.

1.2. MARCO TEÓRICO

1.2.1 Empresas de alto riesgo

Una empresa de alto riesgo tiene como características principales manejar información sensible en el mercado, manejo de bienes de alto valor y un alto riesgo en las operaciones con sus empleados. El manejo de los bienes tangibles e intangibles de alto valor es la base para determinar la sensibilidad de una empresa. Y conforme a ello, poder clasificarlo.

Éstas son definidas con las que operan en un sitio de riesgo o que el fracaso o no cumplimiento de las actividades pueden traer resultados catastróficos, desde el movimiento de dinero de una cuenta o incluso hasta una vida humana, por lo general se dice que las empresas de alto riesgo dentro del Ecuador son aquellas que cuentan con sucursales o trabajos suscritos bajo contratación sea ésta pública o privada en la que el valor monetario del bien que manipulan sea mayor a los 2 millones de dólares o el servicio que presten tenga alguna repercusión importante al medio ambiente. Todas las empresas tienen riesgo al realizar sus actividades y pueden entrar también dentro de esta categoría las empresas que tengan como consecuencia una vida humana. (Gonzales Ernesto, 2010).

1.2.2 Entidades Bancarias

Una entidad bancaria (Bancos y Cajas de Ahorro) es una institución financiera que se encarga de administrar el dinero de unos para prestarlo a otros. La banca, o el sistema bancario, es el conjunto de entidades o instituciones que, dentro de una economía determinada, prestan el servicio de banco o banca.

En de una entidad bancaria existen distintos organismos los cuales están estrictamente regulados y supervisados:

- Bancos: Se dedican al préstamo, recepción de depósitos y prestan servicios financieros. Son clasificados dependiendo del origen de su capital, es decir, si su aportación proviene del estado el banco es público; por otra parte, si provienen de accionistas particulares son privados, y finalmente si sus aportaciones provienen tanto del estado como de accionistas es un banco mixto.

- Cajas de ahorro: Son entidades privadas sin fines de lucro las cuales son controladas por organismos públicos (ayuntamientos, comunidad autónoma, etc). Tienen como obligación distribuir por lo menos un tercio de los beneficios que posee a obras de interés social para el refuerzo de la capitalización de las cajas. Gracias a este aporte social, las cajas no pagan intereses.

- Cooperativas de crédito: Son entidades cuyos propietarios son cooperativistas financieros, y pueden ir junto a asocaciones u otras cooperativas de origen industrial o sectorial.

- Establecimientos financieros de créditos (EFC): Entidades privadas que se dedican a la realización de operaciones en ámbitos específicos que son leasing (arrendamiento financiero con opción de compra), factoring (sesión de una cartera de créditos), créditos al consumo, crédito hipotecario, tarjeta, etc.

El primer banco moderno fue fundado en Génova, Italia en el año 1406, su nombre era Banco di San Giorgio. Los primeros bancos aparecieron en la época del renacimiento.

Las operaciones típicas de los bancos son las pasivas (para captar dinero de personas e instituciones) y las activas (prestar ese dinero a terceros exigiendo un coste mayor del que pagan por sus operaciones de captación de pasivos).

1.2.2.1 Operaciones Pasivas

Se trata de operaciones por las que el banco capta, recibe o recolecta dinero de las personas.

Las operaciones de captación de recursos, denominadas operaciones de carácter pasivo se materializan a través de los depósitos bancarios, que pueden clasificarse en tres grandes categorías:

- Cuentas corrientes,
- Cuenta de ahorro o libreta de ahorros,
- Depósito a plazo fijo.

1.2.2.2 Operaciones activas

La colocación es lo contrario a la captación. La colocación permite poner dinero en circulación en la economía; es decir, los bancos generan nuevo dinero del dinero o los

recursos que obtienen a través de la captación y, con éstos, otorgan créditos a las personas, empresas u organizaciones que los soliciten.

Por dar estos préstamos el banco cobra, dependiendo del tipo de préstamo, unas cantidades de dinero que se llaman intereses (intereses de colocación) y comisiones. Al diferencial entre lo que los bancos cobran por el dinero que prestan y el que abonan a los que les ceden sus ahorros en depósito, se le llama diferencial de tipos de interés, y junto con los ingresos por comisiones bancarias constituyen el negocio bancario.

1.2.3 Introducción a las normas aplicadas ISO

Una norma está definida como una regla que determina el tamaño, composición y varias características que debe tener un producto o servicio y determinan el correcto uso o implementación de estas características.

Las normas ISO se constituyen en una serie de Estándares que podemos agrupar por familias, según los distintos aspectos relacionados con la calidad. Aunque existen más de 18000 normas publicadas por ISO vamos a resaltar las más importantes en cuanto a su aplicación y relevancia de los sectores. Así podemos clasificar las normas según el siguiente criterio:

- Normas relacionadas directamente con la calidad.
- Normas Relacionadas con la calidad en el Medio Ambiente y Sostenibilidad.
- Normas relacionadas con la Gestión de la Seguridad.
- Normas relacionadas con la Calidad en la Investigación y Desarrollo.

Calidad

Tabla 1: Normas ISO para la gestión de la calidad.
Elaborado por: Jean Rodríguez.

SISTEMAS DE GESTIÓN DE CALIDAD	SECTORES
ISO 9001	Todos
ISO TS 16949	Automoción
ISO / IEC 15504	Calidad del software
ISO / IEC 17025	Laboratorios de ensayo y calibración
ISO / IEC 20000	Calidad de los servicios de ti

Medio ambiente y sostenibilidad

Tabla 2: Normas ISO para la gestión medioambiental y sostenibilidad
Elaborado por: Jean Rodríguez.

SISTEMAS DE GESTION MEDIOAMBIENTAL Y SOSTENIBILIDAD	SECTORES
ISO 14001	Medio ambiente
ISO TS 50001	Gestión de la energía

Seguridad

Tabla 3: Normas ISO para la gestión de la seguridad
Elaborado por: Jean Rodríguez.

SISTEMAS DE GESTIÓN DE LA SEGURIDAD	SECTORES
ISO 18001 OHSAS	Seguridad y salud de los trabajadores (ocupacional)
ISO 27001	Seguridad de la información
ISO 22000	Seguridad en el sector de la alimentación

Innovación y nuevas tecnologías

Tabla 4: Normas ISO para la gestión de la innovación
Elaborado por: Jean Rodríguez.

SISTEMAS DE GESTIÓN DE LA INNOVACIÓN	SECTORES
ISO 166001	Proyectos i+d+i
ISO 166002	Gestión de la innovación i+d+i
ISO 20000	Gestión de servicios de nuevas tecnologías ti

A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for

Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- BS 5750. Publicada en 1979. Origen de ISO 9001
- BS 7750. Publicada en 1992. Origen de ISO 14001
- BS 8800. Publicada en 1996. Origen de OHSAS 18001

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un SGSI basado en ISO 27001 en conjunto con otras normas de la serie 27k pero también con otros sistemas de gestión.

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El objetivo último debería ser llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA de mejora continua

común a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes mediante la consulta de sus anexos o, en nuevas publicaciones con ISO/IEC 27001:2013 gracias a su estructura común para la equivalencia en los requisitos similares aplicables a todos los sistemas de gestión (Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.)

1.2.4 Aspectos de la seguridad

La seguridad informática está ligada directamente a salvaguardar salvos aspectos:

1.2.4.1 Confidencialidad

Definiendo un poco:

- En general el término 'confidencial' hace referencia a "Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas."
- En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.
- El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el del ejército de un país. Además, se conoce que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Por otra parte, determinadas empresas a menudo desarrollan diseños que deben proteger de sus competidores. La sostenibilidad de la empresa así como su posicionamiento en el mercado puede depender de forma directa de la implementación de estos diseños y, por ese motivo, deben protegerlos mediante mecanismos de control de acceso que aseguren la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de encriptación utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

1.2.4.2 Integridad

En general, el término 'integridad' hace referencia a una cualidad de 'íntegro' e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable.".

En términos de seguridad de la información, la integridad hace referencia a la la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información. La integridad hace referencia a:

- la integridad de los datos (el volumen de la información)
- la integridad del origen (la fuente de los datos, llamada autenticación)

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

1.2.4.3 Disponibilidad

En general, el término 'disponibilidad' hace referencia a una cualidad de 'disponible' y dicho de una cosa "Que se puede disponer libremente de ella o que está lista para usarse o utilizarse."

En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados”. Es decir, un sistema es disponible si permite no estar disponible, y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.

Como resumen de las bases de la seguridad informática que se ha comentado, se puede determinar que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de no poder acceder a él, inclusive con permisos de administrador o usuario privilegiado.

Dependiendo del entorno de trabajo y sus necesidades se puede priorizar un aspecto de la seguridad o a otro. En aspectos militares se suele priorizar la confidencialidad de la información frente a la disponibilidad. Aunque alguien pueda acceder a ella o incluso pueda eliminarla no podrá conocer su contenido, Excepto el especialista que generó quien podrá recuperar una copia de seguridad (si las cosas se están haciendo bien).

En contextos bancarios es prioritaria la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.

1.2.5 ISO 27000

Según la norma ISO/IEC 27002 (anteriormente denominada ISO 17799) se autodefine como un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013.

El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. En el año 2000 la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento modificado ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.

Los requisitos codificados en ISO 27001 se expanden y se explican en la norma ISO 27002 en la forma de una guía. El manual fue publicado por primera vez en el año 2000, en ese momento con la designación "ISO 17799", bajo el título "Tecnología de la información relacionadas con la seguridad técnicas de Código de prácticas para la gestión de seguridad de la información". En 2007, este fue revisado y alineado a la 27 K familia de normas y la

designación se cambió a la norma ISO 27002. Con el desarrollo de la norma ISO 27002- prácticas comunes a menudo conocidas también como las mejores prácticas, se les ofreció como los procedimientos y métodos probados en la práctica, la cual podría ser adaptado a los requisitos específicos dentro de las empresas.

Con el fin de explicar la importancia de la seguridad de la información para las empresas, y sus riesgos, así también como la necesidad de tener objetivos, acordaron medidas ("controles") en el marco de un SGSI que exponen los pasos necesarios para la identificación y evaluación de riesgos de seguridad. Los cuales se describen con el fin de determinar la necesidad de proteger los sistemas de información y de información.

El continuo desarrollo de la norma ISO 27002 se basa en la presentación de la norma ISO 27001, por lo que los 39 objetivos de control que figuran en el anexo de la norma ISO 27001 se explican con más detalle.

Un total de 134 medidas, justificadas y que se describen en el mismo documento, se asignan a estos objetivos. Las directrices fundamentales para garantizar la seguridad de la información se han de definir y especificar en el documento de políticas de seguridad mediante la gestión de la empresa.

La distribución y la aplicación de estas políticas en la compañía también sirven para notar la importancia de la seguridad de la información y la atención de la administración a estos temas.

La seguridad de la información debe estar anclada organizativamente en la empresa para que las medidas de seguridad de la información puedan ser promovidas y establecerse de manera eficiente. Así roles y responsabilidades deben ser definidos y en funciones particulares para mantener la confidencialidad y las normas para las comunicaciones con las partes externas (clientes, proveedores, autoridades, etc.) han de especificarse.

Todos los bienes tangibles e intangibles que deben ser protegidos por las medidas de seguridad de la información deben ser identificados y clasificados con el fin de elaborar las responsabilidades específicas y los riesgos de manipulación (Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.)

1.2.6 Sistemas de Gestión de Seguridad de la Información

Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: information security management system, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, busca asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe ser eficiente y adaptándose a los cambios internos de la organización así como los externos del entorno.

(Allende, D. C., & Gui, S. G. (2011). Sistema de gestión de la seguridad de la información. Universitat Oberta de Catalunya.)

ISO / IEC 27001, parte de la creciente ISO / IEC 27000 familia de normas, es un (ISMS) estándar de sistema de gestión de la seguridad de la información publicada en octubre de 2005 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Su nombre completo es la norma ISO / IEC 27001: 2013 - Técnicas de seguridad - - Tecnología de la información sistemas de gestión de seguridad de la información - Requisitos pero se conoce comúnmente como "ISO 27001".

ISO / IEC 27001 especifica formalmente un sistema de gestión que pretende aportar seguridad de la información bajo el control explícito de la dirección administrativa. Al ser una especificación formal significa que en ella se prevén requisitos puntuales. Organizaciones que dicen han adoptado, por tanto, la norma ISO / IEC 27001 puede ser auditado y certificado conforme a la norma.

La mayoría de las organizaciones tienen una serie de controles de seguridad de la información, sin un SGSI sin embargo, los controles tienden a ser un poco desorganizado y desarticulada, después de haber puesto en práctica a menudo como soluciones puntuales a situaciones específicas o simplemente como una cuestión de convención. Los modelos de madurez normalmente se refieren a esta etapa como "ad hoc". Los controles de seguridad en el funcionamiento suelen abordar ciertos aspectos de TI y seguridad de datos, en concreto, dejando activos de información (tales como trámites y conocimiento de su propiedad) bien protegidos en el conjunto. La planificación de la continuidad del negocio y la seguridad física, por ejemplo, pueden ser manejados con total independencia de TI o de seguridad de la

información, mientras que las prácticas de recursos humanos pueden hacer poca referencia a la necesidad de definir y asignar roles y responsabilidades de seguridad de la información en toda la organización. (Veritas, G. R. (1916). Information Security Management System-ISO 27001.)

1.2.6.1 Procedimiento de implementación de un SGSI

Según los autores Michelena Jaime y Días Paola. Las políticas de seguridad basadas en objetivos de control tienen como finalidad brindar una guía de procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños. Los beneficios de un sistema de seguridad con políticas claramente concebidas y bien elaboradas son inmediatos, ya que se trabajará sobre una plataforma confiable. Con la implementación de las políticas se logran los 11 objetivos de control indicados en el diseño del SGSI.

Las políticas están enfocadas en dar cumplimiento a los objetivos de control implementados, de igual manera la selección de las herramientas se basa en la funcionalidad que presta cada una de ellas y el soporte que brinda a los controles mencionados en la norma ISO 27002

A continuación se listan los objetivos de control:

1. **Política de Seguridad**: Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requerimientos de la institución y a las leyes y regulaciones vigentes.

2. **Organización de la seguridad de la información:** Gestionar la seguridad de la información.
3. **Gestión de activos:** Alcanzar y mantener una protección adecuada de los activos de la institución asegurando que se aplica un nivel de protección adecuado a la información.
4. **Seguridad de los recursos humanos:** Asegurar que el personal, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen.
5. **Seguridad física y ambiental (Entorno físico de los activos):** Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.
6. **Gestión de las comunicaciones y operaciones:** Asegurar la operación correcta y segura de los recursos de tratamiento de información.
7. **Control de acceso:** Controlar los accesos a la información.
8. **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Garantizar que la seguridad es parte integral de los sistemas de información.
9. **Gestión de incidentes en la seguridad de la información:** Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.
10. **Gestión de la continuidad comercial:** Reaccionar a la interrupción de actividades y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.
11. **Cumplimiento:** Evitar incumplimientos de ley, estatuto, regulación u obligación establecida dentro de la institución.

Herramientas a implementar

- Generador de contraseñas RPG.- IObit Random Password Generator es una herramienta que permite generar hasta cien contraseñas aleatorias. Únicamente es necesario escoger la longitud (desde seis hasta 64 caracteres), el tipo de caracteres y la cantidad de claves a crear. Dependiendo del tipo y cantidad de caracteres, una contraseña será más o menos fuerte. IObit Random Password Generator indicará en la tabla de claves mediante una leyenda de cuatro colores.

- Controlador de dominio con Samba 4.- La implementación del Controlador de dominio se realiza sobre Samba 4 que es un proyecto de código abierto y además es una opción alternativa a Microsoft AD. Uno de los objetivos de Samba4 es implementar un controlador de dominio compatible con varios sistemas operativos.

- iTALC.- Es una aplicación didáctica de monitorización, que ofrece la oportunidad de supervisar e influir en las actividades de los usuarios.Se trata de un software de uso libre y de muy sencilla instalación que permite controlar los equipos de usuarios a distancia.Permite ver el contenido de las pantallas de los usuarios en la propia pantalla del administrador.

- Nagios3-NCONF.- Nagios es una aplicación de código abierto para monitoreo de sistemas y redes. Revisa equipos y servicios que se le específica, alertando cuando el comportamiento de los mismos no sea el deseado. Para poder añadir de una forma sencilla los sistemas que se desea, se utiliza NCONF como herramienta gráfica de configuración para Nagios. NConf es una herramienta de código abierto que permite

administrar los archivos de configuración de Nagios a través del uso de una interfaz gráfica de usuario, en lugar de mantener los archivos de configuración con un editor de texto.

- OCS Inventory.- Open Computer and Software Inventory Next Generation (OCS-NG) es un software libre que permite a los usuarios administrar el inventario de sus activos de TI. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS.

- OTRS (Open-source Ticket Request System). - Es una aplicación web Open Source que permite ofrecer servicio online con la utilización de tickets soportando multi-usuarios. El OTRS permite realizar una gestión integrada de las solicitudes de servicio, información o cualquier requerimiento que realice un usuario a un área, dirección o cualquier entidad o agente que le solicite asistencia.

- Servidor de archivos con samba 3.-Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, podrán tener acceso al archivo del servidor en lugar de tener que pasarlo entre distintos equipos.

- Cobian Backup.- Es un programa multitarea capaz de crear copias de seguridad en un equipo, en una red local o incluso en/desde un servidor FTP. También soporta SSL. Se ejecuta sobre Windows y una de sus grandes ventajas es que consume muy pocos recursos.

- Truecrypt.- Es una aplicación gratuita que permite crear volúmenes cifrados, de manera que todo lo que contengan estos volúmenes pueda ser accedido únicamente si se conoce la contraseña y el fichero clave que se utiliza en su creación.

- UTM.- Los sistemas de Gestión Unificada de Amenazas constituyen una solución de seguridad mejorada ya que integran múltiples tecnologías integradas cubriendo las exigencias básicas de protección integral. El UTM combina un firewall, un proxy, IDS/IPS y herramientas de monitoreo, todo en un único equipo y a tiempo real.
- MRTG.- (Multi Router Traffic Grapher), es una herramienta que permite monitorizar varias características de los servidores reportando la información en gráfica visible por medio de un html.

1.2.7 El delito informático

Según el autor De Sola Quintero, René. El delito informático implica actividades criminales las cuales se han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

En el contexto real cuanto más alcance tengan las leyes, tanto menor será el número de refugios para la delincuencia informática organizada que puede operar con impunidad.

Como señala Camacho Loza, “En todas las facetas de la actividad humana existe el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito.

Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia."

Luego de haber dado una referencia de lo que es delito es importante resaltar cuales son los elementos integrantes del mismo, siendo éstos:

a. El delito es un acto humano tanto en su acción como en su omisión.
b. Este acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
c. Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.
d. El sujeto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
e. La ejecución u omisión del acto debe estar sancionada por una pena.

En general los delitos informáticos tienen características, verdaderamente, particulares que hacen del mismo delito algo peculiar; algunas características:

f. Conductas criminales de cuello blanco, ya que es un número muy reducido y determinado de personas que poseen el conocimiento para llegar a cometerlo.
g. Acciones ocupacionales, en su mayoría se ejecutan cuando el sujeto está trabajando.
h. Acciones de oportunidad, dónde se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
i. Provocan serias pérdidas económicas.

j. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
k. Existen varios casos y muy reducidas denuncias, lo cual puede ser por falta de información para abordar el tema o falta de regulación jurídica.
l. Cuando se dan en el ámbito militar suelen ser sofisticados y no frecuentes.
m. Su comprobación trae dificultad por los ingeniosos medios para realizarse.
n. En gran parte devienen de imprudencia, no teniendo implícita la intención.
o. Con frecuencia se da su comisión por menores de edad.
p. La tecnología ha dado la oportunidad para que éstos puedan darse con mayor frecuencia, por lo que es necesaria su regulación y monitoreo continuo.
q. Han logrado mantenerse en el tiempo, sin tener seguridad preventiva que pueda evitarlos.

Clasificación de los delitos informáticos

Según el autor Galindo A.L.C. Los delitos informáticos se clasifican bajo dos esquemas:

Como instrumento:

Esta categoría contiene las conductas criminales que llevan en su acto el uso de computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques)
2. Variación de los activos y pasivos en la situación contable de las empresas.
3. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude)

4. Lectura, sustracción o copiado de información confidencial.
5. Modificación de datos tanto en la entrada como en la salida.
6. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
7. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
8. Uso no autorizado de programas de cómputo.
9. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
10. Alteración en el funcionamiento de los sistemas a través de los virus informáticos.
11. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
12. Acceso a áreas informatizadas en forma no autorizada.
13. Intervención en las líneas de comunicación de datos o teleproceso.

Como Objeto

Esta categoría contiene toda conducta criminal que va dirigida estrictamente contra computadoras, accesorios y programas como entidad física. Algunos ejemplos podrían ser:

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios.
e. Sabotaje político o terrorismo en que se destruya o surja

f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje. (Galindo, A. L. C. "POLICÍA CIBERNÉT PREVENTIVA, LOS ILÍCITOS INF.)

La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal (COIP)- hasta el 31 de mayo del 2015. A partir del COIP se tipifica este tipo de delitos. (Fiscalía General del estado, 2015).

1.2.8 Diccionario de Controles

Los diccionarios de controles son básicamente una aplicación que se compagina con los datos extraídos del levantamiento de información y los levantamientos de procesos, éste es desarrollado para la política de seguridad y va alineado a la misma. El diccionario de controles es una guía que justifica cuáles son los puntos importantes en dónde se debe llevar a cabo la implementación y la cual nos da los parámetros necesarios para la implementación del manual, como un extra, el diccionario de controles nos ayuda también a realizar (si es necesario) una cotización de cuánto se debe invertir en la política, pero este proceso se debe llevar a cabo a través del tiempo y no hay una fecha límite para acabar la implementación.

Debe contener la actividad de la cual se empieza a derivar los procesos, el número de proceso asignado, los controles existentes y la norma a la cual se está alienando el trabajo, en este caso la ISO 27000, estos datos son también extraídos del ERM, que puede llegar a ser vital para el desarrollo del mismo. Y se justifica por qué se aplica o no se aplica un control, todo esto ajustado a la realidad de la empresa, sus lineamientos y métodos de operación que tengan.

Un diccionario de controles es único para cada empresa, ya que es un trabajo que se realiza con muchas variables extraídas de la organización y dependiendo del avance en su implementación puede ser sujeto a cambios en el tiempo y el espacio requerido.

1.2.9 Análisis de riesgos

Como parte del Sistema de Gestión de Seguridad de la Información, es necesario hacer una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

Son muchas las metodologías utilizadas para la gestión de riesgos, pero todas parten de un punto común: la identificación de activos de información, es decir todos aquellos recursos involucrados en la gestión de la información, que va desde datos y hardware hasta documentos escritos y el recurso humano. Sobre estos activos de información es que hace la identificación de las amenazas o riesgos y las vulnerabilidades

Una amenaza se puede definir entonces como un evento que puede afectar los activos de información y están relacionadas con el recurso humano, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el flujo eléctrico.

Por otra parte, una vulnerabilidad es una característica de un activo de información y que representa un riesgo para la seguridad de la información. Cuando se materializa una amenaza y hay una vulnerabilidad que pueda ser aprovechada hay una exposición a que se presente algún tipo de pérdida para la empresa. Por ejemplo el hecho de tener contraseñas débiles en los sistemas y que la red de datos no esté correctamente protegida puede ser aprovechado para los ataques informáticos externos.

Ahora, para que la empresa pueda tomar decisiones sobre cómo actuar ante los diferentes riesgos es necesario hacer una valoración para determinar cuáles son los más críticos para la empresa. Esta valoración suele hacerse en términos de la posibilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo. La valoración del impacto puede medirse en función de varios factores: la pérdida económica si es posible cuantificar la cantidad de dinero que se pierde, la reputación de la empresa dependiendo si el riesgo pueda afectar la imagen de la empresa en el mercado o de acuerdo al nivel de afectación por la pérdida o daño de la información.

En este punto se deberían tener identificados y valorados los principales riesgos que pueden afectar los activos de información de la empresa. Pero, ¿es suficiente con saber qué puede pasar? La respuesta es no. Una vez identificadas las amenazas, lo más importante del análisis de riesgos es la identificación de controles ya sea para mitigar la posibilidad de ocurrencia de la amenaza o para mitigar su impacto. Las medidas de control que puede asumir una empresa van a estar relacionadas con el tipo de amenaza y el nivel de exposición que represente para la información corporativa.

Una empresa puede afrontar un riesgo de cuatro formas diferentes: aceptarlo, transferirlo, mitigarlo o evitarlo. Si un riesgo no es lo suficientemente crítico para la empresa la medida de control puede ser aceptarlo, es decir, ser consciente de que el riesgo existe y hacer un monitoreo sobre él. Si el riesgo representa una amenaza importante para la seguridad de la información se puede tomar la decisión de transferir o mitigar el riesgo.

La primera opción está relacionada con tomar algún tipo de seguro que reduzca el monto de una eventual pérdida, y la segunda tiene que ver con la implementación de medidas preventivas o correctivas para reducir la posibilidad de ocurrencia o el impacto del riesgo. Finalmente, si el nivel de riesgo es demasiado alto para que la empresa lo asuma, puede optar por evitar el riesgo, eliminando los activos de información o la actividad asociada.

La gestión de riesgos debe garantizarle a la empresa la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten. Esta gestión debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del activo de información para los procesos de la empresa y el nivel de criticidad del riesgo.

1.2.10 Ingeniería de procesos

La administración por procesos es una manera clara, precisa y directa de gestionar una organización en función del análisis del desempeño de sus actividades, resultados y productos, satisfacción de los usuarios y las posibilidades de mejora que tienen cada una de estas actividades.

Su importancia estratégica radica en la asignación de soluciones preventivas sobre la marcha evitando costos hundidos derivados de la implementación de soluciones correctivas; o en algunos casos extremos evitando la ruina de la imagen organizacional por defectos en productos y servicios.

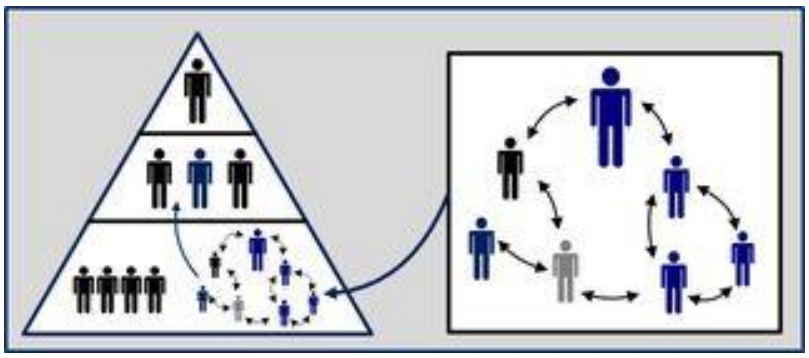
Es conocido que el levantamiento o la sistematización de las acciones o tareas institucionales en procesos, permite a las instituciones lograr estructuras más planas, sencillas, y flexibles; propicia el trabajo en equipo y la medición de resultados en las unidades organizacionales. Esta forma de sistematizar el trabajo facilita además implantar una cultura de servicio en las instituciones, puesto que al diseñar los procesos se pueden focalizar las acciones institucionales hacia las necesidades y expectativas de los usuarios. Las Instituciones organizadas por procesos presentan estructuras lógicas y ordenadas que permiten agilizar las actividades, mejorar los bienes, mejorar el servicio, y sobre todo, permite detectar a tiempo posibles fallas y corregirlas antes de que el bien y/o servicio final se brinde al usuario y se facilite la prestación de los servicios con los niveles de calidad y efectividad requeridos.

La carencia de una adecuada sistematización de procesos es al mismo tiempo causa y consecuencia de estructuras ineficaces, ineficientes y excesivamente burocráticas, que atrapan y anulan los flujos agregadores de valor para clientes internos y externos.

Por ejemplo, en una institución pública o privada excesivamente burocrática suele perderse de vista que los componentes de mayor valor agregado para el cliente externo/interno; lo constituyen de forma general: tiempo de atención, exactitud y precisión y nivel de servicio (características genéricas cuantificables de un proceso); y por ende se los sacrifica

por formularios, firmas, aprobaciones, fiscalizaciones, revisiones técnicas, jurídicas, etcétera. Es decir, se cumplen los requisitos de ley -ser legal no tiene nada que ver con la eficiencia; pero se olvida que el cliente pierde tiempo, se siente mal atendido, y muchas veces se le entregan resultados con errores. Por ende, en escenarios como este, la razón de ser se ha perdido y se puede hablar de una organización fallida.

Figura 1: Sistema de organización en el levantamiento de procesos
Fuente: Levantamiento de Procesos, Organización de Materia, 2010



En función de lo anterior, y antes de iniciar con la descripción sistemática del levantamiento de procesos; es útil recordar entonces que la estructura organizacional debe ajustarse y mejorarse en función de un estudio SERIO de la CADENA DE VALOR de la que forma parte la organización, sus procesos, sus clientes internos y sus clientes externos. Finalmente una creciente tendencia de las organizaciones es querer adquirir soluciones no adecuadas para su grado de madurez institucional. Es decir, una organización que no tiene procesos sistematizados y ordenados, no puede ni debe pensar en automatizar sus procesos; pues lo único que estará consiguiendo será automatizar el desorden.

1.2.10.1 Relación Básica de los procesos: Proveedor – Productor – Usuario.

Base de toda relación de procesos, en ésta, cada eslabón se encuentra interrelacionado y es

interdependiente. De esta manera, el proveedor suministra el insumo de acuerdo con los requerimientos del productor, siendo éste el responsable de la operación y quien entrega el producto (bien/servicio) al usuario (interno/externo), el que finalmente determina sus requerimientos. Estos requerimientos son primordialmente las necesidades y expectativas que poseen los usuarios con respecto a la prestación bienes o servicios por parte de la institución.

1.2.10.2 Etapas para el Levantamiento de los Procesos

Normalmente el levantamiento de los procesos se realiza cuando la institución ya se encuentra conformada y desarrollando las funciones asignadas por la legislación respectiva, sin embargo, es frecuente encontrar instituciones que realizan sus actividades con base en el conocimiento empírico y las costumbres de sus funcionarios mas experimentados, sin contar con un manual de procesos y/o procedimientos que regule y estandarice la realización de sus actividades. El diseño de los procesos se presenta cuando una institución ha sido creada recientemente y tiene que dilucidar la mejor forma de ejecutar las funciones que tiene asignadas, o en su defecto, cuando en una organización existente se crean unidades organizativas encargadas de funciones nunca antes desarrolladas por la institución. En ambos casos, se debe diseñar o establecer la forma en la que los funcionarios de la institución o unidad deben desarrollar las funciones asignadas, y dejar constancia de estos requerimientos haciendo uso de procedimientos debidamente formalizados, los cuales deben ser difundidos entre todos los funcionarios para asegurar la correcta ejecución de las labores

Etapa 1: Formación del Equipo y Planificación del Trabajo.

Al inicio de un despliegue resulta fundamental que los niveles directivos / ejecutivos en una institución se comprometan con el proceso de levantamiento y diseño de los procesos

institucionales, en virtud de que serán ellos los encargados de aprobar los procesos establecidos. Es por esta razón, que al iniciar el proceso debe ser el la autoridad institucional el encargado de conformar un equipo de trabajo, integrado por funcionarios de la institución, por consultores externos, o por una mezcla de los anteriores.

Etapa 2: Identificación de usuarios de los procesos y sus necesidades.

La identificación de los usuarios y las necesidades y/o expectativas que estos tienen en cuanto a los bienes y/o servicios brindados por la institución.

1. Qué hacemos?
2. Para quién lo hacemos?
3. Cómo lo hacemos?

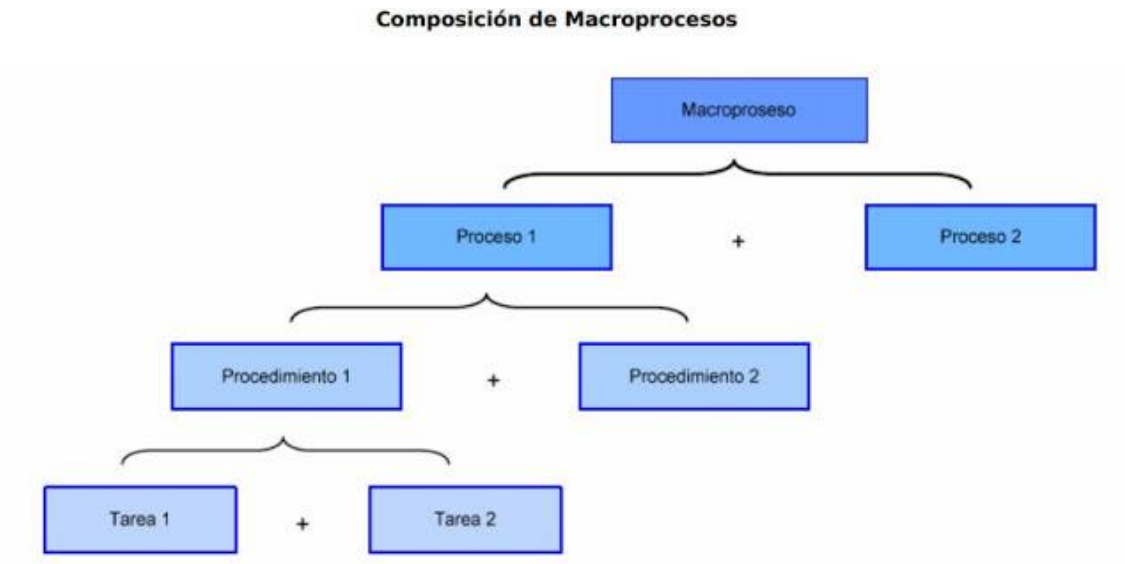
Figura 2: Triangulación de misión, usuario y proceso
Elaborado por: Jean Rodríguez.

Etapa 3: Identificación de los Procesos.

Primeramente se realizará la identificación del marco estratégico institucional para posteriormente realizar la Identificación de los procesos mediante el mapeo de los mismos.

Se entiende por proceso al conjunto de procedimientos que se encuentran interrelacionados y se desarrollan cronológicamente para la consecución de objetivos. Un procedimiento consiste en la descripción de un ciclo de operaciones o tareas necesarias para ejecutar un trabajo, estos generalmente se refieren a labores de varios funcionarios, desarrolladas en sectores distintos. Son establecidos para asegurar el tratamiento uniforme de las operaciones necesarias para producir un bien o servicio. Un procedimiento indica cómo proceder en una situación concreta. Y por último una actividad es el conjunto de operaciones o tareas afines y coordinadas que una persona o entidad debe realizar para cumplir con las funciones que le han sido asignadas.

Figura 3: Composición de los macro procesos, entendiendo la estructura
Fuente: Levantamiento de Procesos, Organización de Materia, 2010



Etapa 4: Descripción y Análisis de procesos

Cada proceso se encuentra conformado por una serie de procedimientos, y estos a su vez por actividades o tareas por desarrollar. Para realizar una adecuada descripción de los procesos, procedimientos y actividades institucionales debe contarse con un conocimiento preciso y claro de los mismos, por ello es bastante recomendable que los funcionarios responsables de su ejecución participen de este proceso descriptivo.

En este punto es fundamental realizar la identificación del objetivo del proceso y de sus responsables.

Etapa 5: Priorización y Aprobación de los Procesos.

Básicamente en este punto se define cuál es prioritariamente el orden de presentación formal de procesos que se presenta en el informe, éstos proporcionan las directrices para avanzar trabajo el cual es objeto de estudio

Etapa 6: Difusión de los Procesos.

La etapa de difusión es sin duda una de las más importantes en cualquier tipo de investigación, análisis y extracción de información, debido a que si no existe una arreglo documentado va a ser siempre más complicado llegar a tener el impacto que se busca, la documentación se hace con el fin de difundirlo de la mejor manera y así dar a conocer un trabajo exhaustivo sobre el levantamiento de procesos.

Etapa 7: Aplicación y Control de los Procesos.

Se requiere manejar la información de la mejor manera para el desarrollo del proyecto en curso.

Etapa 8: Mejoramiento continuo de los Procesos (Rediseño de Procesos).

Como último punto de vida de un proceso se va a re factorizar y descomponer para poder tener una mejora continua, y la etapa de mejoramiento continuo, la etapa de mejoramiento cumple con el auto reparación que idéntica a los procesos vanguardistas y de uso prolongado en el método de una empresa.

CAPÍTULO II

MÉTODO

2.1. ANÁLISIS

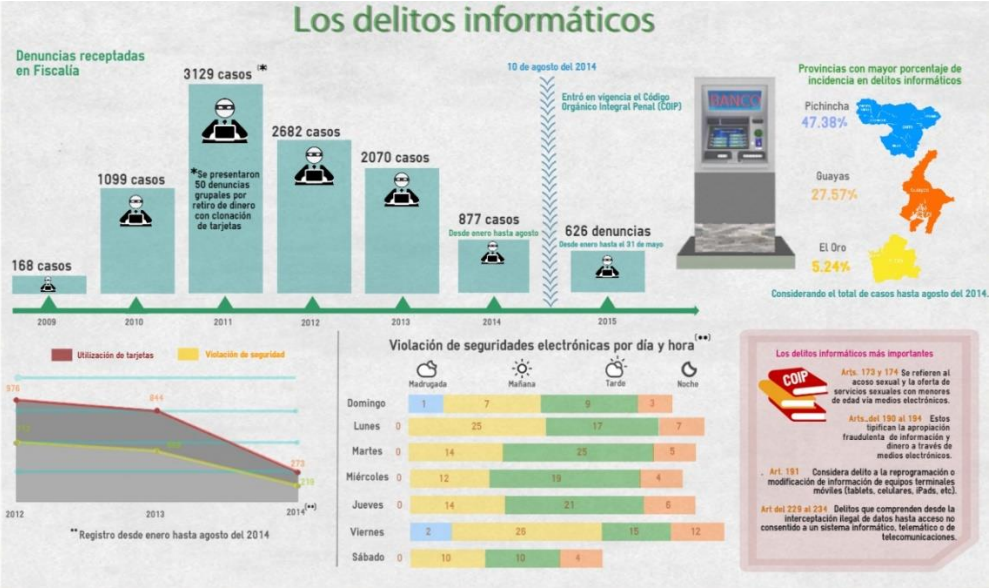
2.1.1 Estudio preliminar

Sector de interés:

El sector de interés del presente estudio son las instituciones públicas o privadas que tengan las necesidades de proteger algún bien tangible o intangible y busquen la mejora integral de su empresa, indistintamente de si su línea de negocios ofrece un servicio o un producto.

En el Ecuador los delitos informáticos crecieron de manera exponencial en el año 2011, fecha en la cual la seguridad de la información no era tomada con la misma seriedad que hoy tiene, sobretodo en entidades bancarias. Como se indica en el siguiente cuadro:

Figura 4: Delitos informáticos en el Ecuador
Fuente: Fiscalía General de Estado, 2014.



En el que se nota que el mayor control aplicado para que la delincuencia informática baje fue la entrada en vigencia del Código Orgánico Integral Penal (COIP). Y aún sin contemplar ninguna política de seguridad de la información, hasta el 2014 la provincia de Pichincha fue víctima del 47.38% de los delitos informáticos en el país.

Lastimosamente en estas estadísticas está presente la COOPCCP causado, por un mal manejo de seguridad de la información, una delegación de funciones no levantada debidamente, falta de personal adecuado para los puestos de trabajo, etc. Problemas que se han ido solucionando al pasar de los años pero continúan existiendo.

Reuniones iniciales

Lo primero fue planear el acercamiento a la entidad mediante pequeñas reuniones para conocer sus necesidades y de igual manera exponer la propuesta del proyecto formando un acuerdo previo al inicio del mismo. Las reuniones se llevaron a cabo con el Ing. Daniel Zurita, actual Jefe de tecnologías y comunicaciones de la COOPCCP junto con el cual se definió el alcance del proyecto, inicio de actividades y se reorganizó para ajustarse a la

realidad de la entidad financiera con las regulaciones de la SEPS, normas nacionales e internacionales, etc. Información que sirvió para presentar la propuesta al consejo de administración, con el fin de obtener la carta de auspicio a la Economista Esperanza Montalvo (Ver anexo 1), quien dio visto bueno al proyecto. Como constancia de cada reunión se firmó un acta de cumplimiento. (Ver anexos del 2 al 5)

Acuerdo de confidencialidad

Antes de obtener información sensible sobre el manejo interno de la institución, fue necesario desarrollar un acuerdo de confidencialidad en el que constó el nivel de acceso con el que se contaba durante la realización del proyecto. El contenido del acuerdo de confidencialidad fue firmado por el Ing. Daniel Zurita, Jefe de Tecnologías de la COOPCCP y el Sr. Jean Rodríguez. Y estuvo estructurado de la siguiente manera: antecedentes, objeto, exposición y cláusulas. (Ver anexo 6)

Levantamiento de información

Tras el acceso a la COOPCCP se recopiló cierta información a manera de conversatorio informal con las personas que se compartía el área de trabajo. Al momento de ingresar se recibió la ayuda directa del jefe de Riesgos, quien aportó en gran medida con su conocimiento de manera operativa y con el jefe de TI, quien aportó con información relevante como es:

- Equipo tecnológico con el que se dispone
- Software en vigencia
- Levantamiento de procesos realizados

- Perfiles duros del personal
- Organigrama institucional
- Informes de auditorías de seguridad
- Manual de políticas de seguridad vigentes
- Carga laboral
- Puestos organizacionales
- Contratos a nivel de servicios

Toda información más detallada o específica sobre temas sensibles fue tratada con total responsabilidad bajo el acuerdo de confidencialidad.

Perfiles de las plazas de trabajo

Los perfiles de los puestos se encontraron en construcción bajo la dirección del Jefe de talento humano, quien estuvo encargada de llevar el proceso para cumplir con las regulaciones de la SEPS, basándose en un trabajo realizado dentro de la COOPCCP por parte de terceros.

Organigrama

Para conocer la estructura y poder hacer un análisis íntegro de la empresa fue requerido también el organigrama vigente en la COOPCCP.

Del cual se basó la estructuración de las reuniones antes del levantamiento de procesos pero al buscar a los responsables de diferentes áreas se encontró con el problema que no todas

las áreas organizacionales están implementadas por lo que no cuentan con el especialista requerido y las obligaciones son delegadas a otras personas que tenían algún tipo de afinidad.

Puestos Organizacionales.

Los puestos con los que consta actualmente la COOPCCP son los siguientes:

Tabla 5: Descripciones de los puestos organizacionales de la COOPCCP.
Elaborado por: Jean Rodríguez.

NRO	*DESCRIPCION CARGO*
1	Administrador DBA (Data Base Administrator)
2	Administrador de Red y Comunicaciones
3	Analista de Procesos
4	Asesora Legal
5	Asistente Administrativo
6	Asistente de Auditoría
7	Asistente de Operaciones
8	Asistente de Recursos Humanos
9	Auditor Interno
10	Auxiliar de Contabilidad
11	Comité de Administración Integral de Riesgo
12	Comité de Calificación de Activos de Riesgo
13	Consejo de Administración
14	Contador General
15	Coordinador de Desarrollo
16	Dueño de Proceso
17	Gerente General
18	Help Desk

NRO	*DESCRIPCION CARGO*
19	Jefe de Agencia
20	Jefe de Crédito y Cobranzas
21	Jefe Administrativo Financiero
22	Jefe de Marketing
23	Jefe Comercial
24	Jefe de Operaciones
25	Jefe de Planificación y Control Presupuestario
26	Jefe de Recursos Humanos
27	Jefe de Servicios Generales
28	Jefe de Tecnología
29	Oficial de Cumplimiento
30	Jefe de Riesgos
31	Operador de Sistemas
32	Presidente del Consejo de Administración
33	Responsable de Servicio de Atención al Cliente
34	Responsable del Manual
35	Coordinador Responsable de Planes Operativos
36	Responsable de Recepción
37	Responsables de Unidades Administrativas
38	Secretario del Comité de Cumplimiento
39	Subgerente General
40	Tesorero General
41	Jefe de Desarrollo Organizacional

Esta información fue proporcionada por el personal de riesgo extraída de la matriz de trabajo con la que se manejan internamente para poder identificar quien reporta, interviene o

responsabiliza de algún evento. Tras hacer una concatenación con la información obtenida, muchos de los puestos que se tipifican no se encuentran con personal o sus funciones son delegadas a otras áreas.

Análisis de Auditoría:

En el mes de Mayo del 2016 se realizó una auditoría informática con profesionales externos a la empresa bajo contacto directo de presidencia de la COOPCCP. De la cual se extrajo un cuadro en el que se analiza el porcentaje de cumplimiento de las estrategias levantadas por el área de Auditoría interna, en los cuales consta la descripción, recomendación y estrategia a cumplir por el responsable de la estrategia, que en este caso viene a ser el responsable de Tecnología de la información.

Herramientas de Riesgos.

Se analizó también las herramientas didácticas de la empresa como la tabla de riesgos en el caso de dicho departamento, la cual ayuda a las personas que necesiten reportar un riesgo a conocer la criticidad del mismo y de qué manera tratarlo. Su funcionamiento consiste en evaluar el impacto y la vulnerabilidad con una escala del 1 al 10 que funcionan en los siguientes rangos:

Tabla 6: Tabla de herramienta de Riesgos A – Rangos de Impacto.
Elaborado por: Jean Rodríguez.

IMPACTO		
Valor	**Definición**	**Descripción**
1	Insignificante	De $0 a $500
2	Insignificante	De $501 a $1.000
3	Impacto menor	De $1.001 a $ 5.000
4	Impacto menor	De $5.001 a $10.000
5	Moderado	De $10.001 a $50.000
6	Moderado	De $50.001 a $100.000
7	Impacto crítico	De $100.001 a $250.000
8	Impacto crítico	De $250.001 a $ 500.000
9	Catastrófico	De $500.001 a $750.000
10	Catastrófico	Más de $750.000

Tabla 7: Tabla de herramienta de Riesgos B – Rangos de Probabilidad.
Elaborado por: Jean Rodríguez.

PROBABILIDAD		
Valor	**Definición**	**Descripción**
1	Muy Baja	Puede ocurrir en circunstancias excepcionales – 2 veces cada 5 años
2	Muy Baja	Puede ocurrir en circunstancias excepcionales – 2 veces cada 5 años
3	Baja	Podría ocurrir en algún momento – 1 vez cada 2 años
4	Baja	Podría ocurrir en algún momento – 1 vez cada 2 años
5	Media	Puede Ocurrir en algún momento – 1 vez al año
6	Media	Puede Ocurrir en algún momento – 1 vez al año
7	Alta	Podría ocurrir en la mayoría de circunstancias – 1 vez cada mes
8	Alta	Podría ocurrir en la mayoría de circunstancias – 1 vez cada mes
9	Muy Alta	Ocurrirá en la mayoría de las circunstancias – Varias veces al mes
10	Muy Alta	Ocurrirá en la mayoría de las circunstancias – Varias veces al mes

Es un recurso didáctico que no consta como método fijo de operar ni se encuentra tipificado en ningún tipo de manual, la concientización de los problemas y el uso de herramientas para poder ayudar a solucionarlas es vital para el funcionamiento y el crecimiento eficiente de cualquier entidad productiva.

Eventos de Riesgo

También se realizó un análisis de los eventos que se dieron con anterioridad en la COOPCCP tipificados el registro y la información de algunas áreas de la COOPCCP

Levantamiento de procesos.

El levantamiento de procesos, hasta en ese entonces vigente, consta en registro para todas las personas de la empresa bajo la herramienta web Anywhere "ISO TOOLS" la cual tiene actualizaciones de acuerdo lo dice el contrato de nivel de servicios. En esta herramienta se encontraron los manuales, reformas, procesos y actividades de la COOPCCP, extraídos con el fin de comenzar el proyecto de tesis.

La suma de todos ellos dan como resultado 43 procesos y 270 procedimientos estructurados en tres niveles: Estratégicos, Operativos y Apoyo. En los que se engloban las 15 áreas organizacionales en las cuales se realiza el trabajo, estas son:

1. Área Comercial
2. Área Jurídico – Legal
3. Tecnología de la Información
4. Talento Humano
5. Riesgos
6. Unidad de Cumplimiento
7. Marketing
8. Auditoría Interna
9. Contabilidad
10. Financiero
11. Desarrollo Organizacional
12. Operaciones
13. Sub Gerencia
14. Servicios Generales
15. Gerencia General

A base de este análisis previo se formuló un esquema para comprobar la veracidad del mismo, en el que, con ayuda de una matriz se llevó a cabo una entrevista con las personas encargadas de cada área denominados "Líderes de procesos"

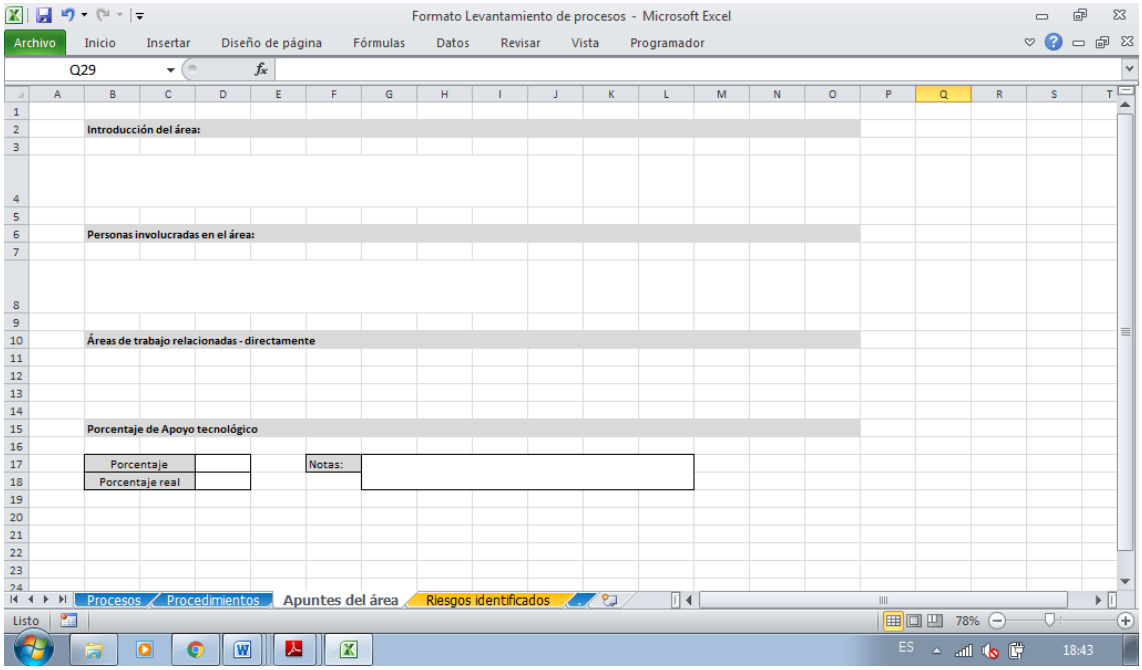
Tabla 8: Personal de la COOPCCP encargadas de las áreas organizacionales.
Elaborado por: Jean Rodríguez.

Área	Líder de proceso / Encargado
Comercial	Andrés Zambrano
Jurídico	Margarita León
Tecnologías de la Información	Daniel Zurita
Talento Humano	Erika Otalia
Riesgos	Gabriel Ripalda
Unidad de Cumplimiento	Gloria Martinez
Marketing	Edgar Rubianez
Auditoria Interna	Sandra Rosero
Contabilidad	Cristian Carrera
Desarrollo organizacional	Alberto Vinueza
Operaciones	Marcelo Males
SubGerencia	Esperanza Montalvo
Servicios generales	Octavio Quishpe
Gerencia General	Fernando Beltrán

En la que se pidió su criterio acerca del funcionamiento de su área, tiempo de trabajo direccionando la misma, áreas con las que tiene un trabajo más relevante, criterio profesional sobre el apoyo de TI en su área, sistemas informáticos utilizados, tipos de controles de acceso, manejo de eventos, nivel de importancia en el manejo de su información, detalle de las actividades. Las matrices fueron llenadas en 3 partes: Conversatorio, Procesos y Procedimientos, cuyo formato se presenta a continuación:

Conversatorio:

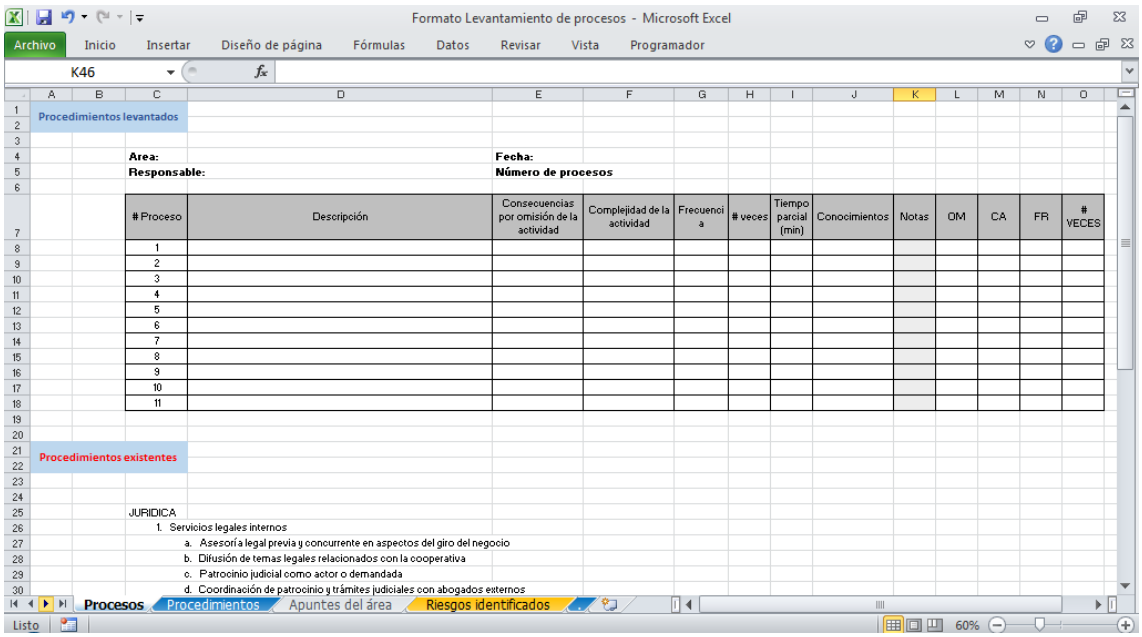
Figura 5: Primera tabla del levantamiento de procesos – Conversatorio.
Elaborado por: Jean Rodríguez.



En este espacio se pidieron introducciones al área, la carga laboral que tiene, equipo de trabajo a nivel nacional, áreas de trabajo relacionadas y apoyo tecnológico.

Procesos:

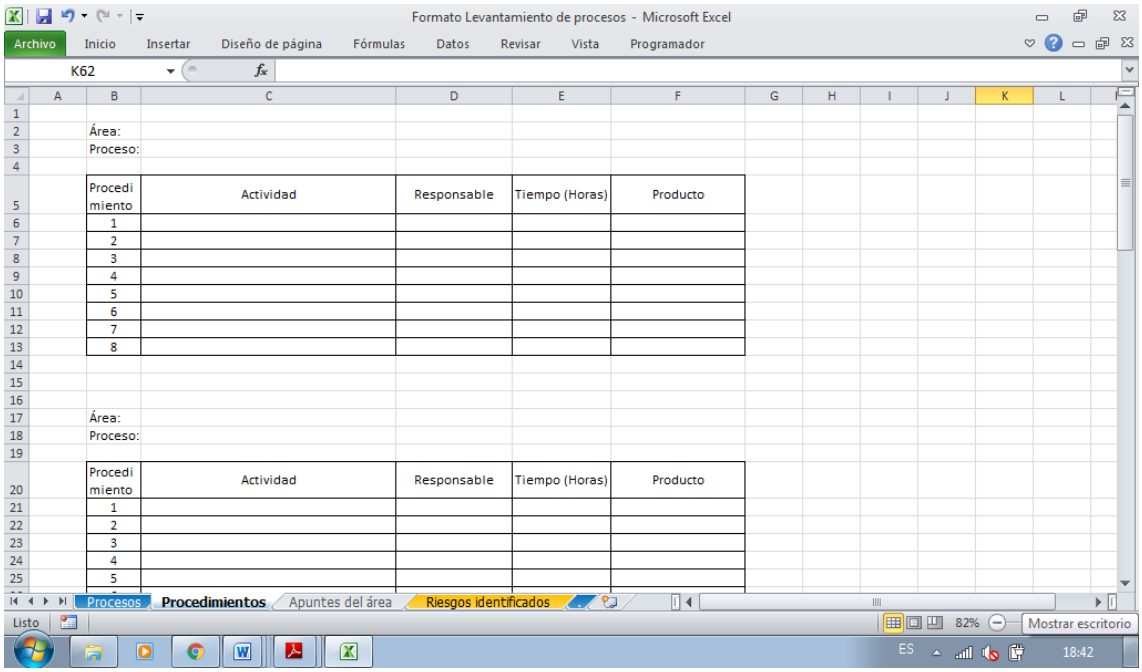
Figura 6: Segunda tabla del levantamiento de procesos – Procesos.
Elaborado por: Jean Rodríguez.



En ésta constan los procesos que se van a levantar y los que existían previamente en el levantamiento de información encontrado en la herramienta "ISO TOOLS". Se pidieron de manera general los datos del entrevistado, fecha, área y de manera específica la descripción de la actividad, las consecuencias por no hacerla, el tipo de complejidad, la frecuencia (Quincenal, mensual, anual) con la que se la realiza, el número de veces que se realiza dentro de la frecuencia, el tiempo que lleva realizar dicha actividad, los conocimientos requeridos para realizar con éxito dicha actividad y notas referentes a cada campo, de ser necesarias.

Procedimiento:

Figura 7: Tercera tabla del levantamiento de procesos – Procedimientos.
Elaborado por: Jean Rodríguez.



En la última matriz se hace énfasis en la explicación de cada uno de los procesos que se pidieron con anterioridad, dentro de ésta constan los datos generales de identificación de proceso, área al que pertenece, descripción del procedimiento, responsable del cumplimiento del mismo, tiempo invertido y el producto de dicho proceso.

Con el fin de no dejar huecos dentro del nuevo SGSI y poder ser aplicado a los problemas actuales de la COOPCCP, se llenaron las matrices con una inversión de tiempo de 1 a 2 horas por reunión. Así es como se diseñó el nuevo levantamiento de procesos y procedimientos con el cual se realizó la nueva política de seguridad de la información.

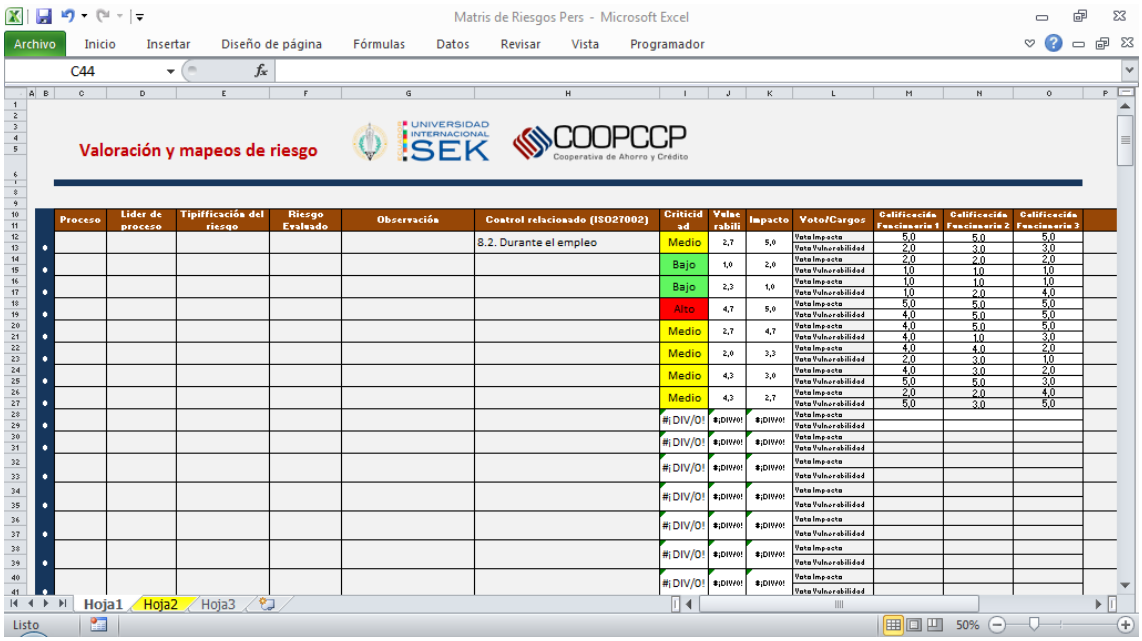
Tras el análisis del nuevo levantamiento de procesos a comparación con el anterior, se evidenció que muchos de estos que constaban en la herramienta de "ISOTOOLS" ya no eran llevados a cabo por las personas que constaban como responsables, sino que era delegado a otras personas u otras áreas. Y salieron a la luz las primeras fallas con lo que respecta a la seguridad de la información.

Ya concluido el levantamiento de procesos se encontró con 105 procesos y 501 procedimientos, una gran diferencia con los 313 levantados con anterioridad en la herramienta "ISOTOOLS". Tras todo este proceso se firmó un documento de constancia.

Análisis de Riesgos

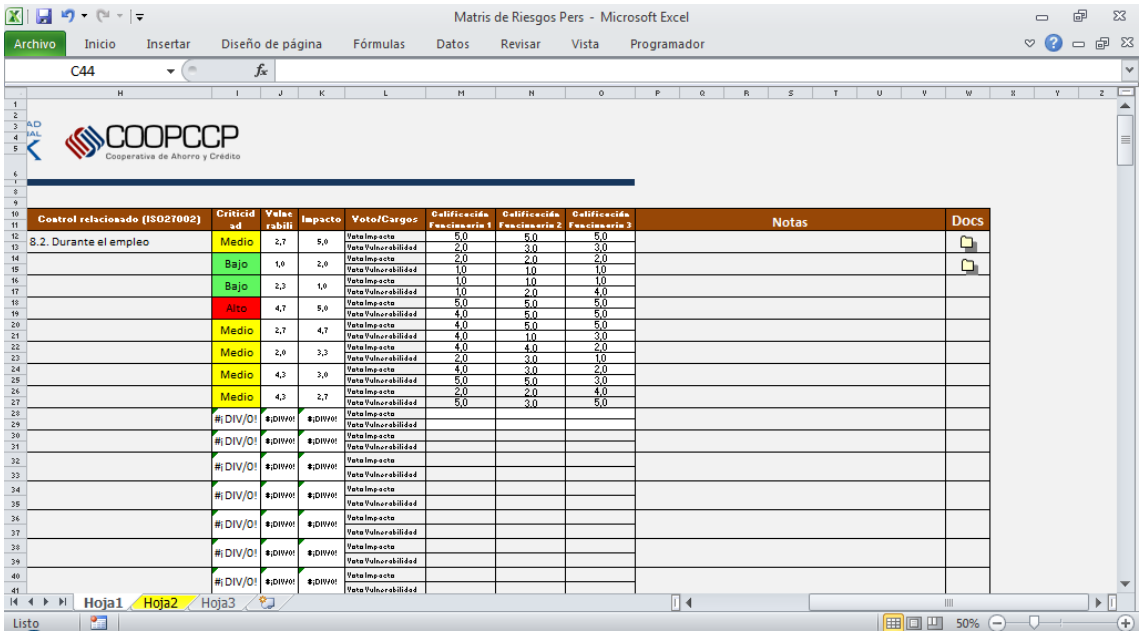
Para el análisis de riesgos se tomaron en cuenta cada uno de los eventos y actividades que se realizan dentro de la COOPCCP en todas las áreas organizacionales, se realizó una proyección de los eventos críticos y las vulnerabilidades existentes, tras identificar las faltas de seguridad se colocó en una matriz con la cual se pudo calcular el riesgo inherente con la opinión de los líderes de procesos.

Figura 8: Primera parte del formato de análisis de riesgos.
Elaborado por: Jean Rodríguez.



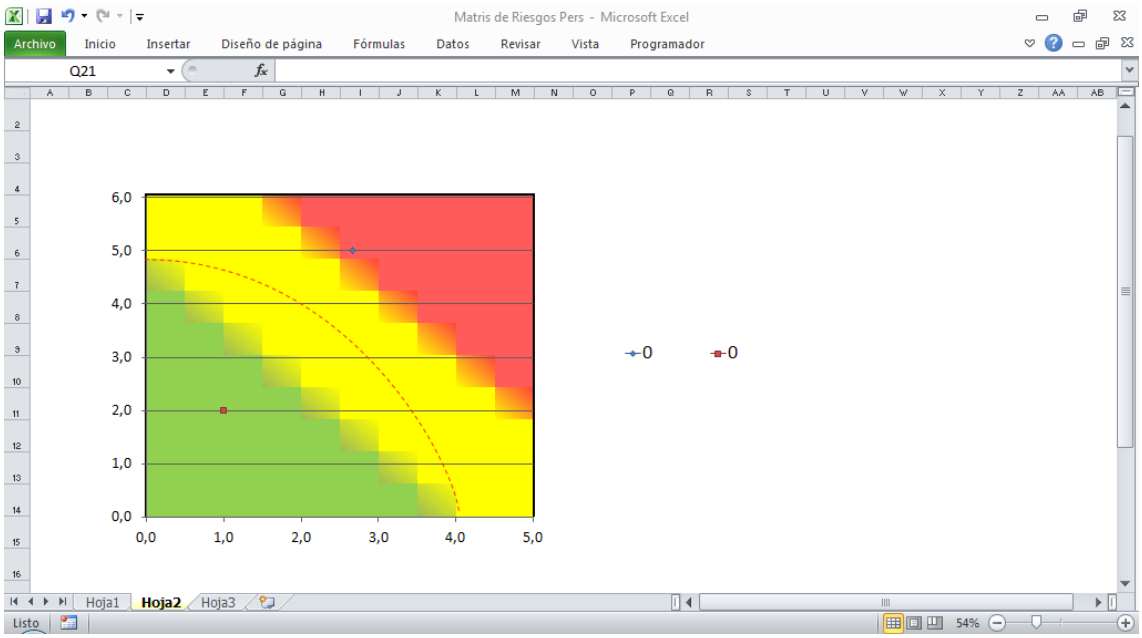
La matriz consta de nombre de proceso, el líder de proceso responsable del mismo, una pequeña descripción del riesgo tipificado de manera técnica, el riesgo que se está evaluando de acuerdo al diccionario de controles, las observaciones de la actividad evaluada, el control relacionado con la norma ISO 27002.

Figura 9: Segunda parte del formato de análisis de riesgos.
Elaborado por: Jean Rodríguez.



En la segunda parte podemos encontrar la evaluación del riesgo como tal. El objetivo es calcular el riesgo en función al impacto por su vulnerabilidad, con la ayuda didáctica de colores se puede tener una visión más acertada sobre el estado actual del evento, esto es con el puntaje de 3 diferentes funcionarios especialistas dentro de la actividad el cuál aporta su voto acerca del impacto y la vulnerabilidad existente.

Figura 10: Tercera parte del análisis de riesgos – Mapa de calor.
Elaborado por: Jean Rodríguez.



La tercera parte consta de una gráfica en la que se ubica a la COOPCCP de manera general en el punto de criticidad que se encuentra antes de aplicar los controles propuestos.

Diccionario de controles

El desarrollo de un diccionario de controles es clave para poder justificar los hallazgos que se consideraron una amenaza dentro de la empresa, lo cual se pudo hacer mediante el desarrollo del ERM, en éste está tipificado el detalle de la vulnerabilidad encontrada, el tipo

de control de la ISO 27002 que contrarresta a esta vulnerabilidad y la justificación del uso del mismo.

Junto al diccionario de controles se presenta un documento formal que conste de la unión del análisis de riesgo y el diccionario de controles. El mismo que es formulado como registro del trabajo realizado y detalla las observaciones encontradas en este documento se puede encontrar también el estado inicial de la COOPCCP y el estado final pero no cuenta con detalles de los valores evaluados, tal y como vemos a continuación:

Antecedentes:

La COOPCCP es una empresa dedicada a la actividad financiera bancaria que actualmente tiene cobertura nacional con 14 sucursales (distribuidas en la costa, sierra, oriente y galápagos del Ecuador) y la matriz funcional en Quito, desde la cual se gestionan todas las 14 anteriores mencionadas. La empresa ha experimentado un crecimiento constante a base de una política de evolución y mejora continua de procesos y procedimientos. Por lo que era natural encontrarse con algunos inconvenientes en esta transición, El ejercicio principal de esta entidad es el manejo de cuentas, transacciones, créditos y servicios varios.

Cuenta actualmente con un organigrama que divide a la organización en 4 niveles, estos son:

Asamblea General (Conjunto a consejo de administración), Gerencia general, Subgerencia general, Jefes de áreas, todas ellas acompañadas con la ayuda de auditoría interna.

Los objetivos son:

- Identificar cuáles son los procesos que necesitan mayor atención
- Mejorar los procesos de la empresa de manera que garantice todos los aspectos de la seguridad de la información dentro de la misma
- Realizar un cotejo con la norma ISO27000 de manera idónea con el fin de reflejar la realidad de la organización

Tras el levantamiento de información se puede comenzar puntuando los potenciales riesgos que se encuentran gracias a los hallazgos de la SEPS proporcionados por algunas áreas de la organización se puede dar un análisis de riesgos definido en cada una de las áreas de trabajo.

Resolución:

El problema común en cualquier empresa, sin importar su línea de negocios es la compartición de datos e información, una actividad que está encasillada dentro de la gestión de operaciones y comunicaciones. Dentro de la misma se pueden encontrar diversos campos a los cuales tratar pero se hará hincapié en una de ellas, debido a que debe considerarse como información cualquier tipo de dato generado dentro de la empresa, las diversas relaciones con los clientes y el manejo de la misma dentro de las sucursales.

ISO 27002: 10.8 Intercambio de información (Problema en toda la empresa)
ISO 27002: 11.3 Responsabilidades de usuario (Problema en toda la empresa)

Área comercial

Gestión de comunicaciones y operaciones

El área comercial está encargado también de las entrevistas y coincidencias en contrataciones para el área, por lo que se considera que el seguimiento y delegación de actividades deben ser supervisados, revisadas y manejadas de la mejor manera para que no existan vacíos en tanto a responsabilidades de cada cargo.

ISO27002: 8.2. Durante el empleo

Tras finalizar las actividades dentro del área comercial, es prudente tener un buen manejo de la información que entre en este proceso, todas las problemáticas de la empresa que se den a partir del cese de actividades de una persona se debe dar a una persona escogida para que administre las actividades que desempeñaba dicho puesto. Contando con la devolución de cualquier documento trabajado y dando de baja sus controles de acceso.

ISO27002: 8.3 Cese de actividad

En lo que respecta al área de Cajas se debe tomar en cuenta que una de las problemáticas que atentan contra los principios de la integridad de los datos es el tipo de seguridades que tengan los equipos, tanto así como los usuarios de otros productos administrados por el área comercial. Para esto se lleva a cabo una implantación de seguridades específicas acorde a la criticidad de la información dentro de un rango establecido.

ISO27002: 9.2 Seguridad de los equipos (por cajas)

Llámese código móvil a todo tipo de Script o protocolo de seguridad que se inicie cuándo se utilice un producto o servicio sin la necesidad de autorizaciones previas en el o los equipos involucrados en el proceso. Este control se realiza de manera general para tener constancia del correcto funcionamiento de los procesos de administración de los productos.

ISO27002: 10.4.2 medidas contra el código móvil

La gestión de productos y servicios dentro de una organización generan datos importantes que son compartidos a diferentes áreas de trabajo pero sin duda pertenecen al proceso de administración del mismo, es por eso que por motivos de seguridad de la información es necesario delegar un tipo de responsabilidades para cada producto o servicio que se ofrece dentro de la cooperativa.

ISO27002: 7.1 Responsabilidades sobre activos (considerando a los productos como activos intangibles)

Las transacciones que se realicen dentro de los servicios ofrecidos a los clientes en la cooperativa necesitan ser censados y gestionados de manera adecuada asegurando así que el proceso sea lo menos disperso posible tratando de manejar de la mejor manera la información que entra a la empresa mediante portales web o servicios que los utilicen sean estos de manera pública o privada

ISO27002: 10.9 Servicios de comercio electrónico

Análisis de la antigua política de seguridad

En abril del 2014 se expidió una política de seguridad para la COOPCCP, no obstante la misma no cumple, en estructura, con lo requerido en la entidad financiera y carece de delegación de tareas, no especifica las áreas organizacionales quienes se encargan de cada control y está orientado al cumplimiento de seguridades bajo el mando del departamento de TI. Motivo por el cuál no fue muy tomada en cuenta ni aplicable.

En base a las observaciones que se obtuvieron del documento de política del 2014, se planeó desarrollar un nuevo SGSI con una estructuración diferente que sea claro y conciso sobre quienes aplica y la delegación de funciones sea relacionado a las áreas organizacionales que actualmente están vigentes, sin dejar delegaciones a personal que no esté en funcionamiento.

El análisis de la antigua política de seguridad es una tarea extensa que se realizó de manera manual en lectura y registro de comentarios en el material impreso.

2.1.2. Estudio de factibilidad

Para evaluar la viabilidad de un proyecto se necesita tomar en cuenta varios aspectos, entre los cuales se consideran ciertas factibilidades:

Tabla 9: Tipos de Factibilidades para el desarrollo del proyecto.
Elaborado por: Jean Rodríguez.

Tipos de Factibilidades

Factibilidad Técnica	Indica la disposición de los conocimientos técnicos necesarios para la culminación del proyecto así también como las habilidades de manejo.
Factibilidad Operativa	Se refiere al personal necesario para poder llevar a cabo el proyecto, en este caso, en seguridades de la información con conocimientos en riesgos.
Factibilidad Tecnológica	Indica si se dispone del equipo y las herramientas necesarias para llevar a cabo el proyecto y de no ser así, si es posible obtenerlas en marcha.
Factibilidad Económica	Se refiere si se dispone del capital para poder llevar a cabo el proyecto, en este caso, si está aprobada la compra de los productos necesarios para desarrollar el proyecto.

2.1.2.1 Factibilidad Técnica

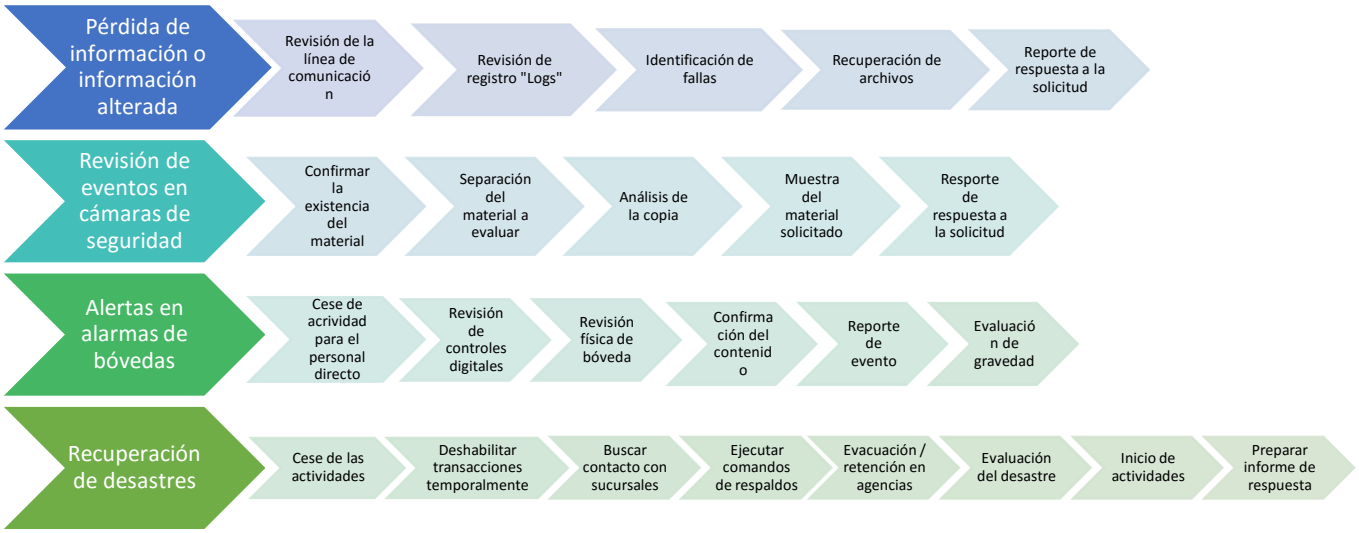
Para que exista una factibilidad técnica es necesario que se cuente con el personal adecuado para poder supervisar el funcionamiento del SGSI quienes contarán también con un manual de políticas de seguridad de la información, la cual tendrá detallado en el los eventos considerados más importantes y que puedan influir directamente al funcionamiento de la empresa.

Las personas encargadas que pertenezcan al departamento de seguridad de la información o cualquier área que la contenga, deben tener un conocimiento extenso sobre la aplicación de los controles de la ISO27000, ya que aunque cuenten con el manual de seguridad de la información, no siempre podrá ser aplicado a algún evento o actividad que se suscite. El criterio profesional del encargado de supervisar esta área es fundamental para su correcto funcionamiento y recuperación en caso de desastres.

Se capacitará a la persona perteneciente a la empresa encargada de poner en marcha el proyecto y quien esté al tanto de cada actualización que se requiera hacer, se espera que todas las personas pertenecientes a la COOPCCP tengan una visión amplia sobre la importancia de

la seguridad de la información y su influencia dentro de la misma en cada área. A continuación se muestra de manera general las soluciones a posibles problemas.

Figura 11: Proceso a seguir como soluciones generales a ciertos eventos.
Elaborado por: Jean Rodríguez.



2.1.2.2 Factibilidad Tecnológica

Tras el análisis y el cumplimiento de todos los procesos que se realizaron en el alcance del proyecto, se puede notar que los cambios más urgentes se encuentran dentro del centro de procesamiento de datos de la COOPCCP, la cual no se encuentra ni siquiera alineado al más bajo nivel de Tier de Datacenter, los problemas vienen desde la manera física de estructurar el ambiente, la falta de ventilación y un trato inadecuado al servidor.

Más allá del problema físico de los datacenter es necesaria también una mejora en todo lo relacionado a la intranet y manejo de flujo de datos que existe en esta misma incluyendo el software y las páginas web.

Todos estos hallazgos son factibles de tratar gracias a que la tecnología aplicada en el Ecuador está a la altura de cumplimiento de estándares internacionales en diseño de Datacenters de Tier 1 al 5. Motivo por el cual los dispositivos, materiales y software necesarios para realizar el proyecto son encontrados en lugares especializados dentro de la región.

El espacio físico de la COOPCCP puede verse algo limitado, problema que se puede solucionar con la reubicación del área con el cuál se ganará eficiencia y velocidad en procesamiento de datos.

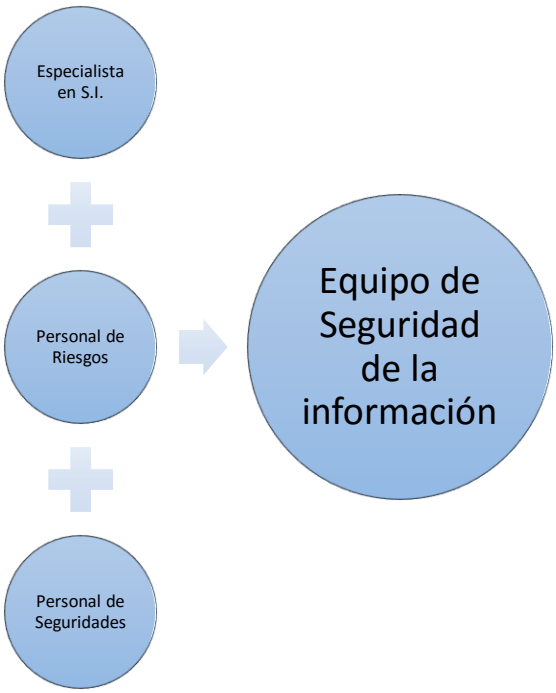
2.1.2.2 Factibilidad Operativa

En la actualidad la seguridad de la información es un campo que se está abriendo paso a nivel nacional, motivo por el cual aún muy pocas personas se dedican al estudio de los SGSI, no obstante existen quienes tienen una formación más completa y también contemplan la puesta en marcha de la seguridad de la información, la cual consiste en velar por la integridad de los datos. Y aunque el número de profesionales sea limitado, es prudente tener al menos personas especializadas en los controles de la ISO 27002, lo cual permitirá realizar el trabajo.

Se debe contar con un equipo de 3 personas, una de ellas será un especialista que se encargue de la toma de decisiones y mantenimiento del SGSI ya que al igual que muchos de los procesos, protocolos y funciones dentro de la COOPCCP cumple con un ciclo PDCA, lo cual, apoyándose siempre en los recursos tecnológicos que más crea conveniente, asegura una mejora continua que no sea intrusiva a ninguno de los procesos de la organización.

Las personas directamente implicadas en el monitoreo y cambio constante de un SGSI deben ser preferencialmente de parte de un área de seguridades de la información. Aunque pueden también formas parte del área de TI, quienes tengan experiencia en el manejo de controles de acceso, seguridades y controles aplicables ya sea de manera física como lógica. Es factible ya que en caso de no contar con el personal especializado existe la posibilidad de capacitarlos con un curso de certificación de la ISO 27002.

Figura 12: Ejemplo de formación del equipo de seguridad de la información
Elaborado por: Jean Rodríguez.



2.1.2.3 Factibilidad Económica

Para el análisis se ha considerado 3 grupos:

Talento Humano

Se detalla el perfil de las personas que deben constar dentro del proyecto así también como las funciones que realizarán, el personal requerido puede ser del área de TI y de seguridades físicas, las dos áreas se encuentran vigentes dentro de la COOPCCP por lo que no hace falta contratar personal extra, solo bastaría en delegar funciones para el cumplimiento de este nuevo objetivo.

Tabla 10: Factibilidad económica – Recursos humanos
Elaborado por: Jean Rodríguez.

TAREA O ACTIVIDAD	TIEMPO DURACION (d)	RECURSOS HUMANOS								
		ESPECIALISTA EN SEGURIDADES			PERSONAL TI			PERSONAL DE SEGURIDAD		
		% Participación	Valor /Hora	Valor Parcial	% Participación	Valor /Hora	Valor Parcial	% Participación	Valor /Hora	Valor Parcial
Planificación de actividades	7	50%	6	42	25%	2,6	18,2	25%	2,6	18,2
Desarrollo inicial de las nuevas aplicaciones	15	50%	6	90	25%	2,6	39	25%	2,6	39
Gestión de proyectos de aplicación de la política	30	50%	6	180	25%	2,6	78	25%	2,6	78
Cumplimiento de tiempos	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
Supervisión de avances	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
Supervisión de cumplimiento de los controles aplicados	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
Respuesta a fallos	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
Acción de respuesta a eventos a largo plazo	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
Manejo de sucursales	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
Implementación de proyectos	360	50%	6	2460	25%	2,6	936	25%	2,6	936
Mantenimiento de controles aplicados	Permanente	50%	6	128,6	25%	2,6	71,42	25%	2,6	71,42
COSTO POR RECURSO				**3.672,00**			**1.571,20**			**1.571,20**

El talento humano contemplado dentro de la tabla puede ser personal contratado en la COOPCCP por lo que se puede decir que se cuenta con el personal dedicado a la puesta en marcha de la política de seguridad, mantenimiento y respuesta a fallos de todas las sucursales existentes a nivel nacional.

Equipos tecnológicos

Los equipos necesarios para la implementación del SGSI son los necesarios para el Data Center, a pesar de que no se pretenda obtener una certificación, es fundamental que su diseño se base en las normas nacionales e internacionales de construcción como TIA, EIA, NFPA, USGBC, RoHS, etc. Por lo cual se deben tomar en cuenta lo siguiente:

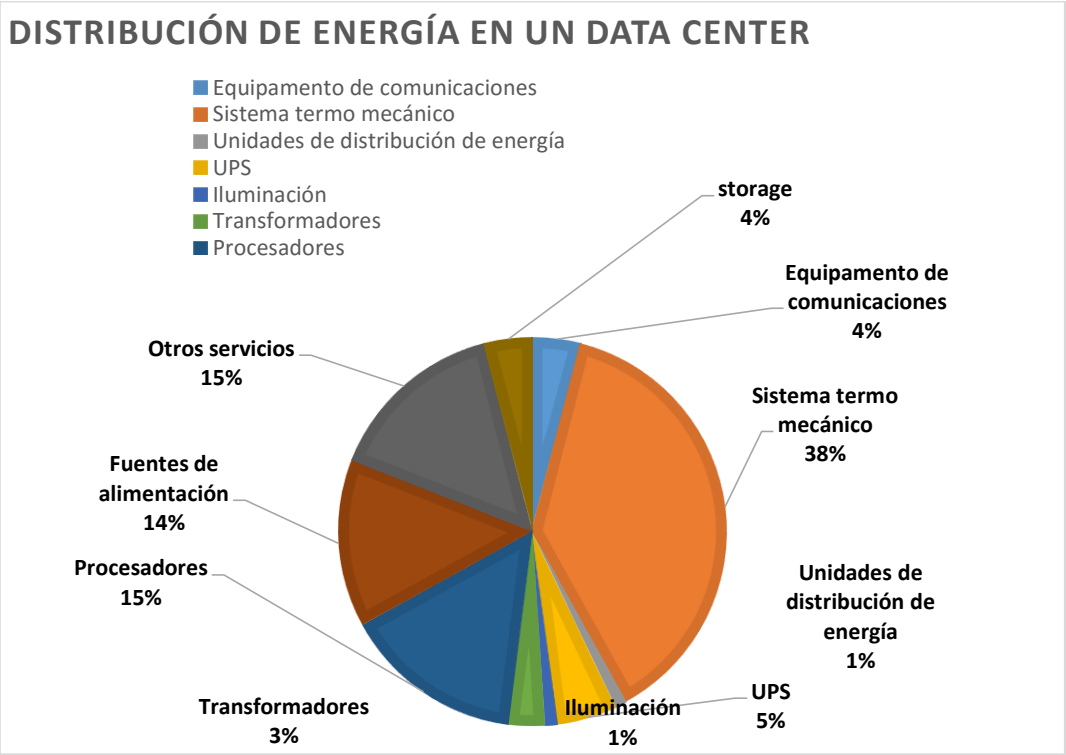
Tabla 11: Recomendaciones para el diseño de un data center
Elaborado por: Jean Rodríguez.

#	Pasos a tomar en cuenta antes de la implementación	Descripción de la recomendación
1	Tipo de Data Center a construir	Al no buscar una certificación puede ser aspirando a tener un Tier 1
2	Equipamiento informático a instalar, presente y futuro	En este punto es preciso saber cuáles son los equipos que se pretenden instalar dentro del datacenter para poder calcular la potencia necesaria y que no sea un gasto excesivo en consumo de electricidad, dentro de la planeación de un data center básico se encuentran los UPS, Transformadores, transformadores, cableado, sistemas de enfriamiento, rejillas, piso y cielo falso, Sistemas de monitoreo, servidores virtuales (opcional), racks, switches, firewalls, routers, etc.
3	Cálculo de refrigeración	En la actualidad, esta etapa es uno de los pasos más complejos y delicados de diseñar. Equipos con elevados consumos de energía, gran disipación de calor, horas pico de procesamiento y dificultades de instalación de los sistemas termomecánicos son algunos de los desafíos con los que nos cruzamos durante el diseño, motivo por el cual se debe tomar especial cuidado en este punto.
4	Cálculo de potencia requerida	Definidos los principales componentes, como el sistema de refrigeración y la potencia deseada por rack, procedemos a calcular el resto de los consumos del centro de cómputos. Cabe aclarar que, al asignar un consumo por rack, aquí están incluidos los consumos de servers, storage y comunicaciones. Nos quedaría dimensionar iluminación, refrigeración de confort, sistemas de extracción de aire, bombas de extracción de agua si las hubiera o sistemas de detección y extinción de incendios. Aquí estimaremos la potencia total de la UPS
5	Conectividad	Independientemente del tamaño del centro de datos debemos pensar como estarán conectados e integrados a la red los servidores, storage o cualquier dispositivo que instalaremos en cada rack.
6	Layout y espacios requeridos	Lo ideal para cumplir con las normativas internacionales es que se escoja una zona dedicada a los racks y servidores, separar los cuartos de enfriamiento y los de distribución de energía, no obstante la arquitectura del diseño se debe realizar conjunto con el jefe del área de TI, quien aportará con su criterio para poder llegar a una esquema factible sin tener que realizar cambios a la edificación.
7	Elección del lugar	Al ser un Tier 1 no es necesario que sea un espacio especial o con medidas exactas, pero es fundamental acercarnos a cumplir con los 1200Kg por metro cuadrado que solicita la norma en cuestión de la resistencia de la losa del datacenter. En la actualidad, equipos de UPS, racks de servidores y storage están superando los 1000Kg de peso en una superficie de 0,60 m2 que ocupa un rack.
8	Sistemas de control de	Los sistemas de seguridad son los puntos en los que se puede tener un costo

	seguridad	alto o bajo dependiendo del equipo que se obtenga, al ser ésta una empresa de alto riesgo es recomendado tener un control alto o moderado.
9	Valorización del proyecto y presupuesto	La valorización del proyecto va conjunto con servicios generales quien podrá buscar cotizaciones específicas con empresas que operen a nivel nacional para poder así obtener la mejor propuesta de equipos requeridos. El presupuesto por otra parte tiene que ajustarse al anual dedicado a los proyectos de TI y Seguridad de la información
10	Confección del proyecto final de construcción	Debe ser apoyado y dirigido conjuntamente con el Jefe de TI, ya que no es un proceso al 100% que compete a seguridad de la información sino también a los encargados del área de TI que son quienes operarán el nuevo Data Center.

También se debe mencionar que la aplicación de un Data Center de Tier 1 tiene un consumo más elevado de electricidad de lo que el DC actual. Para evidenciarlo se presenta la siguiente gráfica:

Figura 13: Consumo de energía de un Data Center.
Elaborado por: Jean Rodríguez.



Es necesario mencionar que se requerirá recursos como cámaras de seguridad, sensores de movimiento para las bóvedas y controles de software que ayuden al monitoreo constante de

estas áreas de la COOPCCP. A continuación se indican los rubros aproximados de los recursos tecnológicos que se utilizarán en el desarrollo del proyecto:

Tabla 12: Costos de recursos tecnológicos para la factibilidad del proyecto.
Elaborado por: Jean Rodríguez.

RECURSOS TECNOLÓGICOS					
EQUIPOS		**SOFTWARE**		**OTROS**	
Descripción	Valor Unitario	**Descripción**	Valor Unitario	**Descripción**	Valor Unitario
Sistema de cámaras de seguridad *	4.000	Sistemas de monitoreo de Data Base	5.000	Rubros mensuales de energía eléctrica	200
Racks *	200	Visual Basic *	200	Cableado necesario	150
Switches *	120	SQL Server 2014 *	200	Fibra óptica (en caso de necesitarla)	100
Routers *	100	Servidores virtuales	300	Piso falso	1.000
Sistema de enfriamiento	5.000	Nuevo Core Bancario	No definido	Cielo falso	1.000
UPS *	100	Proyectos de software interno *	500	Canaletas	300
Sistema de detección de movimiento	2.000	ISOTOOLS *	No definido	Rejillas	150
Medidas contra incendios	5.000	Herramientas de Administración remota	1.200	Vidrio especial para data center	1.500
Sistema de recuperación eléctrico *	2.500	VLAN´S	500	Armario de cables	150
Firewalls	4.000	ROUTING	500		
Medidas contra inundaciones	8.000	Sistema de monitoreo de cámaras *	incluido		
Master Image (en caso de virtualizar)	500				
Puertas blindadas *	2.500				
Servidores *	700				
COSTO POR RECURSO	**34.720,00**		**8.400,00**		**4.550,00**

- **Los artículos marcados con un asterisco (*) existen en la entidad.**

Éstos pueden estar sujetos a cambios y no constan como el valor final ya que pueden existir los mismos ya en la empresa, lo que implicaría un costo menor o la falta de algún componente implicaría un valor elevado

La existencia de empresas dedicadas a la seguridad de medios digitales y físicos hace que sea mucho más factible realizar este tipo de actividades. Ya que son asequibles para la empresa que los necesite.

El proyecto es factible económicamente en función al acuerdo del inicio del proyecto se determinó que la COOPCCP está dispuesta a realizar esta inversión.

Normas

La normativa a utilizar es la ISO27000 la cual se centra en la seguridad de la información y el capítulo en el cuál se apoya serán los controles y las buenas prácticas recomendadas para mantener la integridad de los datos.

De manera didáctica los controles de la ISO27002 están disponibles para cualquier persona, no obstante es necesario obtenerla si se quiere realizar un proyecto de tal magnitud y sus valores son diferentes según la manera que se consiga, oscilan entre $250 y $400 dólares con diversas variantes.

Para la aplicación del proyecto se planteó el uso de la versión ISO27002-2005 debido a que los controles tipificados son más precisos y no tienen tecnicismos en su estructuración, además de que bajo la misma versión de la norma el Instituto Nacional Ecuatoriano de Normalización – INEN realizó una aceptación bajo los términos nacionales.

2.2. DISEÑO

2.2.1. Esquema general de la solución Técnica

Para desarrollar el manual de políticas de seguridad de la información fue necesario cumplir con los diferentes procesos que se mencionaron con anterioridad: levantamiento de información, levantamiento de procesos, ERM, etc. Procesos que tuvieron también una

estructura y protocolo para llevarse a cabo con éxito. A continuación se muestra un esquema de la interacción del desarrollador del proyecto con la empresa:

Esquema general

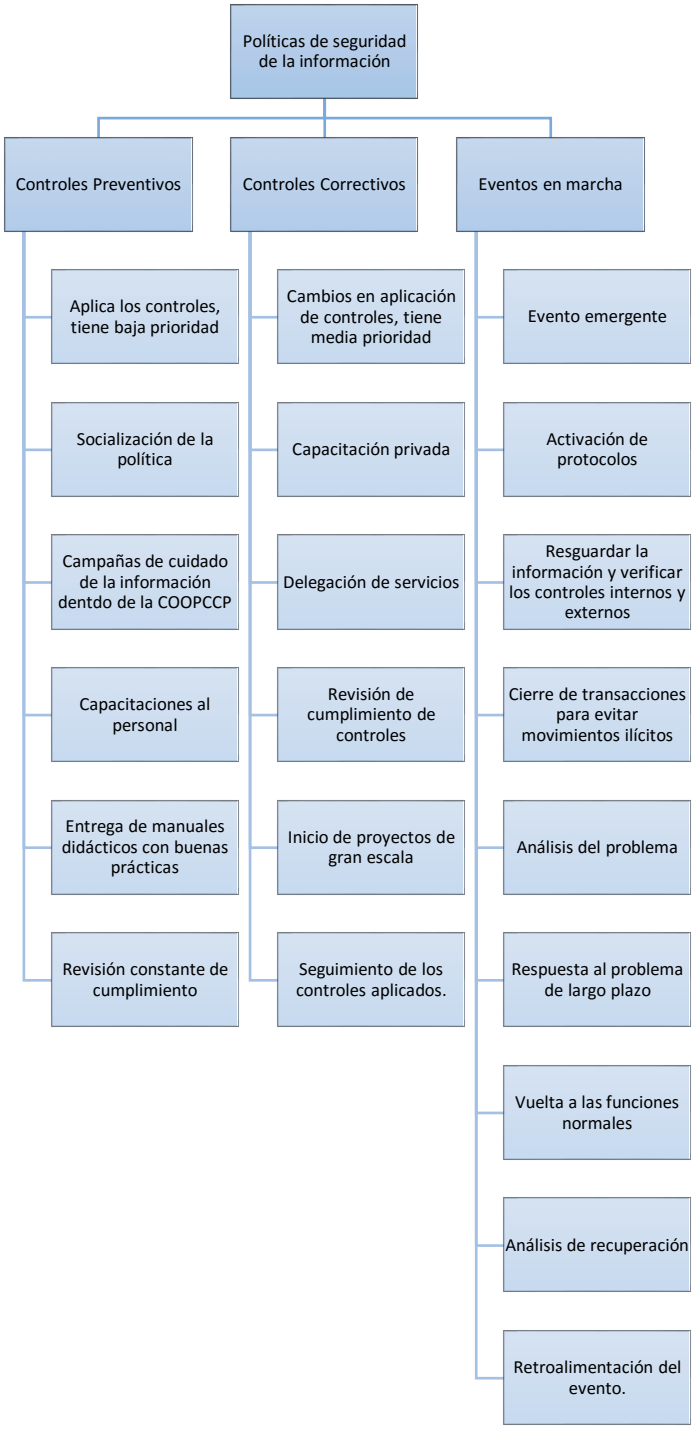
Figura 14: Esquema de la interacción del desarrollador del proyecto con la entidad
Elaborado por: Jean Rodríguez.

Interacción		
Desarrollador del proyecto		**Personal interno**
Levantamiento de información	↔	Previsión de la información
Levantamiento de procesos	↔	Entrevistas y revisión de la información levantada
Perfiles del personal	↔	Previsión de los perfiles
Equipos tecnológicos	↔	Previsión de la información de TI
Controles de acceso	↔	Aceptación de accesos
Controles preventivos	↔	Previsión de información solicitada
Análisis de riesgos	↔	Entrevistas cortas

Este esquema general muestra de una manera muy sencilla la interacción que tiene la persona encargada del desarrollo del proyecto con las demás áreas organizacionales, al no tener controles aplicados en las áreas deben asegurarse del cumplimiento de las solicitudes teniendo en mente siempre proteger la integridad de los datos en las peticiones que se reciba.

Funcionamiento de la política de seguridad de la información:

Figura 15: Modo de trabajo de la Política de la seguridad de la información con los diferentes tipos de amenazas.
Elaborado por: Jean Rodríguez.

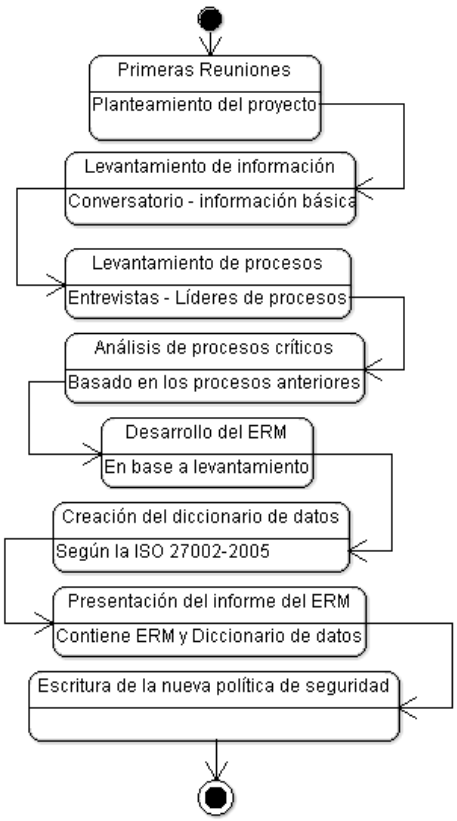


De esta se puede observar cómo la política de seguridad de la información actúa de manera genérica con los eventos inmediatos en su aplicación, considerando una prioridad en los eventos que posean un fuerte impacto y no estaban previstos, luego los vulnerabilidades más

fuertes y por último los controles preventivos, lo que incluye capacitaciones y manuales de buenas prácticas.

Diseño de la política de seguridad de la información:

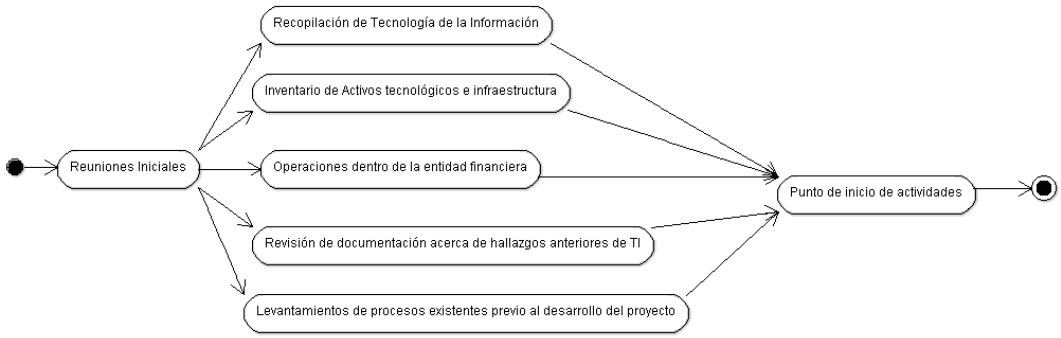
Figura 16: Esquema del diseño de la política de seguridad
Elaborado por: Jean Rodríguez.



La imagen presenta el esquema del proceso general que se realizó para poder realizar el SGSI de principio a fin sin hacer énfasis en ninguno de los puntos. Y a continuación se muestra una división de cómo se realizaron los procesos más importantes. Estos serán divididos en 5 partes, levantamiento de la información, levantamiento de procesos, análisis de riesgos, diccionario de controles y la política de seguridad.

Levantamiento de información:

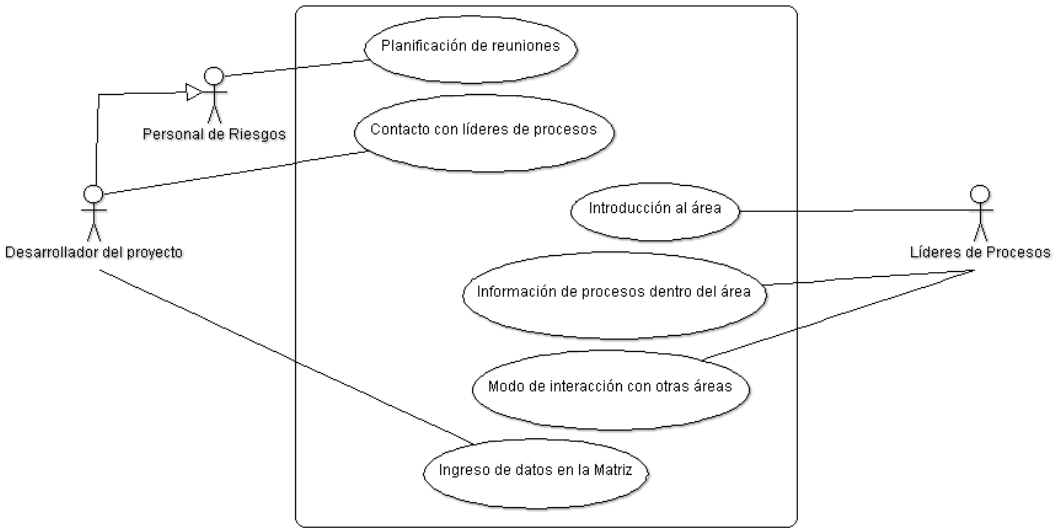
Figura 17: Levantamiento de información: Diagrama de actividades.
Elaborado por: Jean Rodríguez.



En el gráfico se muestra el tipo de información que se recopiló con este proceso de levantamiento de información, esto se hizo mediante conversaciones con el personal especializado de las áreas de TI, Riesgos y seguridades.

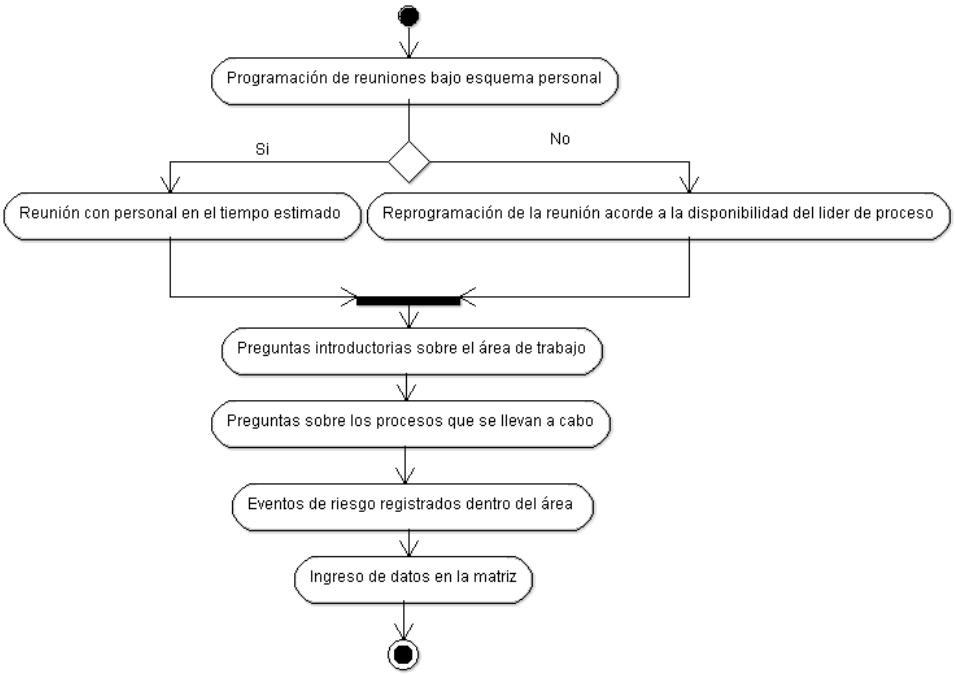
Levantamiento de procesos:

Figura 18: Levantamiento de Procesos – Diagrama de Caso de uso.
Elaborado por: Jean Rodríguez.



Se encuentra de manera general la explicación del proceso de interacción de la empresa con los líderes de procesos y la ayuda con la gestión de las reuniones por parte del área de riesgos.

Figura 19: Levantamiento de procesos: Diagrama de actividades.
Elaborado por: Jean Rodríguez.

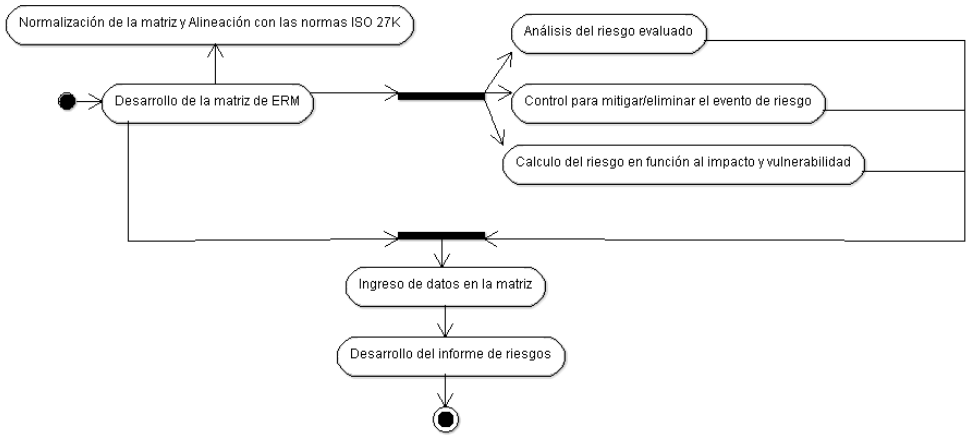


Se presenta el proceso general realizado en el levantamiento de procesos, las reuniones tuvieron un promedio de duración de 1h 30min, La cual se llevó a cabo con cada uno de los líderes de procesos. El tipo de información que se buscó fue de campo, ya que se cuenta con la documentación formal de los procesos, no obstante se notaron ciertas actividades que no constaban en el levantamiento de procesos que reflejan un tiempo de trabajo invertido por el personal de la COOPCCP.

Análisis de Riesgos:

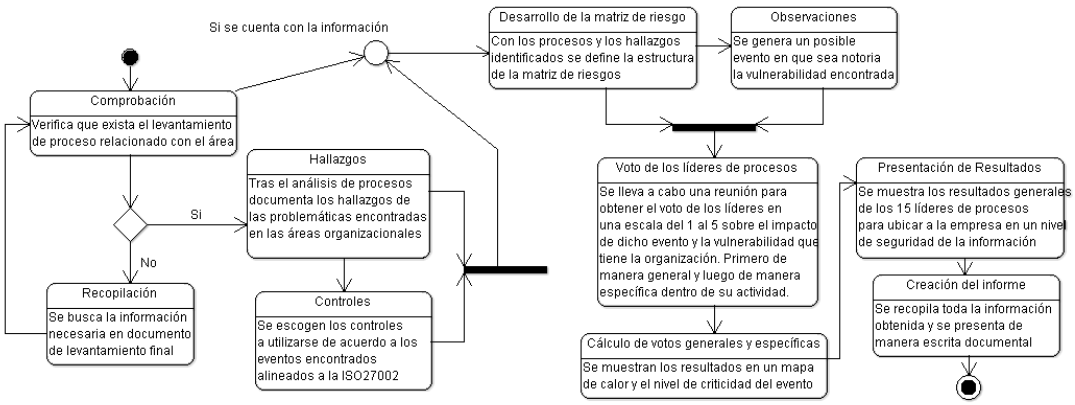
Este fue un proceso que dio como resultado el estado de la empresa a la fecha, ésta contó con la opinión de las personas encargadas en las distintas áreas del manejo de la información.

Figura 20: Análisis de riesgos – Diagrama de actividades.
Elaborado por: Jean Rodríguez.



Se muestra de manera eficiente los pasos tomados en cuenta para llevar a cabo análisis de riesgo, mismas que cuentan con la evaluación general de la empresa y la evaluación específica de cada área. Los Datos conseguidos de esta manera son base para desarrollar el informe del análisis, que explica de manera expresa los procesos críticos y los controles que los contrarrestan.

Figura 21: Análisis de riesgos – Diagrama de Estado
Elaborado por: Jean Rodríguez.

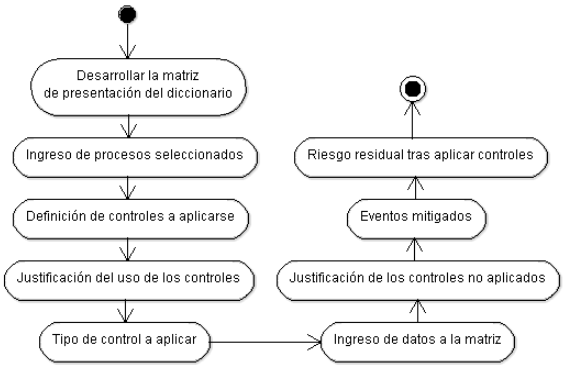


Se muestra de manera específica el desarrollo de las actividades para cumplir con el análisis de riesgo inherente de la COOPCCP.

Diccionario de Datos:

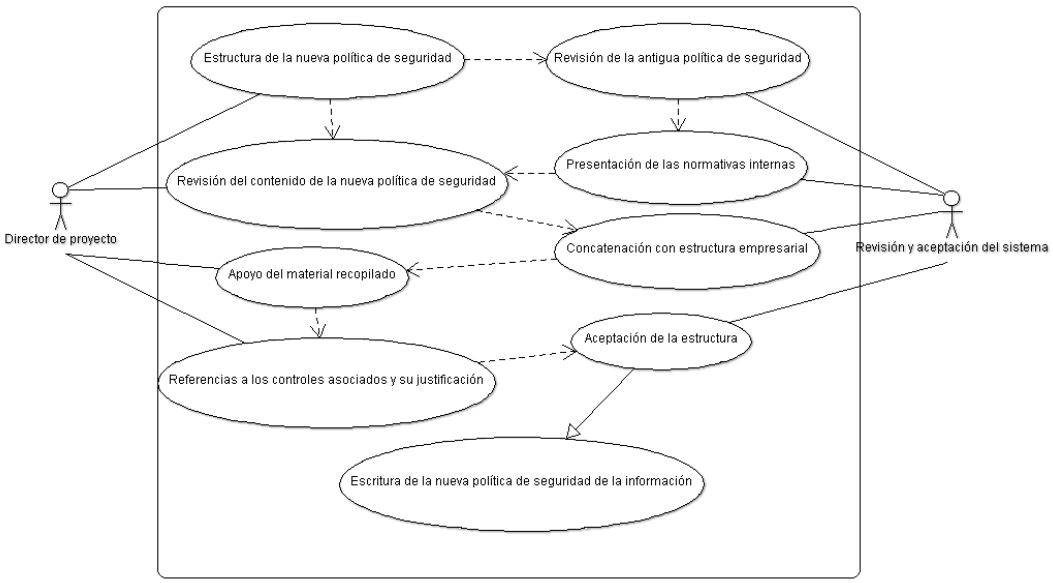
El diccionario de datos se encuentra desarrollado en base al resultado del análisis de riesgo, motivo por el cuál es imprescindible para avanzar en el proceso de desarrollo de un SGSI.

Figura 22: Diccionario de datos – Diagrama de actividades.
Elaborado por: Jean Rodríguez.



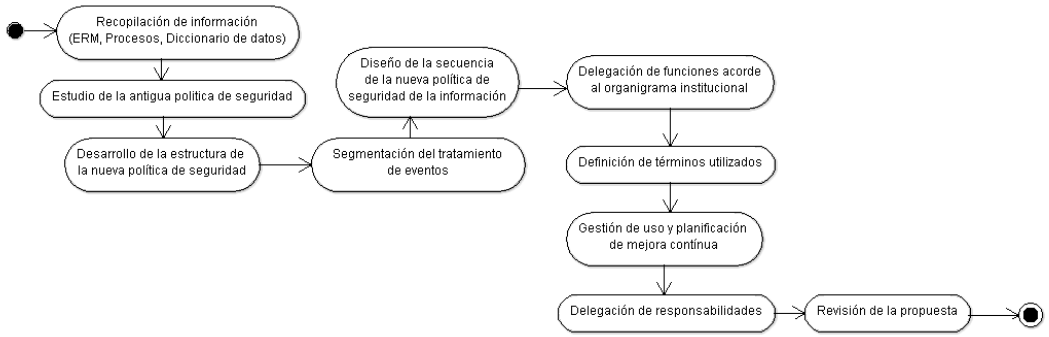
Política de Seguridad:

Figura 23: Política de seguridad – Caso de uso.
Elaborado por: Jean Rodríguez.



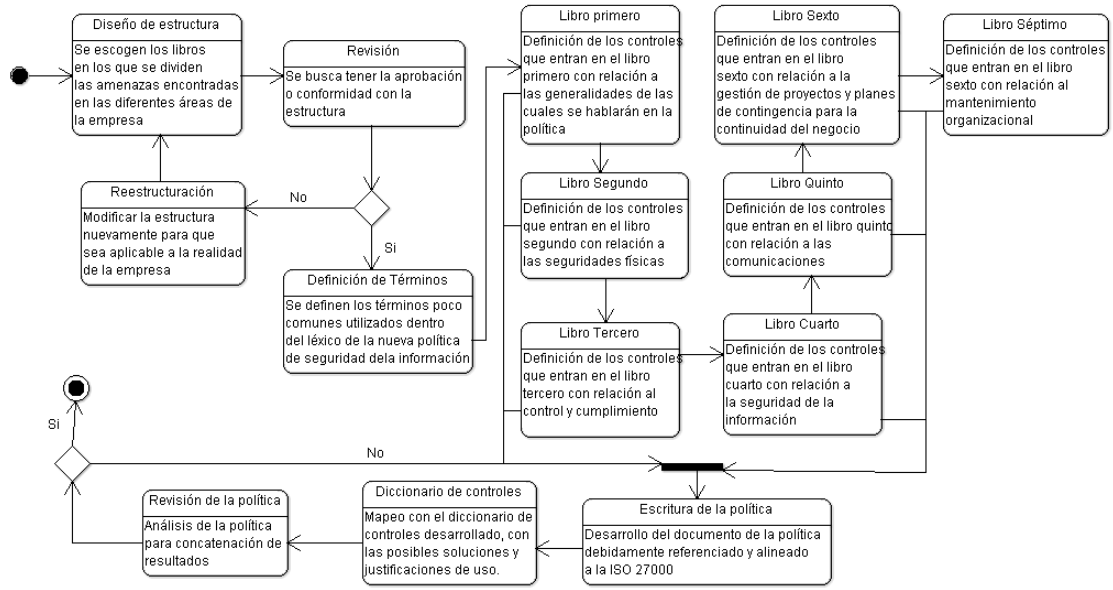
El cuadro presentado muestra la interacción que existe entre la persona que está a cargo de desarrollar el nuevo SGSI y la empresa.

Figura 24: Política de seguridad de la información –Diagrama de actividades.
Elaborado por: Jean Rodríguez.



Se presenta el lineamiento general del desarrollo de la Política de seguridad de la información, tomando en cuenta los macro procesos necesarios, los cuales se desarrollan como etapa final del proyecto y dan como resultado la nueva política de seguridad de la información.

Figura 25: Política de seguridad de la información – Diagrama de estado.
Elaborado por: Jean Rodríguez.



Se muestra la manera de trabajar la nueva política en fase de desarrollo, se requiere la aceptación de cada una de las secciones a trabajar y específica cuales son.

CAPÍTULO III

RESULTADOS

3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.1.1. Introducción:

La política de seguridad de la información desarrollada para la COOPCCP es el resultado de todos los procesos mencionados con anterioridad, los análisis del ERM, el diccionario de controles a utilizar, el organigrama de la compañía, son solo algunos de los puntos importantes tomados en cuenta. Dentro del desarrollo de la misma incide mucho el criterio de la persona que desarrolle el proyecto ya que existen factores de importancia que no pueden ser registrados mediante matrices o encuestas, sino que se ajustan a la necesidad de más de 10 áreas de trabajo.

En el tiempo de desarrollo del proyecto se fueron identificando problemas de seguridad que en un principio no se llegaron a notar incluso con las técnicas de recolección de información, este evento sumado a los problemas y eventualidades que ocurrieron en la época tales como los cambios en la normativa de los entes de control, nuevas herramientas tecnológicas para control del canal de información y el terremoto ocurrido en las costas ecuatorianas el 16 de Abril el cual, puso en marcha varias áreas de la COOPCCP, quienes empezaron a realizar planes de continuidad de negocio y aplicaciones genéricas de planes de contingencia.

Con el tiempo los eventos de riesgo fueron fácilmente identificables y direccionaron a tres problemáticas a las cuales se les debe poner énfasis:

1. La importancia de tener personal especializado para el tratamiento de la seguridad de la información que pueda desempeñar todas las funciones requeridas dentro de la COOPCCP.
2. La falta de conciencia sobre la seguridad de la información dentro de la compañía, motivo por el cual nunca se pensó en la implementación de una política más allá de un requerimiento de los organismos de control.
3. Las fallas de seguridad dentro del corazón de la empresa. Sin el debido tratamiento de la información, con el tiempo se han creado grandes vulnerabilidades que día a día, año a año han dificultado su solución.

Sin duda la implementación de una política de seguridad es necesaria para el correcto manejo de cualquier institución, incluso tras la implementación de ciertos controles dedicados a sectores críticos, se podrían ver mejoras a nivel productivo, económico y social.

3.1.2 Normativas utilizadas:

- La política de seguridad de la información se desarrolló bajo la norma ISO/IEC: 27000 en su versión del año 2005, de manera más específica 27002(Ver anexo 8), la cual muestra los controles a aplicar ante las vulnerabilidades dentro de una empresa, esto es debido a que ésta se encuentra dividida de mejor manera para la realidad de las empresas dentro de los límites nacionales ya que da una segmentación más amplia para el tratamiento de controles físicos no digitalizados y los perímetros de seguridad son mejor esquematizados.
- También se contó con el análisis de la normativa TIA-568B para los sistemas de cableado estructurado, sin hacer énfasis en el uso definido de esta norma, se estudió las directrices para su posible implementación dentro de la COOPCCP.

- Resultado del trabajo conjunto con el área de Riesgos, se realizó el tema de tesis contemplando también la resolución JB- 2014- 3053 de la Superintendencia de Bancos (Ver anexo 9) que ayuda con definiciones pertinentes para el desarrollo del proyecto.
- Así también se tomaron consideraciones de lo que dice el Código del trabajo Ecuatoriano, Constitución de la República del Ecuador, Código penal, Código Civil. Normativas a las cuales la política de seguridad de la información debe estar alineada.

3.1.3 Desarrollo:

Para comenzar con el desarrollo de la política de seguridad se dio una introducción de propiedad de la misma, la cual prohíbe la reproducción total o parcial de la misma. Como segundo punto está la estructura de la política, para ello se decidió separarla por libros, de acuerdo a los puntos más importantes para la COOPCCP. A continuación se presenta esta distribución:

1. **Libro Primero: Generalidades.-** Para el desarrollo del primer libro se consideró el tipo de información general que existe dentro de la política, también se definió el tipo de personal que debe responder ante posibles eventos de riesgo, toda actividad desempeñada en la empresa es una amenaza potencial, por lo que se prevé tener responsables de diferentes áreas supervisando este tipo de eventos. Define también el alcance de la política y el tipo de interacción que tiene con diferentes organismos de regulación, proveedores de servicios, etc. Todo esto se desarrolló en función de los objetivos organizacionales frente a la política y los compromisos que la misma adopta para el correcto funcionamiento de la misma. Se refiere también a los tipos de

sanciones aplicables para el personal o terceros que llegasen a infligir la política de seguridad.

2. **Libro Segundo: Seguridades Físicas.-** El libro de seguridades físicas contempla en primera instancia los objetivos organizacionales, y la aplicación de la misma para los tipos de recursos que se manejen dentro de la COOPCCP. Asignando también al responsable principal de cumplimiento de lo estipulado dentro de la misma sin obviar que el trabajo debe ser realizado conjunto a diferentes responsables de áreas dependiendo de la actividad evaluada. Se tratan todo tipo de problemáticas de accesos físicos con los controles de la ISO 27002 los cuales dan una guía para ubicar las actividades a realizar y finalmente se enuncian sobre puntos que deben ser tomados en cuenta para la adquisición de un seguro para la COOPCCP
3. **Libro Tercero: Control y Cumplimiento.-** Trata directamente la seguridad en el área de Recursos humanos, la importancia de la seguridad de la información dentro del área y su manera de proceder ante eventualidades. En este capítulo se habla también de varios controles preventivos referentes al ingreso de personas y define las responsabilidades ante eventos con terceros. Trata también del desempeño de las funciones dentro del área de cumplimiento con las diferentes políticas de proceder tales como “Conozca a su cliente”, “Conozca a su personal”, “Conozca a su corresponsal”, etc. El capítulo termina con las políticas de prevención de lavados de activos y las sanciones debidas en el caso de infligir cualquier arista de la presente política.
4. **Libro Cuarto: Seguridad de la Información.-** Dentro de la seguridad de la información se habla primero de la preservación de los distintos factores que aseguran la recepción íntegra de los mensajes. Los cuales se notan al inicio del capítulo. Más adelante se definen las principales funciones relativas a la seguridad de la información en la que se expresa las responsabilidades del personal definido en el Libro Primero

pero asociados a la seguridad de la información. Un punto importante dentro del capítulo es la manera que se detalla de manejar la información en relación a la confidencialidad, Integridad y Disponibilidad de la misma. Dando así un sistema a la COOPCCP para el manejo de su información y posterior actualización en la definición de los procesos críticos.

5. **Libro Quinto: Comunicaciones.-** Dentro de éste capítulo se hablan de los objetivos organizacionales ante las comunicaciones ya sean estas controles de accesos remotos, teletrabajo, gestión de red, etc. Que tengan como intermediaria a la red de la empresa o que en su tráfico exista información relevante. Se expresa también el uso de controles, la administración y actualización de los mismos por parte de diferentes responsables dependiendo de la gravedad de la incidencia y la manera de proceder.
6. **Libro Sexto: Continuidad del negocio.-** Dentro de la continuidad del negocio se hablan de planes de acción y todo control que venga derivado de el mismo, lo cual genera la delegación de una persona responsable de la seguridad de encargarse de gestionar todo este tipo de eventos, así mismo cuenta también con los objetivos de la empresa frente a este capítulo y la manera de proceder para mantener los procesos de continuidad de negocios siempre disponibles y eficientes.
7. **Libro Séptimo: Seguridad tecnológica y mantenimiento.-** Dentro de la seguridad de la información se encuentra también el mantenimiento de equipos tecnológicos dedicados y genéricos, la política de seguridad pone a conocimiento el personal responsable encargado del manejo del mantenimiento así como su manera de proceder dependiendo del activo, sistema o proceso que requiera atención.

Para el desarrollo de los diferentes capítulos además se tomaron en cuenta tres consideraciones: los objetivos del libro, las personas involucradas directamente con él y la definición de los controles de la ISO 27002.

3.1.4 Manual:

El manual de la política de seguridad fue presentado a manera de libro (Ver anexo 10) y entregado a cada uno de los líderes de proceso, quienes debieron firmar un documento desprendible de acuerdo que fue guardado por la persona responsable de la Seguridad de la COOPCCP para el caso que se presenten situaciones que involucren al personal de la compañía.

3.1.5 Muestra:

A continuación se encuentran extractos de la política de seguridad de la información que muestran su desarrollo en cada uno de los libros. Debido al acuerdo de confidencialidad que existe en este documento, los datos encontrados reflejo del trabajo realizado se encuentran resumidos y presentados a manera de muestra, mas no representa el producto entregado.

El epítome de normas, leyes y políticas principales que componen este documento se describe a continuación: Norma ISO/IEC 27002, Código del trabajo Ecuatoriano, Constitución de la República del Ecuador, Código penal, Código Civil, Resolución JB- 2014- 3053 Superintendencia de Bancos.

Toda información encontrada en este documento está desarrollada a base a un análisis de los procesos, procedimientos, actividades y formas de tratamiento de la información manejado en las diferentes áreas de la COOPCCP. Estructurando la presente política en un esquema abierto para su aceptación e implementación dentro de la compañía.

LIBRO PRIMERO
GENERALIDADES

Art N. La compañía.- COOPERATIVA DE AHORRO Y CRÉDITO COMERCIO, CONSTRUCCIÓN Y PRODUCCIÓN – COOPCCP LTDA. Es una empresa ecuatoriana que fue puesta en funcionamiento mediante acuerdo Ministerial 1841 del 28 de Julio de 1988 por parte del Ministerio de Bienestar Social., a la misma que para efectos de la presente política se le denominará como "La compañía" o "COOPCCP".

Art N. El objeto general.- Es prestar servicios de intermediación financiera en captaciones con planes de ahorro a la vista, ahorro futuro y depósito a plazo fijo; Colocaciones con Créditos de consumo, microcrédito, crédito de vivienda y crédito comercial; Servicios con acreditación de nómina, servicios exequiales, seguro de desgravamen, tarjeta de cajero, transferencias, remesas, bono de vivienda; y el uso de sus instalaciones para cancelación de servicios públicos, privados, entre otros.

Art N. Operación de la compañía.- Consta dentro del territorio ecuatoriano, en función de las localidades denominadas "sucursales" que se distribuyen por regiones. Las actividades que requieran de un contacto exterior deben ser debidamente manejadas con permisos provistos por Gerencia General, área que posea conocimiento continuo de las posibles excepciones. Tales pueden ser capacitaciones, continuidad en el plan de negocio, adquisiciones o mercadeo. De no ser el caso todas las operaciones realizadas por la compañía se deben llevar a cabo dentro del territorio nacional.

Las actividades se encuentran limitadas, motivo por el cual se prohíbe expresamente el uso de los activos de la empresa, personal, herramientas y delegación de recursos para la práctica de actividades ajenas a La Compañía o a cualquier actividad que se aleje de la línea de negocio que sigue la misma.

Art N. La política.- Por medio del presente documento se muestran los principios básicos de La compañía así también como la planeación para el cumplimiento de metas internas u objetivos de la empresa, contemplando en todo momento los derechos y responsabilidades de los que gozan los empleados como lo estipula el código penal y de trabajo Ecuatoriano para la consecución de los intereses organizacionales.

De manera general se cuentan con los permisos de operación, funcionamiento y bomberos. En el caso de necesitar permisos extras en áreas tales como marketing para la difusión y promoción de La Compañía dentro de los diferentes Gobiernos Autónomos Descentralizados - GAD´s, se gestionan en medida de su importancia e interés organizacional.

También, se denota que la presente política de seguridad afectará a toda La compañía, en todos sus niveles organizacionales, desde su Gerente General hasta el personal que esté contemplado dentro de las operaciones de la misma, quienes se relacionen directa o indirectamente con ella, sean estos empleados, clientes o personas externas como proveedores de servicios o tercializadores.

LIBRO SEGUNDO
SEGURIDADES FÍSICAS

Art N. Los objetivos principales son los siguientes:

a) Resguardar los activos físicos de la empresa dentro y fuera de la misma velando por resguardar la integridad de la información que contiene.
b) Controlar el ingreso de personas no autorizadas a diferentes áreas de La Compañía incluyendo el cuarto de tratamiento de la información, áreas seguras, etc.
c) Proporcionar protección adecuada a los riesgos identificados en toda La Compañía.
d) Controlar a nivel organizacional los posibles eventos emergentes que se den mediante controles de acceso remotos de fácil supervisión.

Esta política se aplica para todo tipo de recurso físico: Instalaciones, equipos de trabajo, equipos dedicados, etc.; perteneciente a la COOPCCP tanto en la matriz como en las sucursales. El responsable de la seguridad de la información junto con el responsable del área y los responsables de los recursos definirán, según corresponda, las medidas de seguridad física por factores internos y factores externos que puedan afectar a La Compañía ya sea en la matriz como en las sucursales teniendo en cuenta que la situación climática cambia para la región costa e insular.

Art N. Perímetros de seguridad interna y externa.- La protección física se llevará a cabo con la creación o mejora de medidas de control ubicadas en los sitios que se encuentren recursos o herramientas consideradas importantes. La Compañía utilizará perímetros de seguridad que serán usados para proteger cualquier área que contenga datos importantes como el centro de tratamiento de la información, área de bóvedas, bodega de documentos, registros y toda área considerada como crítica para para el funcionamiento de las operaciones de La Compañía, Un perímetro de seguridades está delimitado por barreras, controles de acceso y en casos puntuales, personal.

Art N. Controles de acceso Físico.- Las áreas protegidas deberán contar con controles de acceso físico que serán gestionadas por el responsable de la Seguridad, con la finalidad de permitir el acceso solo a las personas autorizadas, cumplirán lo siguiente:

1. Censa el acceso autorizado a áreas designadas.
2. Revisión de la instrumentaría o herramientas que posee la persona.
3. Debido etiquetado e identificación como control de acceso
4. Ajuste de nivel de acceso que maneja
5. Asegura la seguridad del personal dentro de la empresa y los activos

Otros posibles controles pueden hondar dentro de este punto si el responsable de la Seguridad cree necesaria la implementación de controles extra, tales como:

1. Tiempo de acceso máximo
2. Código de ingreso y código de salida
3. Registro físico y/o digital de salida
4. Etc.

LIBRO TERCERO
CONTROL Y CUMPLIMIENTO

Art N. Seguridad del personal.- Se deberá cumplir los objetivos de seguridad del personal los cuales son:

a) Establecer herramientas y protocolos para el trato de eventos especiales en caso de que ser necesario
b) Desarrollar una conciencia de uso de la política de seguridad de la información desde los primeros acercamientos a la empresa.
c) Proteger las plazas de trabajo de personas no aptas para el manejo de información sensible
d) Establecer controles dentro de la COOPCCP que aseguren el desarrollo de actividades con empresas legales, funcionales y que manejen el control pertinente de sus activos así como un correcto manejo de accesos para con sus clientes y ellos mismos.
e) Segmentar las responsabilidades relativas a la seguridad de la información en los diferentes niveles del proceso de selección del personal, cumplimiento de las normas para cliente, empleado y terceros; y las posibles repercusiones legales que puedan darse dentro de dichos procesos.

Este punto de la política se aplica a todas las personas de La Compañía; Personal interno, clientes, corresponsales, proveedores, aspirantes de ingreso, etc. Que requiera un proceso de ingreso a la misma o prestación de servicios sean estos en nombre de una empresa o persona natural.

Art N. Comunicación de incidentes y vulnerabilidades.- Los incidentes relativos a la seguridad de la información serán comunicados a través de medios apropiados lo más pronto que sea posible. Se establecerá un procedimiento formal para la comunicación y respuesta del evento, indicando la acción que se llevará a cabo acorde al tipo de incidente. Dicho procedimiento debe prepararse contemplando una supuesta violación de seguridad o incidente, para la cual el profesional de seguridad deberá tomar responsabilidad tan pronto como se lo haya puesto en conocimiento, también deberá asignar los recursos necesarios para la solución del problemas. En este proceso deberá mantener informado al comité de seguridad del incidente y las acciones tomadas para contrarrestar el evento.

Art N. Prevención de lavado de activos.- Se deberá mantener en todo momento el uso de controles preventivos para detección de lavado de activos, dichos controles deben ser definidos por el responsable de seguridad en colaboración con el comité de seguridad y los miembros del mismo que se crea pertinente. El mantenimiento de dichos controles y avalúo de su efectividad deben ser manejados bajo petición del responsable de cumplimiento por el responsable de seguridad.

LIBRO CUARTO
SEGURIDAD DE LA INFORMACIÓN

Con objeto de delimitar el alcance de los principales conceptos utilizados dentro del presente capítulo, se realiza una descripción de las definiciones encontradas dentro de la política de seguridad.

Art N. Seguridad de la información.- La seguridad de la información se entiende como la preservación dentro de un documento sea éste físico o digital de las siguientes características:

1. **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
2. **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento
3. **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran
4. **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
5. **Audibilidad:** define que todos los eventos deben poder ser registrados para su control posterior.
6. **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
7. **No repudio:** se refiere a evitar que cuando alguien haya enviado o recibido información alegue ante terceros que no la envió o recibió.
8. **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
9. **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Art N. Información.- Refiere a todo tipo de dato que sea comunicado dentro de la empresa y tenga algún valor para la misma, sea éste dado en cualquier formato tales como adaptaciones, transcritos de la información verbal tratada en reuniones, datos cuantificables, registros de incidencias, informes de auditorías, gráficas, etc. Y se encuentren en cualquier medio físico o virtual, sean estos en papel, contenido audiovisual, medios magnéticos, etc.

Art N. Clasificación de la información.-

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad:

a) confidencialidad,
b) integridad,
c) disponibilidad.

Confidencialidad	Integridad	Disponibilidad	Total
3	3	3	27
3	3	2	18
3	3	1	9
3	2	3	18
3	2	2	12
3	2	1	6
3	1	3	9
3	1	2	9
3	1	1	3
2	3	3	12
2	3	2	12
2	3	1	6
2	2	3	12
2	2	2	8
2	2	1	4
2	1	3	6
2	1	2	4
2	1	1	2
1	3	3	9
1	3	2	6
1	3	1	3
1	2	3	6
1	2	2	4
1	2	1	2
1	1	3	3
1	1	2	2
1	1	1	1

18-27	CRÍTICA
12-17	SENSIBLE
6-11	DE USO INTERNO
1-5	DE USO EXTERNO

LIBRO QUINTO
COMUNICACIONES

Art N. Los objetivos principales son los siguientes:

a) Prevenir el acceso no autorizado de terceros a los equipos y redes dentro de La Compañía por vías de comunicación.

b) Restringir el uso de medios no autorizados para minimizar el impacto generado por el uso indebido de medios extraíbles.
c) Mantener los protocolos de seguridad referentes al uso y administración de contraseñas para los sistemas y equipos de la COOPCCP.

Art N. Administración de contraseñas críticas.- El protocolo de administración de contraseñas críticas será diseñada en un trabajo conjunto con el responsable de Operaciones, con quien se designará los controles bajo los que se resguardará y se contarán para proteger su uso no autorizado.

Art N. Administración de contraseñas de usuario.- Las contraseñas de usuario se encuentran estrictamente bajo la administración del responsable de la Seguridad, quien debe tener además un registro físico y digital de la gestión que se da a la misma.

Art N. Autenticación de usuarios para conexiones externas.- El responsable de TI es el encargado de gestionar los controles para la administración de los usuarios en conexiones externas a La Compañía, los cuales deben guardar registros de los usuarios que realicen un proceso de login, capturando sus contraseñas para poder usarla en comprobaciones de ser necesarias.

Art N. Administración de medios removibles.- Es responsabilidad de todos conocer las políticas de seguridad de medios removibles para su uso dentro de las diferentes áreas organizacionales, el responsable de Seguridad es el único encargado de definir este tipo de normativas y pasos a seguir, bajo la dirección del mismo, el responsable de TI acompañará en la aplicación de dicho control para restringir o conceder permisos de uso aceptable de los puertos para medios extraíbles. Como uno de sus demás funciones es la socialización de dichos protocolo y el mantenimiento que requiera.

Art N. Emplazamiento y distribución de equipos.- El equipo tecnológico será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

Art N. Suministros de energía.- El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

LIBRO SEXTO
CONTINUIDAD DEL NEGOCIO

Art N. Seguridad del Negocio.- Los principales objetivos son los siguientes:

a. Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento operativo.
b. Establecer responsabilidades y procedimientos para la gestión de la operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y definición de funciones.

c. Cada Responsable Operativo, junto con el Responsable de Seguridad y el Responsable del Área Tecnológica, determinará los requerimientos para resguardar los recursos por los cuales es responsable.

Art N. Continuidad de las Operaciones.- Sus objetivos principales son:

1. Minimizar los efectos de las posibles interrupciones de las actividades normales de La Compañía (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
2. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
3. Maximizar la efectividad de las operaciones de contingencia de La Compañía con el establecimiento de planes que incluyan al menos las siguientes etapas:

    a. **Activación**: Consistente en la detección y determinación del daño y la activación del plan de emergencia.
    b. **Reanudación**: Consistente en la restauración temporal de las operaciones y recuperación del daño producido.
    c. **Recuperación**: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

4. Asegurar la coordinación con el personal de La Compañía y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

LIBRO SÉPTIMO
MANTENIMIENTO ORGANIZACIONAL

Art N. Objetivos de la seguridad y mantenimiento de equipos.- Dentro de los objetivos de este libro de la política de seguridad de la información se encuentran los siguientes:

a) Mantener en línea todos los controles existentes dentro de la COOPCCP para asegurar el total funcionamiento dentro de todas sus áreas organizacionales.
b) Implementar medidas de protección para los empleados de la cooperativa y los recursos que utilizan.
c) Manejar los recursos internos y externos de La Compañía para evitar problemas de producción.
d) Preparación de ambientes seguros dentro de la COOPCCP para reuniones con socios, presentaciones de productos y asegurar la continuidad del negocio.

Art N. Imagen empresarial.-El cuidado de la imagen empresarial deberá ser manejada por el responsable de Servicios Generales conjunto trabajo con el responsable de operaciones o en su defecto con el responsable de Marketing, quienes pueden hacer las solicitudes formales para dar mantenimiento a todo material relacionado con la imagen empresarial, tras la aceptación éstos se encargarán del manejo de contratos, permisos y etiquetado de la información debido que se remarca dentro de la presente política de seguridad.

Art N. Papelería.- El responsable de Servicios Generales es el único encargado de verificar la existencia de productos de papelería usados por la COOPCCP, en caso de que surja algún requerimiento por parte de otras áreas deben ser reportadas a la persona encargada para que pueda tomar acciones. En caso de registrarse alguna irregularidad es pertinente poner en conocimiento al responsable de la seguridad.

Art N. Contratación de servicios.- Se debe registrar cada una de las propuestas llegadas al responsable de Servicios Generales cuando sea requerida la contratación de servicios dentro de la COOPCCP para cualquier evento que se realice dentro de la misma. El responsable e Servicios Generales debe guardar siempre una copia del contrato con el acuerdo de nivel de servicio para su registro y etiquetado pertinente que sigan las lineaciones de la presente política de seguridad de la información.

Art N. Mantenimiento de bienes.- El encargado de mantener todos los bienes de la COOPCCP tanto sea en el edificio matriz como en las sucursales será el responsable de Servicios Generales, quien deberá seguir una serie de pasos debidamente protocolizados para la identificación, propuesta y ejecución del mantenimiento a los bienes de la empresa con una frecuencia de revisión anual.

Art N. Servicio al cliente.- El servicio al cliente será tratado por la persona responsable del Servicios Generales, quien procederá siempre tras la documentación formal pertinente explicando el tipo de problema general, firmado por el cliente que solicita realizar la reunión.

CAPÍTULO IV

DISCUSIÓN

4.1 Conclusiones

- Tras conocer la línea de negocios y más específicamente los procesos que se realizan en la COOPCCP, se notó una gran diferencia del producto genérico al producto final denominado “política de seguridad”. Ya que tras cada reunión con los profesionales designados como “líderes de procesos”, se notó que manejaban ciertas actividades extras, como el control de accesos y permisos en plataformas web, las cuales deberían ser competencias de un departamento de Seguridad de la Información.

- En el análisis de riesgos se pudo evidenciar que según el criterio de los profesionales representantes de cada área, existen vulnerabilidades que no han sido tratadas con ningún tipo de control y muchas otras que si bien existe el control, éste no contrarresta ni mitiga el riesgo. En base a esa información se pudo clasificar los riesgos, dando a conocer los procesos críticos que requieren mayor atención. Al presentar el informe del ERM se encuentra explicado cada uno de los controles por aplicar.

- Para la creación del diccionario de controles se trabajó conjunto con la norma ISO27002 – 2005 con la que se definieron los controles a aplicar y se encuentran referenciadas dentro de la normativa. Para ello se presentó una matriz con cada uno de los eventos encontrados, vulnerabilidad que genera y manera de mitigar o eliminarla. Para aquellas que no representan un fuerte impacto y no hace falta aplicar un control debido a que el bien resguardado no supera el valor del activo, se encuentra también la debida justificación.

- La política de seguridad de información dentro de la COOPCCP se encuentra dividida en libros que aseguren su uso sin importar el esquema de organización que lleven, lo que contempla cambios en el crecimiento de la organización. Toda información escrita dentro de la COOPCCP es para uso exclusivo de la misma y debe tener mantenimiento acorde a los cambios que se den dentro y fuera de la empresa. Para ello se requiere de un especialista que pueda hacer cumplir con un ciclo PDCA adecuado.

4.2 Recomendaciones

- Es importante mantener la política de la seguridad de la información actualizada cambiando dentro de un ciclo PDCA en función a las mejoras tecnológicas, los cambios normativos de las entidades de regulación o el uso injustificado de los controles en relación al valor del activo que resguarda.

- En el análisis de riesgos es un proceso que no puede tener fin ya que es utilizado como sustento y único registro del estado de una empresa frente a los riesgos que tiene, es importante notar que después de cierto tiempo en el que se maneja la

política es necesario realizar otro informe de riesgos ya que al presentar el los resultados del ERM se encontrarán explicados cada uno de los controles vigentes y se podrá ver un cambio dentro de las matrices.

- Para el cambio de uso de la norma no es necesario hacer un reajuste a la política de seguridad ya que esta contempla su aplicación en relación a los aspectos de seguridad pero no completamente ligada al uso de la norma. De este modo se asegura que los procesos de cambio por los que tenga que pasar la política sean de acuerdo al crecimiento organizacional y no a los cambios externos.

- No todas las empresas tienen la misma carga laboral ni realidad en su funcionamiento, por lo que es necesario contar con un buen criterio profesional al momento de escoger la versión de las normas a utilizar, el tipo de información que recopilarán las matrices y el flujo de datos que se manejará.

BIBLIOGRAFÍA

- Álvarez, M. D. M. S., Valiño, P. C., & Leguía, A. P. (2007). *La responsabilidad social corporativa (RSC): una orientación emergente en la gestión de las entidades bancarias españolas*. In Conocimiento, innovación y emprendedores: Camino al futuro (p. 135). Universidad de La Rioja.
- Ariza Díaz, A. (2013). *Elaboración de un plan de implementación de la ISO/IEC 27001: 2005*.
- Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.
- Callegari, N. (2016). D*elitos informáticos y legislación. Revista de la Facultad de Derecho y Ciencias Políticas*, (70), 111-118.
- Clementes, R. B. (2000). *Guía completa de las normas ISO 14000*. España: Gestión
- De Lema, D. G. P., Pérez, A. A., & Segura, A. C. F. (1995). *Un modelo discriminate para evaluar el riesgo bancario en los creditos a empresas*. Revista Española de Financiación y Contabilidad, 175-200.
- Estrada, A. C. (2006). *ANÁLISIS DE ISO-27001: 2005*. Documento Digital. Extraído el 24 de Mayo del 2016, Obtenido de http://www.iso27000.es/download/analisis_ISO-27001.pdf
- Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). S*oftware para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)*. Información tecnológica, 26(2), 129-134.
- Orrego, V. M. (2013). *La gestión en la seguridad de la información según Cobit, Itil e Iso 27000*. Revista Pensamiento Americano, 4(6).
- Palacio, J. R. S. (2001). *Dirección Estratégica Bancaria: estado actual y temas de investigación. Cuadernos de Economía y Dirección de la Empresa*, (8), 77-107.

- Palazzi, P. A. (2009). *Los delitos informáticos en el Código Penal. Buenos Aires, Abeledo-Perrot*, 130.
- Perals, M. G. (1994*). Los delitos informáticos en el derecho español.Informática y derecho: Revista iberoamericana de derecho informático*, (4), 481-496.
- Pino, F. J., García, F., Ruiz, F., & Piattini, M. (2005). *Adaptación de las normas ISO/IEC 12207: 2002 e ISO/IEC 15504: 2003 para la evaluación de la madurez de procesos software en países en desarrollo*. In JISBD (pp. 187-194).
- Saizarbitoria, I. H., Fa, M. C., & i Viadiu, F. M. (2005). *Análisis y un modelo de la difusión internacional de las normas ISO 9000 e ISO 14000*. Revista Europea de Dirección y Economía de la Empresa, 14(4), 81-100.
- Sánchez, J. I., & Ignoto, M. J. (1991). *La seguridad informática*. *Instituto de la Pequeña y Mediana Empresa Industrial*.
- Sanfilippo Azofra, S. (2005). *Fusiones y adquisiciones bancarias: características e implicaciones de las operaciones realizadas por las entidades de crédito europeas*. *Universidad de Cantabria.*
- Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. Revista Tecnológica-ESPOL, 28(5).
- Van den Berghe, W. (1998). *Aplicación de las normas ISO 9000 a la enseñanza y la formación. Revista Europea de Formación Profesional*, (15), 21-30.
- Vecchietti, A. R. (2000). *Técnicas de optimización basadas en lógica para problemas discretos/continuos en ingeniería de procesos* (Doctoral dissertation).

ANEXOS

Anexo 1: Carta de Auspicio.

UNIVERSIDAD INTERNACIONAL SEK

COOPCCP
Cooperativa de Ahorro y Crédito

Quito, diciembre 18 del 2015

Srta. Econ.

Esperanza Montalvo

SUBGERENTE GENERAL DE LA COOPERATIVA DE AHORRO Y CREDITO CONSTRUCCIONJ COMERCIO Y PRODUCCION LTDA "COOP.C.C.P"

Presente.-

De mis consideraciones

Yo, JEAN PIERRE RODRÍGUEZ GUERRA, con CI N° 1718164898, estudiante de la Universidad Internacional SEK actualmente cruzando el último nivel de la carrera "Ingeniería en Sistemas Informáticos" quiero solicitar por medio de esta carta, a ustedes Cooperativa de Ahorro y Crédito Construcción, Comercio y Producción - COOPCCP el **AUSPICIO** de mi Proyecto de Tesis de Grado titulado "Diseño y creación de una política de Seguridad de la información (SGSI) basado en la normativa ISO 27000 para la Cooperativa Construcción, Comercio y Producción." la cual dará inicio la primera semana de enero y finalizará en el mes de abril del siguiente año y contará con la tutoría del Ing. Sebastián Grijalva MGS Para apoyar en el desarrollo y culminación del proyecto.

El proyecto de grado se adaptará a las necesidades de la línea de negocios de la empresa realizando los cambios pertinentes.

Atentamente

Sr. Jean Rodríguez G.

Firman:

Eco. Esperanza Montalvo

Subgerente General - COOPCCP

Ing. Sebastián Grijalva MGS

Tutor del Proyecto – Universidad SEK

Anexo 2: Primera reunión – 23 de Diciembre.

UNIVERSIDAD INTERNACIONAL SEK

COOPCCP
Cooperativa de Ahorro y Crédito

DOCUMENTO DE CONSTANCIA

Este documento certifica que el día Miércoles 23 de Diciembre del 2015 a las 11:30 am, nos encontramos reunidos JEAN PIERRE RODRÍGUEZ (Autor de la Tesis) y DANIEL ZURITA(Jefe de tecnologías y comunicaciones COOPCCP) para tratar los temas:

1. Presentación Personal
2. Presentación del tema de tesis
3. Presentación del plan de trabajo
4. Normalización requerida
5. Levantamiento de información
6. Acotaciones y cambios dentro del marco institucional específico
7. Consolidación de días a trabajar dentro de la empresa
8. Programación de futuras reuniones.

Este documento queda como constancia del cumplimiento de la reunión.

Firman

Jean Pierre Rodríguez
Autor de tesis

Daniel Zurita
Jefe de Tecnologías y Comunicaciones
COOPCCP

Anexo 3: Segunda reunión – 6 de Enero.

UNIVERSIDAD INTERNACIONAL SEK

COOPCCP
Cooperativa de Ahorro y Crédito

DOCUMENTO DE CONSTANCIA

Este documento certifica que el día Miércoles 6 de Enero del 2016 a las 15:30 am, nos encontramos reunidos JEAN PIERRE RODRÍGUEZ (Autor de la Tesis) y DANIEL ZURITA(Jefe de tecnologías y comunicaciones COOPCCP) para tratar los temas:

1. Reestructuración del tema de tesis
2. Presentación de la nueva propuesta
3. Presentación del nuevo plan de trabajo
4. Acotaciones y cambios dentro del marco institucional específico
5. Programación de futuras reuniones.

Este documento queda como constancia del cumplimiento de la reunión.

Firman

Jean Pierre Rodríguez
Autor de tesis

Ing. Daniel Zurita MGS
Jefe de Tecnologías y Comunicaciones
COOPCCP

Anexo 4: Tercera reunión – 13 de Enero.

UNIVERSIDAD INTERNACIONAL SEK

COOPCCP
Cooperativa de Ahorro y Crédito

DOCUMENTO DE CONSTANCIA

Este documento certifica que el día Miércoles 13 de Enero del 2016 a las 12:30 pm, nos encontramos reunidos JEAN PIERRE RODRÍGUEZ (Autor de la Tesis), DANIEL ZURITA(Jefe de tecnologías y comunicaciones COOPCCP) y varias personas de diferentes sectores de la COOPCCP para tratar los temas:

1. Presentación Personal.
2. Presentación del tema de tesis.
3. Presentación del plan de trabajo.
4. Levantamiento de información.
5. Acuerdo de inicio de actividades.
6. Consolidación de días a trabajar dentro de la empresa.
7. Recursos a utilizar en el proyecto.
8. Programación de futuras reuniones.

Este documento queda como constancia del cumplimiento de la reunión.

Firman

Jean Pierre Rodríguez
Autor de tesis

Daniel Zurita
Jefe de Tecnologías y Comunicaciones
COOPCCP

Anexo 5: Cuarta reunión – 28 de Enero.

UNIVERSIDAD INTERNACIONAL SEK

COOPCCP
Cooperativa de Ahorro y Crédito

DOCUMENTO DE CONSTANCIA

Este documento certifica que el día Jueves 28 de Enero del 2016 a las 11:30 am, nos encontramos reunidos JEAN PIERRE RODRÍGUEZ (Autor de la Tesis) y DANIEL ZURITA(Jefe de tecnologías y comunicaciones COOPCCP) para tratar los temas:

1. Acuerdo de confidencialidad
2. Análisis de Organigramas
3. Revisión de la antigua política de seguridad
4. Planificación de disponibilidad
5. Revisión del estado de madurez de los procesos
6. Revisión del área de Riesgos
7. Revisión general de procesos levantados

Este documento queda como constancia del cumplimiento de la reunión.

Firman

Jean Pierre Rodríguez
Autor de tesis

Daniel Zurita
Jefe de Tecnologías y Comunicaciones
COOPCCP

Anexo 6: Acuerdo de confidencialidad.

COOPCCP
Cooperativa Financiera

COOPERATIVA DE AHORRO Y CREDITO
CONSTRUCCION COMERCIO Y PRODUCCION LTDA.
Unidad de Tecnología de Información y Comunicaciones

ACUERDO DE CONFIDENCIALIDAD

El contenido del acuerdo es el que figura a continuación.

Contenido

DE UNA PARTE: La Cooperativa de Ahorros y Crédito Construcción Comercio y Producción Ltda (COOPCCP) y en su nombre y representación Ing. Daniel Zurita C. MGS, en calidad de Jefe de Tecnología.

DE OTRA PARTE: el Sr. Jean Pierre Rodríguez Guerra egresado de la carrera de Ingeniería de Sistemas Informáticos de la Universidad Internacional SEK.

Reunidos en la ciudad de Quito, a 28 de Enero del 2016

ANTECEDENTES:

En el mes de diciembre del 2015 el Sr. Rodríguez solicita a la Cooperativa de Ahorros y Crédito Construcción Comercio y Producción Ltda (COOPCCP) el auspicio para el desarrollo de su Tesis de Grado previo a la obtención del título de Ingeniero en Sistemas Informáticos, para esto realiza una presentación del tema a desarrollar, dicha Tesis tiene como enfoque principal el tema de Seguridad de la Información para la COOPCCP.

En el mes de enero se realiza una restructuración del Plan de Tesis con el fin de abarcar las necesidades de la Cooperativa en el tema de Seguridad de la Información

Previo a este acuerdo el 13 de enero se aprueba el AUSPICIO de la Cooperativa para que se den las facilidades en el desarrollo del tema de Tesis al Sr. Rodríguez

OBJETO:

El Sr. Rodríguez ha solicitado a La Cooperativa de Ahorros y Crédito Construcción Comercio y Producción Ltda. (COOPCCP) se proporcione información sobre la infraestructura, servicios, aplicaciones, procesos, manuales vigentes, organigrama estructural, manejo del Área de Riesgos y otros con el fin de iniciar con el desarrollo de la Tesis de Grado para la obtención del título de Ing. en Sistemas Informáticos.

EXPONEN

Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente proyecto, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, propietario y dueño de la referida información.

1

CLÁUSULAS

PRIMERA.- Información Propia.

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, y/o técnicos, suministrada a la otra parte como consecuencia de la solicitud de oferta para el desarrollo del presente objeto del contrato, o en su caso, de los acuerdos a los que se lleguen (con independencia de que tal transmisión sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea) tendrá consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento. Esa información, y sus copias y/o reproducciones tendrán la consideración de Información propia los efectos del presente acuerdo.

SEGUNDA.- Custodia y no divulgación.

Las partes consideran confidencial la Información propia de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de la Cooperativa COOPCCP. Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la Cooperativa COOPCCP por parte del Sr. Rodríguez será recibida por éste con el previo consentimiento de la misma.

TERCERA.- Soporte de la Información propia.

Toda o parte de la Información propia, papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología en el que el suministro fuese hecho bajo la condición de Información propia, con independencia del soporte que la contuviera, tendrá la clasificación de secreta, confidencial o restringida

CUARTA.- Incumplimiento.

El incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante.

QUINTA.- Duración del Acuerdo de Confidencialidad.

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones.

DECIMA.- Legislación Aplicable

El presente Acuerdo de Confidencialidad se regirá por la Legislación Ecuatoriana, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo

será sometido a la jurisdicción de los Tribunales de la ciudad de Quito, con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

Y en prueba de esta conformidad, las partes firman o presente acuerdo, por duplicado y a un solo efecto, en el lugar y fecha.

Ing. Daniel Zurita C
Jefe de Tecnología COOPCCP

Firma

C.C.: 1712774593

Sr. Jean Pierre Rodríguez
Egresado de Ingeniería Universidad SEK

Firma

C.C.: 1718164898

Anexo 7: Documento de constancia del levantamiento de procesos.

UNIVERSIDAD INTERNACIONAL SEK

COOPCCP Cooperativa de Ahorro y Crédito

Documento de Constancia

Mediante el presente documento, se certifica que se llevó a cabo un trabajo conjunto con las personas mencionadas posteriormente con el fin de culminar el proceso de Levantamiento de la información dentro de la COOPCCP como parte de la realización del proyecto de tesis titulado "Diseño y creación de una política de Seguridad de la información (SGSI) basado en la normativa ISO 27000 para la Cooperativa Construcción, Comercio y Producción."

Mismas que firman en constancia de eso:

Área	Líder de proceso / Encargado	Fecha de trabajo	Procesos levantados	Procedimientos levantados	Firma
Comercial	Andrés Zambrano	16-02-2016	9	36	
Jurídico	Margarita León	16-02-2016	8	36	
Tecnologías de la Información	Daniel Zurita	19-02-2016	9	56	
Talento Humano	Erika Otalima	23-02-2016	10	45	
Riesgos	Gabriel Ripalda	23-02-2016	11	56	
Unidad de Cumplimiento	Gloria Martinez	23-02-2016	9	43	
Marketing	Edgar Rubianez	24-02-2016	6	34	
Auditoria Interna	Sandra Rosero	24-02-2016	5	60	
Contabilidad	Cristian Carrera	26-02-2016	2	15	
Desarrollo organizacional	Alberto Vinueza	26-02-2016	2	16	
Operaciones	Marcelo Males	27-02-2016	12	30	
SubGerencia	Esperanza Montalvo	03-03-2016	10	21	
Servicios generales	Octavio Quishpe	03-02-2016	8	40	
Gerencia General	Fernando Beltrán	15-03-2016	4	13	

Anexo 8: ISO/IEC 27002

Anexo 9: JB – 2014 – 3053.

Anexo 10: Libro: Manual de Políticas de seguridad de la información COOPCCP 2016.
Elaborado por: Jean Rodríguez.