ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA COOPERATIVAS DE AHORRO Y CRÉDITO EN BASE A LA NORMA ISO 27001"

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER, EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN, MSC.

AUTOR: ING. ANIBAL RUBEN MANTILLA GUERRA
amantilla@andinanet.net

DIRECTOR: ING. JAIME FABIAN NARANJO ANDA, MSC
subdecano.sistemas@epn.edu.ec

Quito, Junio del 2009

DECLARACIÓN

Yo, Ing. Aníbal Rubén Mantilla Guerra declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Ing. Aníbal Rubén Mantilla Guerra, bajo mi supervisión.

_____

Ing. Jaime Naranjo, Msc
DIRECTOR DE TESIS

AGRADECIMIENTO

A todos quienes han hecho posible esta Tesis.

DEDICATORIA

A mi amado padre Wilson Mantilla,
por todo el amor prodigado.

A mi amado Sobrinito, Isidro Montenegro,
Por toda la ternura entregada.

INDICE GENERAL

CAPÍTULO 2.

CAPÍTULO 3.

ÍNDICE DE FIGURAS

FIGURAS DEL ANEXO 3

Estadísticas de las Cooperativas de Ahorro y Crédito Ecuatorianas

INDICE DE TABLAS

RESUMEN

En esta Tesis se diseñó un Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito, en base a la norma ISO 27001, la Ley de la Superintendencia de Bancos y Seguros, la Ley de Cooperativas de Ahorro y Crédito, considerando además, su evolución y problemática en el Sistema Financiero Nacional. De manera metodológica, científica y objetiva, se muestra como identificar, evaluar y gestionar el riesgo, en Cooperativas de Ahorro y Crédito, presentando incluso ejemplos para su aplicación práctica. Este diseño de Sistema de Gestión, fue aplicado a una Cooperativa de Ahorro y Crédito – Caso de Estudio, demostrándose la validez del mismo. En los Anexos se presenta la Norma ISO 27001 y sus exigencias documentales, estadísticas de las Cooperativas de Ahorro y Crédito Ecuatorianas, así como cuestionarios para determinar las condiciones en las que se encuentra su Seguridad de la información.

INTRODUCCIÓN

El trabajo de realización de esta Tesis de Grado de Maestría, lo inicié con un análisis completamente amplio de posibilidades de Temas, relacionados directamente y de la mejor manera con mi formación técnica de Ingeniería en Electrónica y Control, y mi formación de posgrado a nivel de Maestría, en Gestión de las Comunicaciones y Tecnologías de la Información. Esto a su vez, directa y estrechamente relacionado con las necesidades del País y de nuestra sociedad, y de los más altos propósitos Institucionales de la Escuela Politécnica Nacional, de contribuir al desarrollo del País, como lo ha venido haciendo a lo largo de su fructífera existencia. Por otra parte también estuvo la consideración fundamental de que el trabajo de desarrollo de la Tesis estuviera enmarcado en los más altos y actuales niveles y avances de la ciencia y la tecnología. También mantuve incluidas, las orientaciones fundamentales impartidas por la Facultad en la que estudié la Ingeniería, y la Facultad en la que estudié la Maestría.

Con el avance de los análisis correspondientes, fui definiendo el campo de realización de mi Tesis, en el ámbito financiero del País. Después fui haciendo diversos análisis de posibilidades, llegando a concluir, después de los análisis indicados, estudios y numerosas consultas, que el Tema estaría orientado a las Cooperativas de Ahorro y Crédito, por la cantidad de este tipo de Instituciones que existen en el País, por el monto de participación en el Sistema Financiero Nacional, por el número de personas vinculadas al Sistema Cooperativo, y por la evidente necesidad de introducir mejoras en el manejo de las Cooperativas de Ahorro y Crédito, en el aspecto de la Seguridad de la Información. La Ciencia y Tecnologías aplicables, no se utilizan aún en nuestro medio, al menos en forma significativa, y son tendencias mundiales que van ganando importancia en cada vez más países, a partir de los del primer mundo, con el fin de lograr significativas y muy importantes mejoras, para hacer de las Organizaciones, como las Cooperativas de Ahorro y Crédito, Instituciones con las mejores condiciones de eficiencia, seguridad, crecimiento, y lo que quizá es especialmente importante en la actualidad, los más altos índices de competitividad, a nivel local, regional y global, de acuerdo a las exigencias de evolución a nivel mundial.

En consecuencia, y relacionando de la mejor manera posible, las características de mi formación en la Maestría, y lo anteriormente expuesto en relación con las Cooperativas de Ahorro y Crédito, llegué a determinar que la mejor opción era realizar la Tesis sobre el **"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA COOPERATIVAS DE AHORRO Y CRÉDITO EN BASE A LA NORMA ISO 27001" .**

El contenido de la Tesis, en resumen es el siguiente: Introducción; Marco de referencia; Diseño del Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito; Caso de estudio; Conclusiones y recomendaciones; Bibliografía; Anexos; Glosario.

Junto con todas las consideraciones ya indicadas, siempre he tenido presente la idea de producir un documento que fuera de lo más útil posible para nuestro País, que me deje la satisfacción plena de haber correspondido a través este trabajo, con la sociedad que me permitió obtener la elevada formación técnica que poseo, y con el concepto tan alto y trascendente que es el lema de la Escuela Politécnica Nacional, de que **"el bienestar del hombre proviene de la Ciencia"**

He puesto mis mejores esfuerzos en todo sentido, para lograr de la mejor manera estos propósitos.

La Tesis, gracias a todo lo indicado, ha sido realizada exitosamente.

CAPÍTULO 1.

MARCO DE REFERENCIA

Se analiza la naturaleza de los Sistemas de Gestión de Seguridad de la Información, en sus cuatro aspectos básicos: Organización, Personas, Tecnología, y el Aspecto Legal. Se explica la naturaleza, evolución y ciclo metodológico de la Norma ISO 27001.

De manera resumida se presenta las Ley de Cooperativas de Ahorro y Crédito, indicando las responsabilidades y atribuciones de las personas al interior de la misma. Se analiza las estadísticas más trascendentes para la Tesis, de las Cooperativas de Ahorro y Crédito.

Con estos tres elementos, es decir, Sistemas de Gestión de Seguridad de la Información, Ley de Cooperativas de Ahorro y Crédito, y la Norma ISO 27001, se procede a presentar y analizar la problemática y desafíos que deben afrontar en un ámbito nacional e internacional.

1.1 NATURALEZA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para toda organización, es fundamental contar con un sistema de gestión de seguridad de información. Numerosas organizaciones creen tener sistemas eficientes y eficaces para proteger y asegurar la información; tienen controles, software para aplicar los controles, diseñan controles, pero los aplican solo cuando aparecen los incidentes de seguridad; de manera que actúan solo de forma reactiva, sin tener un enfoque claro y bien estructurado de un sistema para gestionar la seguridad de la información.

En la organizaciones se requiere un sistema que permita asegurar la información de manera preactiva, sin embargo, hay organizaciones que han diseñado verdaderos sistemas de gestión de seguridad de la información, pero que al momento resultan caducos, o incluso no aplican sus controles; otras organizaciones ni siquiera cuentan con un sistemas de seguridad de la información.

La seguridad de la información involucra a la tecnología, las personas, la estructura organizacional, las normativas, lo cual hace necesario un amplio conocimiento sobre la gestión de todos estos recursos. Sin embargo, esta gestión puede servir de parcialmente, poco o nada si existen fallas de hardware, de

software, fallas humanas, desastres naturales, ataques terroristas, entre otros, sin que la organización haya estado preparada para estos eventos.
Es fundamental en todo este proceso, saber de proteger, de qué proteger, y cómo proteger, esta es la clave para poder direccional adecuadamente el diseño, la implantación y el mejoramiento continuo del sistema de gestión de seguridad de la información.

Dada la competencia que la globalización y las nuevas formas de comercio internacional, las empresas, sin importar su tamaño, su actividad o ubicación, deben estar preparadas para asegurar su información, de manera preactiva, de manera tal que su productividad mejore, y alcance sus objetivos institucionales.

1.1.1 SEGURIDAD INFORMÁTICA

Seguridad de información es mucho más que establecer firewalls, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, o guardar copias de seguridad en bóvedas.

"Seguridad de información es determinar qué requiere ser protegido y por qué, de qué debe ser protegido y cómo protegerlo."

La seguridad informática es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Dependiendo del tipo de información manejada y de los procesos realizados por una organización, esta podrá destinar más o menos recursos a garantizar la confidencialidad, la integridad o la disponibilidad de sus activos de información.

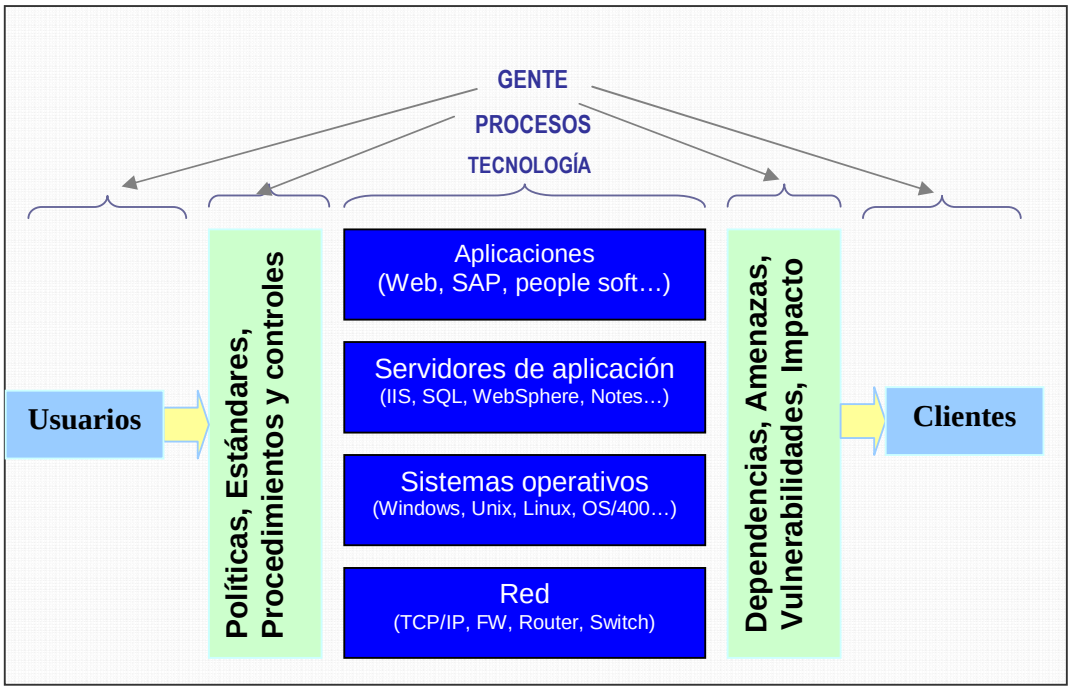

FIGURA 1.1 Elementos de un sistema informático [1]
ELABORADO POR Ing. Mantilla Aníbal

La seguridad del sistema informático depende de varios factores:

- La sensibilización de los directivos y responsables de la organización, que deben ser concientes de la necesidad de destinar recursos a esta función.
- Los conocimientos, las capacidades e implicaciones de los responsables del sistema informático: dominio de la tecnología utilizada en el sistema informático y conocimiento sobre posibles amenazas y los tipos de ataque.
- La mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema.
- Correcta instalación, configuración y mantenimiento del los equipos.
- Soporte de los fabricantes de hardware y software, que permitan realizar actualizaciones, y mejoras para cubrir fallos y problemas relacionados con la seguridad.
- Considerar que hay amenazas internas y externas a la seguridad de la información.
- Adaptación de los objetivos de seguridad y de las actividades a realizar,

[1] Fuente:Above SECURITY, Sergio Quiroz

acorde a las necesidades reales de la organización.

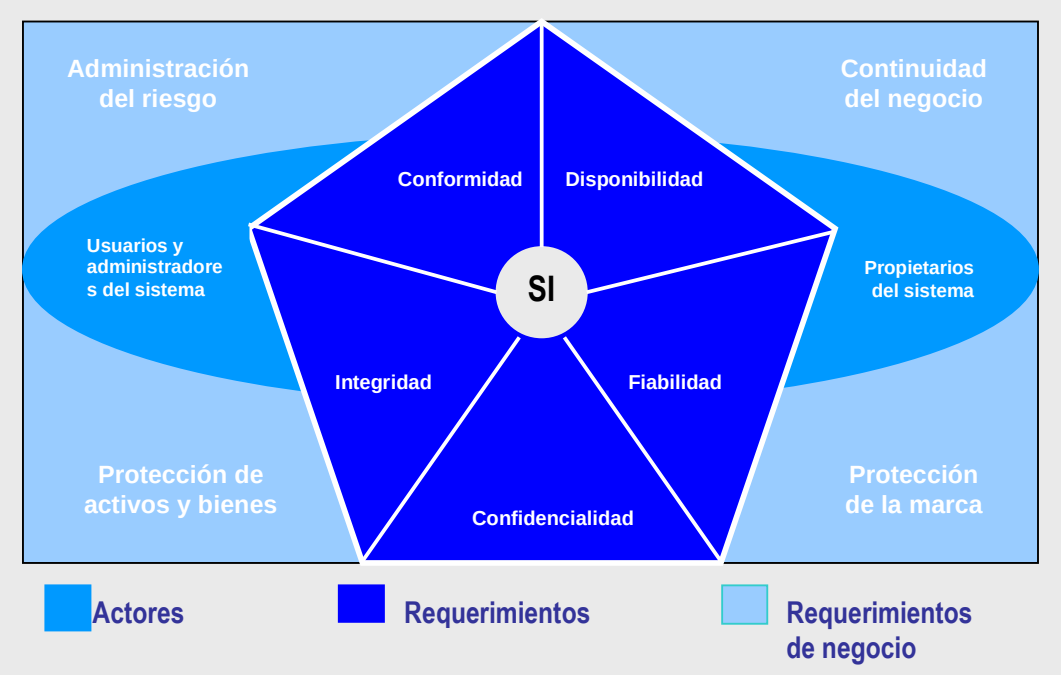

FIGURA 1.2 Aspectos de la seguridad informática[2]
ELABORADO POR Ing. Mantilla Aníbal

Los objetivos de la seguridad informática fundamentalmente son:

1. Minimizar y gestionar riesgos
2. Detectar posibles amenazas y problemas de seguridad
3. Garantizar la adecuada utilización de los recursos y las aplicaciones del sistema
4. Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de incidente de seguridad
5. Cumplir con el marco legal

En base a lo indicado, los planos de actuación de la seguridad de la información son: Técnico, Humano, Organizativo, Legal.

[2] Fuente: Above SECURITY, Sergio Quiroz

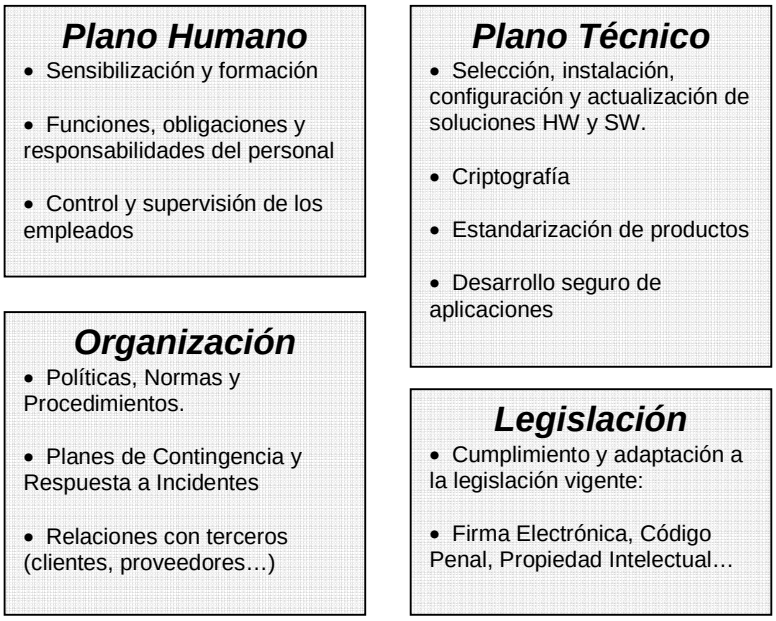

FIGURA 1.3 Planos sobre los que actúa la seguridad de la información[3]
ELABORADO POR Ing. Mantilla Aníbal

La seguridad informática en una organización debe ser un proceso basado en un ciclo iterativo, en el que incluyen actividades como valoración del riesgo, prevención, detección, y respuesta ante incidentes de seguridad.

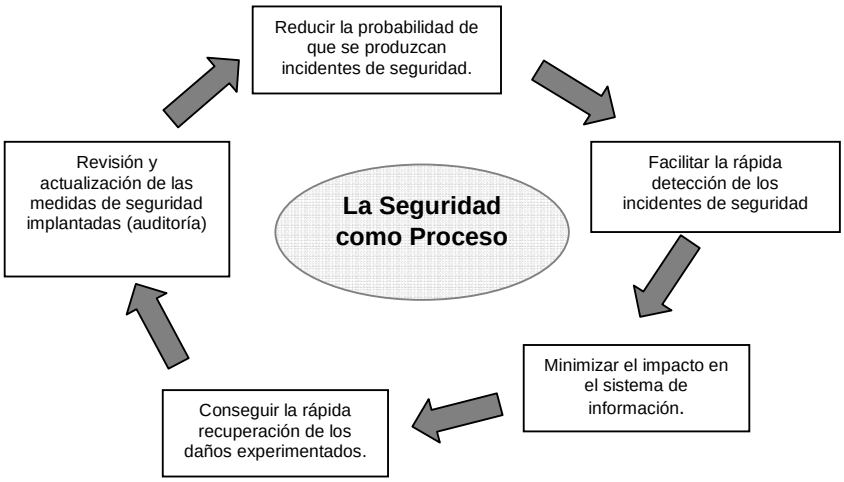

FIGURA 1.4 Seguridad de la información como proceso y no como producto[4]

[3 y 4] Fuente: Enciclopedia de la Seguridad Informática, Álvaro Gómez

Los servicios de la seguridad de información son:

- Confidencialidad
- Integridad
- Disponibilidad
- No repudio

Las consecuencias de la falta de seguridad informática, dependerán de la organización, sus actividades, volumen de sus operaciones, entre otras características propias de la misma. Sin embargo, en una expresión general, en un enfoque local, regional, e incluso global, las consecuencias pueden ser:

- Conflictos sociales y laborales
- Pérdidas económicas en el negocio
- Deterioro de la imagen personal o profesional (empresarial)
- Extorsiones y secuestros
- Robo de información confidencial
- Retrasos en procesos empresariales
- Daños a la salud y pérdida de vidas humanas
- Daños y perjuicios

IMAGEN	VOLUMEN DE NEGOCIO	PRODUCTIVIDAD Y PRESTACION DEL SERVICIO
- Pérdida de imagen respecto de cliente - Pérdida de imagen respecto a proveedores - Pérdida de imagen respecto a otras partes - Ventajas de los competidores - Etc.	-Pérdida de ingresos/ facturación -Posibles indemnizaciones a terceros -Posibles sanciones -Pérdida de oportunidades de negocio -Pérdida de contratos/ caída acciones -Etc.	-Disminución rendimiento laboral -Interrupciones en procesos productivos - Retraso en entregas - Cese de transacciones - Enfado de los empleados - Etc.

TABLA 1.1 Consecuencias de la falta de seguridad en el manejo de la información [5]

[5] Fuente: www.nexusasesores.com

ELABORADO POR Ing. Mantilla Aníbal

1.1.2 VULNERABILIDADES Y AMENAZAS

Existen diferentes **causas** que provocan ***vulnerabilidades*** en los sistemas informáticos, a continuación se mencionan algunas:

- Debilidad en el diseño de los protocolos utilizados en las redes
- Errores de programación
- Configuración inadecuada de los sistemas informáticos
- Políticas de seguridad deficiente o inexistente
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de la informática
- Fácil acceso a herramientas que posibilitan los ataques
- Limitaciones normativas gubernamentales y en las organizaciones
- Descuido de fabricantes

Los tipos de vulnerabilidades se clasifican de diversas maneras, a continuación se presenta una clasificación dependiendo del objeto de afectación:

Vulnerabilidades que afectan a los equipos, se tiene el caso de afectación a routers, cable-modem, cámaras web, servidores de video, impresoras, escaners, faxes, fotocopiadoras, teléfonos móviles, agendas electrónicas, etc.

Vulnerabilidades que afectan a los programas y aplicaciones informáticas, afectan a sistemas operativos, servidores, bases de datos, navegadores, aplicaciones ofimáticas, compresores, etc.

De las numerosas formas de ***amenaza*** a la seguridad informática, se consideran fundamentalmente las siguientes:

- Hackers, Crackers, sniffers, Phreakers, Spammers
- Virus
- Espionaje en redes
- Ciber terrorismo
- Piratas informáticos
- Ex - empleados

- Lammers
- Amenazas del personal interno
- Intrusos remunerados

Las **motivaciones** de los atacantes pueden ser las que siguen:

- Consideraciones económicas
- Diversión
- Ideología
- Autorealización, búsqueda de reconocimiento social y “estatus”

Las **fases de ataque informático**, suelen ser las siguientes:

- Descubrimiento y explotación del sistema informático
- Búsqueda de la vulnerabilidad del sistema
- Explotación de las vulnerabilidades detectadas
- Corrupción o compromiso del sistema
- Eliminación de pruebas que puedan identificar al atacante

Los **tipos de ataque** más comunes son:

- Actividades de reconocimiento de sistemas
- Detección de vulnerabilidades de los sistemas
- Robos de información mediante la interceptación de mensajes
- Modificación del contenido y secuencia de los mensajes
- Análisis del tráfico
- Suplantación de identidad
- Modificación del tráfico y de las tablas de enrutamiento
- Conexión no autorizada a equipos y servidores
- Introducción de malware
- Ataques contra sistemas criptográficos
- Fraudes, engaños y extorsiones
- Denegación de servicio
- Marcadores telefónicos

1.1.3 INLFUENCIA DEL FACTOR HUMANO, LA ORGANIZACIÓN, Y LA TECNOLOGÍA EN LA SEGURIDAD DE LA INFORMACIÓN

El ***factor humano*** refiere a las personas, pues son el elemento más débil dentro de la seguridad informática, por ello es necesario analizar su papel con los sistemas y redes informáticas de la organización. El principio básico es que todas las soluciones informáticas implantadas por la organización (firewall, antivirus, servidores Proxy, planes, políticas), pueden resultar inútiles ante el desconocimiento, la falta de información, desinterés o ánimo de causar daño por parte de algún empleado.

La ***Ingeniería social,*** es otro factor a considerar, se han presentado casos como los siguientes:

- Llamado telefónico de un supuesto investigador amenazando con obstruir la justicia.
- Supuesto técnico que pide autorización para reparar un ordenador.
- Correos electrónicos suplantando identidad
- Utilización de foros y chats, donde se entrega información
- Puesta en marcha de website maliciosos

Por otro lado, muchos empleados con acceso a Internet en la organización, tienden a hacer un mal uso del mismo, pudiendo incluso perjudicar a la organización. Debido a esto, es necesario muchas veces, tomar medidas para controlar y vigilar el uso de los servicios de Internet, como por ejemplo:

- Limitación de los servicios a Internet
- Posibilidad de revisión del correo electrónico del empleado
- Acceso al ordenador de un trabajador, sus archivos y sus carpetas
- Bloque de direcciones web
- Asignación de permisos de acceso en función del perfil del usuario

En lo referente a la ***organización,*** se habla de todo cuanto debe realizase en el ámbito de gestión para la adecuada seguridad de la información. Debería definirse e implantarse Políticas de Seguridad, inventariarse los recursos y definir

los servicios ofrecidos, realizar pruebas y auditorias periódicas. Junto con estos aspectos, es fundamental hacer referencia a:

- Seguridad frente a egreso e ingreso de los empleaos a la organización
- Adquisición de productos
- Relación con proveedores
- Seguridad física de las instalaciones
- Sistemas de protección eléctrica
- Control de emisión electromagnética
- Vigilancia de la red
- Protección de equipos e instalaciones
- Control de equipos que pueden salir de la organización
- Copias de seguridad
- Identificación y autenticación de usuarios
- Seguridad en el desarrollo, implantación y mantenimiento de aplicaciones informáticas
- Auditoria de la gestión de la seguridad

Para contrarrestar las vulnerabilidades y las amenazas, se han desarrollado diferentes ***medios tecnológicos en redes de información***, a continuación se presentan los de más amplio uso:

- Antivirus
- Servidores de autenticación
- Gestores de contraseñas
- Centros de respaldo de datos
- Implantación de sistemas biométricos
- Firma electrónica
- Protocolos criptográficos
- Servidores Proxy
- Cortafuegos (firewall)
- Zona desmilitarizada
- Analizadores de registro de actividad
- Sistemas de detección de intrusos
- Sistemas Honeypots y las Honeynets (Host y redes señuelos)

1.1.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Como puede verse, el manejo de la seguridad informática como un procesos, requiere de conocimientos, habilidades y capacidades en las áreas técnica, legal, humana, y organizacional.

Un sistema en el que se pueden integrar todos estos factores con todos los requerimientos y consideraciones organizacionales, recibe el nombre de SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, conocido por sus siglas como SGSI.

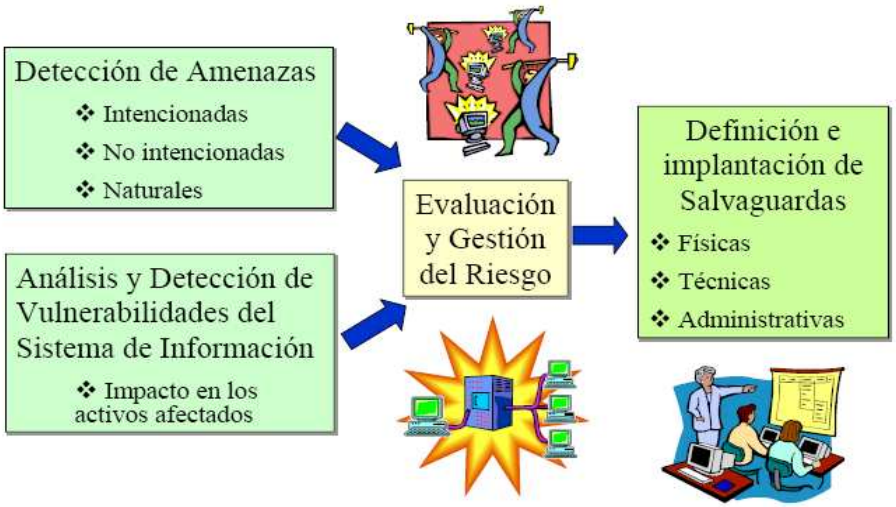

FIGURA 1.5 Gestión de riesgos en una organización[6]

La parte del sistema general de gestión, que comprende a la política, la estructura organizativa, los procedimientos, los procesos, y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización se denomina *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).*

[6] Fuente: Enciclopedia de la Seguridad Informática, Álvaro Gómez

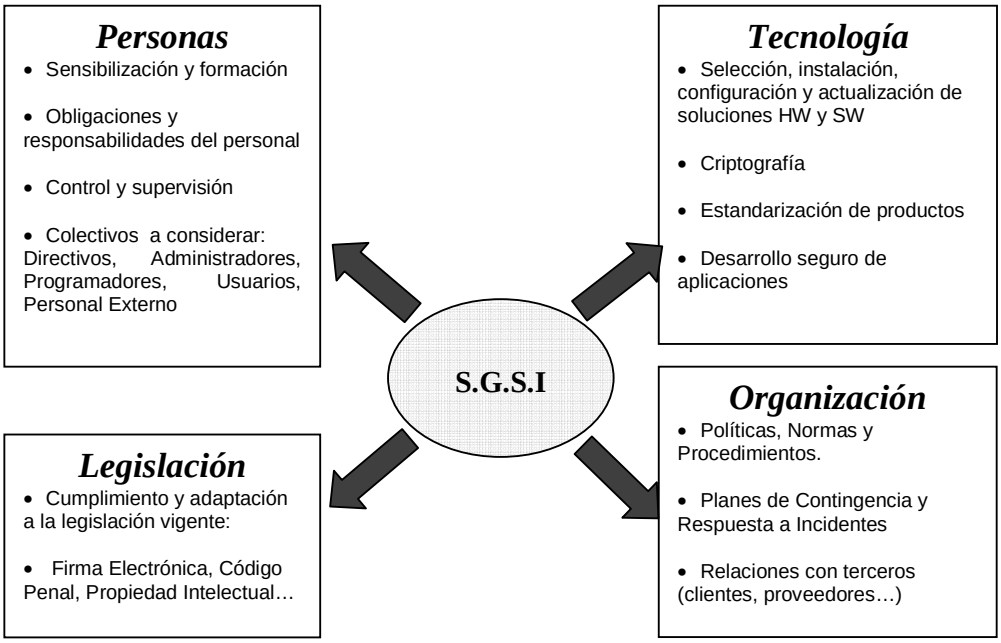

FIGURA 1.6 Aspectos fundamentales del sistema de gestión de seguridad de la información[7]
ELABORADO POR Ing. Mantilla Aníbal

Para implantar un Sistema de Gestión de Seguridad de la Información, una organización debe considerar:

- Formalizar la gestión de la seguridad de la información
- Analizar y gestionar los riesgos
- Establecer los procesos de gestión de la seguridad en base a la metodología
- Certificar la gestión de la seguridad

Para esto debe tenerse en cuenta el marco legal, los estándares, las metodologías, los requerimientos; entre otros aspectos fundamentales.

[7] Fuente: Enciclopedia de la Seguridad Informática, Álvaro Gómez

FIGURA 1.7 Proyectos que constituyen un SGSI [8]
ELABORADO POR Ing. Mantilla Aníbal

Por su trascendencia, es importante mencionar algunos de los enfoques más relevantes al tema de la gestión para la continuidad de las operaciones:

- ***Plan para recuperación ante desastres*** *(Disaster Recovery Planning DRP)****.*** Se enfoca en la recuperación de los servicios de TI y los recursos, dado un evento que ocasionara una interrupción mayor en su funcionamiento.
- ***Plan para reanudación del negocio*** *(Business Resumption Planning BRP)****.*** Se centraliza en la reanudación de los procesos de negocios afectados por una falla en las aplicaciones de TI. Se enfoca en la utilización de

[8] Fuente: Above SECURITY, Sergio Quiroz

procedimientos relacionados con el área de trabajo.

- ***Plan para la continuidad de las operaciones*** *(Continuity of Operations Planning COOP).* Busca la recuperación de las funciones estratégicas de una organización que se desempeñan en sus instalaciones corporativas.
- ***Plan de contingencia*** *(Contingency Planning CP).* Se enfoca en la recuperación de los servicios y recursos de TI, después de un desastre de dimensiones mayores o de una interrupción menor. Especifica procedimientos y lineamientos para la recuperación, tanto en áreas de la empresa como en las alternas.
- ***Plan de respuesta ante emergencias*** *(Emergency Response Planning).* Su objetivo es salvaguardar a los empleados, el público, el ambiente y los activos de la empresa. Últimamente se busca de inmediato llevar la situación de crisis a un estado de control.

Todos estos enfoques tienen un denominador común, el cual, es un limitado alcance. Cada una de estas ópticas de planeación se centra en la protección de aspectos específicos de la organización, ignorando otras áreas críticas. Para atender esta limitación, se requiere un enfoque de planeación integrado, que permita proteger todas las áreas críticas de la organización.

El Plan de Continuidad del Negocio PCN (o por sus siglas en inglés BCP – Business Continuity Plan) integra el alcance y los objetivos de todos estos enfoques.

1.2 LA NORMA ISO 27001

La Norma ISO 27001, es un estándar desarrollado como modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un SGSI para cualquier tipo de organización. Permite diseñar e implantar un SGSI, se encuentra influenciado por las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización.

1.2.1 LA FAMILIA ISO 27000

Dada la importancia que tiene un SGSI para las empresas, en Ginebra, donde se encuentra la sede de ISO, se ha establecido la necesidad de hacer las revisiones a las normas, cada cinco años, para decidir las posibles modificaciones. Así, se ha creado la familia ISO 27000, en la que se encuentra la norma ISO 27001:2005, el código de prácticas ISO/IEC 17799:2005, entre otros.

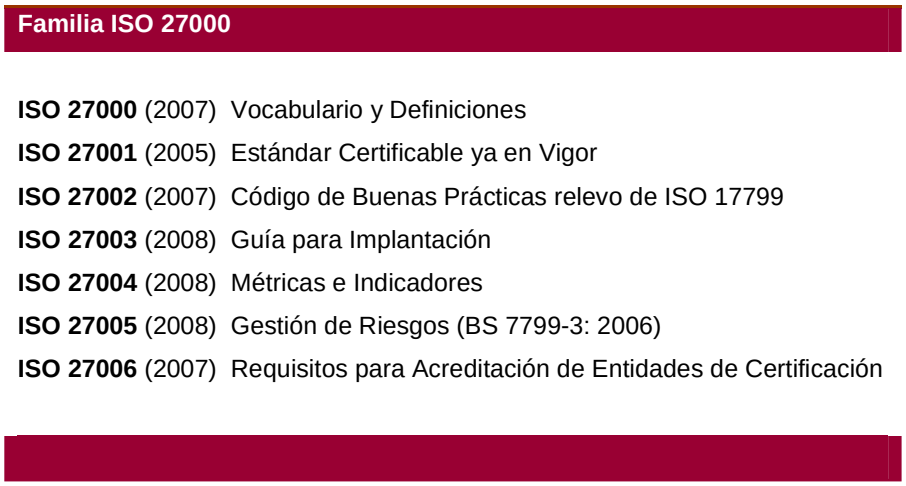

FIGURA 1.8 La Familia ISO 27000[9]
ELABORADO POR Ing. Mantilla Aníbal

[9] Fuente: www.nexusasesores.com

1.2.2 EVOLUCIÓN DE LA NORMA ISO 27001

Su origen es británico, hasta que, en el año 2005, la Organización Internacional para la Normalización (ISO) la oficializó como norma.

El ISO 27001:2005 es el único estándar certificable, aceptado internacionalmente de manera global para la gestión de la seguridad de la información; aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

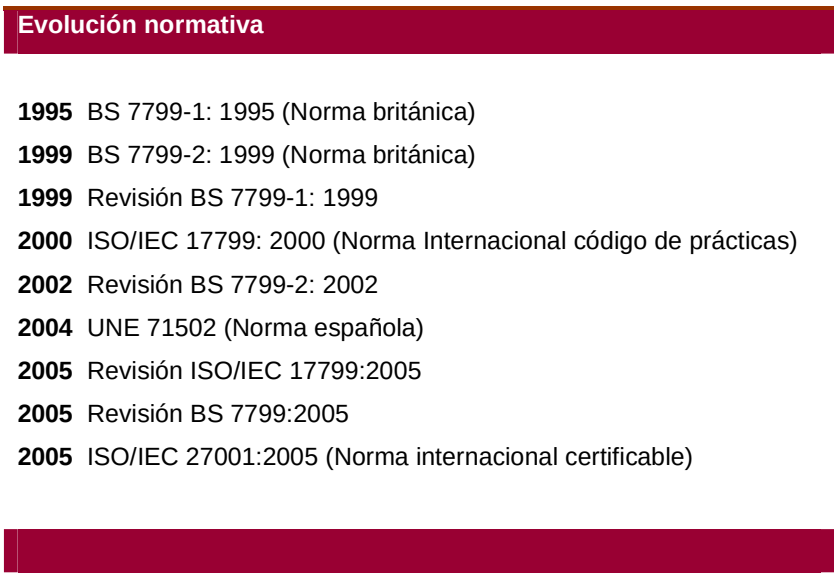

FIGURA 1.9 Evolución de la norma ISO 27001 [10]
ELABORADO POR Ing. Mantilla Aníbal

1.2.3 NATURALEZA DE LA NORMA

La norma ISO 27001, actúa bajo el enfoque de procesos. La aplicación de un sistema de procesos, dentro de la organización, junto con la identificación y las interacciones de estos procesos, así como su gestión, puede denominarse "como enfoque basado en procesos"

El enfoque basado en procesos para la gestión de la seguridad de la información presentado en esta norma, enfatiza a los usuarios, la importancia de:

A) La comprensión de los requisitos de seguridad de la información de una

[10] Fuente: www.nexusasesores.com

organización y la necesidad de establecer la política y objetivos para la seguridad de la información.

B) Implementar y operar controles para dirigir los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización

C) Realizar seguimiento y revisar el desempeño y la eficacia del SGSI; y

D) La mejora continua con base en mediciones objetivas.

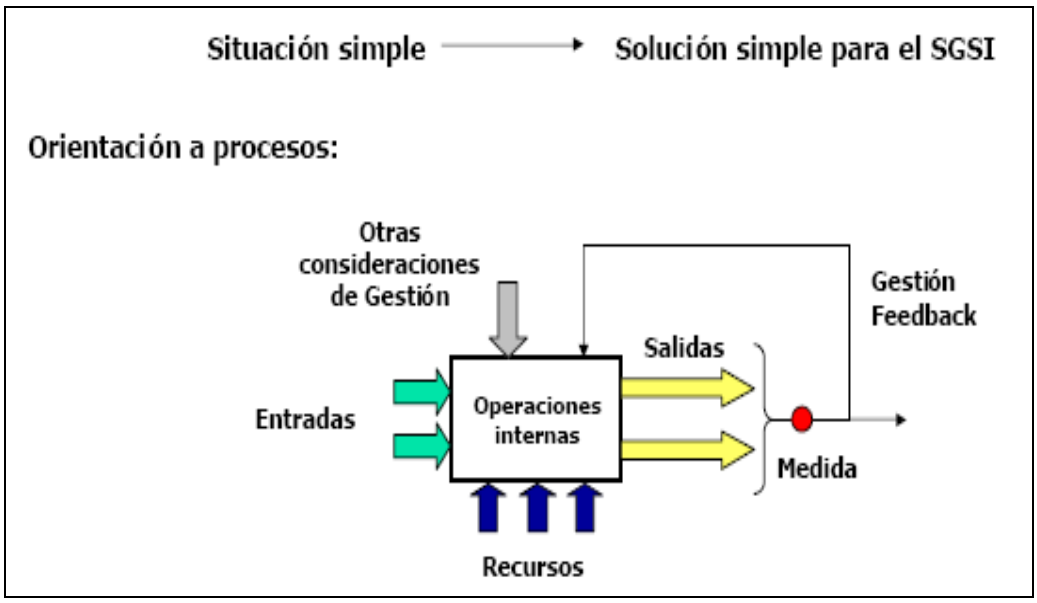

FIGURA1.10 Enfoque del **SGSI** hacia procesos [11]

Esta Norma adopta el modelo "Planificar, Hacer, Verificar, Actuar" (PHVA), el cual se aplica para estructurar todos los procesos del SGSI, y tiene por objeto: establecer, gestionar y documentar el SGSI, responsabilizando a la Dirección, incluso en el monitoreo, auditoria y mejoramiento continuo.

Para cumplir con este objetivo, la norma ISO 27001 ha sido estructurada de forma metodológica con CLAUSULAS y Anexos, que incluyen objetivos de control y controles, así como también su relación con otras normas ISO. Como punto de partida, la norma en referencia presenta un prefacio, de manera seguida se presentan las cláusulas y anexos. En la tabla siguiente se muestra esta estructura:

[11] Fuente:www.nexusasesores.com

CLAUSULA	Nº	SECCIÓN	SUBSECCIÓN
INTRODUCCIÓN	**0**		
OBJETO	**1**		
REFERENCIAS NORMATIVAS	**2**		
TÉRMINOS Y DEFINICIONES	**3**		
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**4**	4.1Requisitos Generales	
		4.2 Establecer y Gestionar el SGSI	4.2.1 Establecer el SGSI
			4.2.2 Implementar y operar el SGSI
			4.2.3 Monitorear y revisar el SGSI
			4.2.4 Mantener y mejorar el SGSI
		4.3 Documentar el SGSI	4.3.1 Generalidades
			4.3.2 Controlar documentos
			4.3.3 Controlar los registros
RESPONSABILIDAD DE LA DIRECCIÓN	**5**	5.1 Compromiso de la dirección	
		5.2 Gestionar los recursos	5.2.1 Provisión de recursos
			5.2.2 Capacitación y entrenamiento
AUDITORÍAS INTERNAS DEL SGSI	**6**		
REVISIÓN POR LA DIRECCIÓN DEL SGSI	**7**	7.1 Generalidades	
		7.2 Elementos de entrada para revisión	
		7.3 Resultados de la revisión	
MEJORA DEL SGSI	**8**	8.1Mejoramiento continuo	
		8.2 Acción correctiva	
		8.3 Acción preventiva	
ANEXOS		A. Normativo	
		B. Informativo	
		C. Informativo	

TABLA 1.2 Estructura de la Norma ISO 27001
ELABORADO POR Ing. Mantilla Aníbal

Los objetivos de control y sus controles respectivos (anexo A - normativo de la norma ISO 27001) enfocan la Seguridad de la Información a través de 11 áreas

fundamentales para la organización, estas son:

A) Política de seguridad
B) Organización de la seguridad de la información
C) Gestión de activos
D) Seguridad de los recursos humanos
E) Seguridad física y del entorno
F) Gestión de las comunicaciones y operaciones
G) Control de accesos
H) Adquisición, desarrollo y mantenimiento de sistemas de información
I) Gestión de los incidentes de seguridad
J) Gestión de la continuidad del negocio
K) Cumplimiento normativo (legales, de estándares, técnicas y auditorias)

En la siguiente figura, puede verse como el objetivo final de la norma ISO 27001 es preservar la disponibilidad, la confidencialidad, la integridad, y el no repudio de la información.

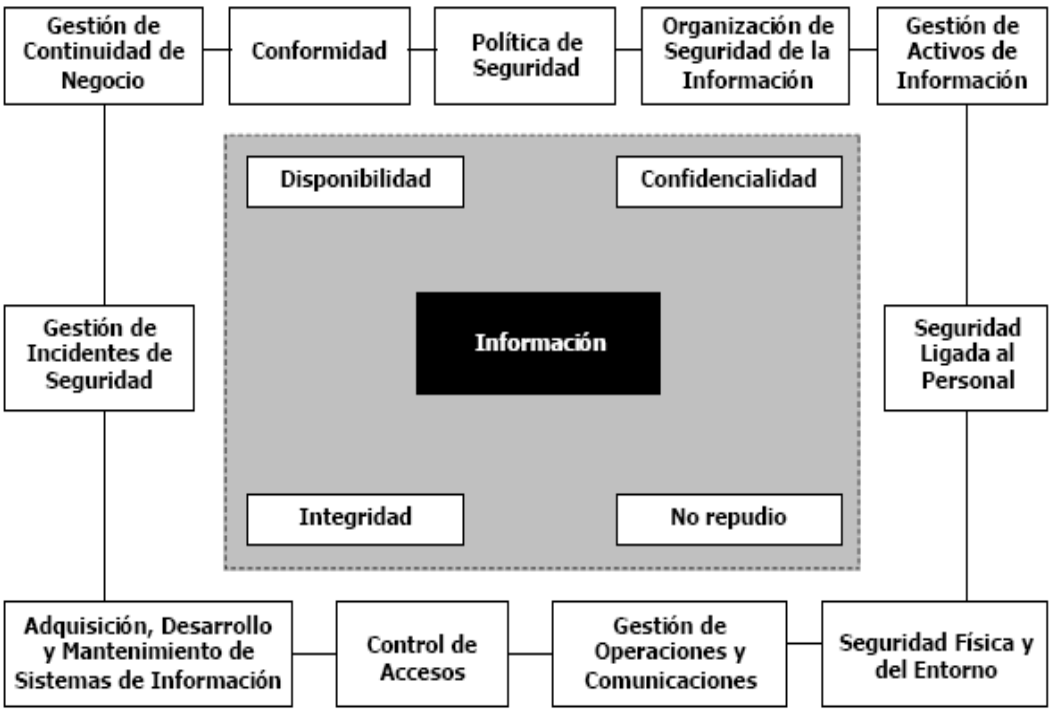

FIGURA 1.11 Enfoque de los controles de la norma ISO 27001 [12]

A continuación por la importancia que tienen estas 11 áreas de control, se detalla a qué refieren cada una de ellas:

Política de seguridad

Se necesita una política que refleje las expectativas de la organización en materia de seguridad con el fin de suministrar administración con dirección y soporte, la cual también se puede utilizar como base para el estudio y evaluación en curso.

Organización de la seguridad de la información

Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

Gestión de activos

Muestra la necesidad de un inventario de los recursos de información de la organización y con base en este conocimiento, asegurar que se brinde un nivel adecuado de protección.

Seguridad de los recursos humanos

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la CAC o se debe implementar un plan para reportar los incidentes.

Seguridad física y del entorno

Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

Gestión de las comunicaciones y operaciones

Los objetivos de esta sección son:

[12] Fuente: www.nexusasesores.com

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de falla de los sistemas.
- Proteger la integridad del software y la información.
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

Control de accesos

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

Adquisición, desarrollo y mantenimiento de sistemas de información

Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

Gestión de incidentes de seguridad

Asegura que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.

Gestión de continuidad del negocio

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes, en caso de una falla grave o desastre.

Cumplimiento Normativo (legales, de estándares, técnicas y auditorías)

Imparte instrucciones para que se verifique si el cumplimiento con la norma técnica ISO 27001 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

1.2.4 ACTIVIDADES PARA ALCANZAR CERTIFICACIÓN ISO 27001

Para alcanzar la certificación internacional, las organizaciones deben realizar una serie de actividades, para posteriormente tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoria para su primera certificación. El proceso para la certificación bebería efectuarse de la manera que indica en la siguiente figura:

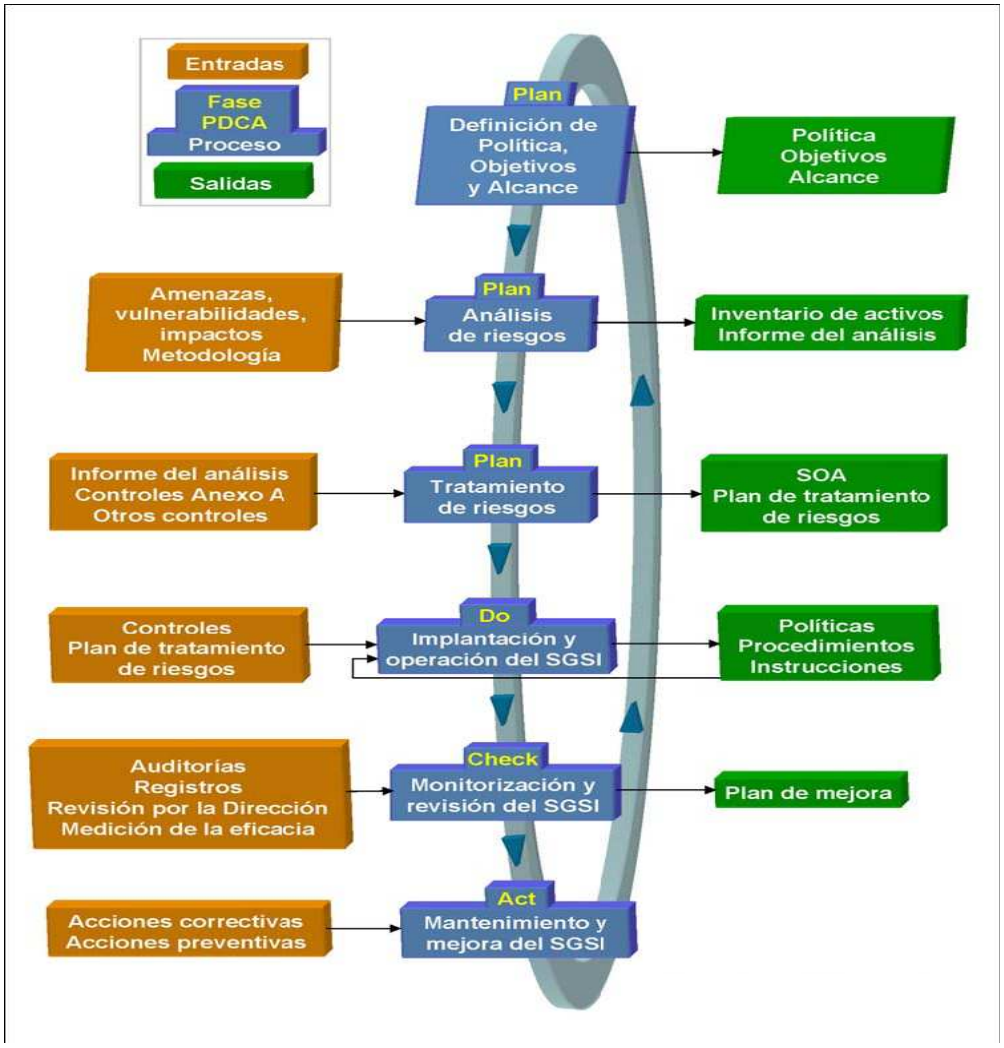

FIGURA1.12 Actividades para alcanzar la certificación ISO 27001 del SGSI [13]

1.2.5 ORGANIZACIONES CERTIFICADAS EN EL MUNDO CON ISO 27001

De acuerdo al Internacional Register of ISMS Certificates, en Febrero del 2009, el número total de organizaciones en el mundo, certificadas con ISO 27001 llegaba a 5200, en la siguiente tabla se muestra la distribución por países, de estas organizaciones:

[13] Fuente: www.ISO27000.es

Japón	2997	Islandia	12	Oman	3
India	435	Pakistán	12	Perú	3
Reino Unido	370	Holanda	11	Portugal	3
Taiwán	221	Singapur	11	Vietnam	3
China	180	Filipinas	10	Bangladesh	2
Alemania	112	Federación Rusa	10	Canadá	2
USA	85	Arabía Saudita	10	Isla de Man	2
Korea	82	Grecia	9	Marruecos	2
República Checa	70	Eslovenia	9	Yemen	2
Hungría	64	Suecia	7	Armenia	1
Italia	58	Eslovakia	6	Bélgica	1
Polonia	35	Sur África	6	Egipto	1
Hong Kong	31	Bahrain	5	Irán	1
España	30	Colombia	5	kazakhstan	1
Austria	29	Croacia	5	Kyrgyzstan	1
Australia	28	Indonesia	5	Líbano	1
Irlanda	26	Kuwait	5	Lituania	1
Malasia	26	Suiza	5	Luxemburgo	1
Brasil	20	Bulgaria	4	Macedonia	1
México	20	Gibraltar	4	Moldavia	1
Tailandia	20	Noruega	4	Nueva Zelanda	1
UAE	18	Qatar	4	Ucrania	1
Turquía	17	Sri Lanka	4	Uruguay	1
Rumania	15	Chile	3	**Total Absoluto**	**5206**
Francia	12	Macau	3		

TABLA 1.3 Organizaciones certificadas con ISO 27001 en el mundo, por países [14]
ELABORADO POR Ing. Mantilla Aníbal

[14] Fuente: Internacional Register of ISMS Certificates

1.3 COOPERATIVAS DE AHORRO Y CRÉDITO EN EL ECUADOR

Las Cooperativas de Ahorro y Crédito han alcanzado una participación que llega al 10% del Sistema Financiero Nacional, incidiendo directamente en la actividad de aproximadamente tres millones de personas. Existen en el Ecuador alrededor de mil trescientas Cooperativas de Ahorro y Crédito, de las cuales solo algo más de treinta son controladas por la Superintendencia de Bancos y Seguros. En forma general, año tras año, desde hace cinco años, los depósitos y el número de socios de las Cooperativas de Ahorro y Crédito han ido en aumento. A continuación se presenta el aspecto reglamentario y estadísticas referentes a este sector de la economía.

1.3.1 LEY DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS PARA APLICACIÓN EN INSTITUCIONES DEL SISTEMA FINANCIERO

A continuación se presenta un extracto de esta Ley, obtenido en base a consideraciones de Gestión integral de la Seguridad informática en Instituciones financieras, y que tienen relación directa y estrecha con el Sistema de Gestión de Seguridad de la Información.

La Ley General de Instituciones del Sistema Financiero dispone que es deber de la Superintendencia de Bancos y Seguros proteger los intereses del público, además, y establece que las Cooperativas de Ahorro y Crédito que realizan intermediación financiera con el público son instituciones financieras.

Establece que las Cooperativas de Ahorro y Crédito que realizan intermediación financiera con el público en general están expuestas a una serie de riesgos, lo que determina la necesidad de identificar, medir, controlar y monitorear los mismos, en función de la naturaleza y complejidad de sus operaciones. Además considera necesario en función de las prácticas modernas, que las Cooperativas de Ahorro y Crédito que realizan intermediación financiera con el público, cuenten con una adecuada disciplina financiera en concordancia con los principios de prudencia y solvencia financiera a fin de ser viables y sostenibles, que facilite el desarrollo de la supervisión por riesgos, tomando en consideración el mercado actual en que esas entidades desenvuelven sus actividades y la dinámica del sistema financiero ecuatoriano, en todo lo cual se tendrá presente los principios del cooperativismo. Expresamente, la Superintendencia de Bancos y Seguros

indica que se debe promover una mayor eficiencia y competitividad en las Cooperativas de Ahorro y Crédito controladas por la Superintendencia de Bancos y Seguros, que redunde en beneficio de los socios de esas entidades. En lo concerniente al Riesgo operativo, tiene cinco partes que se detallan a continuación:

PARTE I: ÁMBITO, DEFINICIONES Y ALCANCE

Para administrar adecuadamente el riesgo operativo, se han establecido disposiciones que son aplicables a las instituciones financieras públicas y privadas, al Banco Central del Ecuador, a las compañías emisoras y administradoras de tarjetas de crédito, entre otras, cuyo control compete a la Superintendencia de Bancos y Seguros, denominadas instituciones controladas. Se establece definiciones fundamentales para la aplicación de las disposiciones

PARTE II: FACTORES DEL RIESGO OPERATIVO

Establece que con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí, estos son:

- Procesos
- Personas
- Tecnología de información
- Eventos externos

PARTE III: ADMINISTRACIÓN DEL RIESGO OPERATIVO

Se debe diseñar un proceso de administración de riesgo operativo, que permita a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones.

Una vez identificados los eventos de riesgo operativo y las fallas o

insuficiencias en relación con los factores de este riesgo y su incidencia para la institución, los niveles directivos están en capacidad de decidir si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos. La administración del riesgo operativo constituye un proceso continuo y permanente. En esta parte, se establece la necesidad de contar con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.

PARTE IV: CONTINUIDAD DEL NEGOCIO

Se establece que as instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. Para el efecto, deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia. Deberá contarse con procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento.

PARTE V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

El directorio u organismo que tenga a su cargo la administración del riesgo operativo, entre otras tiene las siguientes responsabilidades:

- Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo.

- Aprobar las políticas, procesos y procedimientos para la administración del capital humano.
- Aprobar las políticas y procedimientos de tecnología de información
- Aprobar los planes de contingencia y de continuidad del negocio

El Comité de Administración integral de riesgos tendrá entre otras, las siguientes responsabilidades:

- Evaluar y proponer las políticas y el proceso de administración del riesgo operativo, y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo.
- Evaluar las políticas y procedimientos de procesos, personas y tecnología de información, y someterlas a aprobación del directorio u organismo que haga sus veces;
- Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;
- Evaluar y someter a aprobación del directorio u organismo que haga sus veces los planes de contingencia y de continuidad del negocio, asegurar la aplicabilidad y el cumplimiento de los mismos
- Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de contingencia y de continuidad del negocio.

1.3.2 LEYES Y REGLAMENTOS DE LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Al igual que en el caso de la Ley de la SBS para instituciones del Sistema Financiero, en este caso, también se elabora un extracto de las Leyes y Reglamentos de las Cooperativas de Ahorro y Crédito (CAC), que abarca aquellos aspectos relacionados con la Seguridad de la Información, como base fundamental para un adecuado diseño de un Sistema de Gestión de Seguridad de la Información.

En estas Leyes y Reglamentos, se hace referencia a la estructura, operación, funciones, deberes y responsabilidades de los actores internos de la Cooperativa, específicamente a los siguientes:

A) La Asamblea General
B) El Consejo de Administración
C) El Presidente
D) El Comité de Auditoria
E) El Comité de Crédito
F) El Gerente General de la Cooperativa
G) Los procesos de Contabilidad, Información Financiera y Auditoria
H) Las Cooperativas de Ahorro yCrédito de Segundo Piso

A continuación se presentan los aspectos más relevantes de estas leyes y reglamentos, relacionados con la presente Tesis:

A. LA ASAMBLEA GENERAL DE LA COOPERATIVA

La asamblea general es la máxima autoridad de la cooperativa y sus resoluciones son obligatorias para todos sus órganos internos y socios, en tanto sean concordantes con la ley, el presente reglamento, las normas que expida la Superintendencia, el estatuto social y la normativa interna.

- La asamblea general podrá ser de socios o de representantes, pero una vez superados los doscientos socios obligatoriamente será de representantes, en un número no menor de treinta ni mayor de cincuenta.

- Las asambleas generales de socios o de representantes son de carácter ordinario o extraordinario y se reunirán únicamente en el domicilio principal de la cooperativa.
- Las asambleas generales ordinarias serán convocadas por el Presidente y se reunirán una vez al año dentro de los noventa días posteriores al cierre de cada ejercicio económico anual, para conocer y resolver sobre los informes del Consejo de Administración, del Gerente General, del Comité Integral de Riesgos, del Comité de Auditoría, de Auditoría Interna y de Auditoría Externa, aprobar los estados financieros, decidir respecto de la distribución de los excedentes y cualquier otro asunto puntualizado en el orden del día, de acuerdo a la convocatoria.

Son atribuciones de la asamblea general de socios o representantes de la cooperativa:

- Conocer y resolver las reformas del estatuto social, las que entrarán en vigencia una vez aprobadas por la Superintendencia.
- Acordar la disolución y liquidación voluntaria, o fusión de la cooperativa, en los términos previstos en este reglamento; y con el voto conforme de al menos las dos terceras partes del número de socios o representantes establecido en el estatuto social.
- Conocer y resolver sobre la distribución de los excedentes;
- Resolver en última instancia los casos de expulsión de los socios, de acuerdo a lo que establece el estatuto, una vez que el Consejo de Administración se haya pronunciado.
- Aprobar el Reglamento de elecciones de la cooperativa y someterlo a aprobación de la Superintendencia;
- Acordar el monto de aporte obligatorio en certificados de aportación;
- Remover a los miembros de la asamblea general, observando el debido proceso previamente previsto en el estatuto;
- Pedir cuentas al Consejo de Administración y al Gerente General cuando lo considere necesario.

- Reglamentar el pago de dietas y viáticos para los miembros del Consejo de Administración de acuerdo con lo establecido en este reglamento y siempre que conste en el presupuesto aprobado de la cooperativa.

B. EL CONSEJO DE ADMINISTRACIÓN DE LA COOPERATIVA

El Consejo de Administración es el órgano directivo y administrativo de la cooperativa y estará integrado por cinco vocales principales y cinco vocales suplentes. Durarán tres años en sus funciones y podrán ser reelegidos por una sola vez para el período siguiente. Luego de transcurrido un período, podrán ser elegidos nuevamente, de conformidad con estas disposiciones.

El Gerente General asistirá a las reuniones del Consejo de Administración con voz, pero sin derecho a voto. Al menos dos de los vocales del Consejo de Administración deberán tener título profesional y académico de tercer nivel o cuarto nivel en administración, economía, finanzas, contabilidad, auditoría o derecho, registrado en el CONESUP, o haber aprobado un programa de al menos dos años en capacitación especializada en gestión financiera cooperativa, certificado por un centro de educación superior reconocido en el país.

Son atribuciones y deberes del Consejo de Administración:

- Aprobar y revisar anualmente, las estrategias de negocios y las principales políticas de la entidad.
- Presentar para conocimiento y resolución de la asamblea general los estados financieros y el informe de labores del consejo.
- Nombrar y remover al Gerente General y determinar su remuneración.
- Pedir cuentas al Gerente General cuando lo considere necesario.
- Nombrar a los miembros de los comités cuya creación disponga la Superintendencia; y, verificar que se integren conforme con la normatividad vigente.
- Sancionar a los socios que infrinjan las disposiciones legales, reglamentarias o estatutarias previo el ejercicio del derecho de defensa y de acuerdo con las causales y procedimiento previstos en el estatuto social.

- Resolver los casos de expulsión de los socios, de acuerdo a lo que establece el estatuto, una vez que el Gerente General se haya pronunciado.
- Conocer las comunicaciones del organismo de control de acuerdo con lo previsto en la letra b) del artículo 36 de la ley y disponer el cumplimiento de las disposiciones, observaciones o recomendaciones.
- Autorizar al Gerente General otorgar poderes especiales.
- Las demás previstas en la ley, en este reglamento, en las normas expedidas por la Junta Bancaria y en el estatuto.

C. EL PRESIDENTE DE LA COOPERATIVA

Son atribuciones y deberes del Presidente:

- Convocar y presidir las asambleas generales y las reuniones del Consejo de Administración.
- Convocar a pedido del organismo electoral o de la Superintendencia en el caso previsto en este reglamento, a elecciones de representantes de la cooperativa.
- Presidir todos los actos oficiales de la cooperativa.
- Conocer las comunicaciones que la Superintendencia remita e informar de inmediato del contenido de las mismas al Consejo de Administración, y cuando estime, a la asamblea general.

D. EL COMITÉ DE AUDITORÍA

El Comité de Auditoria se integrará y cumplirá las funciones y deberes de conformidad a las normas de carácter general dictadas para el efecto por la Junta Bancaria.

E. EL COMITÉ DE CRÉDITO

Cada cooperativa tendrá un comité de crédito integrado por tres miembros, dos de los cuales serán designados por el Consejo de Administración de entre los funcionarios de la entidad, y por el Gerente General de la cooperativa quien lo presidirá. La función de comité será resolver sobre las solicitudes de crédito en el

marco de las políticas, niveles y condiciones determinados por el Consejo de Administración en el reglamento de crédito.

F. EL GERENTE GENERAL DE LA COOPERATIVA

El Gerente General, sea o no socio de la cooperativa, es el representante legal de la misma y será nombrado sin sujeción a plazo. Para ser nombrado Gerente General se requiere tener título profesional y académico de tercer nivel o cuarto nivel, en administración, economía y finanzas, debidamente registrado en el CONESUP, y acreditar experiencia mínima de cuatro años sea como administrador, director o responsable de áreas de negocios de cooperativas u otras instituciones financieras, y no encontrarse incurso en ninguna de las prohibiciones establecidas en la ley y las normas emitidas por la Junta Bancaria.

Son atribuciones y deberes del Gerente General:

- Representar judicial y extrajudicialmente a la cooperativa.
- Presentar para aprobación del Consejo de Administración el plan estratégico, el plan operativo y el presupuesto de la cooperativa, estos dos últimos hasta máximo el 30 de noviembre del año inmediato anterior a planificar;
- Delegar o revocar delegaciones conferidas a otros funcionarios de la cooperativa, para lo que informará previamente al Consejo de Administración, sin que ello implique exonerarse de la responsabilidad legal.
- Presidir el comité de crédito de la cooperativa y los que determinen las normas de la Junta Bancaria;
- Mantener y actualizar el registro de certificados de aportación.
- Ejecutar las políticas de tasas de interés y de servicios de acuerdo a los lineamientos fijados por el Consejo de Administración;

G. LOS PROCESOS DE CONTABILIDAD, INFORMACIÓN FINANCIERA Y AUDITORÍA

Las cooperativas adoptarán políticas internas de control para administrar prudencialmente sus riesgos en función de las normas que la Junta Bancaria emita para el efecto. Estas políticas serán aprobadas por el Consejo de

Administración y sobre su cumplimiento deberán informar las auditorias interna y externa.

Las cooperativas, entre otras, tienen las siguientes obligaciones:

- Exhibir y conservar en un lugar público y visible el certificado de autorización concedido por la Superintendencia;
- Llevar los libros sociales en orden cronológico y en sistemas impresos y magnéticos;
- Distribuir entre sus asociados el estatuto codificado y remitir a la Superintendencia, una vez aprobado por ella.

H. LAS COOPERATIVAS DE AHORRO Y CRÉDITO DE SEGUNDO PISO

Las Cooperativas de Ahorro y Crédito de segundo piso son instituciones financieras debidamente autorizadas por la Superintendencia y sujetas a su control, que tienen por objeto operar únicamente con las cooperativas asociadas de primer piso. Deberán cumplir con todas las normas de solvencia y prudencia financiera establecidas en la ley y las que expida la Junta Bancaria, especialmente en lo relacionado con el nivel de patrimonio técnico, calificación de activos de riesgo y constitución de provisiones y la gestión y administración integral de riesgos.

1.3.3 ESTADÍSTICAS DE LAS COOPERATIVAS DE AHORRO Y CRÉDITO ECUATORIANAS

La trascendencia de las Cooperativas de Ahorro y Crédito, es cada vez más significativa. Del número de instituciones financieras controladas por la Super Intendencia de Bancos y Seguros, las CAC controladas llegan a un equivalente del 40 %. Miles de personas acceden a sus servicios en todo el país, ubicando a estas, en el tercer lugar de participación del Sistema Financiero Nacional, alcanzando el 10% del mismo. A continuación se presentan tablas en las que se muestra la evolución de las Cooperativas de Ahorro y Crédito, en cuanto a: Participación en el sistema financiero nacional, Número de socios, Depósito y Cartera.

A) PARTICIPACIÓN EN EL SISTEMA FINANCIERO NACIONAL

Como puede verse en la figura 1.13, las Cooperativas de Ahorro y Crédito (controladas y no controladas, en conjunto), año tras año han aumentado su participación en el Sistema Financiero Nacional. Según información documentada de la Federación de Cooperativas de Ahorro y Crédito- FECOAC, la participación en el 2001 era del 4.3%, y para el 2004 era del 8.3%; lo cual significa un incremento de aproximadamente un 100% en su participación.

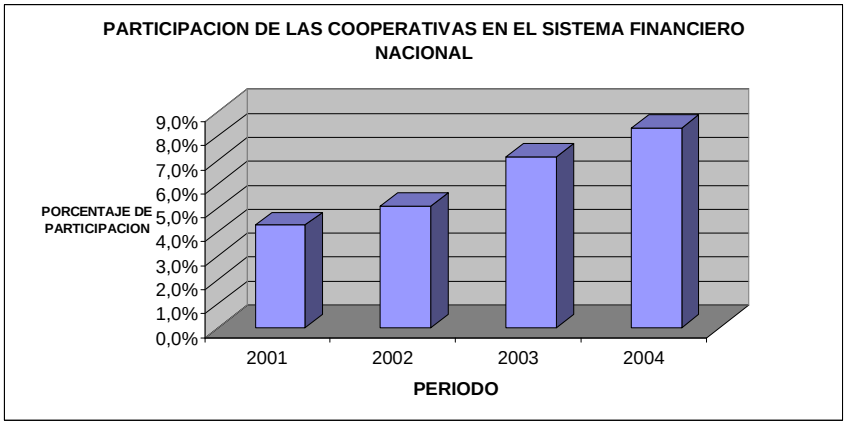

FIGURA 1.13 Participación de CAC en el Sistema Financiero Nacional [15]
ELABORADO POR Ing. Mantilla Aníbal

Para el 2006, según la Asociación de Cooperativas de Ahorro y Crédito controladas por la Superintendencia de Bancos y Seguros (30 aproximadamente), estas alcanzaban una participación del 7% en el Sistema Financiero Nacional, lo cual en aquel momento representaba el 8.41% de la participación que alcanzaban los bancos.

PARTICIPACION DE LAS COOPERATIVAS EN EL SISTEMA FINANICERO NACIONAL DICIEMBRE 2006

EN MILES DE DOLARES
Fuente: Superintendencia de Bancos y Seguros

INSTITUCIONES	ACTIVOS	%	PATRIMONIO	%	CARTERA	%
Cooperativas	**1.001.402**	**7,08%**	**213.835**	**13,26%**	**719.551**	**9,11%**
Bancos	11.890.163	84,10%	1.235.739	76,62%	6.379.867	80,80%
Mutualistas	463.278	3,28%	42.764	2,65%	213.975	2,71%
Financieras	783.740	5,54%	120.578	7,48%	582.967	7,38%
TOTAL SISTEMA	**14.138.583**	**100,00%**	**1.612.916**	**100,00%**	**7.896.360**	**100,00%**

TABLA 1.4 Comparación de la Participación de las CAC en el Sistema Financiero [16]

[15] Fuente: FECOAC- Controladas y no controladas

De acuerdo a información de la Confederación Alemana de Cooperativas- DGRV, para el año 2007, las Cooperativas de Ahorro y Crédito controladas alcanzaban una participación del 8.3% del Sistema Financiero Nacional, al tiempo que las no controladas se posicionaban con una participación del 2%, alcanzando juntas una participación total del 10% del Sistema Financiero Nacional, equivalente al 1643 millones de dólares aproximadamente.

TIPO	Número de Instituciones	Activos (Millones de USD)	Participación en el mercado (%)
CAC Supervisadas	39	1343	8,3
CAC No Supervisadas	1300	300	2,0

TABLA 1.5 Participación de cooperativas en el sistema financiero nacional en año 2007[17]
ELABORADO POR Ing. Mantilla Aníbal

B) NÚMERO DE SOCIOS

En la figura 1.14 puede verse como el número de socios ha aumentado año tras año en las Cooperativas de Ahorro y Crédito controladas por la Superintendencia de Bancos y Seguros, aunque la tasa de crecimiento no ha sido siempre la misma. Lo mismo ha ocurrido con las Cooperativas de Ahorro y Crédito no controladas. La figura en referencia fue elaborada con información de la FECOAC (2001 al 2004), y de la SBS (2005 al 2008).

Para el 2001 el número de socios era de 439889, y para el 2008 era de 2473302, lo cual resulta en un incremento de aproximadamente seis veces el número de socios del año 2001. De acuerdo a información de la FECOAC, el número total de socios que alcanzan las CAC, controladas y no controladas, supera las 3 millones de personas.

[16] Fuente: Asociación de CAC controladas SBS
[17] Fuente: DGRV

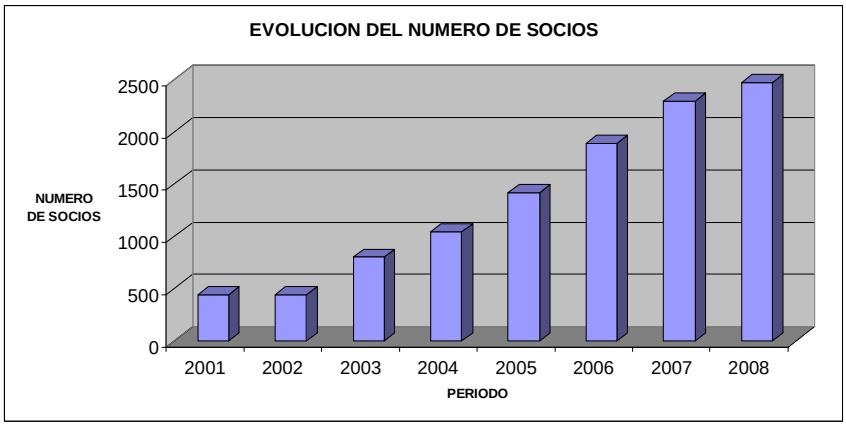

FIGURA 1.14 Evolución del número de socios
ELABORADO POR Ing. Mantilla Aníbal

C) DEPÓSITOS

En la figura siguiente, puede verse como han evolucionado los depósitos en las Cooperativas de Ahorro y Crédito controladas, de acuerdo a información de la Superintendencia de Bancos y Seguros. En el 2005 los depósitos alcanzaban los 540 millones de dólares, mientras que para el año 2008 se había alcanzado la cifra de 1100 millones de dólares, es decir que se había duplicado.

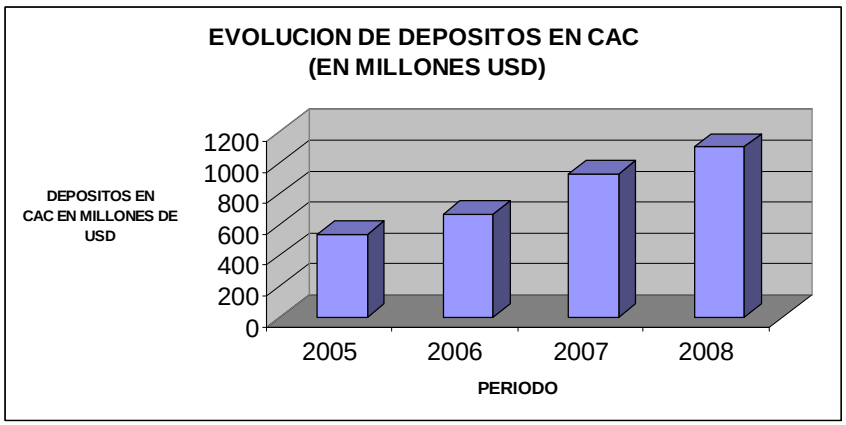

FIGURA 1.15 Evolución de los depósitos en CAC controladas por la SBS
ELABORADO POR Ing. Mantilla Aníbal

D) CARTERA

De acuerdo a la Superintendencia de Bancos y Seguros, las Cooperativas de Ahorro y Crédito controladas pasaron en su cartera, de 632 millones en el 2005, a 1269 millones en el 2008; siguiendo prácticamente la misma tendencia que el comportamiento en los depósitos.

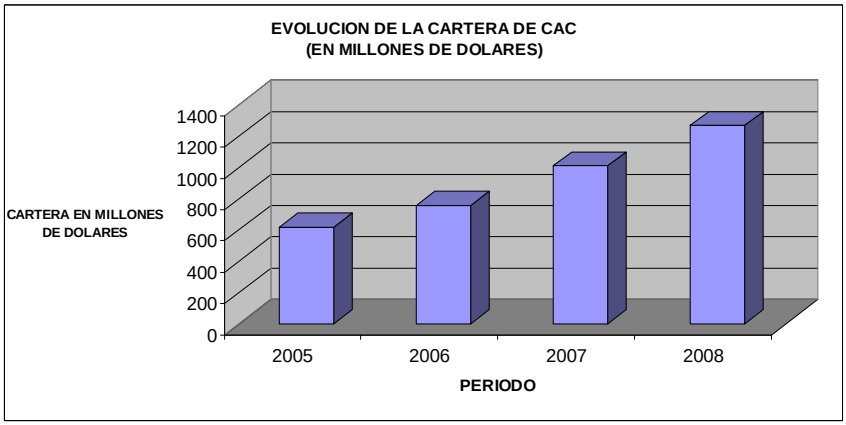

FIGURA 1.16 Evolución de la cartera en CAC controladas por la SBS
ELABORADO POR Ing. Mantilla Aníbal

1.4 ENFOQUE DE LA NORMA ISO 27001 PARA COOPERATIVAS DE AHORRO Y CRÉDITO

Para enfocar la norma ISO 27001 a Cooperativas de Ahorro y Crédito, debe tomarse en cuenta que estas organizaciones están expuestas a diferentes riesgos, sin embargo, el enfoque de la norma se puede establecer en las personas, organización, tecnología y en el ámbito legal. En forma general, los riesgos pueden ser de diferente naturaleza, sin embargo, el Sistema de Gestión de Seguridad de la Información definido en la norma ISO 27001, actúa sobre el riesgo operativo, La siguiente figura muestra este concepto:

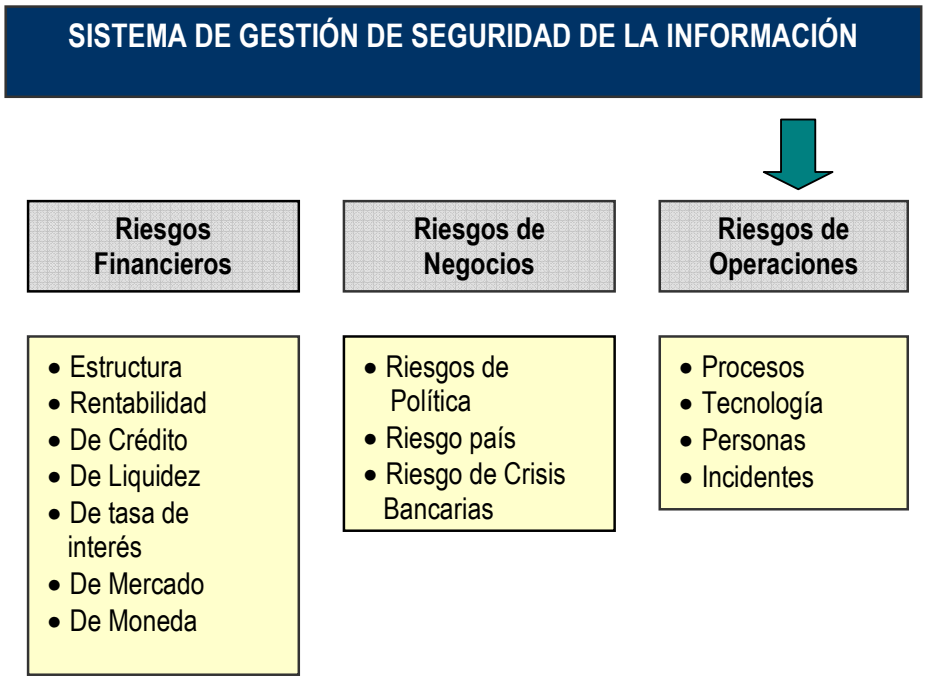

FIGURA 1.17 Actuación del SGSI sobre el Riesgo Operativo
ELABORADO POR Ing. Mantilla Aníbal

1.4.1 ACTORES DEL SISTEMA COOPERATIVO

En las Cooperativas de Ahorro y Crédito, se realizan una gran cantidad de operaciones, tanto hacia adentro como hacia fuera de la organización. En la actual economía global, es importante comprender que la cadena de valor requiere innovación, cambiar el modo de competir, atender adecuadamente a la

Infraestructura de la empresa, la gestión de los recursos humanos, al desarrollo de la tecnología, al aprovisionamiento, a las actividades fundamentales y a las de apoyo; disminuir las barreras y colocarse en el lugar del cliente, sea este usuario final, o proveedor. Es fundamental reconocer y entender adecuadamente a los actores del proceso.

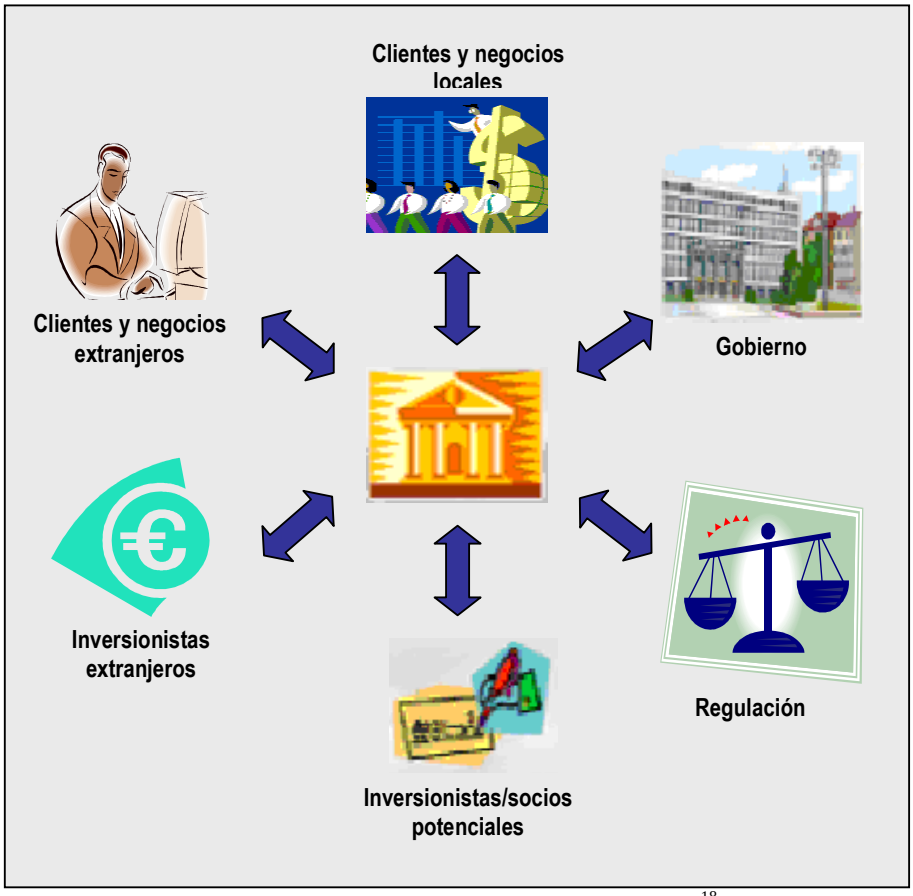

FIGURA 1.18 Actores del sistema cooperativo [18]
ELABORADO POR Ing. Mantilla Aníbal

Para poder alcanzar un elevado nivel de calidad, es necesario dirigir la empresa para los clientes (usuarios finales), estableciendo orden, dando total prioridad a los procesos, midiendo y evaluando lo realmente importante, planificando y expandiendo en forma sostenida a la organización, y preparándose para cualquier escenario impredecible.

[18] Fuente: Above SECURITY, Sergio Quiroz

1.4.2 BENEFICIOS DE UNA COOPERATIVA CON ISO 27001

Los beneficios de un SGSI con ISO 27001:2005 en una organización financiera, son enormes, y repercuten sobre todos los aspectos en los que puede medirse la calidad de una organización.

- Permite a la Organización Financiera alinearse con las exigencias de BASILEA II en relación al riesgo patrimonial
- Desarrolla un sistema para mitigar el riesgo operativo con indicadores de eficacia del desempeño de los controles, facilitando la labor del gobierno corporativo.
- Alto impacto económico al reducir sustancialmente el riesgo operativo en la organización.
- Permite a la empresa tener un sistema que le asegure continuidad en su funcionamiento.

Por ejemplo, en febrero del 2008, la Cooperativa de Ahorro y Crédito “Caja Inmaculada” CAI, obtuvo la máxima certificación de su sistema de gestión de seguridad de la información para todos sus procesos de negocio, conforme a la norma ISO/IEC 27001; siendo la primera entidad financiera española que lo consigue. Esto supone para el cliente disfrutar de los estándares más elevados de seguridad en cuanto a la gestión de sus datos en los distintos canales de la entidad: oficinas, cajeros, Internet y teléfono.

La forma en que la norma ISO 27001:2005 establece Sistema de Gestión de Seguridad de la Información, lo transforma en un recurso valioso que amerita la dedicación de tiempo y esfuerzo. La Política que adopte la organización brinda una base sólida para respaldar el Plan de Seguridad y una base sólida sirve para respaldar empresas sólidas. Dicho de otra manera, esta norma ayuda a formar y mantener sólidas organizaciones.

1.4.3 DESAFÍOS PARA LAS COOPERATIVAS DE AHORRO Y CRÉDITO

En un ámbito local y nacional, las expectativas de las Cooperativas de Ahorro y Crédito, anhelan alcanzar un nivel de cambio que les permita realizar exitosamente el E-Business, una operación global, estándar internacional, entre otros aspectos.

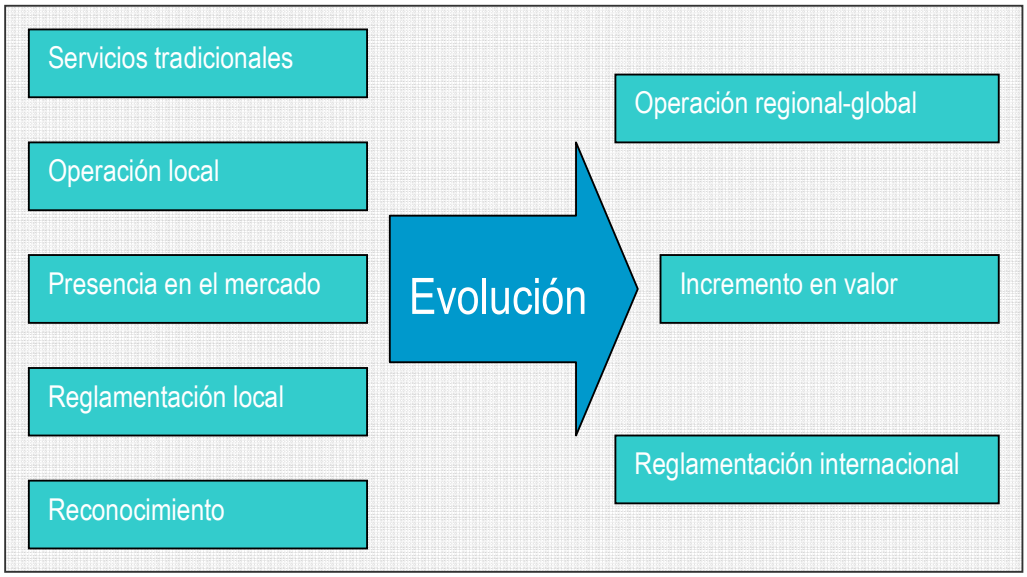

FIGURA 1.19 Retos de las Cooperativas de Ahorro y Crédito [19]
ELABORADO POR Ing. Mantilla Aníbal

Dado que la norma ISO 27001:2005, esta enfocada en los procesos, en la mejora continua, en base al ciclo de Deming (planificar, actuar, medir, corregir), es un excelente soporte para lograr el éxito organizacional en la Gestión de la Seguridad de la Información.

En el ámbito regional latinoamericano, existen también grandes desafíos para las Cooperativas de Ahorro y Crédito; estos son:

Los desafíos en el ámbito regional latinoamericano son:

1. Cooperativas de Ahorro y Crédito bajo supervisión
2. Crecimiento y sostenimiento del sector en el tiempo
3. Gestión adecuada de las TIC's
4. Competitividad y calidad

[19] Fuente: Above SECURITY, Sergio Quiroz

5. Participación trascendente en la Integración de Cooperativas
6. Responsabilidad social
7. Cumplimiento de estándares
8. Capacidad para influir en grandes decisiones de un país
9. Transparencia en sus operaciones
10. Elevado desarrollo interno

Estos desafíos pueden entenderse mejor, al analizar los siguientes datos estadísticos.

En Cooperativas de Ahorro y Crédito de Latinoamérica: [20]

Número de CAC: 7262

Número de CAC supervisadas: 2896

Monto de activos: 29638 USD

Monto de cartera de crédito: 16426 Millones de USD

Número de asociados: 20.306.210

Crédito promedio por asociado: 1236 USD

Asociados PEA: Ecuador: 46.4 %, Paraguay 34%, Costa Rica 34%, Chile 11%.

[20] Fuente: Desafíos para la Gestión de Cooperativas de Ahorro y Crédito en Latinoamérica, Álvaro Durán

CAPÍTULO 2.

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA COOPERATIVAS DE AHORRO Y CRÉDITO

En este capítulo se diseña un Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito, en base a la norma ISO 27001, la ley de la Súper Intendencia de Bancos y Seguros, y la Ley de Cooperativas de Ahorro y Crédito, del Sistema Financiero Ecuatoriano.

Se realiza el análisis y la determinación del Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito, desarrollando de esta manera una guía para la aplicación de las cláusulas y anexos de la norma ISO 27001, seguidamente, de manera resumida a través de un ejemplo se muestra una metodología para el análisis, evaluación y tratamiento del riesgo.

En segundo lugar, dada la importancia que tiene para este tipo de organizaciones, se trata en una sección específica, el Plan para la Continuidad del Negocio, desarrollando de esta manera, una guía para el manejo del mismo en la Cooperativas de Ahorro y Crédito, igual que en el caso anterior, se presenta un ejemplo resumido para desarrollo y aplicación de BCP.

Finalmente, se establece una guía para documentar el Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito, estableciendo lo que verdaderamente tiene importancia para ser documentado por la organización, y una forma adecuada de efectuarlo.

2.1 ANÁLISIS Y DETERMINACIÓN DEL SGSI PARA COOPERATIVAS DE AHORRO Y CRÉDITO

Para poder realizar el proceso de análisis de determinación es fundamental comprender el enfoque de las cláusulas globales y focales de la norma ISO 27001. Es necesario tener el conocimiento de las normas, reglamentos, estatutos, objetivos, políticas de la Cooperativa de Ahorro y Crédito; en está sección, esto se realiza en las CLAUSULAS 0,1, 2 y 3.

El establecimiento y gestión del SGSI, con la metodología para identificar, evaluar, y tratar el riesgo, incluyendo una guía para documentar el SGSI, es abordado en la CLAUSULA 4.

Las CLAUSULAS 5, 6, 7, y 8 hacen referencia a la responsabilidad de la dirección, a las auditorias, al monitoreo y mejoramiento continuo del SGSI.

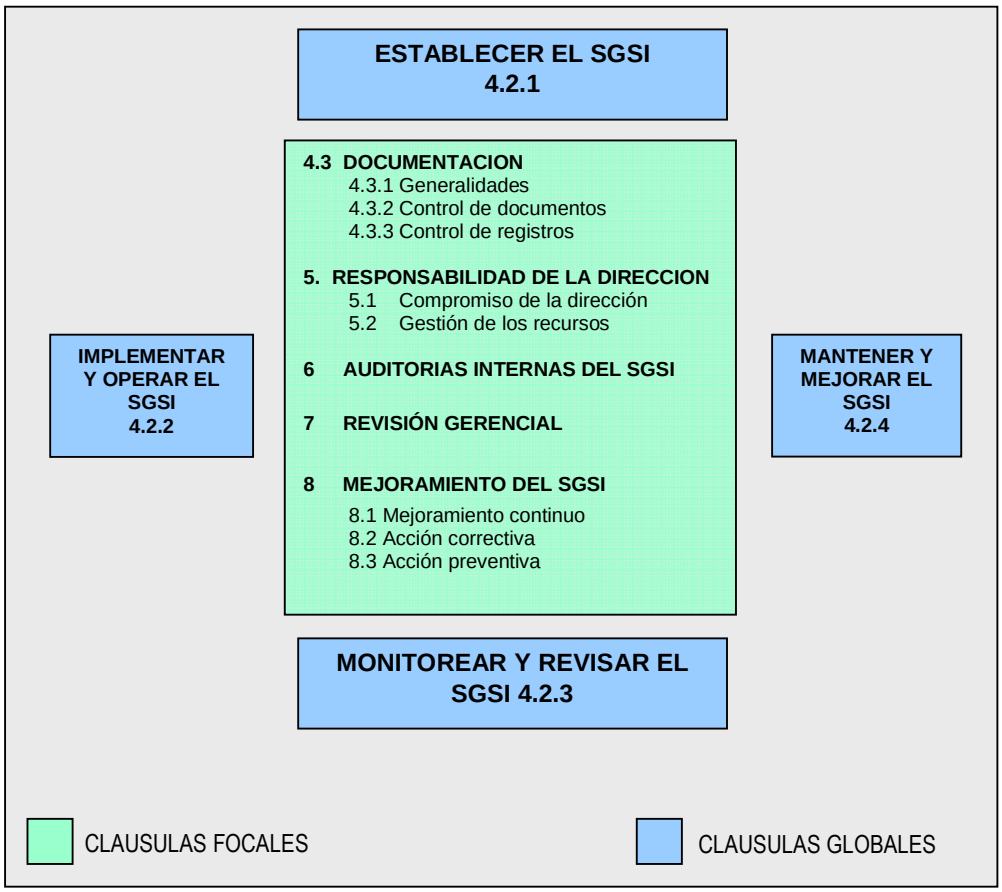

FIGURA 2.1 Secciones de la Cláusulas focales y globales de la Norma ISO 27001[21]
ELABORADO POR Ing. Mantilla Aníbal

2.1.1 DESARROLLO DE GUÍA PARA LA APLICACIÓN DE LAS CLÁUSULAS DE LA NORMA ISO 27001 EN BASE A LA LEY DE LA SBS Y LA LEY DE CAC, DEL SISTEMA FINANCIERO ECUATORIANO.

CLÁUSULA 0. INTRODUCCIÓN

El modelo ISO 27001:2005 está diseñado bajo una óptica de enfoque a procesos. El SGSI está conceptualizado para funcionar en cualquier tipo de organización, operando bajo el enfoque de procesos, sin embargo, cada SGSI se elabora de la manera más adecuada para cada empresa. En el caso de las Cooperativas de Ahorro y Crédito, son un sector en constante crecimiento, que representa a una

[21] Fuente: Implantación del ISO 27001, Alexander, P:hD

parte importante del Sistema Financiero Nacional, razón por la cual requieren un SGSI acorde a su naturaleza y objetivos.

CLÁUSULA 1. OBJETO

En esta cláusula se indica los requerimientos del estándar que no pudiesen ser aplicados debido a la naturaleza de una organización y su negocio, considerando así, exclusiones. Además especifica los requisitos para la implementación de controles de seguridad adaptados a la organización o parte de ella. El objeto en este caso, hace referencia a las más de mil trescientas Cooperativas de Ahorro y Crédito Ecuatorianas, considerando que dependiendo de los montos que manejan, estructura y organización, tienen, unas más que otras, la posibilidad de enfocarse en los procesos de la norma ISO 27001.

CLÁUSULA 2. REFERENCIAS NORMATIVAS

Hace referencia a documentos que son indispensables para la aplicación de esta estándar. Pueden ser documentos fechados como no fechados, en los dos casos se requiere justificación para su uso. En este caso, las referencias normativas alineadas a la norma ISO 27001, son aquellas establecidas por la Superintendencia de Bancos y Seguros, y la Ley de Cooperativas en referencia a las Cooperativas de Ahorro y Crédito.

CLÁUSULA 3. TÉRMINOS Y DEFINICIONES

Aquí se establecen los principales términos y definiciones en base a los cuales trabaja la norma ISO 27001. Algunos de los términos más frecuentemente citados en este desarrollo son:

Activo de información: Es algo que la organización directamente le asigna un valor, y por lo tanto, la organización lo debe proteger.

Amenaza: Cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

CAC: cooperativas de ahorro y crédito

Riesgo: Es la probabilidad de que la amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

SBS: Superintendencia de Bancos y Seguros.

Tecnología de la información: Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros.

Vulnerabilidad: Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir perdidas a la organización.

En el glosario de términos se encuentra una lista más amplia de los términos a los que se hace referencia en este capítulo.

CLÁUSULA 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

Refiere a los requerimientos de la organización, el establecimiento y gestión del SGSI, su respectiva documentación.

CLÁUSULA 4: Sección 4.1 ESTABLECER LOS REQUISITOS GENERALES

Los Requisitos Generales para los SGSI de las Cooperativas de Ahorro y Crédito, son aquellos propios a la naturaleza, operación y riesgos a los que están sometidas.

La implementación de un SGSI requiere el despliegue de recursos significativos; por esto las organizaciones deben estar conscientes sobre sus razones para implantar el sistema. Diferentes organizaciones tendrán distintos estímulos para implantar el SGSI. Los motivos podrán estar derivados de aspectos regulatorios, legales, su estado, el tamaño de la firma, su ubicación geográfica, el tipo de negocio en que están inmiscuidas o el servicio que ofrecen. La razón de por qué implementar el SGSI, debe estar claramente documentada, y debe plantear los costos en contraposición a los beneficios que puedan obtenerse al incrementar la habilidad, al gestionar el riesgo de la información en la empresa.

El SGSI no puede implantarse de manera aislada; la empresa debe considerar los riesgos de la organización y las estrategias globales de la firma. Siempre se debe tener presente que el SGSI es un sistema de gestión, el cual se convierte en una herramienta de la alta gerencia.

Las instituciones controladas por la SBS deben mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

CLÁUSULA 4: Sección 4.2 ESTABLECER Y GESTIONAR EL SGSI

Para el ***Establecer y Gestionar el SGSI*** en Cooperativas de Ahorro y Crédito, se considera documentación de la Superintendencia de Bancos y Seguros, referente a la operación, los riesgos, los controles, las auditorias internas y externas, los planes de continuidad, entre otros, para determinar los activos a proteger y como protegerlos, en el Sistema Financiero. Se ha tomado además, como elemento fundamental para el establecimiento del SGSI, la realidad de la Cooperativas de Ahorro y Crédito, en su desempeño, organización, controles, riesgos, crecimiento, entre otros. Como puede verse en la figura anterior, esta cláusula posee cuatro componentes, que permiten en el SGSI: el establecimiento, la implementación y la operación, el monitoreo y la revisión, y, el mantenimiento y la mejora.

Sección 4.2: Subsección 4.2.1 ESTABLECRE EL SGSI

Las fases que se listan a continuación, son aquellas que deben seguirse para poder establecer el SGSI:

A) Definir el alcance y los límites del SGSI

B) Definir la política para el SGSI

C) Definir el enfoque para la evaluación del riesgo

D) Identificar, analizar y evaluar los riesgos

E) Identificar y evaluar las opciones para el tratamiento del riesgo, incluyendo al riesgo residual

F) Seleccionar los objetivos de control para el tratamiento del riesgo

G) Obtener la aprobación de los riesgos residuales por la dirección

H) Obtener la autorización de la dirección para implementar y operar el SGSI

I) Preparar una declaración de aplicabilidad

A continuación se desarrollan cada una de estas fases:

A. DEFINIR EL ALCANCE Y LOS LÍMITES DEL SGSI

La definición del alcance del SGSI es una de las más importantes decisiones en todo el proceso de su establecimiento. La definición del alcance y su magnitud está en la decisión que tome la empresa. El alcance del SGSI, puede ser toda la organización, o simplemente una parte de ella, o un simple proceso, o un sistema de información.

En esencia, el alcance obedece a decisiones estratégicas de la organización. Una vez determinado el alcance del estándar en la empresa, se debe proceder a identificar los distintos activos de información que se convierten en el eje principal del modelo. La definición del alcance del SGSI debe incluir las interfaces, y debe contemplar los intereses y dependencias del SGSI con otras partes de la organización, otras organizaciones, los proveedores o cualquier otra entidad externa al SGSI. El alcance de un SGSI debe ser adecuado y apropiado, tanto para las capacidades organizacionales y su responsabilidad de proveer seguridad en la información que cumpla con los requerimientos determinados por la evaluación del riesgo, como por los controles regulatorios y legales. Las Cooperativas de Ahorro y Crédito que realizan intermediación financiera con el público en general están expuestas a una serie de riesgos, lo que determina la necesidad de identificar, medir, controlar y monitorear los mismos, en función de la naturaleza y complejidad de sus operaciones. Las prácticas modernas de supervisión han demostrado que es necesario que las Cooperativas de Ahorro y Crédito que realizan intermediación financiera con el público, cuenten con una adecuada disciplina financiera en concordancia con los principios de prudencia y solvencia financiera a fin de ser viables y sostenibles, que facilite el desarrollo de la supervisión por riesgos, tomando en consideración el mercado actual en que

esas entidades desenvuelven sus actividades y la dinámica del sistema financiero ecuatoriano.

B. DEFINIR LA POLÍTICA PARA EL SGSI

En las Cooperativas de Ahorro y Crédito, todo esfuerzo enfocado a la seguridad de la información tiene su base fundamental en las Políticas para la Gestión de las tecnologías de la información y comunicación. El proceso para fortalecer la seguridad de la información debe tener un conjunto de políticas que brinden instrucciones claras y establezcan el soporte sobre el cual se manejará la alta gerencia. Las políticas son usadas como punto de referencia para un sin número de actividades relacionadas con la seguridad de la información tales como: Diseño de controles en los sistemas de información, controles de acceso, análisis de riesgos, sanciones disciplinarias de funcionarios por violaciones en la seguridad, entre otros. Las políticas de seguridad tienen un impacto muy alto en la organización, debiendo ser revisadas periódicamente para asegurar su aplicabilidad en la organización.

El ISO 17799 plantea que el objetivo de la política es proveer a la gerencia dirección y apoyo para la seguridad de la información.

La gerencia debe aprobar la política, y asegurarse de que todos los empleados la han recibido y entienden su efecto en sus tareas cotidianas. En forma general, las políticas deben referirse por lo menos a:

- Diseño claro de los procesos, los cuales deben ser adaptables y dinámicos
- Descripción en secuencia lógica y ordenada de las actividades, tareas, y controles
- Determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros
- Difusión y comunicación de los procesos buscando garantizar su total aplicación

- Actualización y mejora continua a través del seguimiento permanente en su aplicación
- Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas.

La Asamblea General, tiene atribución para conocer el plan estratégico, el plan operativo y presupuesto de la cooperativa, además de nombrar y remover a los vocales del Consejo de Administración. Mientras que el Consejo de Administración debe dictar los reglamentos interno, orgánico - funcional, de crédito y las demás normas internas, con sujeción a las disposiciones contenidas en la ley de CAC y las normas expedidas por la Junta Bancaria, los cuales podrán ser revisados por el organismo de control.

C. DEFINIR EL ENFOQUE PARA LA EVALUACIÓN DEL RIESGO

Es importante que la información de seguridad se gestione con transparencia y consistencia a través de la organización. La gestión de los riesgos puede utilizar distintos enfoques gerenciales y métodos de cálculo que satisfagan las necesidades de la organización. La organización decidirá qué método de cálculo del riesgo se escoge.

En la sección 4.2.1 de la norma ISO 27001:2005, se establece el marco conceptual para escoger el enfoque para hacer el cálculo del riesgo, describiendo los elementos obligatorios que el proceso del cálculo del riesgo debe contener. Los elementos obligatorios a tener en cuenta son:

- Determinación del criterio para la aceptación del riesgo. Se deben documentar las circunstancias bajo las cuales la organización está dispuesta a aceptar los riesgos.

- Identificación de los niveles aceptables del riesgo. Al margen del tipo de enfoque que se utilice para el cálculo del riesgo, deben estar identificados los niveles de riesgo que la organización considere aceptables.
- Cobertura de todos los aspectos del alcance del SGSI. El enfoque escogido por la empresa, para el cálculo del riesgo debe contemplar un análisis exhaustivo de todos los controles presentados en el Anexo A del ISO 27001:2005.
- El cálculo del riesgo debe lograr un claro entendimiento sobre qué factores deben controlarse, en la medida en que estos factores afecten sistemas y procesos que sean críticos para la organización. Las actividades de la gestión del riesgo deben contemplar la relación costo-beneficio y verificar su pragmatismo. Una eficaz gestión del riesgo significa un buen balance entre el gasto en recursos contra el deseado grado de protección, y asegurando que los recursos gastados sean correlacionados con la potencial pérdida y el valor de los activos protegidos.

El enfoque que la empresa escoja y su nivel de detalle y complejidad influencian el esfuerzo y los recursos requeridos durante el proceso del cálculo del riesgo. El cálculo del riesgo debe ser tan detallado y complejo como sea necesario, para así poder atender todos los requerimientos de la organización y lo que se requiera por el alcance del SGSI, pero nada más. El exceso de detalles puede determinar un exceso de trabajo, y un enfoque muy genérico puede conducir a subestimar aspectos de riesgos importantes. Por esta razón, el enfoque debe identificar los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones.

D. IDENTIFICAR, ANALIZAR Y EVALUAR LOS RIESGOS

Este proceso incluye:

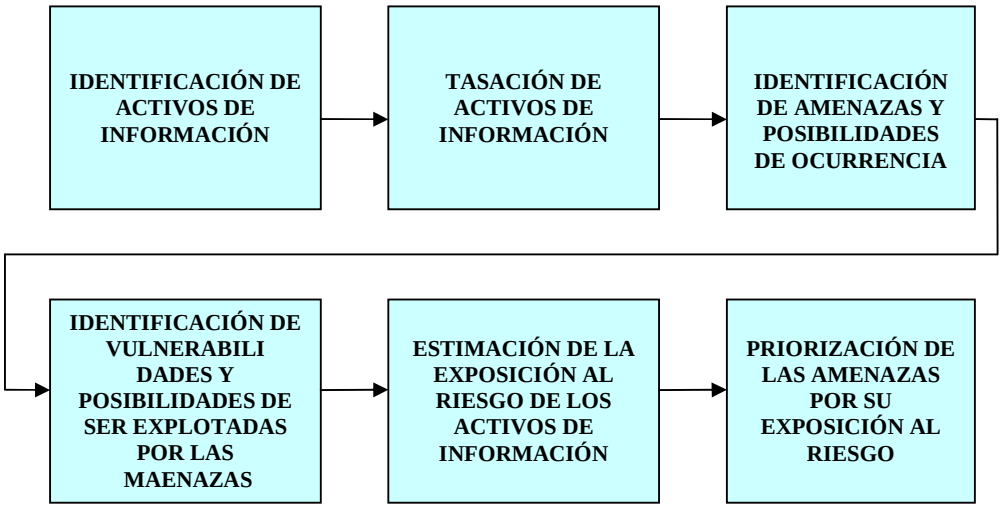

FIGURA 2.2 Pasos metodológicos del análisis del riesgo[22]

ELABORADO POR Ing. Mantilla Aníbal

Identificar los activos de información

El análisis, la evaluación del riesgo, y las decisiones que se tomen en relación con el tratamiento del riesgo en la empresa giran alrededor de los activos de información identificados.

En el contexto del ISO un activo de información es algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger.

El ISO 17799:2005 clasifica los activos de información en las categorías siguientes:

- Activos de información (datos, manuales de usuario, etc).
- Documentos de papel (contratos).
- Activos de software (aplicación, software de sistemas, etc).
- Activos físicos (computadoras, medios magnéticos, etc).
- Personal (clientes, personal).
- Imagen de la compañía y reputación
- Servicios (en comunicaciones).

[22] Fuente: Análisis y evaluación del riesgo de información, Alexander, P:hD

El Gerente General de la CAC, deberá actualizar y mantener bajo su custodia los inventarios de bienes y valores de la entidad, informar al Consejo de Administración sobre la situación financiera de la entidad, de riesgos y su impacto en el patrimonio, cumplimiento del plan estratégico, y sobre otros que sean solicitados, así como presentar el informe anual de gestión.

Identificar los requerimientos legales y comerciales para los activos identificados

Los requerimientos de seguridad en cualquier organización, al margen del tamaño de la empresa, se derivan de tres fuentes. La **primera fuente** deriva de la evaluación de los riesgos que afectan a la organización. Aquí se determinan las amenazas de los activos, luego se ubican las vulnerabilidades, se evalúa su posibilidad de ocurrencia, y se estiman los potenciales impactos. La **segunda fuente** es el aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse. La **tercera fuente** es el conjunto particular de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

Tasar los activos de información

La tasación de activos se la realiza de manera que muestre cualitativamente el valor de los mismos para la organización, se puede utilizar la escala de Likert, la cual establece: 1 – Muy bajo, 2 – Bajo, 3 - Medio, 4 – Alto, 5 – Muy alto.

El propietario de los activos debe ser responsable por definir apropiadamente la clasificación de seguridad y los derechos de acceso a los activos, y establecer los sistemas de control. La responsabilidad del propietario debiera ser también la de revisar periódicamente los derechos de acceso y la clasificación de seguridad. Las personas que utilizan los activos, deben estar conscientes de las reglas para el manejo de activos como parte de su descripción del puesto.

Identificación de amenazas y posibilidad de ocurrencia

Una amenaza es una indicación de un evento desagradable con el potencial de causar daño.

La clasificación de amenazas por su naturaleza, indica lo siguiente:

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, suspensión del servicio de agua, pérdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (pérdida de proveedores, fallas en equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

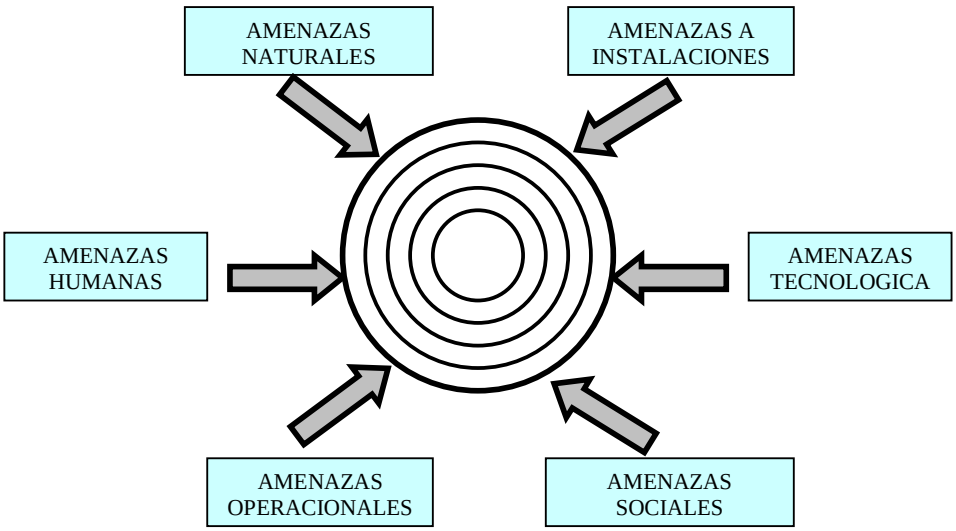

FIGURA 2.3 Clasificación de amenazas a la organización
ELABORADO POR Ing. Mantilla Aníbal

Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño. Una vez identificadas las distintas amenazas que pueden afectar un activo, se debe evaluar su posibilidad de ocurrencia. Una amenaza con baja posibilidad de

ocurrencia pudiera tener severas consecuencias económicas en la organización. Por cada amenaza, para medir la posibilidad de ocurrencia se puede utilizar la escala de Likert: 1 – Muy bajo, hasta 5 – Muy alto.

Identificar las vulnerabilidades y la posibilidad de ser explotadas por las amenazas

Las **vulnerabilidades** son debilidades de seguridad asociadas con los activos de información de una organización.

Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo. La clasificación de las vulnerabilidades en base a la ISO 17799:2005, indica lo siguiente:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).
- Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, passwords sin modificarse).
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje.
- Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).
- Mantenimiento, desarrollo y adquisición de sistemas de información

(protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos).

Una vez identificadas las vulnerabilidades, por cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por la amenaza; para ello se puede utilizar la escala de Likert: 1 – Muy bajo,hasta 5 – Muy alto.
Las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos.

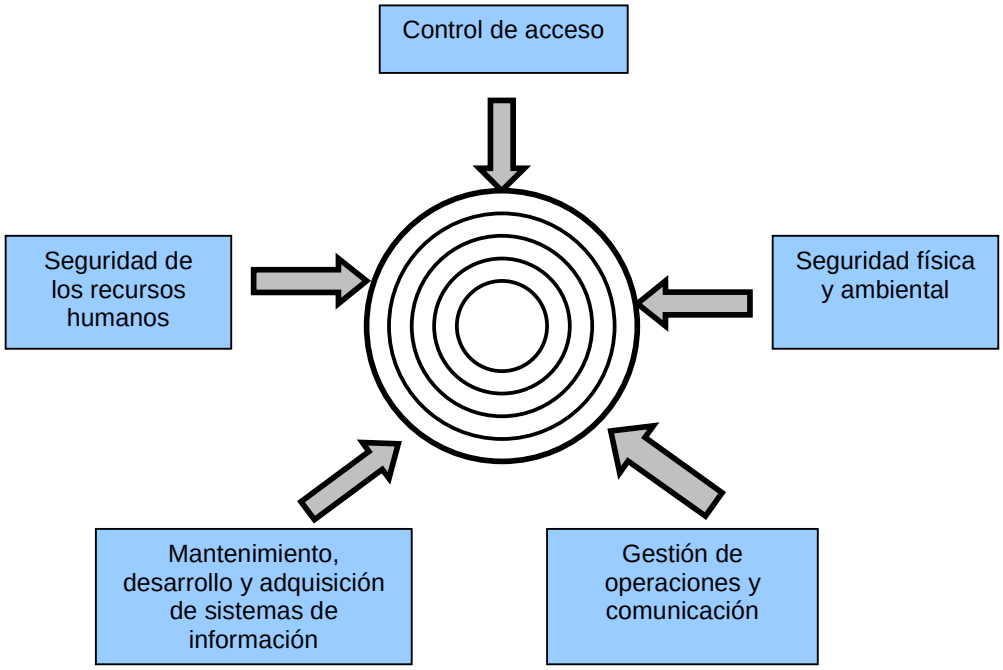

FIGURA 2.4 Clasificación de las vulnerabilidades de la organización
ELABORADO POR Ing. Mantilla Aníbal

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de relación de causalidad y probabilidad de ocurrencia.

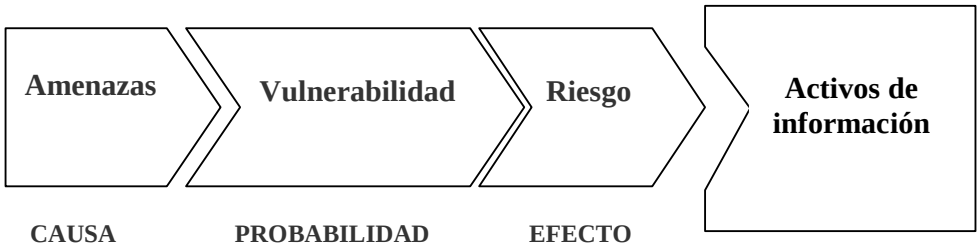

FIGURA 2.5 Relación causa-efecto entre activos, riesgo, vulnerabilidades y amenaza[23]
ELABORADO POR Ing. Mantilla Aníbal

Estimar la exposición al riesgo de los activos de información

El **riesgo** se define como la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

Todo riesgo tiene dos factores: uno que expresa el impacto del riesgo si ocurriera (Valor económico del activo en riesgo), y otro que expresa la probabilidad de que el riesgo ocurra.

Priorizar las amenazas por su exposición al riesgo

Finalmente, las amenazas pueden ser priorizadas en orden, con base en su factor de exposición al riesgo. Esta priorización permitirá tomar las acciones adecuadas al momento de tratar el riesgo.

[23] Fuente: Análisis y evaluación del riesgo de información, Alexander, P:hD

Evaluar el riesgo

Una vez realizado el cálculo del riesgo por cada activo, en relación con su amenaza, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los mas significativos. A este proceso se denomina ***evaluación del riesgo***.

Los criterios que Alberto Alexander, Ph.D. recomienda para determinar los niveles o importancia del riesgo son:

- Impacto económico del riesgo.
- Tiempo de recuperación de la empresa
- Posibilidad real de ocurrencia del riesgo
- Posibilidad de interrumpir las actividades de la empresa

E. IDENTIFICAR Y EVALUAR LAS OPCIONES PARA EL TRATAMIENTO DEL RIESGO, INCLUYENDO AL RIESGO RESIDUAL

Reducción del riesgo

Para todos aquellos riesgos donde la opción de reducidos se ha tomado, se deben implementar controles apropiados para poder reducidos al nivel que se haya definido como aceptable. Al haber identificado el nivel de control, conviene considerar los requerimientos de seguridad relacionados con los riesgos.

Los controles pueden reducir el riesgo estimado en dos maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza
- Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos

Para proteger sus activos, una organización, es decir, la Cooperativa de Ahorro y Crédito escoge adoptar cuál de estas maneras o una combinación de ambas; ésta es una decisión comercial que depende de los requerimientos del negocio, el ambiente y las circunstancias en las cuales la organización necesita operar.

No existe un enfoque universal para hacer la selección de objetivos de control y controles. El proceso de selección comprende numerosas decisiones y consultas, y usualmente discusiones con distintas partes de la organización y con un

determinado número de personas clave. El proceso de selección requiere producir un resultado que más se adecue a la organización en términos de sus requerimientos para la protección de sus activos, inversiones, cultura y tolerancia al riesgo.

Aceptar objetivamente el riesgo

Muchas veces se presenta la situación en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada.

Transferir el riesgo

La transferencia del riesgo es una opción cuando para la compañía es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias. Algo muy importante que debe recordarse es el riesgo residual que siempre estará presente.

Evitar el riesgo

Se refiere a cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular, para así evitar la presencia del riesgo. El riesgo puede evitarse por medio de:

- No desarrollar ciertas actividades comerciales
- Mover los activos de un área de riesgo
- Decidir no procesar información particularmente sensitiva

En la figura 2.6 se presenta en forma esquemática el proceso de toma de decisiones para elegir una opción de tratamiento del riesgo.

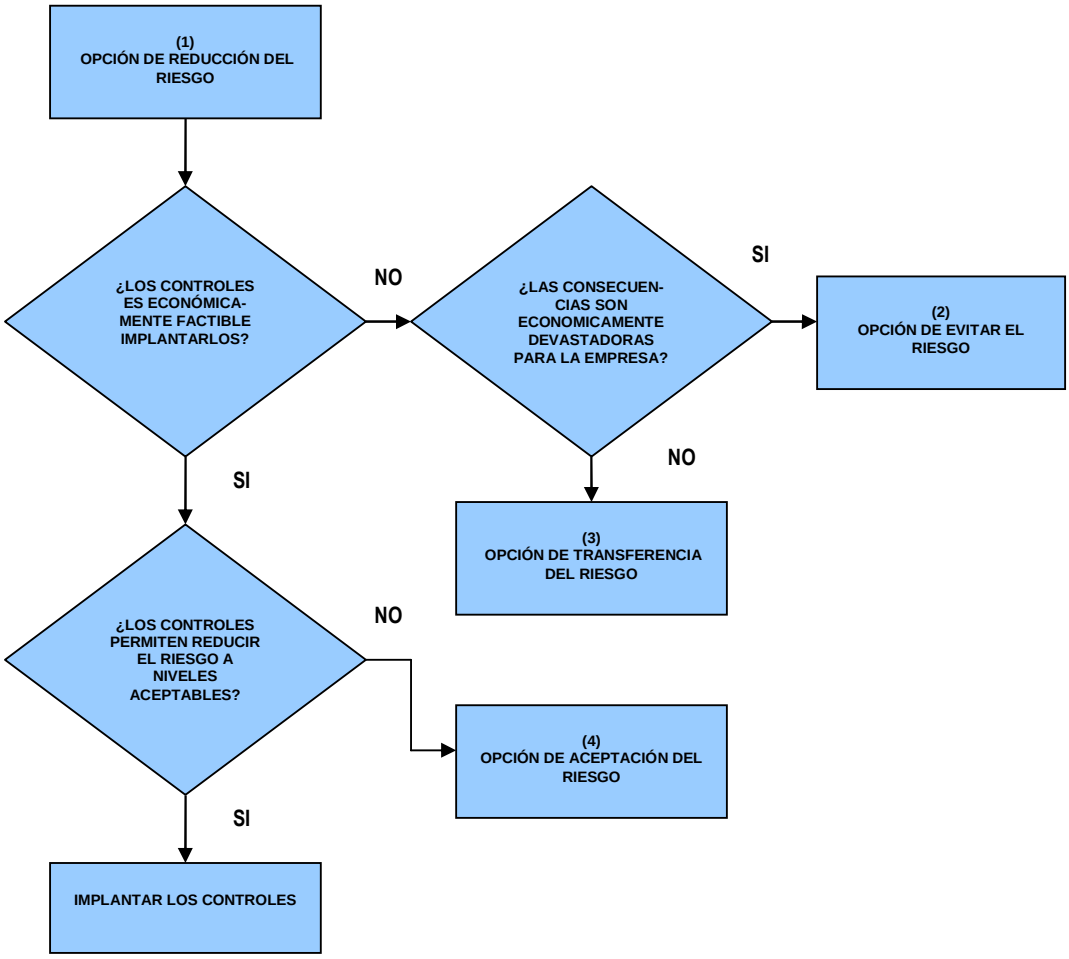

FIGURA 2.6 Proceso de toma de decisiones para el tratamiento del riesgo [24]
ELABORADO POR Ing. Mantilla Aníbal

Riesgo residual

Después de implementar las decisiones relacionadas con el tratamiento de un riesgo, siempre habrá un remanente de ese mismo riesgo. Justamente el riesgo que queda, después de implantar el plan de tratamiento, se denomina riesgo residual, que puede ser difícil de calcular, pero por lo menos debe realizarse una evaluación para asegurar que logra la protección suficiente.

Si el riesgo residual se considerara inaceptable, deben tomarse decisiones para resolver su caso. Una opción es identificar diferentes opciones de tratamiento de riesgo; otra es instaurar más controles, o hacer arreglos con aseguradoras para

[24] Fuente: Gestión del riesgo en el Business Continuity Planning, Alexander, P:hD

reducir finalmente el riesgo a niveles aceptables.

A veces, dada la naturaleza de la industria y de los riesgos inherentes, reducir los riesgos a un nivel aceptable pudiera no ser posible o financieramente aceptable.

Ante estas circunstancias, pudiera necesitarse objetivamente aceptar el riesgo. Todos los riesgos residuales que se hayan aceptado debieran ser documentados y aprobados por la gerencia.

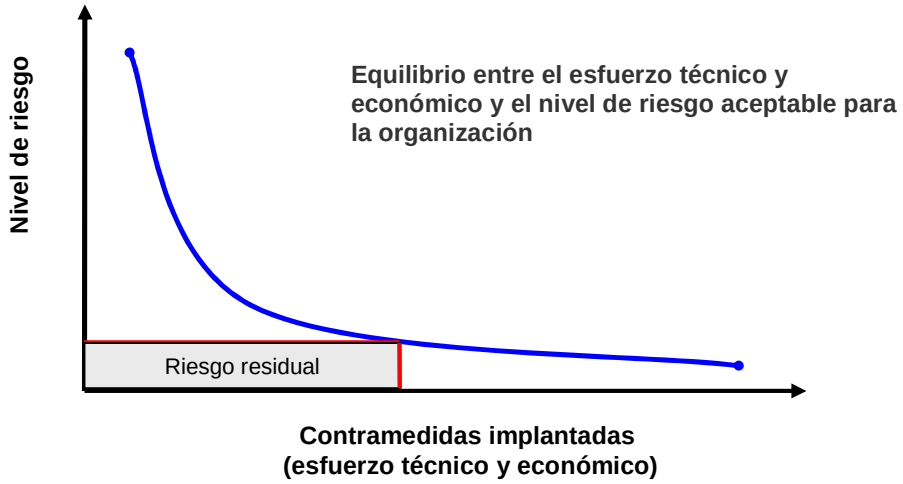

FIGURA 2.7 Nivel de riesgo residual [25]
ELABORADO POR Ing. Mantilla Aníbal

F. SELECCIONAR LOS OBJETIVOS DE CONTROL PARA EL TRATAMIENTO DEL RIESGO

Una vez se realiza el proceso de identificar las opciones de tratamiento del riesgo y haberlas evaluado, la empresa debe decidir cuáles objetivos de control y controles escoger para el tratamiento del riesgo.

La selección de objetivos de control y controles debe efectuarse tomando en cuenta el criterio establecido para la aceptación de los riesgos, así como los requerimientos legales, reguladores y contractuales. La selección de los objetivos de control y los controles, según el ISO 27001:2005, debe ser del Anexo A.

[25] Fuente.Enciclopedia de la Seguridad Informática, Álvaro Gómez

G. OBTENER LA APROBACIÓN DE LOS RIESGOS RESIDUALES POR LA DIRECCIÓN

Es imposible llevar los riesgos a cero en la organización, y aun si fuera posible hacerlo, quizá su costo operativo y financiero lo haría inviable. Esto significa que hay que asumir un riesgo, ya sea para transferirlo a una tercera parte como una aseguradora, o para que la misma organización se encargue de ella. Sin embargo, se requiere que la Dirección empresarial conozca cuales son los riesgos residuales, y que prueben los planes para su tratamiento, ya sea por parte de la organización, o actividad de terceros.

H. OBTENER LA AUTORIZACIÓN DE LA DIRECCIÓN PARA IMPLEMENTAR Y OPERAR EL SGSI

Una vez que se han tomado las decisiones relacionadas con el tratamiento del riesgo, las actividades para poder implantar estas decisiones tienen que ejecutarse. Para este fin hay que identificar y planear las actividades. Cada actividad de implementación debe ser identificada con claridad y desagregarse en una gama de subactividades requeridas para poder distribuir las responsabilidades a las personas, estimar los requerimientos de recursos, el conjunto de entregables, las fechas críticas y la supervisión del progreso.

La implantación del plan de tratamiento del riesgo se convierte en un proyecto, y debe manejarse como tal. La empresa debe hacer hincapié en asignar a la persona idónea para responsabilizarla del proyecto, visualizar los recursos necesarios y manejar los reforzadores de conducta organizacional, que aseguren el correcto desempeño del proyecto.

I. PREPARAR UNA DECLARACIÓN DE APLICABILIDAD

Todos los objetivos de control y controles escogidos del Anexo A forman parte de la declaración de aplicabilidad. La declaración de aplicabilidad debe incluir todos los objetivos de control, los controles seleccionados y se exige que se haga una breve explicación de las razones para su selección. También deben incluirse los objetivos de control y controles existentes y, por último, detallarse la exclusión de cualquier objetivo de control y controles del Anexo A, con la respectiva explicación de su exclusión.

Sección 4.2: Subsección 4.2.2 IMPLEMENTAR Y OPERAR EL SGSI

Deben implementarse controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos. Deben existir controles formales para proteger la información contenida en documentos, medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores. Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deben contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría. El Gerente General debe suministrar la información que le soliciten los socios, representantes, órganos internos de la cooperativa, la Superintendencia y otras instituciones, de acuerdo con la ley.

Sección 4.2: Subsección 4.2.3 MONITOREAR Y REVISAR EL SGSI

Para poder efectuar seguimiento, es necesario contar con adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento. Debe existir además, un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo. El Gerente General deberá responder por la marcha administrativa, operativa y financiera de la cooperativa e informar, al menos trimestralmente, al Consejo de Administración de los resultados; cumplir y hacer cumplir a los socios las disposiciones emanadas de la Asamblea general y del Consejo de Administración.

Sección 4.2: Subsección 4.2.4 MANTENER Y MEJORA EL SGSI

Es fundamental, una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados; Se requiere además, documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución. Mantener los controles y procedimientos adecuados para asegurar el control interno son atribuciones y responsabilidades del Gerente General.

CLÁUSULA 4: Sección 4.3 DOCUMENTAR EL SGSI

Refiere a la necesidad de existencia de Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información. Las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware, con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada.

El Gerente General deberá presentar a la Superintendencia cuando lo requiera, los manuales de control interno, de administración de riesgos y los que disponga la normativa aprobada por la Junta Bancaria; y remitir los informes y otros reportes que sean requeridos por la Superintendencia en la forma y periodicidad que ésta determine.

CLÁUSULA 5. DEFINIR LA RESPONSABILIDAD DE LA DIRECCIÓN

Esta cláusula hace referencia al compromiso de la gerencia y su gestión de los recursos, acorde los requerimientos de la norma ISO 27001. Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor "personas", tales

como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución. Dichos procesos corresponden a:

- **Los procesos de incorporación.-** Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal

- **Los procesos de permanencia.-** Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales.

- **Los procesos de desvinculación.-** Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas. El Gerente General es quien tiene la atribución y el deber de contratar, remover y sancionar, de acuerdo a las políticas que fije el Consejo de Administración a los empleados de la cooperativa, cuyo nombramiento o remoción no sea de competencia de otro órgano de la entidad, y fijar sus remuneraciones que deberán constar en el presupuesto de la entidad;

Las instituciones controladas deben analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional. Además, mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente. El Consejo de Administración debe aprobar el plan estratégico, el plan operativo y el presupuesto y llevados a conocimiento de la asamblea general. De haber modificaciones, éstas no superarán el 10% del presupuesto conocido por la Asamblea.

La dirección, además, es responsable de:

- Apoyar y establecer un compromiso formal con el organismo que haga las veces de alta gerencia.
- Ubicar a una persona que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos.
- Difundir y comunicar a todo el personal involucrado, las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación.
- Conocer los informes que presente el Gerente General sobre la situación financiera de la cooperativa, el diagnóstico de riesgos y su impacto en el patrimonio, el cumplimiento del plan estratégico, así como el informe anual

correspondiente y tomar las decisiones que estime apropiadas; así como también debe conocer el informe que presente el Comité de Administración Integral de Riesgos. En este punto particular, es el Consejo de Administración el llamado a conocer esos informes.

- Capacitar y entrenar técnicamente al personal del área de tecnología de información y a los usuarios de la misma

- Establecer un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes.

- Definir niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude. Además de asegurar instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida.

- Cuidar las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información.

- Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo.
- Aprobar los planes de contingencia y de continuidad del negocio.

- Conocer y aprobar esquemas de administración, que incluyan procedimientos para la administración, gestión y control de riesgos inherentes a su negocio. Además de designar a la firma calificadora de riesgos. Esta responsabilidad corresponde al Consejo de Administración.

- Fijar el monto de la protección que debe adquirir la cooperativa ante posibles riesgos de operación, sin perjuicio de exigir caución a los funcionarios que

defina y por el monto que determine. Igualmente compete al Consejo de Administración.

Es importante indicar, que la autorización para la adquisición de bienes inmuebles o la enajenación o gravamen total o parcial de ellos, así como los contratos para la adquisición de servicios cuyo monto supere el 25% del patrimonio técnico de la institución, es atribución directa de la Asamblea General de la CAC.

CLÁUSULA 6. AUDITAR INTERNAMENTE EL SGSI

Esta cláusula establece que la organización debe realizar auditorias internas del SGSI a intervalos planeados para determinar si los objetivos, controles, procesos y procedimientos de su SGSI.

El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoria interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente. La función de auditoria interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo. Al auditar una entidad financiera, esta mejora en su continuidad y credibilidad de clientes y usuarios. Es la Asamblea General de la Cooperativa de Ahorro y Crédito, quien debe designar al auditor interno y al auditor externo, de las listas de personas calificadas por la Superintendencia, que le presente el Consejo de Administración de la propuesta realizada por el comité de auditoría, así como a removerlos de conformidad con la ley. De esta manera, es el Consejo de Administración quien debe presentar a la asamblea general la terna de personas calificadas por la Superintendencia para la designación de auditor interno y auditor externo, previa propuesta presentada por el Comité de Auditoría.

CLÁUSULA 7. REALIZAR REVISIÓN GERENCIAL

En esta cláusula se evidencia si que la gerencia está comprometida con el SGSI, incluyendo la política de seguridad y los objetivos de seguridad.

Las instituciones controladas deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna.

Los reportes deben contener al menos lo siguiente:

- Detalle de los eventos de riesgo operativo, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operativo y clasificado por líneas de negocio;
- Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución; y,
- Indicadores de gestión que permitan evaluar -la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Estos informes deben ser dirigidos a los niveles adecuados de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, entre otros.

CLÁUSULA 8. MEJORAR EL SGSI

Refiere a la necesidad de realizar una mejora continua para aumentar la probabilidad de incrementar la satisfacción de las partes interesadas.

Para realizar el proceso de mejora continua del SGSI, es necesario definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos, diseñar las políticas y el proceso de administración del riesgo operativo; y monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos.

2.1.2 EJEMPLO DE APLICACIÓN RESUMIDA DE GUIA METODOLÓGICA PARA ANÁLISIS, EVALUACIÓN, Y TRATAMIENTO DEL RIESGO EN CAC

En el siguiente ejemplo, se va desde la identificación de activos, y se llega hasta el establecimiento de los controles para el tratamiento del riesgo al que están expuestos.

Para una Cooperativa de Ahorro y Crédito, los activos de información entre muchos otros podrían ser: Bases de Datos, Equipo de cómputo, Línea dedicada, Internet, Servidor de archivos, Servidor de BD, Copias de respaldo, Switchers, Routers, Módem, Líneas Telefónicas, Central telefónica, Disco duro, cámaras, teléfonos. para este ejemplo específico, se han considerado tres: bases de datos de ahorro – cliente , servidor de bases de datos, copias de respaldo.

El proceso metodológico que se desarrolla a continuación es el siguiente:

Para iniciar el proceso, se identifica y se tasa a los activos de información; reconociendo en unos casos y asignándoles en otros, sus correspondientes custodios y propietarios. Luego, se determina las amenazas y su posibilidad de ocurrencia; de manera seguida se identifica las vulnerabilidades y la posibilidad de que sean explotadas por cada amenaza.

El valor total del riesgo se determina en función del valor del activo de información, y del valor más alto de la posibilidad de que una amenaza explote a una vulnerabilidad. Una vez evaluado el riesgo, es posible determinar la prioridad con que debe ser tratado el riesgo, se elaboran planes para el tratamiento de los riesgos, y finalmente se aplican los controles respectivos a cada uno de los planes.

En las Tablas 2.1, 2.2, y 2.3, se presenta el procedimiento metodológico indicado, con sus respectivos cálculos. Dado que la Norma ISO 27001 está enfocada hacia procesos, es imprescindible que las operaciones de la Cooperativa de Ahorro y Crédito se encuentren establecidas por procesos.

ACTIVOS DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	PROPIETARIOS
BD AHORRO - CLIENTE	5	5	4	**5**	SISTEMAS
SERVIDOR DE BD	5	5	5	**5**	SISTEMAS
COPIAS DE RESPALDO	5	5	3	**4**	SISTEMAS

TABLA 2.1 Tasación de activos de información y sus propietarios
ELABORADO POR Ing. Mantilla Aníbal

En este ejemplo, siguiendo la metodología establecida, la confidencialidad, la integridad y la disponibilidad, han sido evaluados de 1 a 5, dependiendo del activo de información, y su trascendencia para la organización. El valor del activo se obtiene promediando y aproximando a número entero, los valores de confidencialidad, integridad, y disponibilidad. Así, el valor del activo de información denominado BD- Ahorro Cliente (base de datos de ahorros de los clientes), es igual a (5+5+4)/3= 4.67, con lo cual, el valor entero aproximado es 5. Esto representa un valor muy alto para la organización.

Una vez determinado el activo de información se establece quien es el propietario del mismo, para establecer así responsabilidades claras y definidas. Todo esto puede apreciarse en la tabla 2.1 .

Para cada activo de información se determinan las amenazas y la posibilidad de que ocurran en una escala de 1 a 5, de acuerdo a la metodología establecida. Se determinan las vulnerabilidades, y en una escala de 1 a 5 se establece la posibilidad de que una amenaza atraviese a una vulnerabilidad.

ACTIVOS DE INFORMACIÓN	AMENAZA	POSIBILIDAD DE OCURRENCIA	VULNERA-BILIDADES	POSIBILIDAD DE QUE AMENAZA EXPLOTE A UNA VULNERABILIDAD	VALOR DE ACTIVOS DE RIESGOS	POSIBILIDAD DE OCURREN-CIA DE AMENAZA	VALOR TOTAL DEL RIESGO
BD AHORRO / CLIENTE	Virus	3	Falta de antivirus	3	5	4	20
	Daño del HD	5	Falla técnica	4			
SERVIDOR DE BD	Daño de partes	3	Falla técnica	3	5	3	15
	Virus	3	Software desactualizado	3			
COPIAS DE RESPALDO	Daño físico	3	Mal almacenamiento	3	4	3	12

TABLA 2.2 Evaluación total del riesgo de los activos de información
ELABORADO POR Ing. Mantilla Aníbal

Se toma el valor más elevado de la posibilidad de que una vulnerabilidad sea atravesada por una amenaza, y se multiplica por el valor del activo de información. El valor obtenido, representa el riesgo al cual se encuentra expuesto el activo de información. Así, en la tabla 2.2 puede verse que la posibilidad de que el disco duro con la base de datos de ahorros de clientes se dañe por falla técnica es igual a 4, mientras que la posibilidad de que virus afecten a la misma base de datos, es igual a 3. Por esta razón, se toma el valor más alto, esto es 4, y se multiplica por el valor del activo de información, en este caso igual a 5. La multiplicación de estos dos valores es igual a 20, que representa el riesgo al cual esta expuesta esta base de datos.

ACTIVOS DE INFORMACIÓN (en orden de prioridad)	ORDEN DE PRIORIDAD	PLANES PARA TRATAMIENTO DEL RIESGO	CONTROLES
BD AHORRO – CLIENTE	1	-Elaborar una política de seguridad de información incluyendo responsabilidades y sanciones. -Elaborar un programa detallado de capacitación para crear conciencia sobre la importancia de la seguridad de la información.	A.8.1.1 A.8.2.3 A.8.2.2 A.6.1.3
SERVIDOR DE BD	2	-Realizar un plan de mantenimiento de equipos computacionales y una revisión periódica del cableado eléctrico. -Capacitar a los usuarios de los SI sobre sus responsabilidades en el cuidado de los equipos y su información; y establecer responsabilidades para ello.	A.9.2.3 A.9.2.4 A.10.4.1 A.8.2.3
COPIAS DE RESPALDO	3	Elaborar planes para verificar periódicamente respaldos de información.	A.10.5.1

TABLA 2.3 Priorización, planes para tratamiento del riesgo y controles
ELABORADO POR Ing. Mantilla Aníbal

Una vez evaluado el riesgo para cada activo de información, se establece el orden de prioridad, se analizan las opciones para el tratamiento del riesgo, y se elaboran planes. Del Anexo A (normativo) de la norma ISO 27001, se seleccionan los controles y los objetivos de control a aplicarse en cada uno de los planes para el tratamiento del riesgo.

Esto puede verse en la tabla 2.3.

2.2 GESTIÓN PARA LA CONTINUIDAD DEL NEGOCIO

Al analizar la NATURALEZA DEL PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO, se establece que “No sirven de mucho los planes estratégicos, ni los modelos de investigación de mercados, ni los sistemas de aseguramiento de calidad, si no se tiene una metodología implantada que asegure a la cadena de suministros continuidad en el funcionamiento si un desastre se presentara” (Ph.D Alberto Alexander, 2007)

“Las empresas no sólo son vulnerables al impacto de calamidades, sino de pequeños eventos que pueden interrumpir las actividades de la firma. Diversos factores, tales como: a) incremento en la dependencia tecnológica y b) las presiones de "velocidad del mercado", han hecho a las empresas sumamente sensibles a catástrofes o eventos menores que generan perturbación en sus operaciones. Eventos sencillos pero con efecto calamitoso en la empresa, tales como: cortes en el fluido eléctrico, fallas en el sistema de tecnología de información (TI), defectos en equipos de operaciones, materia prima contaminada, errores en el sistema de comunicación y virus en las computadoras” (Ph.D. Alberto Alexander, 2007)

Los sismos, los terremotos, los incendios, los atentados, los asaltos a mano armada, son ejemplos de sucesos o eventos que pudieran ser catastróficos para la organización.

El Plan de Continuidad del Negocio debe ser considerado en **cinco fases secuenciales** (Ph.D. Alberto Alexander, 2007), distribuidas en actividades:

- Gestionar el riesgo
- Analizar el Impacto al Negocio
- Desarrollar estrategias para el plan de continuidad del negocio
- Desarrollar el plan de reanudación de operaciones
- Ensayar el plan de continuidad de negocio

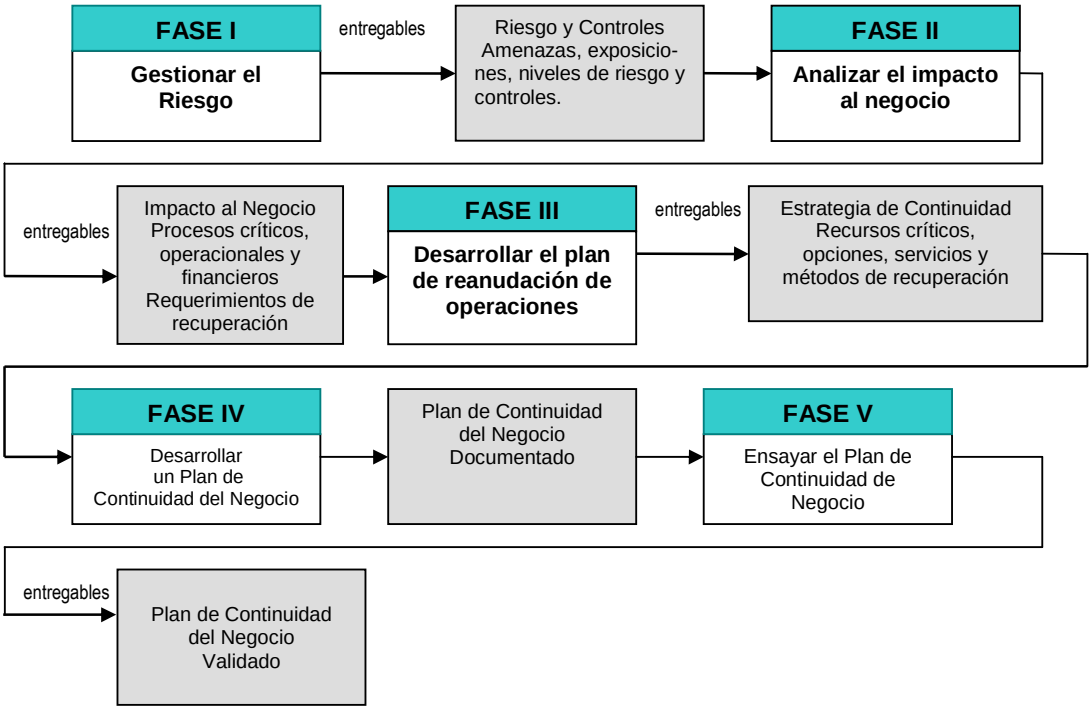

FIGURA 2.8 Fases para el plan de continuidad [26]
ELABORADO POR Ing. Mantilla Aníbal

2.2.1 FASE I: GESTIONAR EL RIESGO

Las actividades de la gestión del riesgo evalúan las amenazas de un desastre, pormenorizan las vulnerabilidades existentes, los potenciales impactos de un desastre, identifican e implementan los controles necesarios para prevenir o reducir los riesgos de un desastre y terminan identificando escenarios de amenazas para aquellos procesos considerados esenciales en el BIA.

Un programa de PCN no sólo debe atender la recuperación de las instalaciones frente a un desastre, sino también contemplar las acciones preventivas a que haya lugar. Para este propósito, en todo programa de PCN, se debe efectuar con regularidad un cálculo del riesgo que no sólo contemple la identificación de amenazas significativas que afecten las operaciones de la empresa, las vulnerabilidades y el grado de exposición al riesgo, sino que igualmente es

[26] Fuente: Gestión del riesgo en el Business Continuity Planning, Alexander, P:hD

necesario identificar los controles a instaurar para minimizar el daño del impacto de un posible desastre en la empresa.

En la metodología del PCN, un resultado esperado del cálculo del riesgo es determinar los distintos escenarios de amenazas que pueden presentarse a los procesos esenciales de la empresa, los cuales se usarán para elaborar las estrategias de continuidad y desarrollo de los planes de reanudación de operaciones.

Los objetivos de esta fase son los siguientes:

A) Identificar las distintas amenazas que podrían impedir el normal desenvolvimiento de las operaciones en la empresa.

B) Identificar la vulnerabilidad organizacional, es decir de la Cooperativa de Ahorro y Crédito, en relación a cada amenaza y determinación de qué tan severamente podrían afectarse las operaciones en la empresa.

C) Revisar los controles actuales para reducir el riesgo o mitigar las pérdidas.

D) Evaluar el nivel de exposición al riesgo.

E) Determinar los escenarios de amenazas para los cuales se deben desarrollar las estrategias de continuidad y los planes respectivos.

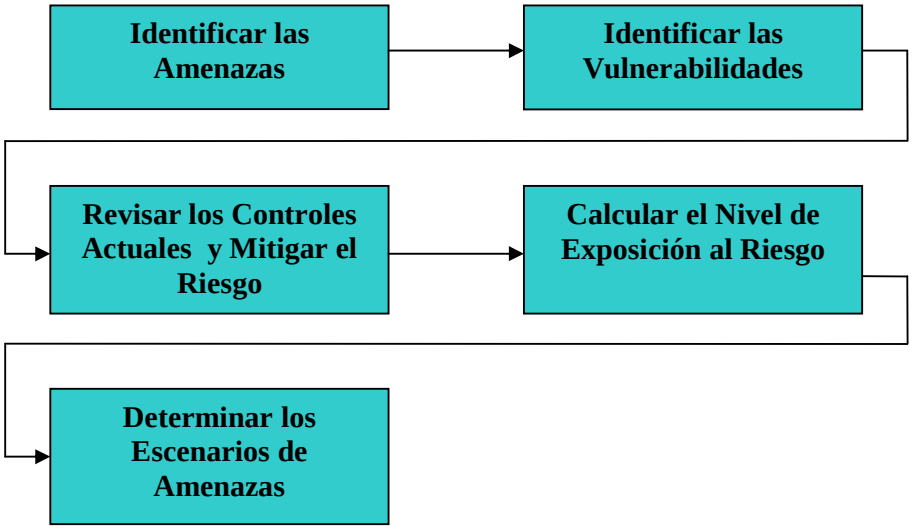

FIGURA 2.9 Metodología para el cálculo del riesgo [27]
ELABORADO POR Ing. Mantilla Aníbal

[27] Fuente: Gestión del riesgo en el Business Continuity Planning, Alexander, P:hD

A. IDENTIFICAR LAS AMENAZAS

Las amenazas que se desea identificar son aquellas que afectan los activos de las funciones organizacionales. El método recomendado para buscar las amenazas tiene dos etapas:

Análisis general de amenazas. Aquí se revisan las distintas potenciales amenazas que pueden afectar la organización. Uno de los objetivos de esta etapa es identificar las exposiciones específicas que puedan requerir medidas protectoras y así minimizar la probabilidad de que las amenazas pudiesen causar daño a la organización. Este análisis es conducido en las instalaciones de la empresa y puede usualmente atender los aspectos siguientes: ubicación de instalaciones, seguridad interna y externa, ambiente físico, protección de activos, protección del personal, protección de información y análisis de la cobertura de pólizas.

Análisis de procesos esenciales. Aquí, en esta investigación se hace especial hincapié en las interrupciones a las que los procesos esenciales están expuestos por la pérdida de recursos básicos, tales como: instalaciones, sistemas de cómputo, registros vitales, sistemas telefónicos, personal clave, conectividad de la red, equipo especializado, materias primas y material de empaque. En este nivel de análisis el objetivo es identificar las funciones organizacionales que tienen la mayor exposición a la interrupción, y poder identificar los recursos de los que dependen las funciones organizacionales.

A cada amenaza identificada se le deben calcular su posibilidad de ocurrencia y el impacto económico que pudiese ocasionar en la organización. En esta etapa la empresa debe tomar decisiones sobre las opciones de tratamiento del riesgo. Decidir cuáles amenazas se reducirán con controles, cuáles se aceptarán y se decidirá vivir con ellas, cuáles se transferirán (por ejemplo, a una aseguradora.) y cuáles se evitarán.

B. IDENTIFICAR LAS VULNERABILIDADES

Por cada amenaza identificada en el paso anterior se deben identificar sus vulnerabilidades. Es fundamental recalcar que una vulnerabilidad no causa daño; simplemente es una condición o conjunto de condiciones que pueden hacer que una amenaza afecte un activo. Una vez identificadas las distintas vulnerabilidades por cada amenaza, se debe hallar el grado en que la amenaza puede explotar cada vulnerabilidad.

Disminuye la vulnerabilidad, el hecho de mantener los sistemas de comunicación y redundancia que permitan garantizar la continuidad de sus servicios; además de contar con Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

C. REVISAR LOS CONTROLES ACTUALES

Al haber identificado las distintas amenazas y las respectivas vulnerabilidades organizacionales, en esta etapa se deben analizar con la debida profundidad las distintas salvaguardas existentes en la empresa. Si una amenaza explota una vulnerabilidad podría generarse un desastre. Deberían existir Controles para minimizar riesgos potenciales de equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros. Además, deberían estar operando políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información critica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;.

D. EVALUAR EL NIVEL DE EXPOSICIÓN AL RIESGO

Una vez detectadas las amenazas, la dependencia de recursos de cada función organizacional y sus vulnerabilidades, se debe proceder a precisar el grado de severidad de cada potencial amenaza identificada y la cobertura, la cual es el grado de protección que tiene la empresa frente a una amenaza en particular. Los niveles de severidad se estiman en una escala de cuatro puntos..

Se empieza con N/A = No Aplica, B = Bueno, M = Moderada y A = Alta
Los grados de cobertura que van de un rango de 0 hasta 100, clasificados en seis categorías. Posteriormente se calcula la exposición al riesgo.

E. DETERMINAR LOS ESCENARIOS DE AMENAZAS

Una vez calculada la exposición al riesgo por cada amenaza potencial y por funciones organizacionales en la empresa, se elaboran escenarios particulares de riesgos que la empresa pudiera tener y el daño que pudiesen causar a las operaciones de la empresa.

Los escenarios de amenazas se clasifican desde los menos graves, que en este caso son el escenario 1, hasta los más complejos que son el escenario 5. Para cada escenario identificado, se requiere elaborar, según la metodología del PCN, las FASES III, IV Y V. Es decir, para cada escenario hay que desarrollar las respectivas estrategias de continuidad del negocio, los planes de continuidad y los ensayos respectivos para cada plan.

Los escenarios, de acuerdo a las amenazas pueden relacionarse de la manera siguiente:

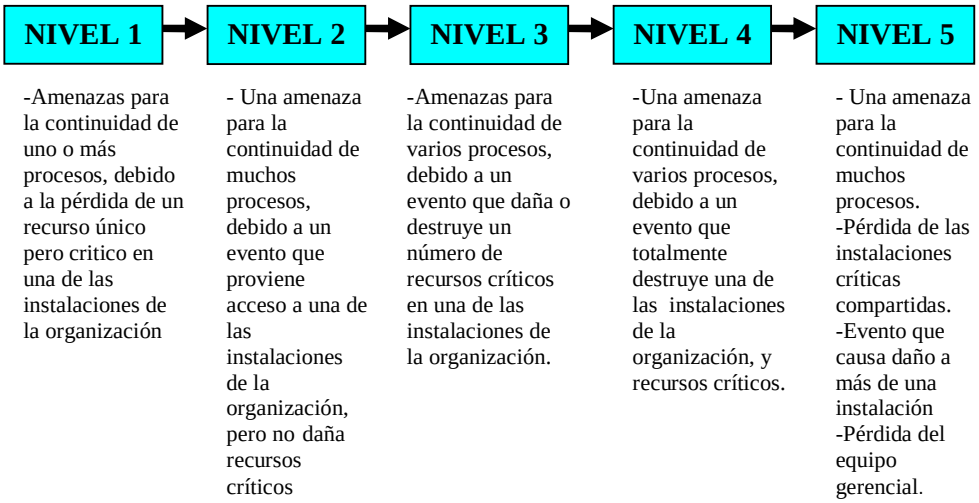

FIGURA 2.10 Escenarios de riesgos en la organización[28]
ELABORADO POR Ing. Mantilla Aníbal

[28] Fuente:www.eficienciagerencial.com

***Amenaza nivel* 1**. Aquí se identifica una amenaza para la continuación de una o más funciones organizacionales en la empresa. Esta amenaza se debe a la pérdida de un recurso único pero crítico en una de las instalaciones de la organización (energía, sistemas de computación, archivos electrónicos, personal clave).

***Amenaza nivel* 2**. En este escenario se identifica una amenaza para la continuidad de muchas funciones organizacionales, debido a un evento que previene el acceso a una de las instalaciones de la organización, pero no daña ningún recurso crítico.

***Amenaza nivel* 3**. Una amenaza para la continuidad de varias funciones organizacionales, debido a un evento que daña o destruye un número de recursos críticos en una de las instalaciones de la organización. Este escenario es una combinación de los niveles 1 y 2.

***Amenaza nivel* 4.** Una amenaza para la continuidad de varias funciones organizacionales en la empresa, debido a un evento que destruye totalmente una de las instalaciones de la organización y sus respectivos recursos críticos. Esto podrían ser imprevistos, tales como incendios o explosiones.

***Amenaza nivel* 5.** Una amenaza para la continuidad de muchas funciones organizacionales e instalaciones múltiples, debido a la pérdida de instalaciones críticas compartidas (energía, telecomunicaciones, sistemas centralizados). El evento causa daño *y/o* acceso restringido a más de una instalación en la organización (sismo o terremoto, huracán, incidente ambiental). Se puede generar pérdida del equipo gerencial (accidente aéreo, bomba, terrorismo biológico).

Una vez identificadas las amenazas y las respectivas vulnerabilidades organizacionales, es fundamental establecer los respectivos controles para fortalecer las vulnerabilidades y minimizar la posibilidad de que el desastre penetre en la empresa y le cause daño.

2.2.2 FASE II: ANALIZAR EL IMPACTO AL NEGOCIO (BIA)

Consiste en identificar aquellos procesos relacionados con apoyar la misión de la empresa, y analizar con muchos detalles los impactos en la gestión comercial del negocio, si esos procesos fuesen interrumpidos como resultado de un desastre. Es necesario analizar los impactos financieros y operacionales de un desastre en la organización, sus áreas y procesos.

Los ***impactos financieros*** se refieren a pérdidas monetarias, tales como pérdidas de ventas, penalidades contractuales o degradación de productos.

Los ***impactos operacionales*** representan pérdidas no monetarias relacionadas con las operaciones del negocio, pueden incluir la pérdida de competitividad, daño a la confidencialidad de la inversión, pobre servicio al cliente y daño a la reputación del negocio.

En base al Análisis de Impacto al Negocio (BIA), es posible determinar lo siguiente:

- Establecer las funciones y procesos organizacionales, esenciales para la supervivencia de la empresa. A los otros procesos no considerados sólo se les prepararán planes de recuperación.
- Calcular las consecuencias operacionales y financieras que una interrupción tendría en los procesos considerados clave.
- Establecer los tiempos requeridos para la recuperación.
- Identificar los requerimientos de recursos indispensables para el funcionamiento de los procesos claves.

La forma metodológica en que debería efectuarse el Análisis de Impacto al Negocio (Ph.D. Alberto Alexander, 2007), se indica a continuación:

A) Evaluar los impactos financieros

B) Evaluar los impactos operacionales

C) Identificar los procesos críticos

D) Establecer los tiempos de recuperación

E) Identificar los requerimientos de recursos

F) Generar un informe del análisis del impacto al negocio

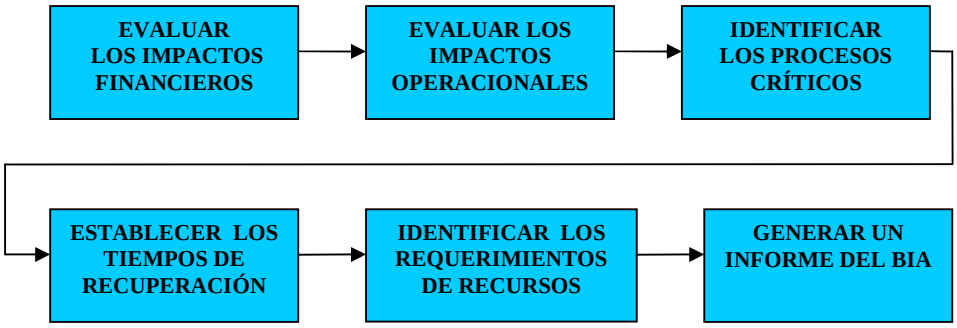

FIGURA 2.11 Pasos para elaborar un BIA [29]
ELABORADO POR Ing. Mantilla Aníbal

A. EVALUAR LOS IMPACTOS FINANCIEROS

En este paso deben evaluarse los impactos de una interrupción en la organización, tanto desde una perspectiva financiera como operacional.

Luego de haber identificado el impacto financiero, se debe medir el impacto en una base de severidad, basada en el valor de la pérdida monetaria. Se recomienda utilizar la escala siguiente:

1. Nivel de severidad 0 (impacto 0).
2. Nivel de severidad 1 (menor impacto).
3. Nivel de severidad 2 (impacto intermedio).
4. Nivel de severidad 3 (impacto mayor).

B. EVALUAR LOS IMPACTOS OPERACIONALES

Por otro lado la medición de los impactos operacionales evalúa el impacto negativo de una interrupción, en varios aspectos de las operaciones del negocio.

[29] Fuente: Gestión del Business Impact Analysis, Alexander, P:hD

Los impactos operacionales se pueden medir utilizando un esquema de jerarquización cualitativo, tal como: bajo, mediano, alto, altísimo y ninguno.

C. IDENTIFICAR LOS PROCESOS CRÍTICOS

La clasificación financiera y operacional de los impactos provee una base para identificar procesos críticos del negocio. Considerando usualmente la jerarquización financiera y operacional, un proceso es crítico si satisface los requerimientos siguientes:

1. Una severidad de 2 o 3 se asigna a sus impactos financieros.
2. Una clasificación de alta se asigna por lo menos a tres de sus impactos operacionales.
3. Una clasificación de alta se asigna al menos a dos, y una clasificación de altísima se asigna a uno de sus aspectos operacionales.
4. Una clasificación de altísima se asigna por lo menos a dos de sus impactos operacionales.

D. ESTABLECER LOS TIEMPOS DE RECUPERACIÓN

Los requerimientos de los tiempos de recuperación consisten en una serie de componentes que tienen que ver con el tiempo disponible para recuperarse de una alteración.

***Tiempo máximo tolerable sin operación (Maximun Tolerable Downtime-* MTD).** Consiste en el espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

Tiempo objetivo de recuperación (Recovery Time Objetive - RTO). Está asociado con la recuperación de recursos, tales como sistemas de computación, equipos de manufactura e infraestructura física. El RTO es el tiempo transcurrido entre una interrupción y la recuperación. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos. Es importante enfatizar que jamás el RTO podría ser superior al MTD.

Punto objetivo de recuperación (Recovery Point Objetive - RPO). Este tiempo está relacionado con la tolerancia que la empresa puede tener, sobre la pérdida de datos, medidos en términos del tiempo entre el último respaldo de datos y el evento del desastre.

Tiempo de recuperación de trabajo (Work Recovery Time - WRT). Se calcula como el tiempo entre la recuperación del sistema y la normalización del procesamiento. Es el tiempo invertido en buscar datos perdidos y realizar reparaciones. El WRT es el tiempo requerido para completar el trabajo interrumpido a fin de volverlo a la normalidad.

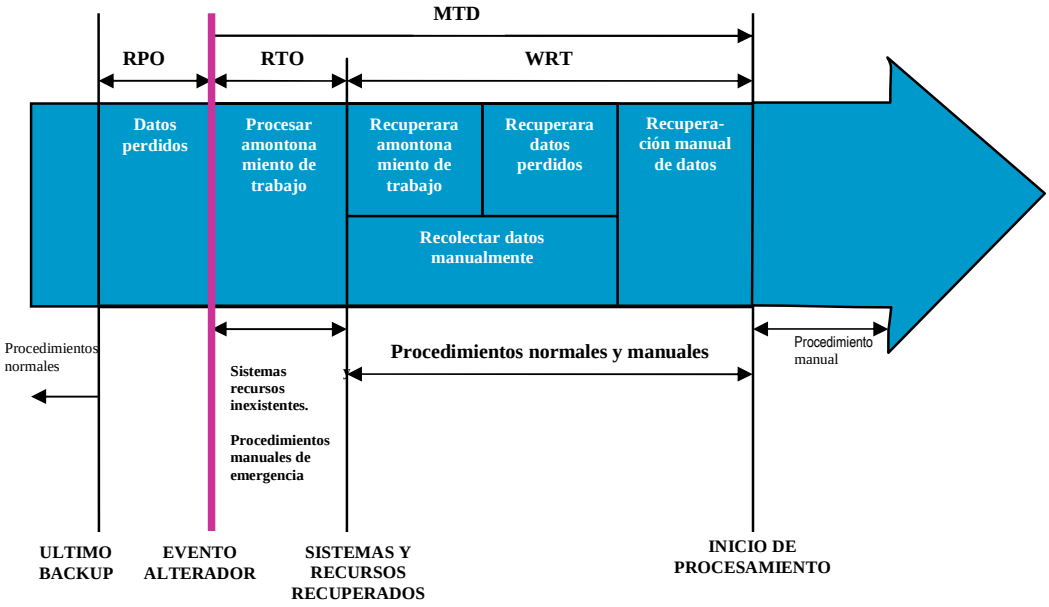

FIGURA 2.12 Tiempos para la recuperación ante un desastre [30]
ELABORADO POR Ing. Mantilla Aníbal

E. IDENTIFICAR LOS REQUERIMIENTOS DE RECURSOS

Un sistema de tecnología de información o una aplicación se considera vital si apoya un proceso crítico del negocio. Este paso identifica sistemas críticos de tecnología de información y aplicaciones que apoyan los procesos identificados en el literal (D).

[30] Fuente: www.eficienciagerencial.com

F. GENERAR UN INFORME DEL ANÁLISIS DEL IMPACTO AL NEGOCIO

Los resultados de los pasos que han precedido se resumen en esta fase para convertirlos en una guía para el BIA.

2.2.3 FASE III: DESARROLLAR ESTRATEGÍAS PARA EL PLAN DE CONTINUIDAD

Aquí se evalúan los requerimientos y se identifican las opciones para la recuperación de procesos críticos y sus recursos, en el escenario en que fuesen interrumpidos por un desastre.

Por cada escenario de amenazas se elaboran estrategias que contemplen los escenarios de amenazas identificados.

El propósito de esta fase del proceso BCP es desarrollar estrategias de continuidad del negocio, que satisfagan los requerimientos de recuperación identificados en la etapa del BIA, y en los escenarios de amenazas.

El diseño de una estrategia de continuidad consiste de cuatro fases secuenciales:

- **Fase A: Identificación de requerimientos de la recuperación.**
  Determina los requerimientos de recuperación para ser atendidos por la estrategia del plan de continuidad.

- **Fase B: Identificación de opciones de la recuperación.**
  Busca identificar posibles opciones como soluciones a los requerimientos de recuperación.

- **Fase C: Evaluación de disponibilidad del tiempo.**
  Elimina aquellas opciones que no cumplen aquellos tiempos de recuperación identificados en el BIA.

- **Fase D: Evaluación de los costos.**
  Con las opciones que quedan, evalúa los costos y las potencialidades para seleccionar las opciones más viables y eficaces.

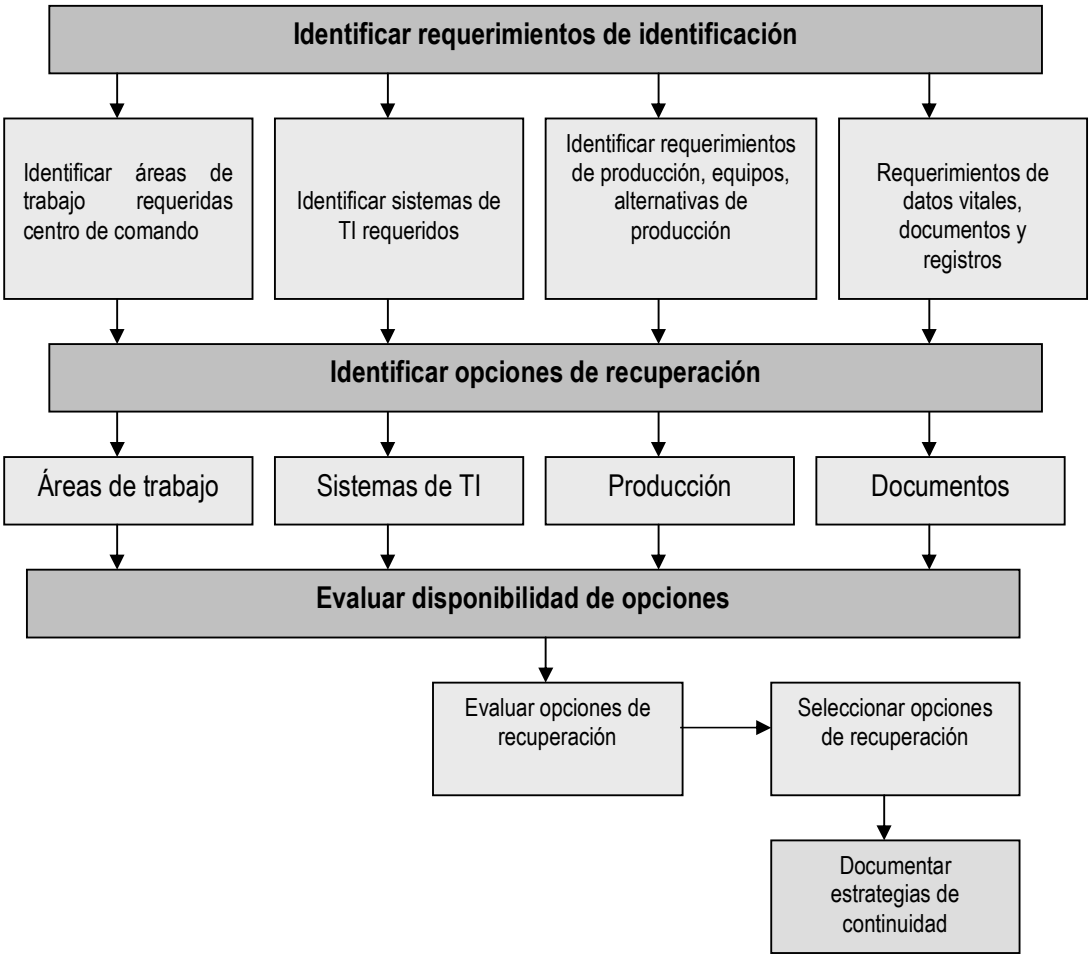

FIGURA 2.13 Desarrollo de una estrategia de continuidad[31]
ELABORADO POR Ing. Mantilla Aníbal

2.2.4 FASE IV: DESARROLLAR EL PLAN DE REANUDACIÓN DE OPERACIONES

Basado en las fases previas, se establece los procedimientos y lineamientos concretos para la recuperación y el restablecimiento de los recursos dañados, y los procesos cuyo desempeño se ha interrumpido.

El objetivo del plan de reanudación de operaciones es la recuperación de procesos críticos en un determinado tiempo.

Un plan de reanudación de operaciones son una serie de actividades

[31] Fuente: www.eficienciagerencial.com

documentadas, que pudiesen requerir desempeñaran los grupos de continuidad del negocio, como respuesta a la aparición de un escenario de amenazas. El plan de reanudación de operaciones lleva a cabo las estrategias de continuidad. Una clásica estructura de equipos consiste en los tipos siguientes:

Grupo comando. Está encargado de dirigir el plan de reanudación de operaciones.

Grupo de respuesta. El conjunto de individuos, usualmente personas relacionadas con las instalaciones y del área de seguridad, que se activa de inmediato si ocurriese una emergencia.

Grupo departamental. Es el conjunto de individuos, usualmente gerentes de primera línea, que pueden ser activados por el grupo comando para coordinar actividades de un departamento operativo específico después del incidente.

Grupo de tecnología de información. Es un conjunto de especialistas en tecnología de información que pueden ser activados por el grupo comando para restablecer la infraestructura tecnológica, los sistemas de computación o los datos electrónicos.

Grupo de apoyo. Es un conjunto especializado que puede ser activado por el grupo comando para ayudar a gestionar las variadas actividades que demanda el incidente.

La estructura del equipo para la continuidad del negocio es lo que hará que los planes funcionen o no. No existe una estructura estandarizada de equipos. El establecimiento de una estructura que sea la correcta para la organización es vital.

Los factores que deben tomarse en cuenta, al estructurar los equipos, son los siguientes:

- Tamaño de la organización,
- Ubicación de las instalaciones y unidades operativas,
- Estructura organizacional,
- Cultura organizacional,

- Escenarios potenciales de amenazas,
- Estrategias de continuidad,
- Complejidad de los planes de continuidad del negocio,
- Conocimiento especializado requerido.

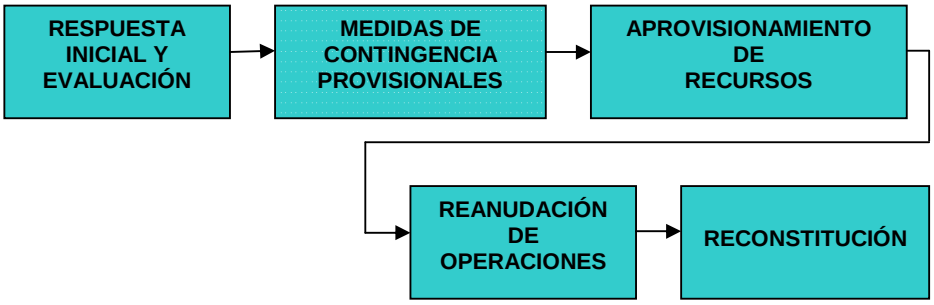

FIGURA 2.14 Fases para el Plan de Reanudación de Operaciones
ELABORADO POR Ing. Mantilla Aníbal

2.2.5 FASE V: ENSAYAR EL PLAN DE CONTINUIDAD DE NEGOCIOS

En esta fase se efectúa el ensayo del plan, con miras a poder determinar su grado de precisión y actualización. El valor de esta fase es ensayar el plan de reanudación de operaciones para que pueda considerarse aceptable.

La fase del ensayo tiene dos objetivos fundamentales:

A) Verificar si el plan de reanudación de operaciones es adecuado y confiable para la recuperación del negocio dentro de un tiempo prudencial.

B) Identificar debilidades y brechas que pudiesen existir en el plan de reanudación de operaciones.

Los tipos de ensayos más utilizados son los siguientes:

A) **Lista de chequeo.** Es el ensayo más básico. Revisa el plan de reanudación de operaciones y chequea la disponibilidad y adecuación de la información y recursos requeridos para la ejecución del plan.

B) **Paseo de revisión.** Éste es un método no costoso. Se realiza usualmente previo a la conducción de un ensayo de simulación. Los equipos se reúnen y

verbalmente describen las actividades, los procedimientos y tareas que seguirían dado un desastre.

C) **Simulación.** En este ensayo se simula un tipo de alteración mediante un escenario de desastre. Permite a los equipos practicar la ejecución del plan de reanudación de operaciones y poder validar una o más partes del plan.

D) **Interrupción completa.** Este ensayo activa todos los componentes del plan de reanudación de operaciones. Este ensayo parte del hecho de que todos los procesos esenciales se han alterado.

2.2.6 EJEMPLO DE APLICACIÓN RESUMIDA DE GUÍA METODOLÓGICA PARA GESTIONAR EL RIESGO A TRAVES DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN CAC

Dada la importancia que tiene el BCP, para que una organización pueda recuperarse rápidamente y continuar operando, cuando sus operaciones han sido gravemente alteradas por causas de desastres, el Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001, lo enmarca específicamente en el área de control “Gestión de la Continuidad del Negocio”, correspondiente al control A.14. Para alcanzar la certificación con esta norma, este control es obligatorio; debiendo ser confiable, ensayado y mantenido en el tiempo.

A continuación se presenta en un ejemplo, de manera resumida el proceso de elaboración de un Plan para la Continuidad del Negocio. En este ejemplo, se presentan, para una Cooperativa de Ahorro y Crédito: la **Gestión de Riesgos** (amenazas, nivel de severidad, exposición - escenario de riesgos), **Análisis del Impacto al Negocio** (funciones, procesos, impacto financiero, impacto operacional, tiempos de recuperación, requerimientos para recuperación), y **Desarrollo de Estrategias para el Plan de Continuidad de Negocio** (estrategias de continuidad, opciones, recursos críticos).

En la siguiente tabla se muestra la forma de calcular a exposición al riesgo, en función del nivel de severidad de cada amenaza potencial identificada y la cobertura de la seguridad de la Cooperativa a cada una de ellas.

NIVELES DE SEVERIDAD					EXPOSICIÓN AL RIESGO
Escala	**N**	**B**	**M**	**A**	**Nivel de severidad x (100% - % cobertura**)
Representación	No aplica	Baja	Moderada	Alta	
Valor	----------	10	50	100	

TABLA 2.4 Metodología para el cálculo de exposición al riesgo
ELABORADO POR Ing. Mantilla Aníbal

AMENAZAS POTENCIALES	SEVERIDAD				COBERTURA (EN %)						EXPOSICIÓN AL RIESGO
	N/A	B	M	A	0 -19	20 - 39	40 - 59	60 - 79	80 - 99	100	
PÉRDIDA DE INFORME FINANCIERO				√					√		**2000**
PÉRDIDA DE SERVICIO DE FAX		√						√			**400**
PÉRDIDA DE SERVICIOS GENERALES			√				√				**3000**
PÉRDIDA DE ENTREGA DE CORREO			√						√		**1000**
PÉRDIDA DE SISTEMA TELEFÓNICO				√					√		**2000**

TABLA 2.5 Cálculo de exposición al riesgo ante amenazas potenciales
ELABORADO POR Ing. Mantilla Aníbal

En la tabla 2.5, primero se determina el nivel de severidad en base a una escala de cuatro niveles, esto es N/A= no aplica, B= Baja, M= Moderada, A= Alta; con sus correspondientes valores, como se indicó en la tabla 2.4. De forma seguida se encuentran los grados de cobertura de la seguridad, clasificados en seis categorías, y luego se calcula la exposición al riesgo en base a la ecuación presentada en la tabla 2.4. Para el caso de este ejemplo, el nivel de severidad de perder la entrega de correo es 50 (nivel de severidad moderado), una cobertura entre 80 y 99. Se escoge siempre el valor más bajo, esto es 80, y se determina la exposición al riesgo, multiplicando 50 con (100 - 80), el resultado obtenido es 50*20=1000, que es la medida de exposición a este riesgo.

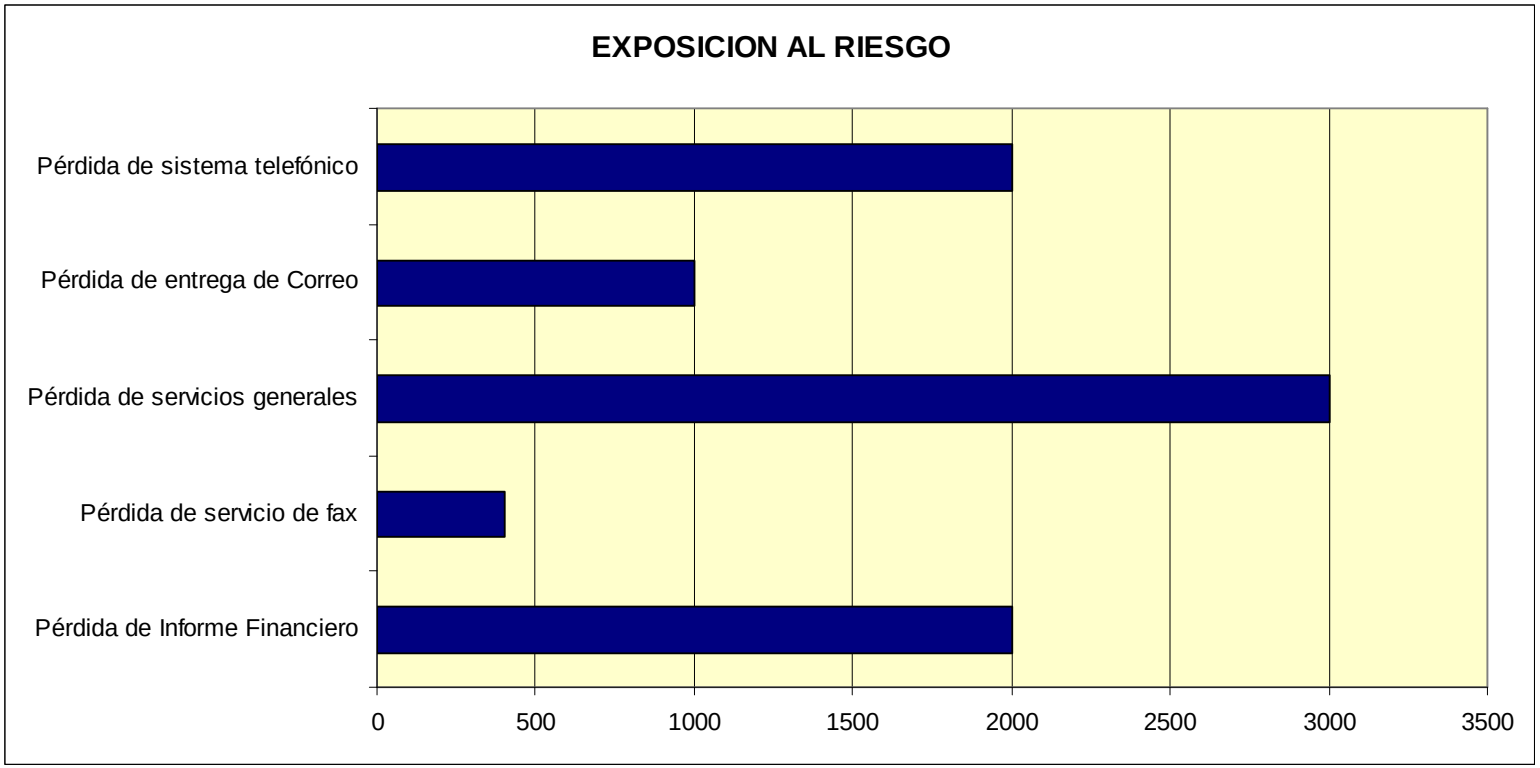

FIGURA 2.15 Exposición a riesgos
ELABORADO POR Ing. Mantilla Aníbal

En la figura 2.15, una vez calculada la exposición al riesgo, se presenta de forma comparativa el valor que este alcanzó, para cada amenaza potencial. En base a estos cálculos y a los datos de la figura 2.10, se determinan los escenarios de riesgo en los que pudiera encontrarse la organización.

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	MAGNITUD DE PÉRDIDA FINANCIERA DIARIA (en USD)	NIVEL DE SEVERIDAD
Créditos	Generación de solicitudes	700	2
	Informe de datos del socio	10000	3
Marketing	Promoción de productos	5000	1
Servicio al cliente	Manejo problemas del cliente	15000	1
	Proceso de solicitudes	30000	1

TABLA 2.6 Funciones del negocio, procesos e ilustración de impacto financiero y nivel de severidad
ELABORADO POR Ing. Mantilla Aníbal

En el proceso de Análisis del Impacto al Negocio, es necesario identificar las funciones y los procesos que son utilizadas para apoyar la misión, las metas y los objetivos donde se encuentra el alcance del Sistema de Gestión de Seguridad de la Información. Estas funciones y procesos son el aspecto fundamental para el Análisis y Desarrollo del BIA. Una vez determinado el Impacto financiero, se mide dicho impacto en una base de severidad, basada en el valor de la pérdida monetaria. La escala utilizada es la siguiente: Nivel de severidad 0 (impacto 0), Nivel de severidad 1 (menor impacto), Nivel de severidad 2 (impacto intermedio), Nivel de severidad 3 (impacto mayor). En este ejemplo de aplicación resumida de metodología para gestionar el riesgo a través de un Plan de Continuidad del Negocio en CAC, se presenta en la tabla 2.6, dichas funciones y procesos, con su correspondiente magnitud de pérdida **(impacto financiero)** y nivel de severidad.

NEGOCIO		JERARQUIZACION DE IMPACTOS OPERACIONALES				
FUNCION	**PROCESO**	**Flujo caja**	**Confianza inversión**	**Participación mercado**	**Competitividad**	**Satisfacción cliente**
Créditos	Generación de solicitudes	**Alto**	**Alto**	**Altísimo**	**Alto**	**Ninguno**
	Informe de datos del socio	**Ninguno**	**Alto**	**Alto**	**Mediano**	**Ninguno**
Marketing	Promoción de productos	**Mediano**	**Bajo**	**Alto**	**Mediano**	**Bajo**
Servicio al cliente	Manejo problemas del cliente	**Bajo**	**Alto**	**Alto**	**Altísimo**	**Mediano**
	Proceso de solicitudes	**Mediano**	**Alto**	**Bajo**	**Mediano**	**Mediano**

TABLA 2.7 Ilustración de impactos operacionales
ELABORADO POR Ing. Mantilla Aníbal

En la tabla 2.7 se muestra como se mide los Impactos Operacionales, utilizando un esquema de jerarquización cualitativa, en este caso: ninguno, bajo, mediano, alto, altísimo. Con la medición del Impacto operacional, es posible evaluar el impacto negativo de una interrupción, en varios aspectos de las operaciones de la organización. Una vez identificados los impactos financieros y operacionales, se puede con mayor facilidad identificar los procesos críticos del negocio, en función de la severidad y la jerarquización del impacto.

FUNCIONES CRÍTICAS DEL NEGOCIO	PROCESOS CRÍTICOS DEL NEGOCIO	MTD (En días)	PRIORIDAD DE RECUPERACIÓN	SISTEMAS DE TI CRÍTICOS Y APLICACIONES
Créditos	Generación de solicitudes	3	1	Sistema de información cliente Sistema entrada de solicitud Aplicaciones e- mail
	Informe de datos del socio	6	3	Sistema de información cliente Sistema entrada de solicitud Aplicaciones e- mail
Servicio al cliente	Manejo problemas del cliente	4	2	Sistema entrada de solicitud Gestión sistema inventario Sistema cobranza clientes

TABLA 2.8 Procesos críticos de negocio, prioridad de recuperación, sistemas críticos de TI y aplicaciones
ELABORADO POR Ing. Mantilla Aníbal

En esta tabla se presentan las funciones y procesos críticos del negocio, el MTD (tiempo máximo de inactividad para la CAC sin colapsar), las prioridades de recuperación, y los recursos de TI críticos, que se requiere para Gestionar el Riesgo con el Plan de Continuidad del Negocio.

En la tabla 2.9 se presenta el **RTO** (tiempo disponible para recuperar el sistema y los recursos que han sufrido alteración) y el **WRT** (tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados). Como puede verse en comparación con la tabla 2.8, la suma entre el RTO y WRT debe ser siempre menor o igual al MTD.

FUNCION CRÍTICA DEL NEGOCIO	PROCESO CRITICO DEL NEGOCIO	APLICACIONES CRITICAS DEL SISTEMA A TECNOLOGÍA INFORMÁTICA	RTO (en días)	WRT (en Días)
Créditos	Generación de solicitudes	- Sistema de información cliente -Sistema entrada de solicitud - Aplicaciones e- mail	2,5 1 2	0,5 2 1

TABLA 2.9 Valores RTO y WRT para el proceso de generación de ordenes
ELABORADO POR Ing. Mantilla Aníbal

Una vez determinado los requerimientos de recursos de TI críticos, se establece todos los recursos que no son de tecnología informática, pero que son fundamentales para los procesos críticos del negocio.

FUNCIONES CRÍTICAS DEL NEGOCIO	PROCESOS CRITICOS DEL NEGOCIO	TIPO DE RECURSO	DETALLES DE RECURSOS
Crédito	Generación de solicitudes	Maquinaría Equipos	Máquina de escribir Copiadora Archivadores
		Materia prima	Hojas de formularios Pegamentos Carpetas

TABLA 2.10 Recursos críticos de manufactura y producción
ELABORADO POR Ing. Mantilla Aníbal

2.3 DOCUMENTACION DEL SGSI

En esta sección, se presenta una guía para elaborar adecuadamente el Manual de Seguridad de la Organización. Cuando se va a iniciar el proceso de documentación del ISO 27001, en una empresa determinada, los grupos responsables del proyecto, deben saber que es lo que se debe documentar, y efectuarlo de una manera adecuada. La trascendencia que tiene está guía, radica en la gran cantidad de documentos y debidamente elaborados, que requiere la ISO 27001; estos requerimientos se presentan en los anexos.

2.3.1 PIRÁMIDE DOCUMENTAL DEL ISO 27001:2005

En la siguiente figura, pueden verse los diferentes componentes, y la interrelación entre ellos.

A) Nivel I - Manual de seguridad

B) Nivel II - Procedimientos

C) Nivel III - Instrucciones de trabajo

D) Nivel IV - Documentos

FIGURA 2.16 Pirámide documental del SGSI [32]
ELABORADO POR Ing. Mantilla Aníbal

[32] Fuente: www.eficienciagerencial.com

A. NIVEL I - MANUAL DE SEGURIDAD

el Manual de Seguridad de Información no es un requisito del modelo. No existe cláusula que lo exija, pero tenerlo organiza la documentación, facilita la auditoría y agrupa la documentación considerada por el modelo ISO 27001:2005 como vital. Los aspectos básicos que un manual de seguridad debiera tener son:

- Enunciados de la política del SGSI
- Alcance del SGSI
- Procedimientos y controles de soporte
- Descripción de la metodología de evaluación del riesgo
- Reporte de evaluación del riesgo
- Plan de tratamiento del riesgo
- Declaración de aplicabilidad

B. NIVEL II - PROCEDIMIENTOS

De acuerdo al ISO 9000, un procedimiento es una manera específica de desempeñar una actividad.

En el ISO 27001:2005, los procedimientos son requeridos en una serie de cláusulas. Cuando en el proceso de "opciones para el tratamiento del riesgo" se decide por la reducción del riesgo, la empresa debe acudir a escoger controles del Anexo A. Se debe por cada control escogido, documentar su procedimiento.

C. NIVEL III - INSTRUCCIONES DE TRABAJO

Una instrucción de trabajo es la "información que explica en detalle cómo se efectúa una operación concreta". Es común utilizar flujogramas. La utilización de instrucciones de trabajo depende directamente de la experiencia y el nivel de entrenamiento por parte del ejecutor de las tareas.

D. NIVEL IV - DOCUMENTOS

Este nivel de la pirámide agrupa tanto los registros como los documentos utilizados en un SGSI.

La sección 4.3.3 de la cláusula 4 de la norma dice que se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI.

El ISO 27001:2005 tiene que utilizarse también para desenredar la complejidad incremental que usualmente se ha ido desarrollando en los sistemas organizacionales, generando altos costos por la mala calidad de su funcionamiento.

2.3.2 GUIA PARA DOCUMENTAR EL SGSI

La metodología sugerida consta de los siguientes pasos:

A) Identificar procedimientos a documentar
B) Definir el formato del procedimiento
C) Identificar actores del procedimiento
D) Levantar y validar el flujograma
E) Redactar toda la información del flujograma
F) Identificar, redactar y validar instrucciones de trabajo
G) Identificar los registros requeridos
H) Identificar los documentos de seguridad de información

A. DENTIFICAR PROCEDIMIENTOS A DOCUMENTAR

Al iniciar un proyecto de documentación del ISO 27001:2005, es importante visualizar todas las actividades que se tendrán que documentar y ordenadas de acuerdo con la naturaleza de las cláusulas del modelo. Se debe identificar todos los procedimientos que se van a documentar y ponerlos en un diagrama Gantt para planificar su realización.

B. DEFINIR EL FORMATO DEL PROCEDIMIENTO

No existe un modelo en particular que se debe seguir para documentar los procedimientos. El ISO 9000 define que "un procedimiento es una manera específica de desempeñar una actividad".

Un formato para organizar la información del procedimiento tiene, en base a la práctica internacional y las empresas certificadoras, seis aspectos (Alexander, 2007), estos son:

Propósito. El propósito es la razón de ser del procedimiento. Se debe definir para qué se crea el procedimiento.

Alcance. Aquí se debe definir la amplitud que tiene el procedimiento. Se debe especificar desde dónde se inicia hasta dónde concluye dicho procedimiento.

Procedimiento. Se deben pormenorizar cada uno de los actores que intervienen en el procedimiento, así como las actividades que realizan. Aquí se explica a cada "quién hace qué" y "cuándo".

Referencias. En este punto, se deben especificar aquellos documentos que se consideran fuentes de consulta o medios de clarificación de algún punto del procedimiento, los cuales no pertenecen al sistema de calidad.

Definiciones. Es necesario explicar algún término que resulte ajeno para los lectores, o para quienes conforman algún grupo o un comité en particular que participe en el procedimiento.

Documentos. Este punto incluye todo documento controlado que incida en el procedimiento que se está elaborando.

C. DENTIFICAR ACTORES DEL PROCEDIMIENTO

Los actores deben participar en el diseño del procedimiento y ser identificados estratégicamente. Un flujograma ayuda a determinar exactamente quienes son los actores del procedimiento. La idea es llegar a tener una representación de un modelo que pudiera ser normativo.

D. LEVANTAR Y VALIDAR EL FLUJOGRAMA

El flujograma permite diseñar estratégicamente el futuro procedimiento con las características particulares de rapidez que se desean, pocos actores y actividades y documentos que den valor agregado.

El propósito es crear un flujograma normativo, que dé valor agregado, que aumente la productividad y reduzca el tiempo del ciclo. El flujograma no es un documento controlado, únicamente es una herramienta gráfica para elaborar el procedimiento. La norma no exige un flujograma.

Es fundamental, validar el flujograma por cada proceso que va siendo analizado y graficado, de no hacerlo, una vez documentado todo el procedimiento, pueden aparecer personas que no están de acuerdo con el resultado final.

E. REDACTAR TODA LA INFORMACION DEL FLUJOGRAMA

Se debe, de una manera sencilla, de fácil lectura y presentada amigablemente, transcribir toda la información que efectúan los actores descritos en el flujograma; así, se permite a los lectores entender fácilmente la secuencia de las actividades comprendidas en el procedimiento y detallar con precisión quién es responsable de ejecutar las tareas. Una vez más, es fundamental la validación del procedimiento, así incluso, se refuerza el hecho de que se involucren los actores del procedimiento.

F. IDENTIFICAR, REDACTAR Y VALIDAR INSTRUCCIONES DE TRABAJO

Con los actores involucrados, hay que identificar si se necesitan instrucciones de trabajo.

Para hacer la redacción de las instrucciones de trabajo, es requisito fundamental que el usuario del documento participe en su elaboración. Se le debe entrevistar, observar en el trabajo, de ser necesario, realizar uno mismo la tarea, para así concluir con una información.

La validación de las instrucciones de trabajo, una vez que se obtenga la versión final, no es solamente asegurarse de la transparencia del proceso, sino cerciorarse de que el usuario la entiende y la utiliza.

G. IDENTIFICAR LOS REGISTROS REQUERIDOS

Una vez concluida la labor de desarrollar el procedimiento, hay que ubicar los documentos que pudiesen presentarse a terceros para dar fe de que se cumplió

con los requisitos indicados de la norma, esto es lo que refiere a un registro. Una metodología adecuada y bien ejecutada para documentar el ISO 27001, debería constituir una herramienta poderosa que ayude al establecimiento del SGSI en la organización.

H. IDENTIFICAR LOS DOCUMENTOS DE SEGURIDAD DE INFORMACIÓN

Al diseñar el flujograma, de manera natural aparecen aquellos documentos que se considerarán parte del Sistema de Seguridad de Información. Hay que cuestionarse sobre la validez de los documentos, en especial si datan de mucho tiempo atrás, perteneciendo a otra época empresarial. Es fundamental, una vez identificado el documento, verificar con el usuario si el contenido del documento genera la información necesaria. Las políticas de seguridad de información son consideradas también como documentos.

CAPÍTULO 3.

CASO DE ESTUDIO

En base al Diseño del Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito efectuado en el capítulo 2, se procede a realizar un diagnóstico de la Cooperativa del caso de estudio, indicando las áreas evaluadas y la forma de hacerlo, se realiza un análisis de resultados que hace posible determinar los riesgos para la organización, y los planes para su tratamiento.

3.1 ANALISIS DE LA COOPERATIVA DE AHORRO Y CRÉDITO DEL CASO DE ESTUDIO, EN REFERENCIA A LA GESTION DE LA SEGURIDAD DE LA INFORMACION

Para analizar la situación actual de la Cooperativa de Ahorro y Crédito, primero fue necesario realizar un diagnóstico de su situación en cuanto a la Gestión de la Seguridad de la Información. Se indican las 11 áreas evaluadas, se presenta de forma gráfica los resultados, y luego se efectúa su respectivo análisis.

3.1.1 DIAGNOSTICO

Para poder realizar el diagnóstico, se realizó consultas, entrevistas, y visitas técnicas, tanto a la propia Cooperativa, como a otras organizaciones del ámbito del sector cooperativo, entre ellas la FECOAC y a la SBS. Se elaboró un conjunto de preguntas para realizar encuestas, en base a la publicación “Auditoria de la Tecnologías de la Información y Comunicación de Cooperativas de Ahorro y Crédito”, desarrollado por la Confederación Alemana de Cooperativas. En este proceso, entre otras personas, fue fundamental, la participación de:

- Presidente de la Cooperativa
- Gerente
- Responsable del sistema informático
- Personal de dicha Institución.

En el anexo 4, se encuentran los cuestionarios, que fueron uno de los medios utilizados para obtener información. La evaluación de la información recopilada,

esta realizada en base a la norma ISO 27001, la parte correspondiente de la ley de Superintendencia de Bancos y Seguros, la ley de Cooperativas en su parte pertinente a las Cooperativas de Ahorro y Crédito, y en consideración de la estructura y estatutos de la Cooperativa del caso de estudio; esto es, en apego al Sistema de Gestión de Seguridad de la información diseñado en al Capítulo 2.

3.1.2 ASPECTOS EVALUADOS

Los aspectos evaluados fueron aquellos que la Norma ISO 27001, considera fundamentales para poder llegar a establecer, implementar, operar, monitorear y corregir, con la correspondiente documentación y mejora continua. Así, la evaluación versó sobre 11 áreas de control que son: Política de seguridad, Organización de la seguridad de la información, Gestión de activos de información, Seguridad de los recursos humanos, Seguridad física y ambiental, Gestión de comunicaciones y operaciones, Control de accesos, Adquisición - desarrollo y mantenimiento de los sistemas, Gestión de incidentes de seguridad, Gestión de continuidad del negocio, Cumplimiento Normativo.

La referencia con respecto a la cual se evaluaron estos aspectos, está constituida por el Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito, desarrollado en el capítulo 2. De esta manera se evalúa el grado de cumplimiento, y a su vez se determina la brecha existente con los más altos niveles que harían posible una Certificación Internacional ISO 27001.

3.1.3 RESULTADOS

Una vez que se procesó toda la información a la que se tuvo acceso, en la Cooperativa de Ahorro y Crédito, fue posible realizar un diagnóstico cuyos resultados se presentan en la Tabla 3.1. Estos resultados se presentan de forma gráfica para facilitar su interpretación.

En cada gráfico de pastel, el área de color azul muestra el grado de cumplimiento en referencia al SGSI diseñado en el capítulo II; mientras que el área blanca indica la brecha existente con el grado de cumplimiento.

Cobertura alcanzada en Gestión de la Seguridad de la Información por la CAC
Medida de la brecha existente con relación al SGSI diseñado para CAC

Nº	ASPECTOS EVALUADOS	GRADO DE CUMPLIMIENTO
1	Política de seguridad	
2	Organización de la seguridad de la información	
3	Gestión de activos	
4	Seguridad de los recursos humanos	
5	Seguridad física y ambiental	
6	Gestión de comunicaciones y operaciones	
7	Control de accesos	
8	Adquisición, desarrollo y mantenimiento	
9	Gestión de incidentes de seguridad	
10	Gestión de continuidad del negocio	
11	Cumplimiento Normativo	

TABLA 3.1 Indicadores de la situación actual de la CAC
ELABORADO POR Ing. Mantilla Aníbal

3.1.4 ANALISIS DE LOS RESULTADOS

Todos los indicadores están interrelacionaos entre sí, ya que obedecen al enfoque en procesos y determinan desde perspectivas diferentes pero complementarias, la medida de la Gestión en cuanto a la Seguridad de la Información en la Cooperativa de Ahorro y Crédito del caso de estudio.

Como puede verse, la Política de Seguridad de la Información que es la base fundamental para un Sistema de Gestión de Seguridad de la Información, debe recibir especial atención, pues el nivel alcanzado es mínimo, al igual que indicadores como los de Gestión de Incidentes de seguridad, Gestión para la Continuidad del negocio, y el Cumplimiento normativo.

Si bien es cierto que dentro de los niveles alcanzados por la CAC, en lo referente a la Seguridad de los Recursos humanos, a la Gestión de Comunicaciones y Operaciones, y al Control de accesos, tienen los valores más altos en la Tabla 3.1, la verdad es que deben realizarse muchas actividades aún para llegar a los niveles que plantea el SGSI diseñado en el capítulo II.

Con la información de la Tabla 3.1, es posible determinar las vulnerabilidades y amenazas que podrían producir riesgos para la Cooperativa, por supuesto, las posibles medidas a tomar para mitigar o asumir el riesgo.

3.2 ELABORACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL CASO DE ESTUDIO

Dado que la norma ISO 27001 trabaja sobre un enfoque a procesos, una aplicación detallada y puntual de la misma, requiere de un manual de procesos completa y debidamente establecidos, definidos, documentados y validados.

La aplicación de la norma en referencia y el modelo del SGSI diseñado, a más de proteger la información, hace más dinámica la operación de la organización, sin embargo, si no se ha aplicado una reingeniería de procesos a la organización, esta se vuelve muy lenta en sus operaciones.

Según la información obtenida, la Cooperativa de Ahorro y Crédito del caso de estudio no cuenta con un manual de procesos documentado, que permita analizar sobre cada uno de ellos y en su interrelación, las amenazas, las vulnerabilidades, y los riesgos; identificando los activos de información, los custodios de dichos activos, y más elementos que forman parte del SGSI diseñado.

Para determinar y evaluar los riesgos en una organización, se requiere entre otros: especialistas en seguridad informática, encargados de levantar flujogramas de procesos con los actores de los mismos y su correspondiente validación, el compromiso de la Dirección, la participación activa del personal de la organización, los recursos necesarios, entre otros.

La elaboración del SGSI para el caso de estudio, muestra la determinación y análisis de los riesgos, a los que esta sometida la Cooperativa, incluidos aquellos que pudieran resultar desastrosos para la organización, en caso de ocurrir. Tanto la determinación de riesgos, como el Plan para el tratamiento del riesgo, cubren los cuatro aspectos que establece el Sistema de Gestión de Seguridad de la Información: Organización, Personas, Tecnología, Marco Legal.

Aún cuando no es posible aplicar en el caso de estudio, en forma puntual el modelo diseñado con enfoque a procesos, se sigue estrictamente los principios metodológicos establecidos, esto es:

- Determinación de amenazas, vulnerabilidades, y riesgos
- Planes para el tratamiento del riesgo

FIGURA 3.1 Aspectos que abarca el SGSI en la Cooperativa del caso de estudio
ELABORADO POR Ing. Mantilla Aníbal

Para facilitar la organización y presentación de estos dos aspectos , en las dos secciones siguientes respectivamente, se conserva los colores distintivos de los aspectos: Organizacional, Personal, Tecnológica y Legal, de acuerdo a lo establecido en la Figura 3.1

3.2.1 DETERMINACION Y ANALISIS DE RIESGOS EN LA CAC

A continuación se presentan tablas en las que pueden verse las amenazas, las vulnerabilidades y los riesgos, sobre la seguridad de la información de la Cooperativa. Estas tablas se encuentran en el orden siguiente:

- Organizacional
- Personal
- Tecnológica
- Legal

Todas las tablas y su contenido fueron elaboradas por el autor de esta Tesis.

AREA: ORGANIZACIONAL	
AMENAZA - VULNERABILIDAD - RIESGO	**IMPLICACIÓN A LA SEGURIDAD DE LA INFORMACIÓN**
Pérdida de información producto de infección por virus informático	El riesgo de pérdida de información por virus informático es alto si no se administra adecuadamente el sistema antivirus y los usuarios no han sido concientizados en seguridad de la información.
Fuga de información a través del personal que ingresa en forma temporal	El personal que ingresa temporalmente podría realizar actividades no autorizadas, lo cual podría ser detectado en algunos casos, únicamente al finalizar las actividades de la Cooperativa. Esto podría ser más grave de lo previsible, si se considera que no existe una total división física de áreas de trabajo, ni política de mesas vacías.
Gestión de Tecnologías de la Información y Comunicación	A partir del 11 de Septiembre del 2001, la Gestión de TIC's, considera con mucho más énfasis, la seguridad de la información, lo cual hace necesario que todo el personal tenga conocimientos sobre SGSI, y los interiorice.
Fuga de información estratégica mediante la sustracción de computadoras	Es posible obtener información existente en las computadoras mediante el robo de las mismas, en especial si son equipos portátiles de altos directivos de la Cooperativa.
División inadecuada de espacios de trabajo	Esto imposibilita un manejo más confidencial de la información, haciendo más complicada la situación, el hecho que no hay política de mesas vacías, con lo cual la información sobre dichas mesas esta al alcance de muchas manos.

TABLA 3.2 Determinación y análisis del riego, en el área organizacional[33]

AREA: ORGANIZACIONAL

[33] **ELABORADO POR:** Ing. Mantilla Aníbal

AMENAZA - VULNERABILIDAD - RIESGO	IMPLICACIÓN A LA SEGURIDAD DE LA INFORMACIÓN
Medio de comunicación	No existe un grupo o persona específicamente designada para dar información en caso de incidentes de seguridad, para evitar rumores, malos entendidos, desinformación e incluso pérdida de seguros y pólizas.
Inexistencia de manual de procesos para la Cooperativa de Ahorro y Crédito	Se imposibilita la planificación, la evaluación, el control y las correcciones, necesarias en los modelos de procesos. No es posible aplicar un SGSI con enfoque a procesos.
Inexistencia en el organigrama de la Cooperativa, de un departamento o persona destinado a la Gestión de la Seguridad Informática	Se determina la existencia de fallas en la documentación de la Cooperativa. No se ha considerado una Política de Seguridad, que ubique cerca de la alta gerencia, a un Departamento fundamental para la seguridad.
Inexistencia de una clasificación de la información en términos de su uso	Como consecuencia de esto pudiera hacerse un mal manejo de la información, que afecta su seguridad y por ende a los intereses de la Cooperativa.
Asalto o robo	Si bien es cierto, se ha mejorado la seguridad física y los controles de acceso, no existe un detector de metales que permita conocer si hay personas armadas intentando ingresar a la Cooperativa
Riesgo de incendio	En la Cooperativa existe una gran cantidad de material inflamable, y no existen las debidas protecciones, ni plan ni política ni capacitación al personal, en caso de incendios. Dependiendo de la magnitud de un incendio en la Cooperativa, este hecho pudiera resultar catastrófico para la organización.

TABLA 3.2 Determinación y análisis del riego, en el área organizacional (continuación)[33]

De igual manera, en apego al enfoque a procesos presentado en el Diseño del SGSI del capítulo 2, la determinación de los riesgos que de ocurrir pueden

[33] **ELABORADO POR:** Ing. Mantilla Aníbal

resultar desastrosos para la organización, incluida la continuidad de sus operaciones, requiere de las actividades secuenciales siguientes:

- Determinación de la exposición al riesgo y controles
- Determinación de impactos financieros, impactos operacionales, procesos críticos, tiempos críticos, requerimientos de recursos.
- Elaboración de planes en base a estrategias, desarrollo de los planes seleccionados con su respectiva documentación.
- Ensayo del Plan de Continuidad de Negocio

Sin embargo, dado que no es posible contar con todo esto para el desarrollo de esta Tesis, no se desarrolló un Plan de Continuidad de Negocio (lo cual en sí mismo podría constituir una Tesis de Grado), sino que se elaboró un Plan de Contingencias para la Organización. A continuación se realiza el cálculo de la exposición al riesgo a amenazas potenciales a los que está sometida la Organización.

AMENAZAS POTENCIALES	SEVERIDAD			
	N/A	B	M	A
Pérdida de Personal clave			√	
Pérdida debido a incendios				√
Pérdida de la red de computadores		√		
Pérdida del sistema telefónico			√	
Pérdidas debido a robo				√

TABLA 3.3 Estimación del nivel de severidad de amenazas potenciales[34]

AMENAZAS	COBERTURA (EN %)	EXPOSICIÓN

[34] **ELABORADO POR:** Ing. Mantilla Aníbal

POTENCIALES	0 -19	20 - 39	40 - 59	60 - 79	80 - 99	100	
Pérdida de Personal clave					√		**1000**
Pérdida debido a incendios		√					**8000**
Pérdida de la red de computadores					√		**200**
Pérdida del sistema de comunicaciones con el exterior					√		**400**
Pérdidas debido a robo			√				**6000**

TABLA 3.4 Cálculo de exposición al riesgo ante amenazas potenciales[35]

Como se indicó en el capítulo 2, para calcular la exposición al riesgo se requiere multiplicar el nivel de severidad y la medida en que está desprotegida (sin cobertura de seguridad) la Cooperativa. Estos valores fueron determinados en función de la naturaleza, ubicación, sistemas de apoyo, más aspectos inherentes a la Cooperativa del caso de estudio. Los cálculos realizados fueron los siguientes:

1. Pérdida de personal clave: 50 (100-80)= 50 (20) = 1000
2. Pérdida debido a incendios: 100 (100-20)=100 (80) = 8000
3. Pérdida de la red de computadores: 10 (100-80)= 10 (20) =200
4. Pérdida del sistema de comunicaciones con el exterior: 10(100-60)=10(40) = 400
5. Pérdidas debido a robo: 100 (100 – 40) = 100 (60) = 6000

En la siguiente figura se han graficado los valores de exposición al riesgo, para que de manera visual sea más fácil poder compararlos, y visualizar la magnitud de cada uno de ellos.

[35] **ELABORADO POR:** Ing. Mantilla Aníbal

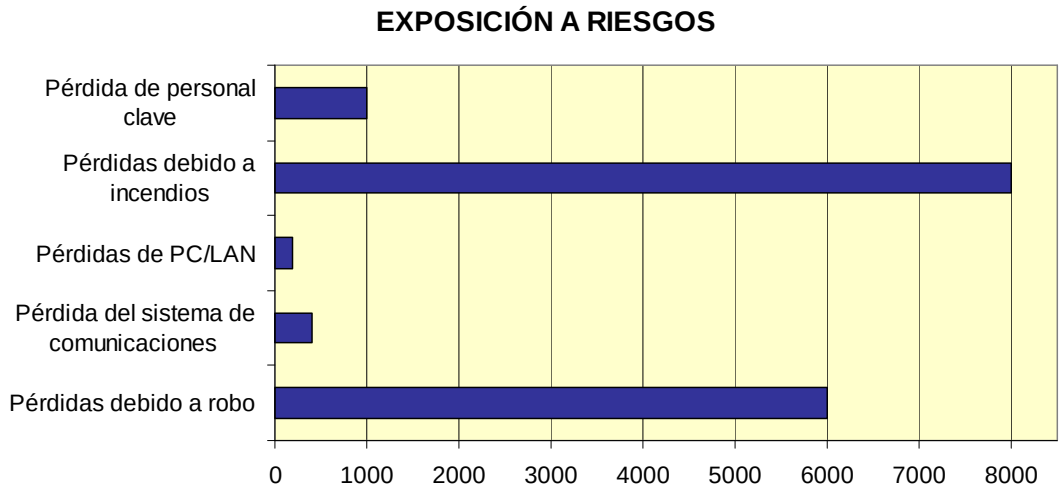

FIGURA 3.2 Representación gráfica de la exposición al riesgo ante amenazas potenciales[36]

Como puede ver en la figura 3.2, los riesgos de pérdidas debido a incendios y de pérdidas debido a robo, superan por mucho a las otras pérdidas que pudieran producirse por amenazas potenciales.

El orden de prioridad con el que deberían atenderse estos riesgos es el siguiente:

1. Perdida debido a incendios
2. Perdidas debido a robo
3. Perdida de personal clave
4. Pérdida del sistema de comunicaciones con el exterior
5. Perdida de la red de computadores

A continuación se presenta la determinación y análisis de amenazas, vulnerabilidades y riesgos en la Cooperativa Caso de estudio, para las áreas Personal, Tecnológica, y Legal:

[36] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: PERSONAL	
AMENAZA - VULNERABILIDAD - RIESGO	**IMPLICACIÓN A LA SEGURIDAD DE LA INFORMACIÓN**
Interés en obtener información estratégica de la Cooperativa, con fines políticos y económicos	Existe información de la Cooperativa que pudiera ser atractiva para empresas, personas, instituciones, y hacer un mal uso de ella.
Interés en obtener beneficios económicos mediante actividades fraudulentas.	Dado el monto de dinero que es administrado por la Cooperativa, pudiera resultar muy tentador, a personal interno y externo a la Cooperativa, el intento de obtener beneficio económico, a través de actividades fraudulentas
Actividad Vandálica	La disponibilidad, la integridad de la información de la Cooperativa pudieran verse afectadas por personal interno o externo a la misma, como por ejemplo el caso de personas que pudieran haber salido resentidas de la organización.
Falta de conciencia en seguridad de la información por parte del personal de la Cooperativa	El personal de la Cooperativa es el vínculo entre la política de seguridad y su implementación final; se pueden establecer controles y monitoreo constante, pero la persona es siempre el punto más débil en el sistema de seguridad; esto constituye un riesgo para la organización, más aun si el personal no recibe una adecuada capacitación y orientación sobre la seguridad de la información.
Fuga de información a través del personal	Puede suceder que personal de la organización comente sobre procesos de la Cooperativa y su información, que puedan hacer daño a la misma, aun existiendo algún compromiso sobre confidencialidad
Controles adecuados para información almacenada en computadores personales	Es común que el personal de organizaciones posea en los computadores a su cargo, aplicaciones e información, que no corresponden a las actividades de la organización, haciendo un mal uso de estos equipos, y poniendo en riesgo a la organización.

TABLA 3.5 Determinación y análisis del riego, en el área personal[37]

[37] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: TECNOLOGICA	
AMENAZA - VULNERABILIDAD - RIESGO	**IMPLICACIÓN A LA SEGURIDAD DE LA INFORMACIÓN**
Computadores personales	- Se debe contar con adecuados controles de acceso a información existente en computadores personales. - Se requieren adecuados controles de acceso a la información de los sistemas desde las computadoras personales de usuarios. - Debe tenerse un mismo sistema operativo en todo el parque de computadores, para estandarizar la configuración de los mismos. - Debe haber un control sobre los dispositivos que pudieran facilitar la fuga de información (memorias pen drive, flash, cd's, impresoras personales, cámaras digitales, etc.) - Se debe controlar y monitorear las aplicaciones y sistemas existentes en los PC's.
Correo electrónico	- Posibilidad de interceptación no autorizada de mensajes de correo electrónico - Posibilidad de utilización de recursos por parte de personas no autorizadas para enviar correo electrónico a terceros. - Posibilidad de recepción de correo inservible (SPAM).
Conexión a Internet	- Riesgos de accesos no autorizados desde el Internet y redes externas hacia los sistemas de la Cooperativa. - Riesgos de uso inadecuado de Internet por parte de usuarios.
Fuga de información estratégica de computadoras en sistemas inalámbricos	Con la actual tecnología para comunicación móvil, fácilmente podría extraerse información de PC's, que se encuentren en enlace inalámbrico

TABLA 3.6 Determinación y análisis del riego, en el área tecnológica[38]

[38] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: LEGAL	
AMENAZA - VULNERABILIDAD - RIESGO	**IMPLICACIÓN A LA SEGURIDAD DE LA INFORMACIÓN**
Existen aplicaciones sin las debidas licencias	Esto podría impedir actualizaciones, introducir virus al sistema, incompatibilidad con sistemas, aplicaciones, y hardware; además de hacer perder las garantías de contratos de aseguramiento.
No se cumplen normas de seguridad en la prevención y control de incendios.	Por efectos de incendio, podría perderse gran cantidad de información, equipos, vidas humanas; todos ellos considerados como activos de información. Los efectos de un incendio pudieran ser devastadores para la organización
No existe política de seguridad, documentada y llevada a norma.	La Política de seguridad establece la guía y directriz para las actividades de la organización en cuanto a su seguridad informática. Esta política llevada a norma interna establece responsabilidades y sanciones por su incumplimiento. Por falta de esta normativa, podría estar afectándose gravemente a la confidencialidad y a la integridad de la información que maneja la Cooperativa.

TABLA 3.7 Determinación y análisis del riego, en el área legal [39]

[39] **ELABORADO POR:** Ing. Mantilla Aníbal

3.2.2 PLAN PARA EL TRATAMIENTO DE LOS RIESGOS

Una vez que se han determinado los riesgos y su implicación a la seguridad de la información de la Cooperativa del Caso de estudio, se debe buscar la manera de tratar el riesgo. El riesgo puede ser mitigado, evitado, transferido o asumido. Para que este proceso se lleve a efecto, es necesario que todos los elementos de la organización, es decir, personas, equipos, instalaciones, procesos, tareas, documentos, y más componentes de la misma, se encuentren perfectamente alineadas a Directrices claras y documentadas que establezcan lo que debe hacerse, la manera de hacerlo, y las responsabilidades por su incumplimiento. De aquí, se deriva la urgente necesidad de contar con una Política de seguridad para la organización, como un factor fundamental y básico para enfocar la actividad de la seguridad de la información de manera efectiva.

La Política de Seguridad, es la base sobre la cual más tarde se podrá construir un Sistema de Gestión de Seguridad de la Información, para el caso de la presente Tesis, alineado al estándar internacional ISO 27001, y a la realidad del sector de las Cooperativas de Ahorro y Crédito ecuatorianas, de acuerdo al Diseño del SGSI realizado en el capítulo 2 de esta Tesis.

Este Plan para el tratamiento del riesgo posee varios subplanes, que abarcan a todos los elementos enfocados por el Sistema de Gestión de Seguridad de la Información; estos son:

- Organizacional
- Personal
- Tecnológica
- Legal

De acuerdo a los requerimientos del diseño, por su trascendencia para la organización, se incluye también, el enfoque para la continuidad de operaciones, en este caso, un Plan de contingencias, de acuerdo a lo establecido también en la Ley de la Superintendencia de Bancos y Seguros, para las Instituciones del Sistema Financiero. A continuación se presentan tablas, en las que pueden verse los planes antes mencionados:

AREA ORGANIZACIONAL

En esta área, se plantean los siguientes Subplanes para el tratamiento del riesgo:

- Definir políticas de seguridad
- Clasificar la información
- Incorporar un departamento de seguridad informática
- Registrar e inventariar los accesos a los sistemas informáticos
- Adaptar contratos con proveedores
- Elaborar un manual de seguridad
- Contratar seguros
- Gestionar incidentes de seguridad
- Plan de contingencias: actividades contra incendios

AREA: **ORGANIZACIONAL**	**SUBPLAN :** **DEFINIR POLITICAS DE SEGURIDAD**
OBJETIVO	
Proveer dirección y guía, a todas las actividades de la organización y en todos los niveles jerárquicos, para asegurar la información en base a un enfoque global, con normas, responsabilidades y procedimientos para el efecto.	
ACTIVIDADES	
POLITICAS DE SEGURIDAD GENERALES PARA LA ORGANIZACIÓN - Debe existir un comité de sistemas (informática), conformado por funcionarios de áreas de administración, que será el encargado de avalar los requerimientos de hardware o software de la CAC. - Se debe asignar presupuesto por área, para todo lo que tiene que ver con recursos de informática. - Se debe realizar compras, cambios o eliminaciones de elementos de software o Hardware, con las debidas justificaciones. - Deben existir alternativas manuales que garanticen normal desempeño. - Continuamente deben difundirse las políticas de seguridad - Contar con respaldo técnico y garantía tecnológica. - Capacitar y entrenar permanentemente a usuarios de computadores	

TABLA 3.8 Subplan para Definir políticas de seguridad[40]

[40] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN : (CONTINUACIÓN) DEFINIR POLITICAS DE SEGURIDAD

ACTIVIDADES

POLITICAS DE SEGURIDAD PARA EL SOFTWARE
- Debe cumplirse con leyes de Propiedad Intelectual
- Debe desarrollarse software de acuerdo a estándares
- Documentar el desarrollo de sistemas y aplicaciones que usan
- Realizar auditorías

POLITICAS DE SEGURIDAD PARA EL HARDWARE
- Aplicar criterios de compatibilidad con la base instalada de equipos de la CAC
- Compartir al máximo los recursos, definiendo restricciones de seguridad.
- Realizar un inventario periódico.
- Documentar cambios de localización, apertura y mantenimiento de equipos.
- Justificar solicitudes de equipos de tecnología informática

POLITICAS DE SEGURIDAD QUE DEBE SEGUIR EL USUARIO
- Justificar toda solicitud de programas o equipos de acuerdo con los procedimientos de compras de la CAC.
- Responsabilizarse por de la correcta administración de la información que utilice, previendo las acciones de seguridad y confidencialidad.
- Identificar individualmente cada acceso.
- Verificar un espacio adecuado en el disco duro del servidor para el sistema operativo, programas de aplicación o utilitarios; de la misma manera en los demás computadores.
- Prohibir el uso de cualquier tipo de software que no esté autorizado por la CAC

POLITICAS DE SEGURIDAD PARA EL ÁREA DE SISTEMAS
- Atender a usuarios de manera continua y segura.
- Mantener la continuidad en el procesamiento
- Verificar el espacio en disco necesario para almacenamiento de datos.
- Garantizar la permanencia fiel de los datos que residan en discos del servidor.

TABLA 3.8 Subplan para Definir políticas de seguridad (continuación)[40]

[40] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN: CLASIFICAR LA INFORMACIÓN

OBJETIVO

Priorizar adecuadamente la utilización de recursos para asegurar de mejor manera la información. Determinar en forma específica, las personas y las circunstancias en que puede utilizar la información de la Cooperativa.

ACTIVIDADES

- Elaborar un inventario de activos de información incluyendo información almacenada en medios digitales e información impresa.
- Definir responsables por activos identificados.
- Clasificar la información en base a los siguientes criterios:
  - **Información Restringida** (R): Información con mayor grado de sensibilidad; el acceso a esta información debe de ser autorizado caso por caso.
  - **Información Confidencial** (C): Información sensible que solo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.
  - **Información de Uso Interno** (I): Datos generados para facilitar las operaciones diarias; deben de ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.
  - **Información General** (G): Información que es generada específicamente para su divulgación al público en general. Puede ser de mucha sensibilidad; el acceso a esta información debe de ser autorizado caso por caso.
- Determinar las medidas de seguridad a ser aplicados para cada activo clasificado.

TABLA 3.9 Subplan para Clasificar la información[41]

[41] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN : INCORPORAR UN DEPARTAMENTO DE SEGURIDAD INFORMATICA

OBJETIVO

Contar con un departamento con alta jerarquía organizacional, con capacidad para intervenir en todos los aspectos de planificación, ejecución, control, cambio, mantenimiento, auditoria y actualización, en aspectos relacionados con el Sistema de Gestión de Seguridad de la Información.

ACTIVIDADES

- Crear un Departamento de Seguridad informática con jerarquía alta y suficiente para disponer con autoridad e independencia frente a los departamentos usuarios.
- El Departamento de Seguridad informática debe depender directamente de la Dirección General, así incluso, no dejará dudas sobre su ecuanimidad.
- El Director de este Departamento debe ser miembro del Comité de Dirección
- Este departamento debe incorporarse al Organigrama de la Cooperativa, y a su vez, tener su propio organigrama.
- En este departamento deben definirse clara y documentadamente, las responsabilidades de cada uno de sus miembros, y esta información debe darse a conocer a los miembros de la organización relacionados con el departamento.
- Debe asegurarse la segregación de funciones.
- Una de las responsabilidades del Departamento es el Aseguramiento en la Calidad del servicio que prestan, en base a estándares y metodologías.
- Es fundamental que el Departamento elabore planes de contingencia para Hardware, Software y comunicaciones. Documentados, validados y difundidos.
- Participar en la planificación y adquisición de los recursos de tecnologías de información que requiere la organización, así como de auditorias relacionadas a este aspecto.
- Este departamento juega un papel muy importante en el establecimiento y posterior implantación de un Sistema de Gestión de Seguridad de la Información en la Cooperativa.

TABLA 3.10 Subplan para Incorporar un departamento de seguridad informática[42]

[42] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN : REGISTRAR E INVENTARIAR LOS ACCESOS A LOS SISTEMAS INFORMATICOS
OBJETIVO	
Controlar de manera adecuada el acceso de los usuarios a los sistemas de la Cooperativa.	
ACTIVIDADES	
- Elaborar un inventario de las aplicaciones, los sistemas de la Cooperativa y los perfiles de acceso en cada caso - Verificar los perfiles definidos en los sistemas para cada usuario - Revisar y aprobar los accesos por parte de las gerencias respectivas - Depurar los perfiles accesos de los usuarios a los sistemas. - Realizar mantenimiento periódico del inventario. - Realizar revisiones periódicas de los accesos otorgados en los sistemas	

TABLA 3.11 Subplan para Registrar e inventariar los accesos a los sistemas informáticos[43]

AREA: ORGANIZACIONAL	SUBPLAN : ADAPTAR CONTRATOS CON PROVEEDORES
OBJETIVO	
Asegurar el cumplimiento de las políticas de seguridad de la Cooperativa en relación con los proveedores, y las cláusulas de los contratos establecidos con estos.	
ACTIVIDADES	
- Elaborar cláusulas estándar referidas a seguridad de información, para ser incluidas en los contratos con proveedores - Elaborar un inventario de los contratos existentes con proveedores - Revisar los contratos y analizar el grado de cumplimiento de la política de seguridad. - Modificar los contratos en caso de ser necesario. - Negociar con los proveedores para la inclusión de las cláusulas en los contratos.	

TABLA 3.12 Subplan para Adaptar contratos de proveedores [44]

[43] - [44] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN : ELABORAR UN MANUAL DE SEGURIDAD

OBJETIVO

Documentar instrucciones de trabajo, procedimientos, políticas, evaluación del riesgo y su tratamiento, entre otros aspectos fundamentales del SGSI, para manejar de mejor manera la seguridad informática, aplicar una reingeniería a la organización, y preparase mejor para alcanzar una certificación internacional ISO 27001.

ACTIVIDADES

- Recopilar los registros y documentos relacionados con el Sistemas de Gestión de Seguridad de la Información

- Aplicar una reingeniería sobre las Instrucciones de trabajo, que se realizan en la Cooperativa, en apego a la Política de seguridad.

- Documentar las nuevas instrucciones de trabajo

- Revisar y modificar si es necesario, los procesos y su interrelación.

- Documentar los procedimientos relacionados con la Seguridad de la Información.

- Incorporar en un solo manual, lo siguiente:
  - Enunciados de la política del SGSI
  - Alcance del SGSI, Procedimientos y controles de soporte
  - Descripción de la metodología de evaluación del riesgo
  - Reporte de evaluación del riesgo
  - Plan de tratamiento del riesgo
  - Declaración de aplicabilidad
  - Todos aquellos documentos adicionales que la Cooperativa considere necesarios para la Seguridad de la Información.

- Revisar periódicamente la validez de las tareas, instrucciones de trabajo, procesos, enfoque de los procesos, procedimientos.

- Incluir todas las modificaciones y actualizaciones al Manual de Seguridad

TABLA 3.13 Subplan para Elaborar manual de seguridad de la información [45]

[45] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN : CONTRATAR SEGUROS

OBJETIVO

Cubrir las perdidas ocasionadas a través de impactos financieros y operacionales, causadas por amenazas que han explotado vulnerabilidades, una vez que el riesgo ha sido tratado en cualquiera de las siguientes formas: evitarlo, transferirlo, mitigarlo, o asumirlo.

ACTIVIDADES

- Inventariar todos los activos de información.
- Tasar los activos de información
- Determinar el nivel de exposición al riesgo de los activos
- Determinar el impacto sobre la organización
- Para el caso de afectación o pérdida de instalaciones, se debería considerar la contratación de los siguientes seguros:
  - Contra incendios
  - Contra amenazas naturales (erupciones, terremotos, rayos)
  - Contra el ataque a las instalaciones por parte de personas o bandas organizadas.
- Para el caso de personal clave, podrían considerarse seguros de vida, seguros de accidentes laborales, seguros por daños a la reputación de las personas.
- Podría considerarse además, un seguro en caso de accidentes aviatorios relacionados con los edificios de la Organización, y que pudieran afectar a las operaciones de la Cooperativa.
- Seguros contra robo, daño o destrucción de equipos vitales para la organización.
- Seguros en caso de incumplimiento de contratos de confidencialidad, incluyendo además, los productos de propiedad intelectual de la Cooperativa.
- Contratar un seguro que posibilite los recursos para enfrentar desastres y poder aplicar el Plan para la Continuidad del Negocio.

TABLA 3.14 Subplan para Contratar seguros[46]

[46] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	SUBPLAN : GESTIONAR INCIDENTES DE SEGURIDAD
OBJETIVO	
Actuar de forma proactiva ante incidentes de seguridad, asegurar un correcto manejo del incidente, evitar que el incidente de seguridad se convierta en problema de seguridad, así como también, que vuelva a suceder.	
ACTIVIDADES	
- Definir un plan de actuación y de procedimientos ante incidentes de seguridad, con la adecuada documentación de los mismos. - Comprobar que el plan cumple con los requisitos legales - Adquirir los medios tecnológicos que faciliten la Gestión de incidentes - Aislar los equipos afectados por el incidente - Capturar y proteger toda la información relacionada con el incidente - Analizar la información del incidente para catalogarlo - Comunicar sobre el incidente a quienes tengan la competencia del caso - Aplicar soluciones de acuerdo al plan de actuación - Eliminar los medios que faciliten un nuevo incidente similar - Recuperar la actividad normal de los sistemas afectados - Identificar las lecciones y conclusiones de cada incidente - Incorporar las lecciones aprendidas a las Políticas	

TABLA 3.15 Subplan para Gestionar incidentes de seguridad[47]

[47] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: ORGANIZACIONAL	DENTRO DEL PLAN GENERAL, EL PLAN DE CONTINGENCIAS: ACTIVIDADES CONTRA INCENDIOS

OBJETIVO

Elaborar de manera documentada y normativa, un plan que permita prevenir incendios, actuar adecuadamente durante el siniestro, establecer condiciones adecuadas para la organización después del siniestro. En esencia, minimizar las potenciales pérdidas en la Cooperativa, y si es posible evitar el incendio.

ACTIVIDADES

- Contratar un seguro contra incendios en el local de la Cooperativa.
- Prohibir que se fume en la Organización
- Liberar de obstáculos las puertas y pasillos
- Revisar las condiciones del sistema eléctrico
- Disminuir la cantidad de material inflamable e incluso innecesario en las oficinas de la Cooperativa
- Adquirir e instalar extintores de incendio en áreas visibles y accesibles; se debería también considerar mangueras para incendio. Los extintores deberán contener los compuestos químicos correspondientes a un incendio en la Cooperativa, y periódicamente deberán ser revisados.
- Instalar varios sensores detectores de humo y revisarlos periódicamente
- Capacitar y orientar al personal en el uso de extintores
- La información vital debe protegerse en armarios antifuego
- Deberían instalarse salidas de humo
- Capacitar al personal en primeros auxilios, para atender rápidamente a los lesionados.
- Contar con un botiquín de primeros auxilios bien equipado
- El plan de contingencia debe ser documentado y difundido
- Se deberán realizar simulacros, contando con la supervisión del Cuerpo de Bomberos
- La persona que se percate de la existencia de humo o fuego, debe alertar inmediatamente sin provocar pánico a la persona designada de antemano para liderar las actividades ante un incendio.
- Formar tres Grupos: Grupo de lucha contra el incendio, Grupo de primeros auxilios, Grupo de información (este grupo es fundamental también, pues el responsable de dar la información certera a las personas y autoridades competentes, incluidas las de las aseguradoras, y evitar así perder con el seguro en el cumplimiento normativo o las cláusulas del contrato)
- Tratar de desalojar lo más rápidamente y en orden las instalaciones, de no ser posible, evitar lo más posible el humo y por supuesto el fuego, a menos que se cuente con los medios efectivos para extinguirlos.
- Tener una lista de fácil acceso, con los teléfonos de emergencia (ambulancias, Cruz Roja, Bomberos, Hospitales, Policía, Defensa Civil, etc.)

TABLA 3.16 Plan de contingencia – Actividades contra incendios [48]

[48] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA PERSONAL

Para elaborar estos Subplanes, a más de las consideraciones mencionadas antes para el tratamiento del riesgo, se ha tomado en cuenta los roles y actividades de las personas que conforman la organización. Los Subplanes son los siguientes:

- Concientizar a los funcionarios y empleados de la cooperativa
- Capacitar al personal en uso seguro de los servicios de internet

AREA: **PERSONAL**	**SUBPLAN :** **CONCIENTIZAR A LOS FUNCIONARIOS Y EMPLEADOS DE LA COOPERATIVA**
OBJETIVO	
Lograr un alto grado de compromiso y capacitación de los funcionarios y empleados de la Cooperativa en temas relacionados con la seguridad de la información en la organización; estableciendo en forma documentada y normativa, los beneficios y responsabilidades, incluso de índole penal, que cada uno tiene en la seguridad de la información.	
ACTIVIDADES	
- Establecer como prioridad, la interiorización de la necesidad y conveniencia de tener un adecuado Sistema de Gestión de Seguridad de la Información, hasta que llegue a ser parte de la cultura organizacional de la Cooperativa. - Definir de forma fácilmente comprensible el mensaje a transmitir y material a ser empleado para los distintos grupos de usuarios, entre ellos: • **Personal en general**: información general sobre seguridad, políticas y estándares incluyendo protección contra virus, contraseñas, seguridad física, sanciones, correo electrónico y uso de Internet. • **Personal de Sistemas**: Políticas de seguridad, estándares y controles específicos para la tecnología y aplicaciones utilizadas. • **Gerencias y jefaturas**: Monitoreo de seguridad, responsabilidades de supervisión, políticas de sanción. Identificación del personal de cada departamento que se encargará de actualizar a su propio grupo en temas de seguridad. - Establecer un cronograma de capacitación, el cual debe incluir a los empleados nuevos.	

TABLA 3.17 Subplan para Concientizar a los funcionarios y empleados de la Cooperativas[49]

[49] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: PERSONAL	SUBPLAN : CAPACITAR AL PERSONAL EN USO SEGURO DE LOS SERVICIOS DE INTERNET

OBJETIVO

Obtener el máximo aprovechamiento de los servicios que posibilita el Internet, en función de los roles y funciones de cada empleado y departamentos de la Cooperativa, minimizando los riesgos de virus, spam, estafas y más riesgos existentes al usar de manera insegura el Internet.

ACTIVIDADES

- Interiorizar en las personas, las responsabilidades, amenazas y riesgos que puede correr la persona y la Cooperativa cuando no usa de manera segura el Internet.
- Limitar el acceso a Internet a los usuarios, dependiendo de las actividades que realizan en la Organización. Sin embargo, aún cuando tengan accesos limitados diferentes, afrontarán amenazas comunes al usar los servicios de Internet.
- Una vez configurados los controles de acceso para cada usuario, éste no debe cambiarlos, pero en el caso de los programas exploradores de Internet, debe saber como se han configurado los controles de contenido, pues puede haber aplicaciones que pidan excepciones o consultas al usuario para poder operar.
- Capacitar al usuario en el uso seguro del correo electrónico, y un uso adecuado de los sistemas antivirus.
- Tomar medidas para minimizar el spam
- Sobre todo dependiendo de las responsabilidades y atribuciones de los funcionarios y empleados, debe capacitarse al personal para evitar las estafas por Internet, especialmente por tratarse de una entidad financiera.

TABLA 3.18 Subplan para Capacitar al personal en el uso seguro de los servicios de internet[50]

[50] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA TECNOLOGICA

Para realizar los Subplanes del área Tecnológica, se han considerado aspectos fundamentales para mejorar la Seguridad de la Información en la Cooperativa, todos ellos alineados a lo que más tarde será documentado y normado como Política de Seguridad. Estos Subplanes son:

- Adaptar los sistemas de comunicación
- Adaptar la arquitectura de red
- Estandarizar y actualizar el software

AREA: **TECNOLOGICA**	**SUBPLAN:** **ADAPTAR LA CONFIGURACIÓN DE LOS SISTEMAS DE COMUNICACION**
OBJETIVO	
Alinear la configuración en hardware y software de los sistemas de comunicación, con las políticas de seguridad, tanto para la operación interna como para la operación externa de la organización, pues en última instancia son las personas quienes producen ataques a la seguridad de la información, siendo estos equipos, medios de defensa, o en el caso contrario medios de vulnerabilidad.	
ACTIVIDADES	
- Elaborar un inventario de equipos de comunicaciones (routers, switches, firewalls, etc) - Elaborar estándares de configuración para los equipos de comunicaciones (basarse en la política de seguridad definida, documentación de proveedores, etc.) - Evaluar equipos identificados. - Adaptar los equipos a la política de seguridad.	

TABLA 3.19 Subplan para Adaptar la configuración de los sistemas de comunicación[51]

[51] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: TECNOLOGICA	SUBPLAN : ADAPTAR LA ARQUITECTURA DE RED

OBJETIVO
Crear una red que sea rápida, eficiente y segura, al soportar todos los requerimientos de la Cooperativa, y en apego a las políticas de la seguridad

ACTIVIDADES
Implementar una red DMZ: para evitar el ingreso de conexiones desde Internet directamente hacia la red interna de datos; además debe evitar el tráfico ilegítimo entre la Cooperativa y el Internet. Esta zona desmilitarizada consta de dos cortafuegos; un cortafuegos protege los accesos desde el exterior hacia la zona desmilitarizada y el otro protege los accesos desde la zona desmilitarizada hacia la Intranet. Un ataque de Denegación de Servicio, que saturara o comprometiera al cortafuegos exterior, no pondría en peligro al cortafuegos interno. En esta zona desmilitarizada se instalará un servidor Proxy, para recuperar la información que haya solicitado un usuario interno, y almacenándola para que pueda ser recuperada desde la intranet; si el requerimiento de información es en sentido contrario, el usuario interno coloca esta información en la zona desmilitarizada, y luego esta es entregada a un equipo externo. **Implementar un sistema de Antivirus:** para servicios de Internet (SMTP, FTP, HTTP) que requiere la Cooperativa, con la adecuada configuración, mantenimiento, actualización, y documentación. **Implementar sistemas de Alta Disponibilidad:** para aumentar la seguridad y fiabilidad de la red, es necesario instalar sistemas de redundancia, para ser utilizados en firewalls, servidores, y otros equipos de comunicación. **Implementar un sistema de detección de Intrusos (IDS):** para detectar los intentos de intrusión o ataque desde redes externas hacia la red de datos de la Cooperativa, así como aquellos ataques realizados desde la red interna de la organización.

TABLA 3.20 Subplan para Adaptar la arquitectura de red[52]

[52] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA: TECNOLOGICA	SUBPLAN : ESTANDARIZAR Y ACTUALIZAR EL SOFTWARE
OBJETIVO	
Determinar fácil y rápidamente vulnerabilidades en el software, elevar los niveles de protección de la información, disminuir los incidentes de seguridad, y responder más eficaz y eficientemente ante amenazas y riesgos potenciales.	
ACTIVIDADES	
- Elaborar un inventario de sistema operativo de servidores y computadores personales. - Elaborar una base de datos de aplicaciones. - Actualizar permanente y periódicamente, los antivirus tanto de los servidores como de los PC's de cada usuario en cada uno de los departamentos. - Mantener el sistema operativo permanentemente actualizado - Elaborar estándares de configuración para los sistemas operativos de las PC's de la Cooperativa - Elaborar una guía para configuración de aplicaciones - Mantener las aplicaciones permanentemente actualizadas - Evaluar permanentemente la estandarización y actualización del software. - Elaborar guías de chequeo y revisión para establecer si se están cumpliendo las políticas de seguridad en el software que utiliza la Cooperativa.	

TABLA 3.21 Subplan para Estandarizar y actualizar el software[53]

[53] **ELABORADO POR:** Ing. Mantilla Aníbal

AREA LEGAL

Toda la actividad de la Cooperativa del Caso de estudio, debe realizarse en base al cumplimiento legal, pues a más de ser lo que corresponde a una organización que aspira a mejorar sus niveles de desempeño en la seguridad de la información en base a estándares internacionales, podrá lograr así, efectividad en sus operaciones, minimizará las interferencias en el procesos de auditoría de sistemas, y evitará pérdidas a la organización.

AREA: **LEGAL**	**SUBPLAN :** **VERIFICAR EL CUMPLIMIENTO LEGAL**
OBJETIVO	
Evitar incumplimientos de cualquier ley, reglamento, norma, o contrato, para asegurar el cumplimiento de los sistemas con las Políticas de Seguridad.	
ACTIVIDADES	
- Revisar que la actividad informática se la realiza dentro de las normas legales, referentes a: • Normas laborales • Propiedad intelectual del software • Requisitos en la cobertura de seguros • Prevención de riesgos. - Debe cumplirse con la Ley en lo que corresponde a : • Órgano de Supervisión y Control en el Sistema Financiero Nacional • Ley de Cooperativas de Ahorro y Crédito • Normativa propia de la Cooperativa, incluyendo los puntos específicos de la Política de seguridad. - Al implementarse medidas para la seguridad de la información, debe tenerse cuidado de no contradecir los principios del derecho a la intimidad de las personas, y aquellos establecidos en la ética laboral, personal y profesional. - Así mismo, debe verificarse el cumplimiento legal con usuarios y proveedores; no hay que olvidar que las cláusulas de confidencialidad tienen implicaciones legales, en algunos casos penales. - Para el efecto se deberán realizar Comités, reuniones departamentales, y controles de auditoría.	

TABLA 3.22 Subplan para Verificar el cumplimiento legal[54]

[54] **ELABORADO POR:** Ing. Mantilla Aníbal

CAPÍTULO 4.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se han cumplido completamente con todos los objetivos planteados para la realización de esta Tesis. Sin embargo, en el desarrollo de este trabajo, siempre tuve la predisposición y la actitud permanente de alcanzar los más altos y mejores resultados, que incluso fueron más allá del cumplimiento de los objetivos inicialmente planteados. Puse lo mejor de mis conocimientos y mis recursos en este propósito.

- La función de la Seguridad de la Información en cualquier tipo de organización, debe ser considerada como un factor básico empresarial fundamental, de la misma trascendencia que los aspectos comercial, financiero, administrativo.

- No es necesario que se dispongan en el País, de las normas correspondientes a la Seguridad de la Información, para afrontar y resolver los problemas de seguridad en las empresas nacionales, pues puede recurrirse a normas ya adaptadas o existentes en otros países.

- La aplicación exhaustiva y detallada del **Diseño de un Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito en base a la norma ISO 27001**, requiere de procesos claros, validados, optimizados, actualizados, para evitar que la implantación del SGSI conlleve a procesos confusos, demasiado complejos y lentos, que a la final, en lugar de mejorar a la organización, le resten eficiencia y competitividad.

- La seguridad de la información es un aspecto, que debe ser parte de la cultura organizacional; cursos, seminarios, y talleres no bastan, hay que interiorizar en las personas de la organización, la necesidad y beneficios de dicha cultura, así como los riesgos de no tenerla.

- El Sistema de Gestión de Seguridad de la Información debe ser permanentemente revisado, mejorado y actualizado, para que brinde la máxima utilidad que la organización espera.

- Una eficiente Gestión de la Seguridad de la Información, debe considerar los aspectos: organizacional, personal, tecnológico y legal, en base a un enfoque sistémico, en el que cada uno de sus componentes esta interrelacionado con los demás, en su operación y funcionamiento; y cada uno de ellos como todo el sistema, obedece al principio fundamental causa – efecto.

- En el desarrollo de la presente Tesis, se ha comprobado la evidente necesidad de que las Cooperativas de Ahorro y Crédito del Ecuador, implanten Sistemas de Gestión de Seguridad de la Información para una mayor eficiencia en sus actividades, que les proporcione un crecimiento sostenido y productivo, a la vez que propenda a la mejora de la calidad de vida de sus socios, y a un mayor desarrollo del País.

4.2 RECOMENDACIONES

- Se considera importante, que tomando como base inicial esta Tesis, se establezcan y desarrollen Proyectos en varias Tesis de Maestría, sucesivas y concatenadas, en los siguientes aspectos:
    - Implantar el Plan para el tratamiento de los riesgos elaborado en el Capítulo tres de esta Tesis, en la Cooperativa de Ahorro y Crédito del Caso de estudio, a través de los diferentes Subplanes (organizacional, personal, tecnológico, y legal), como una etapa previa y alternativa mientras la organización se prepara para llegar a la certificación internacional.
    - Desarrollar la planificación y las actividades necesarias, para obtener la certificación internacional ISO 27001, para la Cooperativa de Ahorro y Crédito del Caso de estudio.

- Se sugiere la publicación y difusión de este trabajo, a nivel nacional, para que pueda ser utilizado en beneficio del mejoramiento de las Cooperativas de Ahorro y Crédito; particularmente en lo que se refiere al tema tratado en esta Tesis, esto es, la Seguridad de la Información en una perspectiva global y como un pilar fundamental en las actividades de estas instituciones.

- Incorporar a la estructura organizacional de las Cooperativas de Ahorro y Crédito, un departamento que trabaje de manera proactiva y reactiva, en Sistemas de Gestión de Seguridad de la Información.

BIBLIOGRAFÍA

LIBROS

- ABAD Alfredo, Redes de Área Local, McGraw Hill. 2001
- DURAN Alvaro, Desafíos para la gestión de Cooperativas de Ahorro y Crédito de América Latina y el Caribe, 2007
- GÓMEZ V. Alvaro, Enciclopedia de la seguridad informática, Alfaomega 2007
- GORDILLO Estuardo, Memoria estadística de las Cooperativas de Ahorro y Crédito ecuatoriano, FECOAC, 2005
- HILL Brian, Manual de referencia CISCO, McGraw Hill,2002.
- INSTITUTO ARGENTINO DE NORMALIZACIÓN, Norma ISO 17799, "Código de Practica para la Gestión de Seguridad de la Información", 2002
- JAMES A. O' Brien. Sistemas de Información Gerencial. McGraw Hill. 2003
- KENNETH C. Laudon. Sistemas de Información Gerencial. Prentice Hall. 2006
- LEY DE COOPERATIVAS ECUATORIANAS, Editorial Forum,2008
- NARANJO Jaime. Gestión de Proyectos. Escuela Politécnica Nacional, 2006
- Norma Venezolana - Tecnologías de la Información, Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. FONDONORMA- ISO/IEC 27001:2005
- OCHOA José, 101 claves de Tecnologías de Información para Directivos,Prentice Hall, 2004
- PENIN, Aquilino, Sistemas SCADA, Alfaomega, 2007
- PIATTINI Mario, Auditoria de Tecnologías y Sistemas de Información, Alfaomega, 2008.
- PRESSMAN Roger, Ingeniería del Software, McGraw Hill, 2005
- RENDER. Administración de Operaciones. Prentice Hall. 2004
- ROBBINS Stephen, Fundamentos de Administración, Prentice Hall, 2002
- SAMANIEGO Gustavo, Redes de Computadoras, Escuela Politécnica Nacional, 2006

- SOSA Pablo, Sistemas de Gestión de Seguridad de la Información, Escuela Politécnica Nacional, 2006
- TANEMBAUM Andrew, Redes de Computadoras, Prentice Hall, 2003
- VASQUEZ Rodrigo, Antecedente y Contemporaneidad del Pensamiento Cooperativo, FECOAC, 2008
- WEITZENFELD Alfredo, Ingeniería de Software Orientada a Objetos, Thomson, 2005

SITIOS WEB

- www.dgrv.org
- www.igepn.edu.ec
- www.pnud.org.ec
- www.stgestionriesgos.gov.ec
- www.nexusasesores.com
- www.eficienciagerencial.com
- www.iso27000.es
- www.dpya-sa.com.ar
- www.comercio.com.ec
- www.superban.gov.ec
- www.dinacoop.gov.ec
- www.acsb.fin.ec

ANEXOS

ANEXO 1

LA NORMA ISO 27001

En este anexo se presenta la norma ISO 27001 de manera resumida, la cual consta de un Prefacio, 8 Cláusulas, un anexo Normativo y dos anexos Informativos. El anexo normativo (Anexo A de la norma ISO 27001) presenta los controles que deben aplicarse en las once áreas de control que establece esta norma; para una mejor identificación, se presentan en tablas separadas y con diferentes colores. En los anexos Informativos, se presenta la relación de esta norma con los principios de la Organización para la Cooperación y el Desarrollo Económico (OEDC), y con otras normas ISO; en los anexos B y C de la norma ISO 27001, respectivamente.

En la tabla siguiente se muestra los elementos, estructura organización de esta norma:

ELEMENTO	ASPECTO SOBRE EL QUE TRATA
PREFACIO	PRESENTACION
CLAUSULA 0.	INTRODUCCIÓN
CLAUSULA 1.	OBJETO
CLAUSULA 2.	REFEENCIAS NORMATIVAS
CLAUSULA 3.	TÉRMINOS Y DEFINICIONES
CLAUSULA 4.	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
CLAUSULA 5.	RESPONSABILIDAD DE LA DIRECCIÓN
CLAUSULA 6.	AUDITORÍAS INTERNAS DEL SGSI
CLAUSULA 7.	REVISIÓN POR LA DIRECCIÓN DEL SGSI
CLAUSULA 8.	MEJORA DEL SGSI
ANEXO A.	NORMATIVO
ANEXO B.	INFORMATIVO
ANEXO C.	INFORMATIVO

TABLA 1 del Anexo 1 Elementos de la norma ISO 27001
ELABORADO POR Ing. Mantilla Aníbal

A continuación se detallan cada uno de estos elementos:

PREFACIO

Hace referencia a las razones por loas cuales fue desarrollada esta norma y su trascendencia a nivel mundial para un manejo adecuado de la seguridad

Informática, a través de un Sistema de Gestión que abarca en su actividad a todos los elementos de la organización

CLÁUSULA 0. INTRODUCCIÓN

El ISO 27001:2005 define la seguridad de información como la "preservación de la confidencialidad, integridad, no repudio y confiabilidad". Se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un SGSI para cualquier clase de organización.

El diseño y la implantación de un SGSI se encuentran influenciados por las necesidades, los objetivos, los requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización.
El modelo ISO 27001:2005 está diseñado bajo una óptica de enfoque a procesos.
El SGSI está conceptualizado para funcionar en cualquier tipo de organización, operando bajo el enfoque de procesos, sin embargo, cada SGSI se elabora de la manera más adecuada para cada empresa.

FIGURA 1del Anexo 1 Enfoque de la norma hacia procesos a través del ciclo de Deming [55]

[55] Fuente: www.nexusasesores.com

CLÁUSULA 1. OBJETO

En la sección 1.2 del estándar se precisa su aplicación. Aquí se puntualiza que el modelo se ha creado para ser aplicable a toda clase de organización, sin importar su tipo, el tamaño y la naturaleza del negocio. Aquí también se explica que si algunos de los requerimientos del estándar no pudiesen ser aplicados debido a la naturaleza de una organización y su negocio, se puede considerar el requerimiento para su exclusión.

Para que las exclusiones sean válidas, no podrán afectar la capacidad y / o la responsabilidad de la organización a fin de proporcionar seguridad en la información que satisfaga los requerimientos de seguridad determinados por la evaluación del riesgo y los requerimientos reguladores aplicables. Las cláusulas de las secciones 4 a 8 no son excluibles. Además especifica los requisitos para la implementación de controles de seguridad adaptados a la organización o parte de ella.

CLÁUSULA 2. REFERENCIAS NORMATIVAS

Hace referencia a documentos que son indispensables para la aplicación de esta estándar. Pueden ser documentos fechados como no fechados, en los dos casos se requiere justificación para su uso.

CLÁUSULA 3. TÉRMINOS Y DEFINICIONES

En esta cláusula se indican los términos y definiciones fundamentales para esta norma, relacionados directamente con el Sistema de Gestión de Seguridad de la Información. Entre otros términos, se tiene: activo de información, disponibilidad, confidencialidad, seguridad de la información, evento de seguridad de la información. Más términos con sus correspondientes definiciones se encuentran en el Glosario de Términos.

CLÁUSULA 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CLÁUSULA 4: Sección 4.1 ESTABLECER LOS REQUISITOS GENERALES

El SGSI debe ser establecido, implementado, monitoreado, corregido, documentado, mejorado, de acuerdo a los requerimientos específicos de la organización.

CLÁUSULA 4: Sección 4.2 ESTABLECER y GESTIONAR EL SGSI

Sección 4.2: Subsección 4.2.1 ESTABLECER EL SGSI

Actividades organizacionales

A) Definir el alcance y los límites del SGSI

B) Definir la política para el SGSI

C) Definir el enfoque para la evaluación del riesgo

D) Identificar, analizar y evaluar los riesgos

E) Identificar y evaluar las opciones para el tratamiento del riesgo, incluyendo al riesgo residual

F) Seleccionar los objetivos de control para el tratamiento del riesgo

G) Obtener la aprobación de los riesgos residuales por la dirección

H) Obtener la autorización de la dirección para implementar y operar el SGSI

I) Preparar una declaración de aplicabilidad

Sección 4.2: Subsección 4.2.2 IMPLEMENTAR Y OPERAR EL SGSI

Actividades organizacionales:

A) Formular un plan para el tratamiento del riesgo

B) Implementar plan para el tratamiento del riesgo

C) Implementar los controles seleccionados

D) Definir como mediar la eficacia de los controles seleccionados

E) Implementar programas de formación y toma de conciencia

F) Gestionar la operación del SGSI

G) Gestionar los recursos para el SGSI

H) Implementar los procedimientos y otros controles capaces de permitir la pronta detección de los eventos de seguridad y la respuesta a incidentes de seguridad

Sección 4.2: Subsección 4.2.3 MONITOREAR Y REVISAR EL SGSI

Actividades organizacionales:

A) Realizar el seguimiento y revisar los procedimientos
B) Llevar a cabo revisiones regulares de eficacia del SGSI (incluyendo el cumplimiento de la política y objetivos del SGSI)
C) Medir la eficacia de los controles
D) Realizar las evaluaciones del riesgo a intervalos planificados, revisar los riesgos residuales y los niveles de riesgo aceptables.
E) Conducir auditorias internas
F) Revisión del SGSI por parte de la dirección sobre una base regular
G) Actualizar los planes de seguridad
H) Registrar las acciones y los eventos que podrían tener un efecto obre la eficacia o el desempeño del SGSI.

Sección 4.2: Subsección 4.2.4 MANTENER Y MEJORAR EL SGSI

Actividades organizacionales:

A) Implementar las mejoras identificadas
B) Tomar adecuadas acciones correctivas y preventivas
C) Comunicar los resultados a todas las partes interesadas
D) Asegurar que las mejoras alcanzan los objetivos deseados

CLÁUSULA 4: Sección 4.3 DOCUMENTAR EL SGSI

Sección 4.3: Subsección 4.3.1 GENERALIDADES

Aquí, se establece que los documentos del SGSI son los siguientes:

1. Los enunciados de la política de seguridad, los procedimientos y los objetivos de control.
2. El alcance del SGSI, los procedimientos y los controles que sostienen el SGSI.

3. El plan de tratamiento del riesgo.
4. Los procedimientos documentados necesarios para la organización, a fin de asegurar la planeación, la operación y el control efectivos de sus procesos de seguridad de la información.
5. Los registros requeridos por el estándar.
6. Declaración de aplicabilidad.
7. El reporte de evaluación del riesgo.
8. La descripción de la metodología de evaluación del riesgo

Sección 4.3: Subsección 4.3.2 CONTROLAR LOS DOCUMENTOS

En este apartado se pide tener un procedimiento documentado que defina las acciones gerenciales para:

A) Aprobar la idoneidad de los documentos antes de su emisión.
B) Revisar y actualizar los documentos conforme sea necesario, y reaprobarlos.
C) Asegurar que se identifiquen los cambios y el estatus de la revisión actual de los documentos.
D) Asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso.
E) Asegurar que los documentos se mantengan legibles y fácilmente identificables.
F) Asegurar que se identifiquen los documentos de origen externo;
G) Asegurar que se controle la distribución de documentos;
H) Evitar el uso indebido de documentos obsoletos;
I) Aplicar a los documentos una identificación adecuada si se van a retener por algún propósito.

Sección 4.3: Subsección 4.3.3 CONTROLAR LOS REGISTROS

Esta cláusula plantea que se tenga un procedimiento documentado para ejercer un control relevante para la identificación, el almacenaje, la protección, la recuperación, el tiempo de retención y la disposición de los registros. Por disposición se entienden las acciones que se toman con los registros, al vencer el tiempo de retención.

CLÁUSULA 5. DEFINIR LA RESPONSABILIDAD DE LA DIRECCIÓN

Sección 5.1: COMPROMISO DE LA DIRECCIÓN

Esta cláusula está dirigida a la gerencia y a puntualizar sus responsabilidades en relación con el SGSI; el modelo es muy puntual. La gerencia debe desempeñar un papel protagónico en el manejo de un SGSI.

Sección 5.2 : GESTIONAR LOS RECURSOS

Sección 5.2: Subsección 5.2.1 PROVISIÓN DE LOS RECURSOS

En esta cláusula se le dan varias exigencias a la organización, por medio del gráfico de la gerencia. Las exigencias son las siguientes:

A) Establecer, implementar, operar y asegurar que los procedimientos de seguridad de la información sostengan los requerimientos comerciales;
B) Asegurar que los procedimientos de seguridad de la información, respalden los requerimientos comerciales.
C) Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
D) Mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
E) Llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
F) Mejorar la efectividad del SGSI donde se requiera.

Sección 5.2: Subsección 5.2.2 CAPACITACIÓN, CONOCIMIENTO Y CAPACIDAD

En esta cláusula la norma tiene cuatro exigencias específicas:

1. Se debe determinar los perfiles requeridos del personal al que se le asigna responsabilidades en el SGSI y diagnosticar sus necesidades de entrenamiento.
2. Capacitar y seleccionar al personal para satisfacer los perfiles requeridos.
3. Efectuar una evaluación de la eficacia del entrenamiento efectuado.

4. Mantener expedientes del personal en detalle sobre: educación recibida, capacitación realizada, capacidades desarrolladas, experiencias profesionales y calificaciones obtenidas.

CLÁUSULA 6. AUDITAR INTERNAMENTE EL SGSI

En esta cláusula la norma es muy precisa, al detallar el propósito de las auditorias. Establece que la organización debe realizar auditorias internas del SGSI a intervalos planeados para determinar si los objetivos, controles, procesos y procedimientos de su SGSI:

A) Cumplen con los requerimientos de este estándar y la legislación o regulaciones relevantes.
B) Cumplen con los requerimientos de seguridad de información identificados.
C) Son implementados y mantenidos de manera efectiva.
D) Se desempeñan como se esperaba.

CLÁUSULA 7. REALIZAR REVISIÓN GERENCIAL

Debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad. La revisión gerencial se convierte en una excelente evidencia objetiva de que la gerencia está comprometida con el SGSI. Cuando el SGSI está en proceso de implantación, es conveniente que las referidas revisiones se hagan con mayor frecuencia.

CLÁUSULA 7: Sección 7.1 GENERALIDADES

Como parte del ciclo de Deming, la Dirección debe realizar continuas revisiones a todos los elementos que forman parte del Sistema de Gestión de Seguridad de la Información, con resultado documentados que deben propender oportunidades de mejora

CLÁUSULA 7: Sección 7.2 ELEMENTOS DE ENTRADA PARA REVISIÓN

Como elemento fundamental dentro de los elementos de entrada para revisión, se encuentra la retroalimentación de las partes interesadas; así como también las acciones tomadas en revisiones previas, cualquier cambio en el SGSI y la evaluación previa de riesgo realizada, ente otras.

CLÁUSULA 7: Sección 7.3 RESULTADOS DE LA REVISIÓN

Estos resultados se relacionan con la mejora de la eficacia del SGSI, la actualización en la medición y plan para tratamiento del riesgo, necesidades de los recursos, y modificación de procedimientos que pudieran impactar al SGSI.

CLÁUSULA 8. MEJORAR DEL SGSI

Esta cláusula hace referencia a la necesidad de mejorar continua y permanentemente el Sistema de Gestión de Seguridad de la Información, en concordancia con los ciclos de mejora continua, tomando como elemento fundamental, la acción correctiva y la acción preventiva.

CLÁUSULA 8: Sección 8.1 MEJORAMIENTO CONTÍNUO

La mejora continua es visualizada como el conjunto de acciones emprendidas por la organización, para aumentar la probabilidad de incrementar la satisfacción de las partes interesadas.

En esta cláusula, la norma especifica que la organización debe tomar como fuente de inspiración, para iniciar la mejora continua:

- La política de seguridad de la información
- Los objetivos de seguridad
- Los resultados de auditoría
- El análisis de los eventos monitoreados
- Las acciones correctivas y preventivas
- La revisión gerencial

CLAUSULA 8: Sección 8.2 ACCIÓN CORRECTIVA

La acción correctiva se define como "acción tomada para eliminar la causa de una no-conformidad detectada u otras situaciones indeseables" (ISO 9000:2000). En el contexto del SGSI, una no-conformidad es el" incumplimiento de un requisito."
Cada vez que algo que se haya planificado, o un requerimiento de la norma que no se hubiese cumplido, automáticamente se debe iniciar la acción correctiva.

CLAUSULA 8: Sección 8.3 ACCIÓN PREVENTIVA

La acción preventiva se entiende como la acción tomada para eliminar la causa de una no-conformidad potencial u otra situación potencialmente indeseable" (ISO 9000:2000).

ANEXO A DE LA NORMA ISO 27001:

OBJETIVOS DE CONTROL Y CONTROLES

En esta sección, se presentan los objetivos de control y controles de la norma, en base a las 11 áreas de control establecidas por la misma. Pueden considerarse todos los controles, una parte de ellos, e incluso controles adicionales dependiendo de los requerimientos de la organización y su estructura. Sin embargo si lo que se busca es la Certificación Internacional, deben aplicarse todos los controles de una forma exhaustiva

A.5 POLÍTICA DE SEGURIDAD

OBJETIVO: DIRIGIR Y DAR SOPORTE A LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. DE ACUERDO CON LOS REQUISITOS DEL NEGOCIO, LAS LEYES Y REGLAMENTOS PERTINENTES.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.5.1.1	Documento de la política de seguridad de la información	Un documento de política de seguridad de información será aprobado por la dirección, publicado y comunicado a todos los empleados y partes externas pertinentes.
A.5.1.2	Revisión de la política de seguridad de la información	La política de seguridad de la información debe revisarse a intervalos planificados, o si ocurren cambios significativos asegurar su conveniencia, adecuación y eficacia continua.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1 ORGANIZACIÓN INTERNA **OBJETIVO:** GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA ORGANIZACIÓN		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.6.1.1	Compromiso de la dirección para la seguridad de la información	La dirección debe apoyar activamente la seguridad dentro de la organización a través de la dirección clara, del compromiso demostrado, la asignación explícita, y el reconocimiento de las responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información	Las actividades de seguridad de la información deben coordinarse con representantes de diferentes partes de la organización, con roles y funciones de trabajo pertinentes.
A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	Deben definirse claramente todas las responsabilidades de seguridad de la información.
A.6.1.4	Proceso de autorización para los recursos de procesamiento de la información	Debe definirse e implementarse un proceso de autorización para cada nuevo recurso de procesamiento de la información.
A.6.1.5	Acuerdos de confidencialidad	Debe identificarse y regularmente revisarse los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización, para la protección de la información.
A.6.1.6	Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con grupos interesados especiales	Deben mantenerse los contactos apropiados con grupos interesados especiales u otros foros de especialistas de seguridad y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos, y procedimientos para la seguridad de la información) deben revisarse de forma independiente, a intervalos planificados, o cuando ocurren cambios significativos en la implementación de la seguridad.

A.6.2 PARTES EXTERNAS **OBJETIVO:** MANTENER LA SEGURIDAD DE LA INFORMACIÓN Y RECURSOS DE PROCESAMIENTO DE LA INFORMACIÓN DE LA ORGANIZACIÓN QUE SON ACCESADOS, PROCESADOS, COMUNICADOS, O GESTIONADOS POR ENTIDADES O PARTES EXTERNAS.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.6.2.1	Identificación de riesgos relacionados a partes externas	Los riesgos a la información y recursos de procesamiento de la información de la organización, para los procesos del negocio que involucran partes externas, deben identificarse y deben implementarse los controles apropiados antes de otorgar el acceso.
A.6.2.2	Tratamiento de la seguridad en las relaciones con clientes	Todos los requisitos de seguridad identificados deben tratarse antes de dar el acceso al cliente a la información, o posesiones de la organización.
A.6.2.3	Tratamiento de la seguridad en los acuerdos de terceras partes	Los acuerdos con usuarios de terceras partes que involucran acceder, procesar, comunicar o gestionar la información de la organización o los recursos para el tratamiento de la información, o agregar productos o servicios a recursos para el tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.

A.7 GESTIÓN DE ACTIVOS

A.7.1 RESPONSABILIDAD POR LOS ACTIVOS **OBJETIVO:** ALCANZAR Y MANTENER LA PROTECCIÓN APROPIADA DE LOS ACTIVOS DE LA ORGANIZACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.7.1.1	Inventario de activos	Todos los activos deben identificarse claramente y elaborarse, y mantenerse el inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Toda información y activos asociados con las instalaciones de procesamiento de la información deben ser "dueño"' por una parte designada de la organización.
A.7.1.3	Utilización aceptable de los Activos	Deben identificarse, documentarse e implementarse las reglas, para la utilización aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

A.7.2 CLASIFICACIÓN DE LA INFORMACIÓN **OBJETIVO:** ASEGURAR QUE LA INFORMACIÓN RECIBA UN NIVEL APROPIADO DE PROTECCIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.7.2.1	Directrices de clasificación	La información debe clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2	Etiquetado y manejo de la Información	Un conjunto apropiado de procedimientos para etiquetar y manejar la información debe desarrollarse e implementarse de acuerdo con el esquema adoptado por la organización.

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

A.8.1 ANTES DEL EMPLEO **OBJETIVO:** ASEGURAR QUE LOS EMPLEADOS, LOS CONTRATISTAS Y USUARIOS DE TERCERAS PARTES COMPRENDAN SUS RESPONSABILIDADES. Y QUE SEAN APROPIADOS PARA LOS ROLES CONSIDERADOS, Y PARA REDUCIR EL RIESGO DEL ROBO, FRAUDE O MAL USO DE LOS RECURSOS.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.8.1.1	Roles y responsabilidades	Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios terceras partes deben definirse y documentarse de acuerdo con la política de seguridad de la información de la organización.
A.8.1.2	Selección	La verificación de los antecedentes sobre todos los candidatos para empleados, contratistas, y usuarios de terceras partes deben llevarse a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y proporcionales a los requisitos del negocio, a la clasificación de la información a ser accesada, y los riesgos percibidos.
A.8.1.3	Términos y condiciones de Empleo	Como parte de su obligación contractual, los empleados contratistas y usuarios de terceras partes deben acordar y firmar los términos y condiciones de su contrato de trabajo, que debe declarar sus responsabilidades por la seguridad de la información de la organización.

A.8.2 DURANTE EL EMPLEO		
OBJETIVO: ASEGURAR QUE TODOS LOS EMPLEADOS, CONTRATISTAS Y USUARIOS DE TERCERAS PARTES SON CONSCIENTES DE LAS AMENAZAS Y ASPECTOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN, SUS RESPONSABILIDADES Y OBLIGACIONES, Y QUE ESTÉN EQUIPADOS PARA RESPALDAR LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN EN EL CURSO NORMAL DE SU TRABAJO, Y REDUCIR EL RIESGO DE ERROR HUMANO.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.8.2.1	Responsabilidades de la Dirección	La dirección debe requerir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización y, cuando sea pertinente, los contratistas y usuarios de terceras partes deben recibir la formación en toma de conciencia y las actualizaciones regulares apropiadas en las políticas y procedimientos de la organización, como sea pertinente para su función de trabajo.
A.8.2.3	Proceso disciplinario	Debe haber un proceso disciplinario formal para los empleados quienes cometan un incumplimiento de seguridad.

A.8.3 TERMINACIÓN O CAMBIO DE EMPLEO		
OBJETIVO: ASEGURAR QUE LOS EMPLEADOS, CONTRATISTAS Y USUARIOS DE TERCERAS PARTES SE RETIRAN DE UNA ORGANIZACIÓN O CAMBIAN EL EMPLEO DE UNA MANERA ORDENADA.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.8.3.1	Responsabilidades de la terminación	Deben definirse y asignarse claramente las responsabilidades para llevar a cabo la terminación o cambio de empleo.
A.8.3.2	Devolución de los activos	Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos de la organización en su posesión, una vez terminado su empleo, contrato o acuerdo.
A.8.3.3	Retiro de los derechos de acceso	Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a la información y recursos para el procesamiento de la información deben retirarse una vez terminado su empleo, contrato o acuerdo, o una vez ajustado el cambio.

A.9 SEGURIDAD FÍSICA Y AMBIENTAL

A.9.1 ÁREAS SEGURAS **OBJETIVO:** PREVENIR EL ACCESO FÍSICO NO AUTORIZADO, DAÑO E INTERFERENCIA A LAS INSTALACIONES E INFORMACIÓN DE LA ORGANIZACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.9.1.1	Perímetro de seguridad física	Los perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjeta, o puesto de recepción manual) deben utilizarse para proteger las áreas que contienen la información, y las instalaciones de procesamiento de la información.
A.9.1.2	Controles físicos de entrada	Las áreas de seguridad deben estar protegidas por controles de entrada apropiados que aseguren el permiso de acceso sólo al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones e instalaciones.	Debe diseñarse y aplicarse la seguridad física para oficinas, habitaciones, e instalaciones.
A.9.1.4	Protección contra las amenazas externas y ambientales	Debe diseñarse y aplicarse la protección física contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre.
A.9.1.5	Trabajo en áreas seguras	Deben diseñarse y aplicarse la protección física y las directrices para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso al público, entrega y carga	Los puntos acceso, como las áreas de entrega y carga y otras donde las personas no autorizadas pueden entrar en las instalaciones, deben controlarse y, si es posible, aislarse de instalaciones de procesamiento de la información para evitar el acceso no autorizado.

A.9.2 SEGURIDAD DE LOS EQUIPOS **OBJETIVO:** PREVENIR PÉRDIDAS, DAÑOS, ROBO O COMPROMETER LOS ACTIVOS E INTERRUPCIÓN DE LAS ACTIVIDADES DE LA ORGANIZACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.9.2.1	Ubicación y protección del equipo	El equipo debe ubicarse o protegerse para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado.
A.9.2.2	Servicio de apoyo	El equipo debe protegerse contra fallas de energía y otras interrupciones eléctricas causadas por fallas en los servicios de apoyo.
A.9.2.3	Seguridad del cableado	El cableado de energía eléctrica y de comunicaciones, que transporta datos o brinda apoyo a los servicios de información, debe protegerse contra interceptación o daño.
A.9.2.4	Mantenimiento de equipos	Los equipos deben mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.
A.9.2.5	Seguridad de equipos fuera de las instalaciones de la organización	Debe aplicarse la seguridad a los equipos exteriores teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Seguridad en la reutilización o eliminación de equipos	Todos los elementos del equipo que contengan dispositivos de almacenamiento de datos deben controlarse, para asegurar que cualquier dato sensible y software bajo licencia ha sido removido o tachado antes de su disposición.
A.9.2.7	Retiro de la propiedad	No deben sacarse de las instalaciones, sin autorización, los equipos, la información o el software.

A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

A.10.1 PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIÓN **OBJETIVO:** ASEGURAR LA OPERACIÓN CORRECTA Y SEGURA DE LOS RECURSOS DE TRATAMIENTO DE INFORMACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.1.1	Documentación de procedimientos operativos	Los procedimientos operativos deben documentarse, mantenerse, y estar disponibles a todos los usuarios que los necesitan.
A.10.1.2	Gestión de cambio	Deben controlarse los cambios para los recursos y sistemas de procesamiento de la información.
A.10.1.3	Segregación de tareas	Las tareas o áreas de responsabilidad deben segregarse para reducir las oportunidades de modificación no autorizada o mal uso de los activos de la organización.
A.10.1.4	Separación de los recursos para el desarrollo, prueba/ ensayo y operación.	Deben separase los recursos para el desarrollo, prueba/ensayo y operación para reducir los riesgos del acceso no autorizado o cambios al sistema operativo.

A.10.2 GESTIÓN DE ENTREGA DE SERVICIO DE TERCERA PARTE **OBJETIVO:** IMPLEMENTAR Y MANTENER EL NIVEL APROPIADO DE SEGURIDAD DE LA INFORMACIÓN Y LA ENTREGA DEL SERVICIO EN LÍNEA CON LOS ACUERDOS DE ENTREGA DE SERVICIO DE TERCERA PARTE.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.2.1	Entrega del servicio	Debe asegurarse que los controles de seguridad. las definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio de tercera parte son implementados, operados, y mantenidos por la tercera parte.
A.10.2.2	Seguimiento y revisión de los servicios de tercera parte	Los servicios, informes y registros suministrados por la tercera parte deben ser seguidos y revisados regularmente, y deben ser llevadas a cabo auditorias regularmente.
A.10.2.3	Gestión de cambios para los servicios de tercera parte	Los cambios para el suministro de servicios, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de información existentes, deben gestionarse, tomando en cuenta la criticidad del sistemas del negocio y los procesos involucrados y la reevaluación de los riesgos.

A.10.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA **OBJETIVO:** MINIMIZAR EL RIESGO DE FALLAS DE LOS SISTEMAS.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.3.1	Gestión de la capacidad	Deben realizarse seguimiento, ajustes, y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para asegurar el desempeño del sistema requerido
A.10.3.2	Aceptación del sistema	Deben establecerse los criterios de aceptación para los nuevos sistemas de información y versiones nuevas o mejoradas y deben desarrollarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación.

A.10.4 PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y MOVIBLE		
OBJETIVO: PROTEGER LA INTEGRIDAD DEL SOFTWARE Y DE LA INFORMACIÓN.		
A.10.4.1	Controles contra código- malicioso	Deben implantarse los controles de detección, prevención y recuperación para la protección contra código malicioso, y procedimientos adecuados de toma de conciencia de los usuarios.
A.10.4.2	Control contra código movible	Donde la utilización de código movible está autorizada, la configuración debe asegurar que el código movible autorizado opera de acuerdo con una política de seguridad claramente definida, y debe prevenirse el ejecutar el código movible no autorizado.

A.10.5 COPIA DE SEGURIDAD		
OBJETIVO: MANTENER LA INTEGRIDAD Y LA DISPONIBILIDAD DE LA INFORMACIÓN Y LOS RECURSOS DE PROCESAMIENTO DE LA INFORMACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.5.1	Copia de seguridad de la Información	Las copias de seguridad de la información y software deben ser tomadas y probadas con regularidad de acuerdo con la política de copia de seguridad acordada.

A.10.6 GESTIÓN DE SEGURIDAD DE LA RED		
OBJETIVO: ASEGURAR LA PROTECCIÓN DE LA INFORMACIÓN EN LAS REDES Y LA PROTECCIÓN DE SU INFRAESTRUCTURA DE SOPORTE.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.6.1	Controles de red	Las redes deben gestionarse y controlarse adecuadamente, a fin de estar protegidas de las amenazas, y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de servicios de red	Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red deben identificarse e incluirse en cualquier acordado de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratados.

A.10.7 MANEJO DE MEDIOS DE INFORMACIÓN		
OBJETIVO: PREVENIR LA DIVULGACIÓN, MODIFICACIÓN, ELIMINACIÓN O DESTRUCCIÓN NO AUTORIZADA DE LOS ACTIVOS, E INTERRUPCIÓN DE LAS ACTIVIDADES DEL NEGOCIO.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.7.1	Gestión de medios removibles	Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Disposición de medios	Cuando ya no son requeridos, los medios de información deben eliminarse de forma segura y sin peligro, utilizando procedimientos formales.
A.10.7.3	Procedimientos de manejo de la información	Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada.
A.10.7.4	Seguridad de la documentación de sistemas	La documentación de sistema debería protegerse contra el acceso no autorizado.

A.10.8 INTERCAMBIO DE INFORMACIÓN		
OBJETIVO: MANTENER LA SEGURIDAD DE LA INFORMACIÓN Y EL SOFTWARE INTERCAMBIADO DENTRO DE UNA ORGANIZACIÓN Y CON CUALQUIER ENTIDAD EXTERNA.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.8.1	Políticas y procedimientos de intercambio de información	Deben establecerse políticas, procedimientos de intercambio formales, y controles para proteger el intercambio de información a través de la utilización de toda clase de recursos de comunicación.
A.10.8.2	Acuerdos de intercambio	Deben establecerse acuerdos, para el intercambio de información y software entre la organización y partes externas.
A.10.8.3	Medios de información físicos en tránsito	Los medios que contienen la información deben protegerse contra el acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensaje electrónico	Debe estar apropiadamente protegida la información involucrada en el mensaje electrónico.
A.10.8.5	Sistemas de información del Negocio	Deben desarrollarse e implementarse las políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.

A.10.9 SERVICIOS DE COMERCIO ELECTRÓNICO		
OBJETIVO: ASEGURAR LA SEGURIDAD DE SERVICIOS DE COMERCIO ELECTRÓNICO, Y SU UTILIZACIÓN SEGURA.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.9.1	Comercio electrónico	La información involucrada en la transferencia de comercio electrónico en redes públicas debe protegerse de la actividad fraudulenta, litigios contractuales, y la divulgación o modificación no autorizada.
A.10.9.2	Transacciones en línea	La información involucrada en las transacciones en línea debe protegerse para prevenir la transmisión incompleta, pérdida de rutas, alteración de mensaje no autorizado, divulgación no autorizada y duplicación o repetición de mensaje no autorizada.
A.10.9.3	Información disponible Públicamente	La integridad de la información que está disponible sobre un sistema disponible públicamente debe protegerse para prevenir la modificación no autorizada.

A.10.10 SEGUIMIENTO		
OBJETIVO: DETECTAR LAS ACTIVIDADES DE PROCESAMIENTO DE LA INFORMACIÓN NO AUTORIZADAS.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.10.10.1	Registro de auditoría	Deben producirse y mantenerse los registros de auditorias que registren actividades, excepciones y eventos de seguridad de la información del usuario, durante un periodo definido para ayudar en futuras investigaciones y seguimiento del control de accesos.
A.10.10.2	Seguimiento de la utilización de los sistemas	Deben establecerse los procedimientos para el seguimiento de la utilización de los recursos de procesamiento de la información, y los resultados de las actividades de seguimiento revisadas regularmente.
A.10.10.3	Protección de la información del registro	Deben protegerse los recursos de registro e información de registro contra el acceso manipulado y no autorizado.
A.10.10.4	Administrador y operador de Registros	Deben registrarse las actividades del administrador y el operador del sistema.
A.10.10.5	Registro de fallas	Las fallas deben registrarse, analizarse y tomarse las acciones apropiadas.
A.10.10.6	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de la información pertinentes, dentro de una organización o dominio de seguridad, deben sincronizarse con una fuente de tiempo exacta acordada.

A.11 CONTROL DE ACCESOS

A.11.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESOS **OBJETIVO:** CONTROLAR LOS ACCESOS A LA INFORMACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.11.1	Política de control de accesos	Debe establecerse, documentarse y revisarse una política de control de accesos, basada en los requisitos del negocio y de seguridad para el acceso.

A.11.2 GESTIÓN DE ACCESO DE USUARIOS **OBJETIVO:** ASEGURAR EL ACCESO DEL USUARIO AUTORIZADO Y PREVENIR EL ACCESO NO AUTORIZADO A LOS SISTEMAS DE INFORMACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.11.2.1	Registro de usuarios	Debe existir un procedimiento formal de registro y desregistro de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Deben restringirse y controlarse la utilización y la asignación de privilegios.
A.11.2.3	Gestión de contraseñas de usuario	Debe controlarse la asignación de contraseñas a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso de usuario	La dirección debe revisar los derechos de acceso de los usuarios a intervalos regulares, utilizando un proceso formal.

A.11.3 RESPONSABILIDADES DE USUARIOS **OBJETIVO:** PREVENIR EL ACCESO DE USUARIOS NO AUTORIZADOS, Y COMPROMETER O ROBAR LA INFORMACIÓN Y LOS RECURSOS DE PROCESAMIENTO DE INFORMACIÓN.		
SECCION	**REQUERIMIENTO**	**CONTROL**
A.11.3.1	Uso de contraseñas	Debe requerirse a los usuarios seguir las buenas prácticas de seguridad para la selección y uso de sus contraseñas.
A.11.3.2	Equipo desatendido	Los usuarios deben asegurar que los equipos desatendidos estén debidamente protegidos.
A.11.3.3	Políticas de escritorios y pantallas limpias	Para los recursos de procesamiento de información, debe adoptarse una política de escritorios limpios de papel y de dispositivos de almacenamiento removibles, y una política de pantallas limpias.

A.11.4 CONTROL DE ACCESO A LA RED **OBJETIVO:** PREVENIR EL ACCESO NO AUTORIZADO A LOS SERVICIOS DE RED.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.11.4.1	Política de utilización de los servicios de red	Los usuarios sólo deben tener acceso a tos servicios que han sido específicamente autorizados a utilizar.
A.11.4.2	Autenticación de usuarios para conexiones externas	Deben utilizarse métodos de autentificación apropiados para controlar el acceso por usuarios remotos.
A.11.4.3	Identificación de equipo en Redes	Debe considerarse la identificación de equipo automático como un medio de autentificar las conexiones de ubicaciones y equipos específicos.
A.11.4.4	Protección del diagnóstico remoto y de la configuración de puerto	Debe controlarse el acceso físico y lógico para el diagnóstico y configuración de los puertos.
A.11.4.5	Segregación en redes	Deben segregarse los grupos de los servicios de información, los usuarios, y los sistemas de información en las redes.
A.11.4.6	Control de conexión de redes	Para redes compartidas, especialmente aquellas que atraviesan las fronteras de la organización, la capacidad de usuarios a conectarse a la red debe restringirse, de acuerdo con la política de control de acceso y los requisitos de las aplicaciones del negocio
A.11.4.7	Control de direccionamiento en la red	Deben implementarse los controles de direccionamiento a redes, para asegurar que las conexiones entre computadora y los flujos de información no violen la política de control de acceso de las aplicaciones del negocio.

A.11.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO **OBJETIVO:** PREVENIR EL ACCESO NO AUTORIZADO A LOS SISTEMAS OPERATIVOS.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.11.5.1	Procedimientos de conexión segura	Debe controlarse el acceso a los sistemas operativos por un procedimiento de conexión segura.
A.11.5.2	Identificación y autenticación del usuario	Todos los usuarios deben disponer de un identificador único (ID de usuario) sólo para su uso personal, y debe seleccionarse una técnica de autenticación adecuada, para probar la identidad declarada de un usuario.
A.11.5.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos, y deben asegurar la calidad de las contraseñas.
A.11.5.4	Utilización de las prestaciones del sistema.	Debe restringirse y controlarse estrechamente la utilización de programas de servicio que podrían ser capaces de eludir las medidas de control del sistema y de las aplicaciones.
A.11.5.5	Sesión inactiva	Las sesiones inactivas deben apagarse después de un periodo definido de la inactividad.
A.11.5.6	Limitación del tiempo de Conexión	Las restricciones al horario de conexión deben ser utilizadas para proporcionar seguridad adicional a las aplicaciones de alto riesgo.

A.11.6 CONTROL DE ACCESO A LAS APLICACIONES E INFORMACIÓN **OBJETIVO:** PREVENIR EL ACCESO NO AUTORIZADO A LA INFORMACIÓN CONTENIDA EN LOS SISTEMAS DE APLICACIÓN.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.11.6.1	Restricción de acceso a la información	El acceso a la información y las funciones del sistema de aplicación por usuarios y personal de soporte debe restringirse, de acuerdo con la política de control de acceso definida.
A.11.6.2	Aislamiento de sistemas Sensibles	Los sistemas sensibles deben tener un entorno informático dedicado (aislados).

A.11.7 COMPUTACIÓN MÓVIL Y TRABAJO A DISTANCIA **OBJETIVO:** ASEGURAR LA SEGURIDAD DE LA INFORMACIÓN CUANDO SE UTILIZAN RECURSOS DE COMPUTACIÓN MÓVIL Y DE TRABAJO A DISTANCIA.		
SECCIÓN	**REQUERIMIENTO**	**CONTROL**
A.11.7.1	Computación móvil y comunicaciones	Debe implantarse una política formal, y deben adoptarse las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar recursos de computación móvil y de comunicación.
A.11.7.2	Trabajo a distancia	Deben desarrollarse e implementarse políticas, planes operacionales y procedimientos para las actividades de trabajo a distancia.

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO

A.1 2.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN **OBJETIVO:** ASEGURAR QUE LA SEGURIDAD ES UNA PARTE INTEGRAL DE LOS SISTEMAS DE INFORMACIÓN.		
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Las declaraciones de los requisitos del negocio para los nuevos sistemas de información o mejoras a los sistemas de información existentes deben especificar los requisitos de control de seguridad.

A.12.2 PROCESAMIENTO CORRECTO EN LAS APLICACIONES **OBJETIVO:** PREVENIR LOS ERRORES. PÉRDIDA. MODIFICACIÓN NO AUTORIZADA O MAL USO DE LA INFORMACIÓN EN LAS APLICACIONES.		
A.12.2.1	Validación de datos de entrada	Deben validarse los datos de entrada a las aplicaciones para asegurarse de que éstos son correctos y apropiados.
A.12.2.2	Control del procesamiento Interno	Deben incorporarse a las aplicaciones las comprobaciones de validación para detectar cualquier corrupción de la información a través de los errores de procesamiento o actos deliberados.
A.12.2.3	Integridad de mensaje	Deben identificarse los requisitos para asegurar la autenticidad y proteger la integridad de mensajes en aplicaciones. e identificarse e implementarse los controles apropiados.
A.12.2.4	Validación de los datos de Salida	Deben validarse los datos de salida de una aplicación para asegurarse de que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.

A.12.3 CONTROLES CRIPTOGRÁFICOS **OBJETIVO:** PROTEGER LA CONFIDENCIALIDAD. AUTENTICIDAD O INTEGRIDAD DE LA INFORMACIÓN POR LOS MEDIOS CRIPTOGRÁFICOS.		
A.12.3.1	Política sobre la utilización de controles criptográficos	Debe desarrollarse e implementarse una política sobre la utilización de controles criptográficos para la protección de la información.
A.12.3.2	Gestión de claves	Debe establecerse la gestión de clave para dar apoyo a la utilización por la organización de técnicas criptográficas.

A.12.4 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA **OBJETIVO:** ASEGURAR LA SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA		
A.12.4.1	Control del software operativo	Deben existir procedimientos establecidos para controlar la instalación del software en sistemas en funcionamiento.
A.12.4.2	Protección de los datos de prueba del sistema	Deben seleccionarse cuidadosamente y protegerse y controlarse los datos de prueba.
A.12.4.3	Control de acceso al código fuente del programa	Debe restringirse el acceso al código fuente del programa.

A.12.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE **OBJETIVO:** MANTENER LA SEGURIDAD DEL SOFTWARE Y LA INFORMACIÓN DEL SISTEMA DE APLICACIÓN.		
A.12.5.1	Procedimientos de control de de cambios	La implementación de los cambios debe ser controlada por la utilización de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de aplicaciones después de los cambios de sistema operativo	Cuando los sistemas operativos son cambiados, deben revisarse y probarse las aplicaciones críticas del negocio para asegurarse de que no hay impacto adverso sobre las operaciones, o la seguridad de la organización.
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Las modificaciones a paquetes de software deben ser desalentadas, limitadas a los cambios necesarios, y todo cambio debe controlarse estrictamente.
A.12.5.4	Fuga de información	Deben prevenirse las oportunidades de fuga de información.
A.12.5.5	Desarrollo de software contratado externamente	La organización debe supervisar y realizar seguimiento al desarrollo de software contratado externamente.

A.12.6 GESTIÓN DE VULNERABILIDAD TÉCNICA **OBJETIVO:** REDUCIR LOS RIESGOS QUE RESULTAN DE LA EXPOSICIÓN DE LAS VULNERABILIDADES TÉCNICAS PUBLICADAS.		
A.12.6.1	Control de las vulnerabilidades técnicas	Debe obtenerse la información oportuna sobre las vulnerabilidades técnicas del sistema de información que está siendo utilizado, evaluarse la exposición de la organización a tales vulnerabilidades, y tomarse las medidas apropiadas para tratar el riesgo asociado.

A.13 GESTIÓN DE INCIDENTE DE SEGURIDAD

A.13.1 REPORTAR LOS EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN **OBJETIVO:** ASEGURAR QUE LOS EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN ASOCIADAS CON LOS SISTEMAS DE INFORMACIÓN SEAN COMUNICADOS DE UNA MANERA TAL QUE PERMITA QUE LA ACCIÓN CORRECTIVA SEA TOMADA OPORTUNAMENTE.		
A.13.1.1	Reporte de los eventos de seguridad de información	Deben reportarse los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente como sea posible.
A.13.1.2	Reporte de debilidades de seguridad	Debe requerirse a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información, detectar e informar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada.

A.13.2 GESTIÓN DE LOS INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN **OBJETIVO:** ASEGURAR QUE UN ENFOQUE COHERENTE Y EFICAZ ES APLICADO A LA GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.		
A.13.2.1	Responsabilidades y procedimientos	Deben establecerse las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información.
A.13.2.2	Aprendizaje de los incidentes de seguridad de la información	Deben establecerse mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de seguridad de información.
A.13.2.3	Recolección de evidencias	Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de la información que involucra acciones legales (civiles o criminales), deben recolectarse, conservarse y presentarse evidencias conforme a las reglas establecidas por la legislación aplicable, o por el tribunal que sigue el caso.

A.14 GESTIÓN DE CONTINUIDAD DEL NEGOCIO

A.14 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO **OBJETIVO:** CONTRARRESTAR LAS INTERRUPCIONES DE LAS ACTIVIDADES DEL NEGOCIO Y PROTEGER LOS PROCESOS CRITICOS DEL NEGOCIO DE LOS EFECTOS DE FALLAS SIGNIFICATIVAS O DESASTRES DE LOS SISTEMAS DE INFORMACIÓN, Y ASEGURAR SU REANUDACIÓN OPORTUNA.		
A.14.1.1	La información en el proceso de gestión de la continuidad del negocio	Un proceso dirigido debe ser desarrollado y mantenido para la continuidad del negocio, a través de la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad del negocio y evaluación del riesgo	Los eventos que pueden causar interrupciones a los procesos del negocio deben identificarse, al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información	Deben desarrollarse e implementarse planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos, tras la interrupción o la falla en los procesos críticos del negocio.
A.14.1.4	Marco de planificación para la continuidad del negocio	Se debe mantener un esquema único de planes de continuidad del negocio, para asegurar que dichos planes son coherentes, para tratar coherentemente los requisitos de seguridad de la información, y para identificar las prioridades de prueba y mantenimiento.
A.14.1.5	Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio	Deben probarse y actualizar con regularidad los planes de continuidad del negocio, para asegurarse de su actualización y eficacia.

A.15 CUMPLIMIENTO NORMATIVO

A.15.1 CUMPLIMIENTO DE REQUISITOS LEGALES **OBJETIVO:** EVITAR INCUMPLIMIENTOS DE CUALQUIER LEY, ESTATUTO, OBLIGACIÓN, REGLAMENTARIOS O CONTRACTUALES, Y DE CUALQUIER REQUISITO DE SEGURIDAD.		
A.15.1.1	Identificación de la legislación aplicable	Deben definirse, documentarse y mantenerse actualizados todos los requisitos legales, reglamentarios y contractuales pertinentes y el enfoque de la organización que cumplan estos requisitos para cada sistema de información y de la organización
A.15.1.2	Derechos de propiedad intelectual (DPI)	Deben implementarse los procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados.
A.15.1.3	Protección de los registros de la organización	Deben protegerse los registros importantes contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales y del negocio.
A.15.1.4	Protección de datos y de la privacidad de la información personal	Deben asegurarse la protección de datos y la privacidad como sea requerido en la legislación, las reglamentaciones pertinentes, y, si es aplicable, en las cláusulas contractuales.
A.15.1.5	Prevención del mal uso de los recursos de procesamiento de la información	Debe disuadirse a los usuarios de utilizar los recursos de procesamiento de la información para propósitos no autorizados.
A.15.1.6	Regulación de controles criptográficos	Deben utilizarse los controles criptográficos en cumplimiento con todos los acuerdos, leyes, y regulaciones pertinentes.

A.15.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y EL CUMPLIMIENTO TÉCNICO **OBJETIVO:** ASEGURAR EL CUMPLIMIENTO DE LOS SISTEMAS CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD DE LA ORGANIZACIÓN.		
A.15.2.1	Cumplimiento con las políticas y normas de seguridad	Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad son llevados a cabo correctamente, para alcanzar el cumplimiento con las normas y políticas de seguridad.
A.15.2.2	Comprobación del cumplimiento técnico	Debe comprobarse regularmente la compatibilidad de los sistemas de información con las normas de implementación de seguridad.

A.15.3 CONSIDERACIONES DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN **OBJETIVO**: MAXIMIZAR LA EFECTIVIDAD Y MINIMIZAR LAS INTERFERENCIAS EN EL PROCESO DE AUDITORIA DEL SISTEMA DE LA INFORMACIÓN.		
A.15.3.1	Control de auditoria de los sistemas de información	Deben planificarse cuidadosamente y acordarse los requisitos y actividades de auditoria que involucren comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Debe protegerse el acceso a las herramientas de auditoria del sistema de la información para prevenir cualquier posible mal uso o compromiso.

ANEXO B DE LA NORMA ISO 27001:

PRINCIPIOS OECD Y LA ISO 27001

Los principios dados en las directrices OECD, para los sistemas de seguridad de la información y redes, aplican a todos los niveles de la política y operacional que rigen los sistemas de seguridad de la información y las redes. Esta Norma proporciona un marco al sistema de gestión de seguridad de la información para implementar algunos de los principios de OECD, utilizando el modelo PHVA. El modelo está alineado con las guías y principios de la Organización para la Cooperación y el Desarrollo Económico., OEDC.

PRINCIPIO OECD	PROCESO CORRESPONDIENTE DE LA NORMA DE SISTEMA DE GESTIÓN Y ETAPA PHVA
Toma de conciencia Los participantes deberían estar conscientes de las necesidad de los sistemas de seguridad de la información y redes y de que pueden ellos hacer para incrementar la seguridad.	Esta actividad es parte de la etapa Hacer
Responsabilidad Todos los participantes son responsables de los sistemas y de seguridad de la información y redes.	Esta actividad es parte de la etapa Hacer
Respuesta Los participantes deberían actuar de manera temprana y cooperativa para prevenir, detectar y responder a los incidentes de seguridad.	Esta es una parte de la actividad de seguimiento de la etapa Verificar y una actividad de respuesta de la etapa Actuar. Esto también puede estar cubierto por algunos aspectos de las etapas Planificar y Verificar.
Evaluación del riesgo Los participantes deberían conducir las evaluaciones del riesgo.	Esta actividad es parte de la etapa Planificar Y la reevaluación del riesgo es parte de la etapa.
Diseño e implementación de la seguridad Los participantes deberían incorporar la seguridad como un elemento esencial de los sistemas de información y las redes.	Una vez que la evaluación del riesgo ha sido completada, los controles son seleccionados para el tratamiento de los riesgos como parte de la etapa Planificar. La etapa Hacer entonces cubre la implementación y el uso operacional de éstos controles
Gestión de la seguridad Los participantes deben adoptar un enfoque amplio para la gestión de la seguridad.	La gestión del riesgo es un proceso que incluye la prevención, la detección y la respuesta a los incidentes, el mantenimiento continuo, la revisión y la auditoría. Todos estos aspectos son cubiertos en las etapas Planificar, Hacer, Verificar y Actuar.
Reevaluación Los participantes deben revisar y deben revaluar la seguridad de los sistemas de información y redes, y hacer modificaciones apropiadas a las políticas, prácticas, mediciones y procedimientos de seguridad.	La reevaluación de la seguridad de la información es una parte de la etapa Verificar donde revisiones regulares deberían emprenderse para verificar la efectividad del sistema de gestión de seguridad de la información, y la mejora de la seguridad que es parte de la etapa

ANEXO C DE LA NORMA ISO 27001:
CORRESPONDENCIA CON LA ISO 9001:2000, ISO 14001:2004

La norma esta diseñada que sea compatible con el ISO 9001:2000 y con el ISO 14001:2004.

Norma ISO 27001	ISO 9001 :2000	ISO 14001:2004
0 Introducción 0.1 Generalidades 0.2 Enfoque de procesos 0.3 Compatibilidad con otros sistemas de gestión	0 Introducción 0.1 Generalidades 0.2 Enfoque de procesos 0.3 Relación con ISO 9004 0.4 Compatibilidad con sistemas de Gestión	**Introducción**
1 Objeto y campo de aplicación 1.1 Generalidades 1.2 Aplicación	1 Objeto y campo de aplicación 1.1 Generalidades 1.2 Aplicación	**1 Objeto y campo de aplicación**
2 Referencias normativas	**2 Referencias normativas**	**2 Referencias normativas**
3 Términos y definiciones	**3 Términos y definiciones**	**3 Términos y definiciones**
4 Sistema de Gestión de Seguridad de la Información 4.1 Requisitos generales 4.2 Establecimiento y gestión de SGSI 4.2.1Establecimiento del SGSI 4.2.2Implementación y operación del SGSI 4.2.3Seguimiento y revisión del SGSI 4.2.4 Mantenimiento y mejora del SGSI	4.1 Requisitos generales 8.2.3 Seguimiento y medición de los procesos 8.2.4 Seguimiento y medición del producto	4 Requisitos SGA 4.1 Requisitos generales 4.4 Implementación y operación 4.5.1Seguimiento y medición
4.3 Requisitos de la documentación 4.3.1 Generalidades 4.3.2 Control de los documentos 4.3.3 Control de los registros	4.2 Requisitos de la documentación 4.2.1 Generalidades 4.2.2 Manual de la Calidad 4.2.3 Control de los documentos 4.2.4 Control de los registros	4.4.5Control de la documentación 4.5.4 Control de los registros
5 Responsabilidad de la dirección 5.1 Compromiso de la dirección	5 Responsabilidad de la dirección 5.1 Compromiso de la dirección 5.2 Enfoque al cliente 5.3 Política de la calidad 5.4 Planificación 5.5 Responsabilidad, autoridad y Comunicación	4.2 Política ambiental 4.3 Planificación
5.2 Gestión de los recursos 5.2.1 Provisión de recursos 5.2.2 Formación, toma de toma de conciencia y competencia	6 Gestión de los recursos 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2Competencia, toma de conciencia y formación 6.3 Infraestructura 6.4 Ambiente de trabajo	4.4.2 Competencia, formación y toma de conciencia
6 Auditorías internas del SGSI	8.2.2 Auditorias internas	4.5.5 Auditorias internas
7 Revisión por la dirección del SGSI 7.1 Generalidades 7.2 Revisión de los elementos de entrada 7.3 Revisión de los resultados	5.6 Revisión por la dirección 5.6.1 Generalidades 5.6.2 Revisión de los elementos de entrada 5.6.3 Revisión de los resultados	4.6 Revisión por la dirección
8 Mejora del SGSI 8.1 Mejora continua	8.5 Mejora 8.5.1 Mejora continua	4.5.3 No-conformidad, acción correctiva y acción preventiva
8.2 Acción correctiva	8.5.3 Acciones correctivas	
8.3 Acción preventiva	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles Anexo B Principios OECD y esta norma Anexo C Correspondencia entre la Norma ISO 9001 :2000, ISO 14001:2004y esta Norma	Anexo A Correspondencia entre ISO 9001 :2000 e ISO 14001 :1996	Anexo A Orientaciones para la utilización de esta norma Anexo B Correspondencia entre ISO 14001:2004 e ISO 9001:2000

ANEXO 2

DOCUMENTOS EXIGIDOS POR EL ISO 27001

DOCUMENTOS EXIGIDOS POR EL ISO 27001 :2005

En la sección 4.3, el ISO 27001:2005 plantea que los documentos y registros pueden estar en cualquier forma o medio.

1. Documentar el alcance del modelo
2. Documentar la política de seguridad de información
3. Documentar la metodología de evaluación del riesgo
4. Documentar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables
5. Documentar el inventario de activos y sus propietarios
6. Documentar la tasación de los activos de información
7. Documentar las amenazas y vulnerabilidades de los activos de información
8. Documentar los niveles de riesgo estimados
9. Documentar el proceso de evaluación de opciones de tratamiento del riesgo
10. Documentar el proceso de selección de objetivos de control y controles para el tratamiento del riesgo
11. Documentar la aprobación de la gerencia para los riesgos residuales propuestos
12. Documentar la autorización de la gerencia para implementar y operar el SGSI
13. Documentar el enunciado de aplicabilidad
14. Documentar el plan de tratamiento del riesgo
15. Documentar la asignación del roles y responsabilidades del plan de tratamiento del riesgo
16. Documentar cómo medir la efectividad de los controles o grupos de controles seleccionados, y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control, para producir resultados comparables y reproducibles
17. Documentar la implementación de los programas de capacitación y conocimiento
18. Documentar cómo detectar prontamente los errores en los resultados de procesamiento

19. Documentar cómo detectar prontamente los incidentes y violaciones de seguridad fallidos y exitosos
20. Documentar cómo la gerencia determina si las actividades de seguridad delegadas a las personas, e implementadas mediante la tecnología de información, se están realizando como se esperaba
21. Documentar cómo se detectan los eventos de seguridad, para evitar los incidentes de seguridad mediante el uso de indicadores
22. Documentar el procedimiento para verificar si las acciones tomadas para resolver una violación de seguridad han sido efectivas
23. Documentar el procedimiento para medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad
24. Documento para revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado
25. Documento para actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión
26. Elaborar el registro de las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI
27. Procedimientos y controles de soporte
28. Procedimientos para describir cómo medir la efectividad de los controles
29. Procedimiento para el control de documentos
30. Mantener registros del desempeño del proceso y todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI
31. Establecimiento de objetivos y planes del SGSI
32. Documentar el establecimiento de roles y responsabilidades para la seguridad de información.
33. Registros de educación, capacitación, capacidades, experiencias y calificaciones
34. Definir en un procedimiento documentado las responsabilidades, los requerimientos para la planeación y realización de las auditorías y para el reporte de resultados y mantenimiento de registros .

35. Registros de las revisiones gerenciales
36. Procedimiento documentado para el manejo de la acción correctiva
37. Procedimiento documentado para el manejo de la acción preventiva
38. Documentar las responsabilidades por la seguridad de información de las personas en la empresa
39. Documentación de la política del proceso disciplinario en la empresa
40. Procedimiento para reportar eventos de seguridad
41. Documentar los requerimientos legales de los sistemas de información.
42. Procedimiento para validar el insumo de data en las aplicaciones, para asegurar que la data sea correcta y apropiada
43. Procedimiento para incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información, a través de errores de procesamiento o actos deliberado
44. Procedimiento para identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones. En el procedimiento se pueden incluir la identificación y la implementación de los controles apropiados
45. Procedimiento para validar el resultado de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias
46. Procedimiento para obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso
47. Procedimiento para evaluar la exposición de la organización ante las vulnerabilidades técnicas
48. Procedimiento para tomar las medidas apropiadas para tratar el riesgo asociado con vulnerabilidades técnicas
49. Documentar las responsabilidades para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información
50. Procedimiento documentado para crear el mecanismo para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información
51. Procedimiento documentado para recolectar, mantener y presentar evidencias para cumplir las reglas de evidencia establecidas en las

jurisdicciones relevantes, cuando la acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de la información, involucra una acción legal (civil o criminal)

52. Documentar el proceso de análisis y evaluación del riesgo para el diseño de un plan de continuidad del negocio
53. Documentar un Business Impact Analysis en el cual se identifiquen los: procesos esenciales, los requerimientos de recursos y los tiempos de recuperación
54. Documentar los escenarios de amenazas para la continuidad del negocio
55. Documentar las estrategias de continuidad para el negocio
56. Documentar los planes de reanudación de operaciones para la continuidad del negocio
57. Procedimiento documentado para los ensayos orientados a probar los planes de continuidad del negocio
58. Procedimiento documentado para efectuar el mantenimiento a los planes de continuidad del negocio
59. Documentar los controles para la identificación, el almacenaje, la protección, la recuperación, el tiempo de retención y la disposición de los registros
60. Evidencia documentada que asegure que los procedimientos de seguridad de la información respaldan los requerimientos comerciales
61. Evidencia documentada donde se identifican y se tratan los requerimientos legales y reguladores y las obligaciones de seguridad contractuales
62. Evidencia documentada de mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados
63. Evidencia documentada de mejorar el SGSI donde se requiera
64. Evidencia documentada donde se determinan las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI
65. Evidencia documentada donde se proporciona la capacitación o se realizan otras acciones para satisfacer estas necesidades
66. Evidencia documentada donde se evalúa la efectividad de las acciones tomadas

67. Evidencia documentada donde las actividades de seguimiento de las auditorias internas incluyen la verificación de las acciones tomadas y el reporte de los resultados de verificación

ANEXO 3

ESTADÍSTICAS DE LAS COOPERATIVAS DE AHORRO Y CRÉDITO ECUATORIANAS

1. ESTADISTICAS DE COOPERATIVAS DE AHORRO Y CRÉDITO EN EL CONTEXTO NACIONAL

A) EVOLUCIÓN SOCIO ECONÓMICA DE LAS COOPERATIVAS DE AHORRO Y CRÉDTIO

En las siguientes figuras, puede verse como han crecido los fondos, los activos, el número de socios, el número de empleados, indicando que es un sector en total crecimiento financiero, lo cual no se refleja de la misma manera en el desarrollo regional de sus actividades.

Todos estos datos estadísticos fueron extraídos de la FECOAC y elaborados por el Ing. Aníbal Mantilla

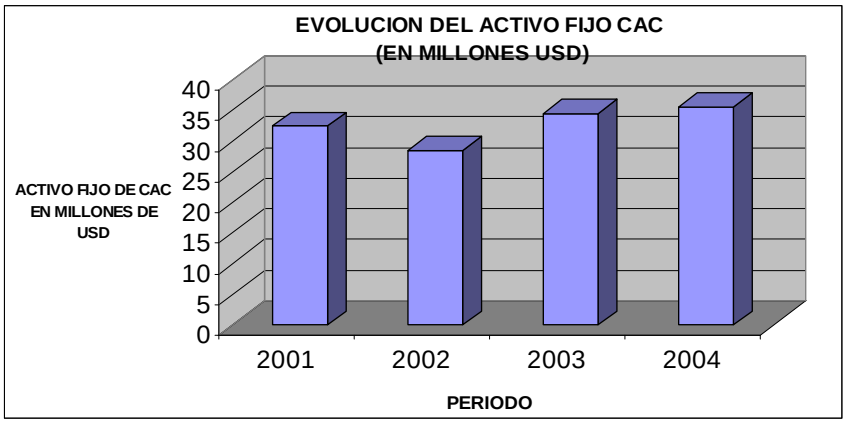

FIGURA 1del Anexo 3 Evolución del activo fijo en las CAC

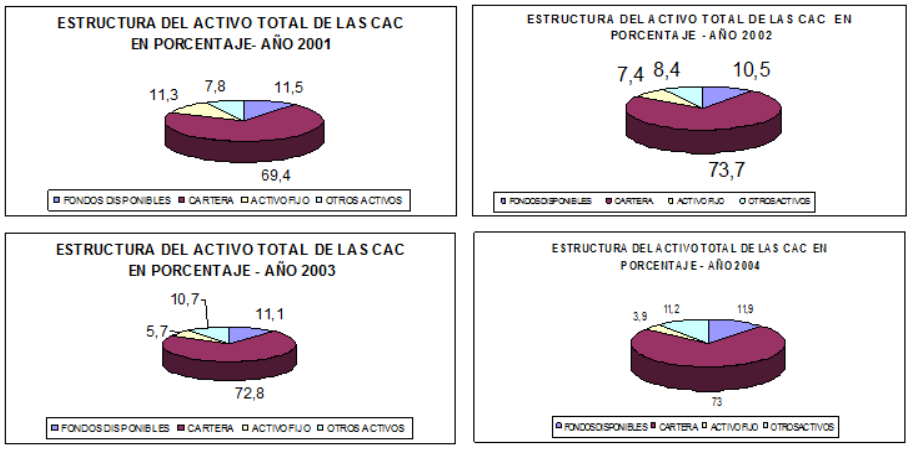

FIGURA 2 del Anexo 3 Estructura del activo total de las CAC - Del año 2001 al año 2004

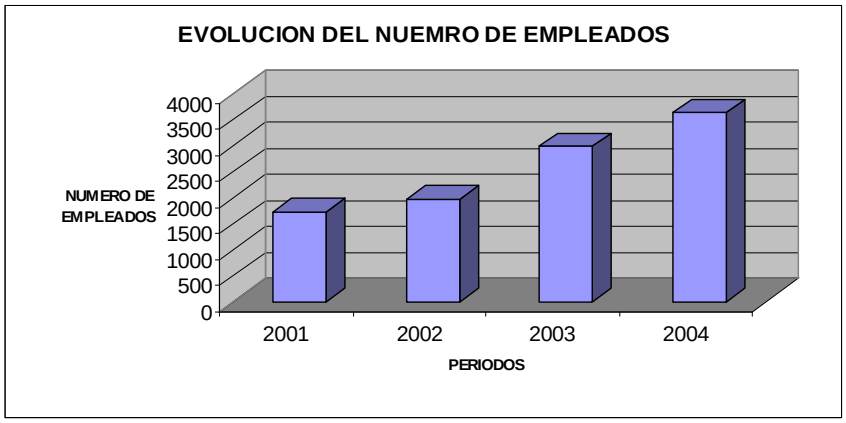

FIGURA 3 del Anexo 3 Evolución del número de empleados

B) COMPARACIÓN ENTRE COOPERATIVAS DE AHORRO Y CRÉDTIO CON BANCOS PRIVADOS

La expansión de las CAC ha sido dinámica en esos años, evidenciando en algunos caos, una tasa de crecimiento aun mayor que de los bancos. Esto hace que las Cooperativas de ahorro y crédito, tengan cada vez una mayor relevancia en el mercado financiero nacional.

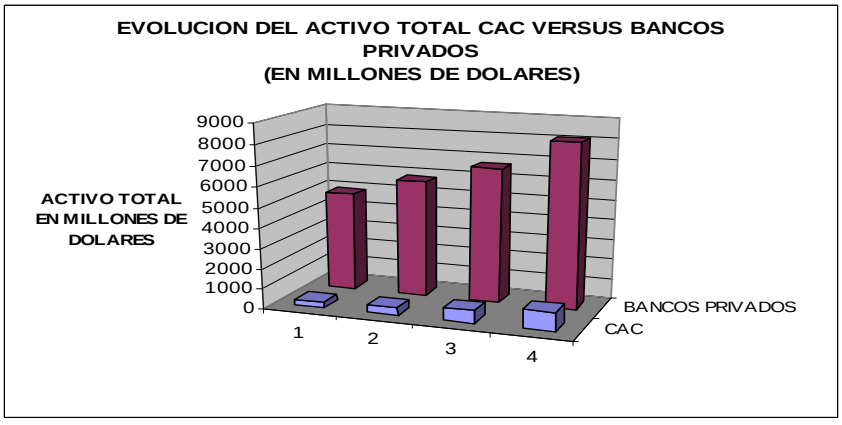

FIGURA 4 **del Anexo 3** Evolución del activo total CAC versus bancos privados

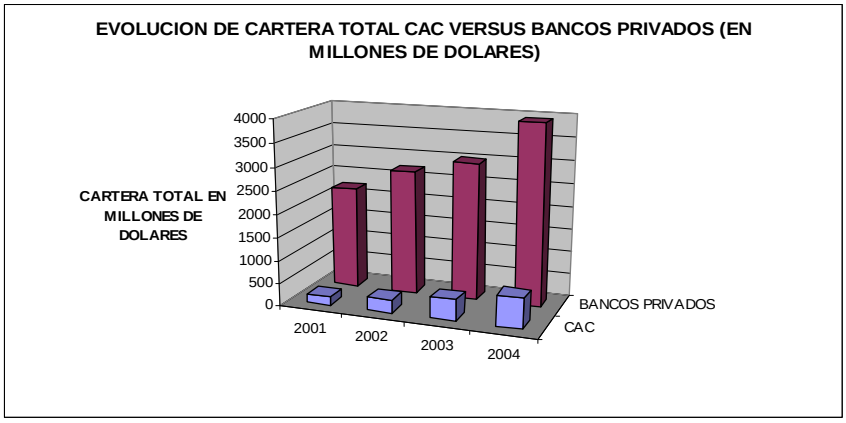

FIGURA 5 **del Anexo 3** Evolución de cartera total CAC versus bancos privados

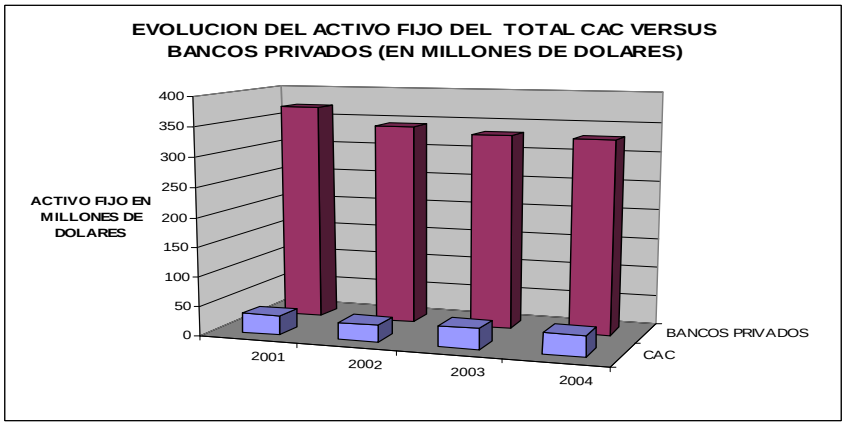

FIGURA 6 **del Anexo 3** Evolución del activo fijo del total CAC versus bancos privados

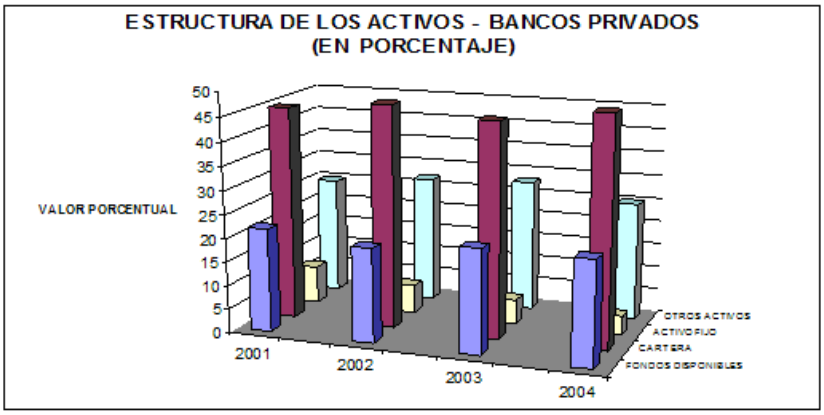

FIGURA 7 del Anexo 3 Estructura de los activos - CAC y Bancos Privados

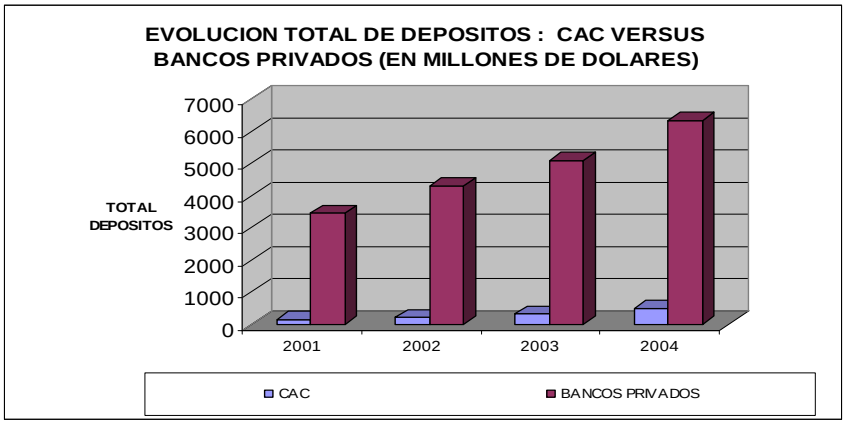

FIGURA 8 del Anexo 3 Evolución total de depósitos: CAC versus bancos privados

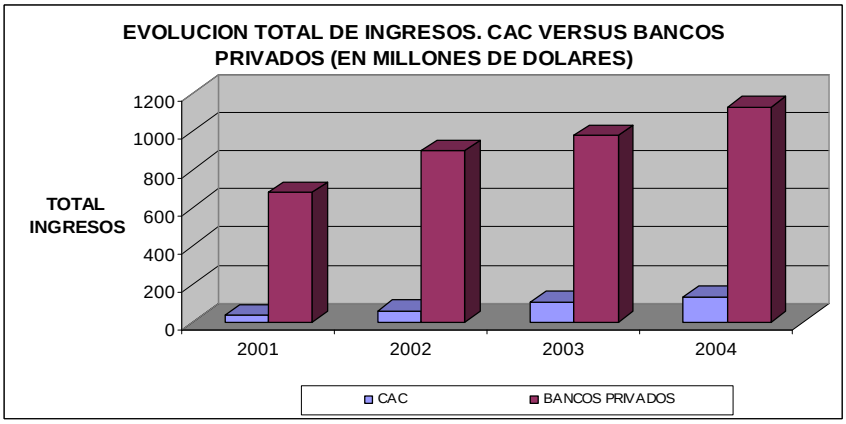

FIGURA 9 del Anexo 3 Evolución total de ingresos. CAC versus bancos privados

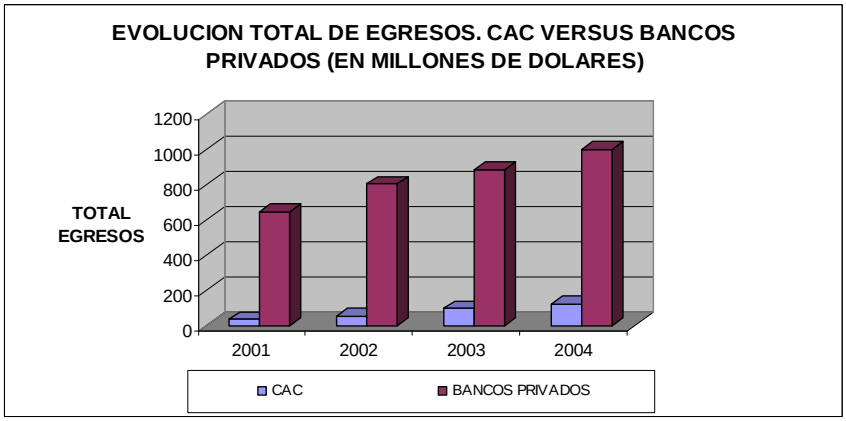

FIGURA 10 del Anexo 3 Evolución total de egresos. CAC versus bancos privados

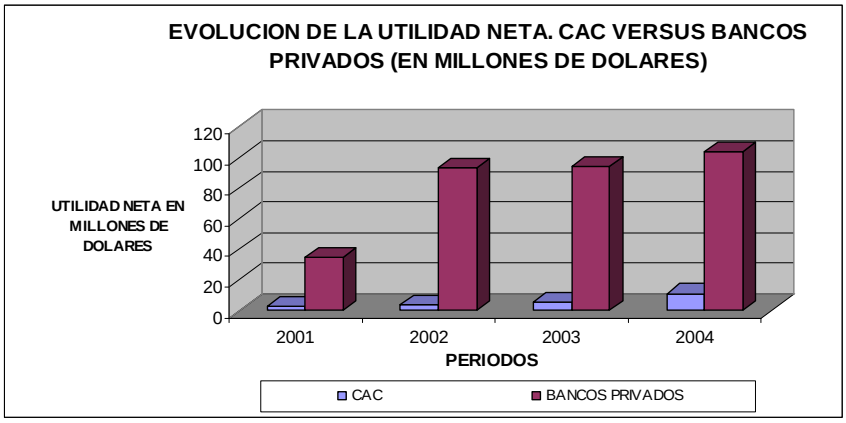

FIGURA 11 del Anexo 3 Evolución de la utilidad neta. CAC versus bancos privados

C) PARTICIPACIÓN REGIONAL DE LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Las Cooperativas de Ahorro y Crédito han tenido un desenvolvimiento mucho mas amplio en la Sierra que en la Costa; en el Oriente, el desarrollo aun es mínimo. Esto puede apreciarse en varios indicadores.

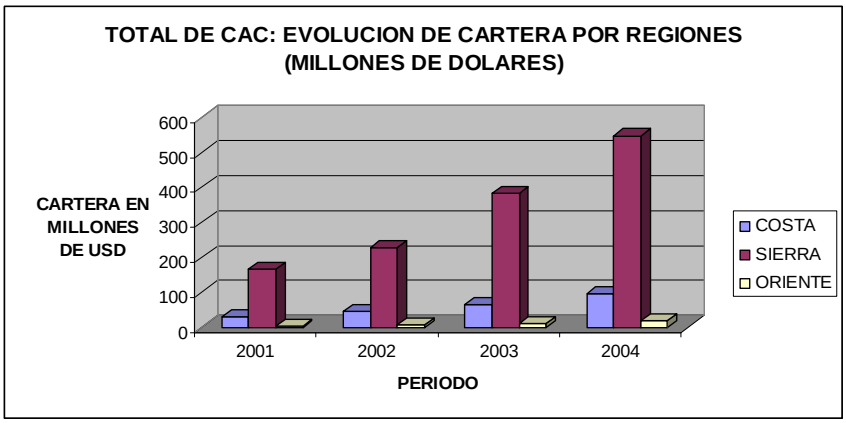

FIGURA 12 del Anexo 3 Total de CAC: evolución de cartera por regiones

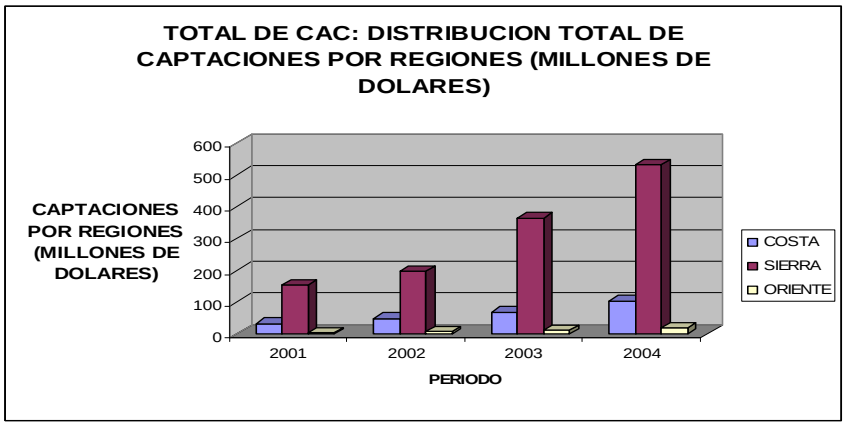

FIGURA 13 del Anexo 3 Total de CAC: distribución total de captaciones por regiones

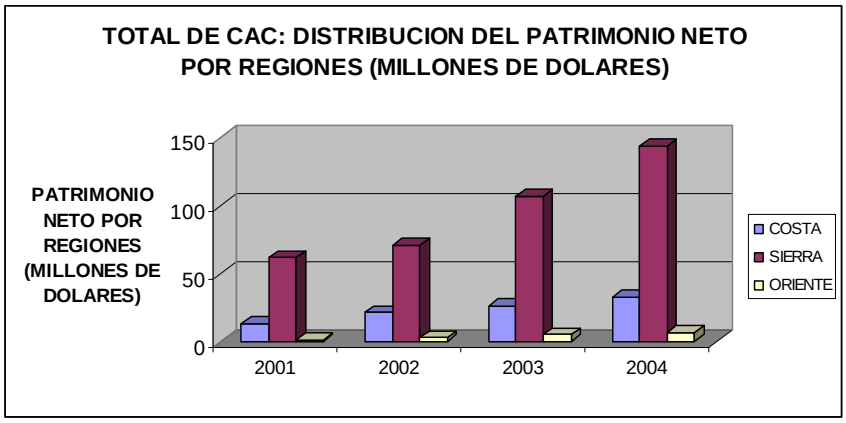

FIGURA 14 del Anexo 3 Total de CAC: distribución del patrimonio neto por regiones

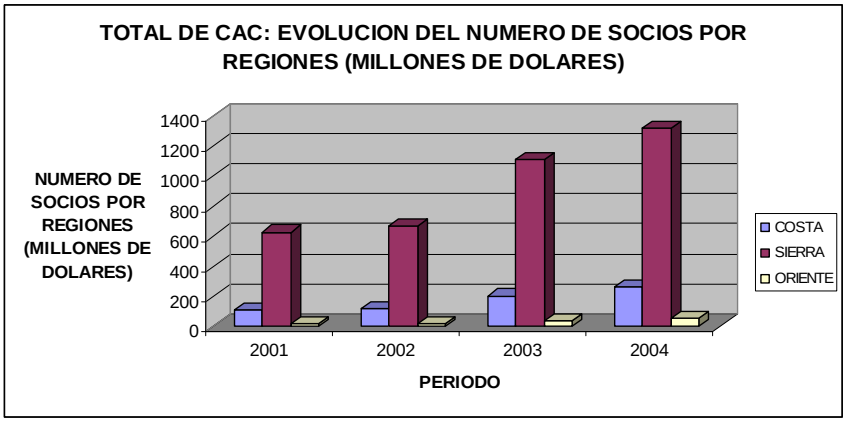

FIGURA 15 del Anexo 3 Total de CAC: evolución del número de socios por regiones

2. ESTADISTICAS DE LAS CAC EN EL AMBITO LATINIAMERICANO

País	Instituciones			Activos en MN (en mill.)	Moneda	Equivalente En USD (mill)
	tipo	total	De las coop`s: Supervisadas por la SB/BC			
Bolivia	CACs Abiertas	23	23	2974	Bolivarianos	394
	CACs Cerrada	97	0	743		99
	Bancos	12		40983		5430
Brasil	Coop. De Crédito y Coop. Centrales	1460	1460	38008	Reales	21467
	Bancos Coop.	22		10554		5961
	Bancos	152		2346666		1325426
Ecuador	CACs (DECOOP)[1]	1300	39	300	USD	300
	CACs supervisadas (incl.2do piso)	39		1343		1343
	Bancos	24		13735		13735
El salvador	CACs supervisadas	7	6	740	USD	740
	CACs no supervisadas	80		160		160
	Bancos Trab. Y Cajas no supervisadas	9		469		469
		51		13058		13058
Nicaragua	CACs *	180	0	225	Córdobas	12
	Bancos	7		60316		3191
Panamá	CACs	168	0	507	Balboa/USD	507
	Bancos	44		56325		56325
Paraguay	CACs	779	0	7194093	Guaraní	1515
	Bancos	14		21861093		4602
Perú	CACs	168	168	2272	Nuevos Soles	758
	Bancos	13		108349		36164
Venezuela	CACs*	1755	0	251000	Bolívares	251
	Bancos	54		215864494		2150846

* No hay datos exactos

\- Dato no disponible

TABLA 1 del Anexo 3 Monto de participación de CAC y Bancos en América Latina al 2007[56]
ELABORADO POR Ing. Mantilla Aníbal

[56] Fuente. www.dgrv.org

País	Tipo de Instituciones	Número de instituciones		Activos (USD Millones)		Participación mercado (%)	
		1998	2007	1998	2007	1998	2007
Bolivia	CACs supervisadas	17	23	256	394	3,9	6,7
	CACs no supervisadas	103	97	-	99	-	1,7
Brasil	Coop. De Crédito	1198	1460	2358	21,467	0,5	1,4
	Bancos Coop.	2	2	283	5961	0,1	0,4
Colombia	Bancos cooperativos	3	0	1707	-	3,6	-
	Coop. Financieras	44	6	934	1084	2,0	1,3
	CACs	451	209	1176	2326	2,5	2,8
	Organismo grado superior	1	1		45	-	0,1
Costa Rica	CACs supervisadas	36	30	502	1510	3,3	7,4
	CACs no supervisadas	74	35	89	151	0,6	0,7
	Bancos cooperativos	2	-	18		1,0	
Ecuador	CACs supervisadas	26	40	75	1343	0,8	8,3
	CACs no supervisadas		1300		300		2,0
Nicaragua*	CACs	-	180	191	225	-	0,4
Panamá *	CACs	187	168	359	507	1,0	1,0
Paraguay	CACs		779	749	1515	7,0	22,9
Perú	CACs	198	168	244	759	1,2	1,9
República Dominicana*	CACs	71	18	43	329	0,8	2,5
Venezuela*	CACs	45	1755		251		0,1

- Dato no disponible

* No se supervisa ninguna cooperativa

TABLA 2 del Anexo 3 Evolución financiera de CAC y Bancos en América Latina[57]
ELABORADO POR Ing. Mantilla Aníbal

[57] Fuente. www.dgrv.org

ANEXO 4

CUESTIONARIOS PREPARADOS PARA DETERMINAR LA SITUACIÓN DE LA GESTION DE LA SEGURIDAD INFORMÁTICA EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO

CUESTIONARIO 1: **APLICACIONES**

NOTA:	En las preguntas cuya respuesta sea afirmativa, la valoración de la escala planteada, cualitativamente corresponde a los siguientes parámetros:			
1	2	3	4	5
Casi nunca	**Regularmente**	**Bueno Frecuentemente**	**Muy Bueno Casi Siempre**	**Excelente Siempre**

Nº	**Preguntas**	**No**	**Si**				
			1	**2**	**3**	**4**	**5**
1	**POLITICAS Y PROCEDIMIENTOS**						
	Existen manuales y procedimientos que documentan la aplicación?						
	Existen diagramas de flujo de datos que documenten las operaciones que se describan?						
2	**ESTANDARES DE DESARROLLO Y PRODUCCIÓN**						
	Se evalúa el procedimiento de actualización de los estándares?						
	Los mantenimientos efectuados a la aplicación se ajustan a los estándares de desarrollo?						
	Se cumplen las políticas de backups?						
	Se verifica que todos los procesos que se corren queden registrados?						
	Los procesos de almacenamiento y restauración de datos cumplen con los estándares de producción?						
3	**DATOS DE ENTRADA** Se verifica la consistencia e integridad en la información en los siguientes aspectos?						
	Legibilidad de la información						
	Manejo de errores en el documento fuente						
	Políticas de retención de los documentos						
	Control de los documentos confidenciales						
	Almacenamiento de los documentos no diligenciados						
	Sistema de control sobre documento digitado						
	Sistema de control de lotes o grupos de documentos procesados						
	Conservación del consecutivo del documento						
4	**PROCEDIMIENTO Y ACTUALIZACIÓN DE INFORMACIÓN**						
	Se ejecutan pruebas a los programas correspondientes a la aplicación?						
	Se verifica la consistencia de la información (informes o reportes por pantalla y listados) ?						
	Se analiza los programas fuente para los programas más críticos?						
	Existen consistencia entre los campos de los archivos con la información que debe ser almacenada en ellos?						
	Utiliza alguna metodología para la actualización de los archivos?						
	Se realizan cambios y mantenimiento de los programas verificando las debidas autorizaciones ?						

5	**INFORMES DE COMPUTADOR**						
	Se utiliza una matriz para revisar la estructura de los informes?						
	Se analiza el origen y destino final de los informes?						
	Se evalúa el sistema de archivo y retención de los informes del computador?						
	Se evalúa la información de salida a la luz del sistema de información requerido por la gerencia?						
6	**DOCUMENTACIÓN**						
	Se documentan las modificaciones que evidencian los programas?						
7	**SEGURIDAD**						
	Se evalúa el sistema de seguridad lógico a través del archivo de seguridad y los archivos de usuarios con privilegios?						
	Se analiza el periodo de modificaciones de los password propios de la aplicación?						
	Se verifica en el log del sistema de los accesos que observan los programas y archivos más críticos?						
8	**PROCEDIMIENTOS DE RESPALADO**						
	Existe un plan de contingencia de las aplicación y el conocimiento del mismo por parte de los usuarios?						
	Se evalúa el sistema de backups utilizado para los archivos de datos?						
9	**CAPACITACION Y SOPORTE A USUARIOS**						
	Se determina el grado de conocimiento que tienen los usuarios para el manejo de los módulos propios de la aplicación?						
	Se revisan los procedimientos de capacitación que son utilizados para la instrucción de los usuarios?						
	Se analizan las respuestas que tienen los usuarios sobre los problemas tanto de hardware como de programas?						

CUESTIONARIO 2: **CENTRO DE CÓMPUTO / CAC : COOPERATIVA DE AHORRO Y CREDITO**

NOTA:	En las preguntas cuya respuesta sea afirmativa, la valoración de la escala planteada, cualitativamente corresponde a los siguientes parámetros:			
1	2	3	4	5
Casi nunca	**Regularmente**	**Bueno Frecuentemente**	**Muy Bueno Casi Siempre**	**Excelente Siempre**

Nº	**Preguntas**	**No**	**Si**				
			1	**2**	**3**	**4**	**5**
1	**PREGUNTAS CLAVE**						
	Tienen procedimientos escritos que se manejan. Manuales por aplicación(sistemas y operación) ?						
	Cual es el diagrama de red de la cooperativa?						
	Cuantos servidores tienen?						
	Cual es la ubicación de los servidores?						
	Cual es el numero de terminales conectadas?						
	Cual es el numero de usuarios conectados al servidor?						
	Cuales son los protocolos y servicios instalados ?						
	Reciben y/o envían archivos a entidades externas?						
	Cuales son sus principales proveedores de tecnología?						
	Hay sistemas de seguridad electrónica instalados?						
	Actualmente se tiene auditoria del sistema?						
	Hay planes de contingencia para el área informática?						
	Hay proyectos futuros?						

2	**CUIDADO DE LAS INSTALACIONES**						
	Ubicación						
	Es adecuada la ubicación del centro de computo?						
	Es adecuada la ubicación de la estantería?						
	Es adecuada la ubicación de la luz?						
	Existe un procedimiento claro de limpieza y aseo para los computadores y el centro de cómputo?						
	Electricidad						
	Tienen reguladores de voltaje?						
	Hay corriente regulada identificada?						
	Existen pruebas de funcionamiento de la UPS?						
	Existe plano eléctrico de la CAC?						
	Se cuenta con planta eléctrica? Se tienen procedimientos claros para su uso y mantenimiento?						
	Se hace revisión de los circuitos eléctricos de la instalación?						
	Aire acondicionado						
	Hay sistema de aire acondicionado?						
	Hay sistema de reserva energética para el aire acondicionado?						
	Es suficiente para el área del centro de computo? Controla la humedad del aire?						
	Se tiene sistema redundante de aire acondicionado?						
	Protección contra incendios						
	Tienen sistema de protección contra incendios?						
	Se hizo capacitación al personal del área para el manejo de los extintores y se han probado?						
	Tienen procedimientos de emergencia?						
	Existen normas o actividades ante un desastre?						
	Existen estrategias para la evacuación?						
	Seguros						
	Están asegurados, contra qué, qué está protegido, en qué medida?						
	Es seguro el sitio de ubicación del bien asegurado?						
	Se evalúa los procedimientos para el manejo de los seguros?						
	Se revisa el inventario de equipos de cómputo de la cooperativa y se notifica a la aseguradora?						
	Hardware						
	Están asegurados los PC?						
	Se verifica sobre qué están asegurados los PC?						
	Software						
	Tiene licencias?						
	Pólizas de manejo						
	Hay pólizas de manejo?						
	Cuál es su cobertura?						
	Quiénes están incluidos?						

3	**OPERACIÓN DE LOS SERVIDORES**						
	Registro de operaciones						
	Evalúa el manejo de bitácoras en el centro de cómputo.						
	Cada cuánto se revisan los registros?						
	Procedimientos del operador						
	Tienen manual de funciones?						
	Sus actividades están basadas en normas claras?						
	Hay procedimientos para Prender el Servidor?						
	Hay procedimientos para Apagar el Servidor?						
	Hay procedimientos para Otorgar permisos en el sistema?						
	Programación de actividades						
	Son programadas las actividades del operador?						
	Manejan cronogramas, planes de trabajo y/o acuerdos de servicio?						
	Mantenimiento de archivos maestros						
	Se chequea o revisa las tablas principales del sistema contable y las aplicaciones de misión crítica?						
	Se evalúa la frecuencia de depuración de los archivos maestros?						
	Se revisar los procedimientos de depuración de archivos maestros?						
4	**CONTROL DE ENTRADAS Y SALIDAS**						
	Entradas						
	Que control hay sobre el documento que se recibe?						
	Salidas						
	Existen hoja de ruta de los informes?						
	Se comparan los informes contra los documentos de entrada?						
5	**SEGURIDAD EN INSTALACIONES**						
	Administración general de la seguridad						
	Considera a los sistemas de vigilancia adecuados?						
	Hay garantías de seguridad del sitio donde está ubicado el centro de cómputo?						
	Seguridad externa						
	Los controles de acceso son adecuados?						
	Seguridad interna						
	Son independientes las áreas de trabajo?						
	Los computadores están ubicados en sitios seguros?						
	Se protegen los equipos con cobertores plásticos?						
	Hay canaletas, iluminación y ergonomía en el área?						
6	**ORGANIZACIÓN Y PERSONAL**						
	Organización y personal						
	Cuáles son los criterios de administración?						
	Cuáles son los periodos vacacionales?						
	Hay rotación de analistas en su cargo?						
	Cuáles son las estrategias de promoción?						
	Cuáles son los parámetros de ascenso establecidos?						
	Segregación de funciones						
	Se detecta concentración de funciones en algún empleado?						
	Existen criterios en el área para difundir o multiplicar conocimientos?						
	La capacitación esta relacionada con los proyectos del área?						

7	**PLANES DE CONTINGENCIA**						
	Creación del plan						
	Existen planes de contingencias?						
	Están documentados?						
	Está establecido el personal que participa en la definición del plan de contingencias. ?						
	Hardware						
	Tienen equipo de soporte?						
	Tienen acuerdos con otras compañías?						
	Tienen acuerdos con los proveedores?						
	Tienen dispositivos claves?						
	Software						
	Tienen procedimientos manuales que garanticen la continuidad del servicio?						
	Tienen previsto personal para el plan de contingencias?						
	Existe matriz de sustitutos - Quien reemplaza a quien?						
	Se realiza difusión del plan?						
	Hay planes de difusión y entrenamiento?						
	Se realizan pruebas de simulación (ensayos)?						

CUESTIONARIO 3: NUEVOS DESARROLLOS

NOTA:	En las preguntas cuya respuesta sea afirmativa, la valoración de la escala planteada, cualitativamente corresponde a los siguientes parámetros:			
1	2	3	4	5
Casi nunca	**Regularmente**	**Bueno Frecuentemente**	**Muy Bueno Casi Siempre**	**Excelente Siempre**

Nº	**Preguntas**	**No**	**Si**				
			1	**2**	**3**	**4**	**5**
1	**PLANEACIÓN Y ANÁLISIS DEL PROYECTO**						
	Se encuentra establecido el objetivo del proyecto?						
	Se encuentra establecido el personal involucrado?						
	Se encuentra establecido el cronograma de trabajo?						
	Se encuentra establecido el presupuesto?						
	Se encuentra establecido el equipo y aplicaciones asociados?						
	Se encuentra establecida la participación y aceptación por parte del usuario?						
	Como se aplica la metodología de desarrollo?						
2	**EN LA ETAPA DEL DISEÑO**						
	Se ha revisado el cumplimiento de normas legales, políticas, procedimientos, normas contables y tributarias?						
	Se han considerado períodos de retención de archivos, backup, procedimientos de recuperación?						
	Se ha revisado el plan de pruebas y/o conversión de programas.						
	Se ha revisado el plan de migración de datos?						
	Se ha revisado la matriz de acceso a la aplicación?						
	Se ha propuesto tablas-auditor para datos críticos, previa discusión con el usuario?						
	Se ha sugerido cifras de control para los datos?						
	El grupo de diseño realiza reportes y consultas de control?						
3	**CONSTRUCCIÓN Y PRUEBAS**						
	Se han implantado controles?						
	Se cumple con la documentación referida en los estándares?						
	Se ha revisado el cumplimiento del presupuesto?						
	El usuario a participado y ha aprobado las pruebas de aplicaciones y pruebas de conversión y/o migración de programas y datos?						
	La auditoría interna ha participado en pruebas a programas?						
	Se han cumplido los planes de entrenamiento?						
	Existen controles automáticos?						
	Se ha revisado el plan de contingencias de la aplicación?						
4	**EN CONVERSIÓN E INSTALACIÓN**						
	Se realiza revisiones al proceso de conversión?						
	Se realiza revisiones finales de los procedimientos. ?						
	Se verificar la creación de controles recomendados?						
	Se verificar la completa aceptación del usuario?						
	Se realizan pruebas completas antes de instalarse en producción?						
	Se informa sobre el cumplimiento de los presupuestos iniciales?						

CUESTIONARIO 4: MICROCOMPUTADORES Y REDES LAN

CAC : COOPERATIVA DE AHORRO Y CREDITO

NOTA:	En las preguntas cuya respuesta sea afirmativa, la valoración de la escala planteada, cualitativamente corresponde a los siguientes parámetros:			
1	2	3	4	5
Casi nunca	**Regularmente**	**Bueno Frecuentemente**	**Muy Bueno Casi Siempre**	**Excelente Siempre**

Nº	**Preguntas**	**No**	**Si**				
			1	**2**	**3**	**4**	**5**
1	**POLÍTICAS ADMINISTRATIVAS**						
	Existe una política documentada para la adquisición de microcomputadores?						
	Existe una política documentada para el uso de microcomputadores?						
	Se mantiene una lista actualizada de todos los usuarios de microcomputadores?						
	Existe un grupo de trabajo o comité para coordinar los proyectos desarrollados en micros?						
	Se evalúan los medios de difusión periódica de nuevos desarrollos?						
2	**ADQUISICIÓN DE HARDWARE**						
	Existe un respaldo, con análisis de costo-beneficio, de las solicitudes de compra de equipos por parte del usuario?						
	Qué documentación existe para el hardware?						
	Se hace una planeación del sitio en que se instala los equipos para garantizar:						
	Protección antimagnética?						
	Servicio eléctrico regulado?						
	Conexión a la red?						
	Seguridad física?						
	La memoria RAM del servidor, frente al número de usuarios que posee es adecuada?						
	La capacidad del disco duro del servidor, con relación al número de usuarios es adecuada?						
	Hay un registro de uso de microcomputadores para cada área usuaria?						
3	**ADQUISICIÓN DE SOFTWARE**						
	Existen políticas para uso y adquisición de software. ?						
	Tienen una lista de las versiones de paquetes en uso, en los diferentes micros, y se verifican que sean copias originales y licenciadas por la CAC ?						
	Existen alternativas manuales, para llevar a cabo las tareas que actualmente se procesan en micros?						
	Existe un plan general sobre los desarrollos propuestos por los usuarios?						

4	**DOCUMENTACIÓN**						
	Existe un catálogo actualizado del software aplicativo, desarrollado y adquirido por la CAC?						
	Existe una metodología de desarrollo para micros?						
	Existe documentación de aplicaciones desarrolladas en microcomputadores?						
5	**COMUNICACIONES** Tomando como base los 7 niveles de red OSI:						
	Nivel 1. Físico						
	Se evalúa el plano de la red, con base en los siguientes aspectos? :						
	Dispositivos adjuntos						
	Diagramas del cableado						
	Documentación						
	Actualización						
	Se tiene procedimientos para mantenimiento periódico?						
	Se tiene soporte de proveedores alternos, si el proveedor falla?						
	Existen procedimientos para recuperación de fallas?						
	Nivel 2: De enlace de datos						
	Existe un monitoreo de transmisiones continuo ?						
	Existen tasas de estadísticas de errores ?						
	Se investigan altas tasas de error?						
	Nivel 3: De redes						
	Verifican las estrategias para monitoreo de las tasas de tráfico de la red?						
	Existen tablas de ruta de la red?						
	Se revisa las estadísticas de tráfico?						
	En que medida aprovecha las herramientas que provee el sistema operativo (Monitor de eventos, Monitor del sistema, Optimización del desempeño, Uso de alertas, Manejo de espacio en disco, Servicios instalados del servidor?						
	Se verifica la conectividad a Internet en cuanto a:						
	-Controles de acceso a Internet. ?						
	-Firewall?						
	-Proxy ?						
	-DNS ?						
	-DHCP?						
	-Uso de correo electrónico, administración del servicio, definición de usuarios etc, tamaños de adjuntos?						
	-Administración del Antivirus?						
	Nivel 4: De transporte						
	Hay procedimientos actuales para la red después de:						
	La instalación inicial?						
	Falla o modificación?						
	Operación diaria?						
	Se cuenta con los medios para detectar errores y corregirlos, en transmisiones fin a fin :						
	Con monitoreo ?						
	Con estadísticas?						
	Con investigación de alzas?						
	Existe un registro automático diario o huella de Auditoría para los cambios a las tablas?						
	Existen backups de las tablas del sistema operativo?						

	Nivel 5: De sesión **PARA CADA ESTACIÓN DE TRABAJO Y EL SERVIDOR DE RED:**						
	Se verifica si se puede acceder el sistema operativo?						
	Se verifica si las claves de acceso son:						
	Usadas adecuadamente?						
	Compartidas?						
	Cambiadas periódicamente?						
	Cambiadas cuando el personal es transferido?						
	Requeridas para todas las estaciones de la red?						
	Requeridas por el sistema operacional de la red?						
	Existe un procedimiento para recuperación de claves de acceso?						
	Existe un procedimiento de control para claves de acceso, a la red de microcomputadores?						
	Se controla a través del sistema operativo de la red:						
	Las actividades realizadas en cada estación de trabajo?						
	Las violaciones de acceso realizadas por estación de trabajo?						
	Los controles de acceso para tablas de seguridad son adecuados?						
	Las tablas de seguridad son respaldadas frecuentemente y almacenadas fuera del sistema?						
	Existe una huella de Auditoría o un registro automático diario?						
	Nivel 6: De presentación						
	Existe criptografía por software ?						
	Existe criptografía por hardware?						
	Cuantas claves se usan?						
	Suministran seguridad apropiada?						
	Las claves son cambiadas y con qué frecuencia?						
	Nivel 7: De aplicación						
	Se establece si las aplicaciones son individualmente seguras?						
	Existen limitaciones de clase de transacción, para determinados usuarios?						
	Existen restricciones establecidas para cada nivel de acceso diferente?						
	Existe algún seguimiento para actividades inválidas?						
	El analista de la red es informado de la violación; y éste avisa a los usuarios involucrados?						
	Se usan archivos para pistas de Auditoría, disco o servidor para respaldo?						
	Existe un procedimiento para ayudar a los usuarios en la recuperación?						
	Existe alguien más responsable para el respaldo del servidor?						
	Existe un procedimiento definido para backups?						
	Se revisa el software, antes de instalarse definitivamente en las áreas de Producción?						
	Son adecuados los sitios de almacenamiento de la documentación sensible, cuando no está en uso?						
	Son usadas versiones de red (actualizadas) de programas de aplicación?						
	Se determina si hay violación de área entre los usuarios?						

6	**ENTRENAMIENTO Y SOPORTE A USUARIOS**						
	Existe un programa de capacitación definido, para los usuarios en hardware y software?						
	Existe material para auto estudio?						
	Se incluye en la capacitación a los usuarios, la difusión de normas y políticas establecidas por la empresa con respecto a los micros?						
	Se analizan las necesidades de capacitación de los usuarios?						
7	**MANTENIMIENTO**						
	Se evalúan los contratos de mantenimiento actuales.						
	Existe un programa para el mantenimiento preventivo y si existe, que conozcan los usuarios?						
	Existe un control que relacione los números de serie de las partes de los equipos que son llevados a mantenimiento a otras empresas?						
	Existe un procedimiento a seguir en caso de daño de equipo y es conocido por los usuarios?						
	Hay instrucciones al personal de limpieza, cuando éste se encuentra en un área de micros?						
	Se protegen con forros plásticos el teclado, la pantalla y CPU?						
	Se revisa el tipo de mantenimiento?						
	Existe un programa de las actividades del mantenimiento preventivo del contratista?						
8	**SEGUROS**						
	Tienen pólizas de seguros que amparen los microcomputadores?						
	Se verifica si las estipulaciones de las cláusulas corresponden con las características físicas de los micros (tarjetas, velocidad, valor, etc.) ?						
	Se revisan los procedimientos de reporte a la aseguradora con respecto a los eventos ocurridos con los equipos?						
9	**SEGURIDAD**						
	Seguridad del hardware						
	Se tiene un registro de todos los números seriales de los equipos periféricos y sus partes más relevantes (tarjetas especiales) ?						
	Se hacen comparaciones periódicas entre el inventario físico y el registro?						
	Están los microcomputadores ubicados en áreas de tráfico limitado?						
	Se puede determinar cuando un equipo ha sido destapado sin autorización?						
	Seguridad del software						
	Se tiene establecido el procedimiento para autorización de nuevos usuarios?						
	Se tienen identificados los archivos de datos confidenciales?						
	Se registra el acceso y uso de los equipos?						
	Se tienen identificados, para cada aplicación, los archivos que deben mantenerse residentes en el disco duro?						

10	**RESPALDO DE EQUIPOS Y PERIFÉRICOS**						
	Existen procedimientos definidos para el uso de otros equipos, en caso de fallas prolongadas?						
	Se tienen procedimientos manuales documentados, en caso de que el procedimiento no pueda ser realizado en el microcomputador?						
	Se tienen identificadas las prioridades a seguir, en caso de daños en los equipos?						
	Se utilizan programas de utilidad aprobados, para recuperar datos en medios destruidos?						

CUESTIONARIO 5: SEGURIDAD FISICA (CONTROL DE ACCESO)

CAC : COOPERATIVA DE AHORRO Y CREDITO / CPD: CENTRO DE PROCESAMIENTO DE DATOS

NOTA:	En las preguntas cuya respuesta sea afirmativa, la valoración de la escala planteada, cualitativamente corresponde a los siguientes parámetros:			
1	2	3	4	5
Casi nunca	**Regularmente**	**Bueno Frecuentemente**	**Muy Bueno Casi Siempre**	**Excelente Siempre**

Nº	**CONTROL DE ACCESO**	**No**	**Si**				
			1	**2**	**3**	**4**	**5**
1	Se ha realizado un estudio de riesgo de intrusión en el edificio?						
2	Se ha realizado un análisis del riesgo de acceso al CPD?						
3	El CPD está completamente aislado del resto del edificio y sus accesos controlados?						
4	Existe un circuito cerrado de televisión que controle el acceso al CPD y las puertas de emergencia?						
5	Existe un registro escrito o impreso de todos los accesos a todas las salas de equipos informáticos?						
6	Existe un sistema de control de acceso biométrico?						
7	Todas las personas con acceso autorizado tienen una tarjeta de identificación y están controlados?						
8	Todo el personal, ajeno o no a la empresa, exhibe de forma clara la tarjeta de identificación?						
9	Se utiliza un sistema de control de acceso automático para el acceso al CPD?						
10	El acceso al CPD está auditado, tanto para la entrada como para la salida?						
11	Existen procedimientos específicos de control de acceso para el personal ajeno a la empresa?						
12	Existe una vigilancia exterior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?						
13	Todas las salidas de emergencia están equipadas con un dispositivo de control, unido a un puesto permanente de vigilancia que alerte de su apertura?						
14	Las oficinas se cierran con llave y se verifica su cierre al terminar la jornada laboral?						
15	Se aplica a la empresa la política de mesas vacías?						
16	Se ha verificado la resistencia de los muros del edificio ante un intento de intrusión?						
17	Se ha verificado la resistencia de las puertas (calidad de los marcos, resistencia de la puerta, calidad de los cerrojos y cerraduras, etc.)?						
18	Se ha verificado la resistencia de las ventanas?						
19	Las ventanas de las plantas bajas disponen de rejas o barrotes y se ha verificado su resistencia?						
20	Se necesita un permiso expreso para acceder al CPD?						
21	Se notifican al CPD con suficiente antelación las visitas previstas?						
22	Hay un control y archivo diario de las grabaciones del sistema de vigilancia?						

23	Existe un servicio de vigilantes de seguridad?						
24	Existe un procedimiento de rondas y verificación de la seguridad física?						
25	Existe un procedimiento de recepción de materiales, que garanticen su inspección antes de su traslado al interior del edificio?						
26	Existe un control de la entrada y salida de material?						
27	Existe un sistema de detección de metales?						
28	Existe un procedimiento específico de control de acceso del personal de limpieza?						

CUESTIONARIO 5: SEGURIDAD FISICA (INCENDIO)

CAC : COOPERATIVA DE AHORRO Y CREDITO / CPD: CENTRO DE PROCESAMIENTO DE DATOS

NOTA:	En las preguntas cuya respuesta sea afirmativa, la valoración de la escala planteada, cualitativamente corresponde a los siguientes parámetros:			
1	2	3	4	5
Casi nunca	**Regularmente**	**Bueno Frecuentemente**	**Muy Bueno Casi Siempre**	**Excelente Siempre**

Nº	**INCENDIO**	**No**	**Si**				
			1	**2**	**3**	**4**	**5**
1	Se ha realizado un estudio de los riesgos de incendio que cubra tanto la prevención como la protección?						
2	Los tabiques y revestimientos de muros, techos y suelos están fabricados con materiales ignífugos?						
3	El mobiliario del edificio del CPD es ignífugo?						
4	Existe un sistema automático de detección de incendios y está conectado a una central de alarmas?						
5	Los conductos de aire acondicionado/ventilación están equipados con válvulas automáticas contra incendios?						
6	Se activa automáticamente el sistema de corte de energía eléctrica tras la detección de un incendio?						
7	Hay barreras como puertas antifuego y/o cortinas antihumos en los lugares susceptibles de ser utilizadas?						
8	Las puertas cortafuegos se cierran automáticamente al saltar la alarma?						
9	Existe una instalación fija contra incendios en el CPD?						
10	Existe un suministro adecuado de agua para los sistemas de extinción de incendios?						
11	La instalación de detección automática de incendios está compuesta por al menos dos tipos de detectores (por ejemplo: detectores de humo iónicos y ópticos)?						
12	Existe un indicador luminoso y sonoro fuera del CPD cuando el sistema contra incendios se dispara?						
13	Estas instalaciones son revisadas periódicamente, conforme a la reglamentación y tiene un mantenimiento adecuado?						
14	El número y distribución de dispositivos de alarmas contra incendios es el adecuado?						
15	Las instalaciones de extinción automática están realizadas según la normativa vigente y están certificadas como tales?						
16	Las instalaciones de extinción automática se verifican periódicamente de acuerdo con la normativa, y su mantenimiento se realiza regularmente?						
17	Cuando las instalaciones de extinción automática se quedan fuera de servicio, ¿se señaliza automáticamente en un puesto permanente de vigilancia ocupado por dos personas como mínimo?						
18	Existe una instalación de extintores portátiles en el conjunto de los locales informáticos y el equipamiento del entorno?						
19	La instalación de extintores portátiles cumple la normativa vigente?						

20	Existen indicaciones claramente visibles acerca de las condiciones de uso de los extintores?						
21	Los extintores portátiles se verifican periódicamente de acuerdo con la normativa y su mantenimiento se realiza adecuadamente?						
22	Se utilizan solo papeleras metálicas en el edificio y papeleras ignífugas con sus correspondientes tapas en las salas de ordenadores?						
23	La cantidad de papel almacenada en las salas de impresión es inferior a las necesidades de un día de producción?						
24	Los productos diversos de mantenimiento, fácilmente inflamables, ¿se almacenan fuera del CPD?						
25	Los documentos o soportes informáticos de interés para la empresa se guardan en armarios ignífugos?						
26	Está prohibido fumar en el CPD y se respeta la prohibición?						
27	Se efectúa una limpieza periódica de los espacios ocultos (bajo el falso suelo, escalera, etc.)?						
28	Se evita la acumulación de material innecesario en el CPD’						
29	Se utilizan contenedores de basura resistentes al fuego?						

GLOSARIO DE TÉRMINOS

Aceptación del riesgo: Es la decisión para aceptar un riesgo.

Actividad: Es el conjunto de tareas.

Activo de información: Es algo que la organización directamente le asigna un valor, y por lo tanto, la organización lo debe proteger.

Administración de la información: Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes

Alta gerencia: La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada.

Amenaza: Cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización. Es la indicación de un potencial evento no deseado. Es una indicación de un evento inminentemente desagradable. Es una persona u objeto vista como posible fuente de peligro o catástrofe. En síntesis amenaza es una indicación de un evento desagradable con el potencial de causar daño.

Análisis del riesgo: Es la utilización sistemática de la información para identificar las fuentes y estimar el riesgo.

Aplicación: Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones.

BASILEA II: Representa una serie de recomendaciones para garantizar la adopción y aplicación de prácticas adecuadas de gobierno corporativo. Promueve una mayor consistencia en la forma en que los bancos y las entidades reguladoras bancarias consideran la administración del riesgo a través de diversas fronteras nacionales.

BCP: Business Continuity Planning.

BIA: Business Impact Analysis.

CAC: Cooperativas de Ahorro y Crédito.

Confidencialidad: Es la garantía de que sólo el personal autorizado accede a la información preestablecida. Es la propiedad de que la información no esta disponible o divulgada a individuos, entidades o procesos no autorizados.

Cumplimiento: Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos.

Datos: Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.
Declaración de aplicabilidad: Es la declaración documentada que describe los objetivos de control y controles que son pertinentes y aplicable al SGSI de la organización.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades. Propiedad de estar accesible y utilizable bajo demanda de una autoridad autorizada.

Eficacia: Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos.

Eficiencia: Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores.

Encriptación: Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino.

Enfoque basado en procesos: Es la aplicación de un sistema de procesos dentro de la organización, junto con la identificación y las interacciones de estos procesos, así como su gestión.

Evaluación del riesgo: Es el proceso global del análisis del riesgo y la valoración del riesgo.

Evento de riesgo operativo: Es el hecho que puede derivar en pérdidas financieras para la institución controlada.

Evento de seguridad de la información: Es una ocurrencia identificada de un estado del sistema, servicio o red que indica una brecha posible en la política de seguridad o falla de las salvaguardas, o de una situación previamente desconocida que puede ser pertinente a la seguridad.

Factor de riesgo operativo: Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos.

Gestión del riesgo: Son las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: Es la medición y la valoración del tamaño que podría producir a la organización un incidente de seguridad. Es la evaluación del impacto del riesgo

Incidente de seguridad: Es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles perdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza. Es uno o una serie de eventos de seguridad de la información, indeseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio, y amenacen la seguridad de la información.

Información: Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones.

Información crítica: Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.

Ingeniería social: Conjunto de técnicas y trucos empleados por intrusos y hackers para extraer información sensible de los usuarios de un sistema informático.

Instalaciones: Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información.

Instrucción de trabajo: Las instrucciones de trabajo son información muy detallada sobre el "cómo" efectuar un trabajo en particular. Pueden presentarse de varias formas. Las más usadas son las listas de chequeo, las tablas de decisiones, los flujogramas y dibujos. Es la información que explica en detalle como se efectúa una operación concreta.

Insumo: Es el conjunto de materiales, datos o información que sirven como entrada a un proceso.

Integridad: Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento. Es la propiedad de salvaguardad la exactitud y totalidad de los activos.

Línea de negocio: Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad

Manual de Seguridad: Es el documento que especifica o describe el SGSI de la organización, definiendo responsabilidades, compromisos, autoridades y metodologías.

Medios electrónicos: Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.

No repudio: Negativa de organización o persona de haber enviado una determinada información, que efectivamente si envió.

PEA: Población económicamente activa

PCN: Plan de continuidad del negocio.

Pista de auditoria: Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoria.

Plan de seguridad: Es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.

Política de seguridad: Es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y

delimitar las responsabilidades para las diversas actuaciones técnicas organizativas que requieran.

Procedimiento: Es la manera específica de desempeñar una actividad o proceso.

Procedimientos de seguridad: Es la definición detallada de los pasos a ejecutar para llevar a cabo tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización.

Proceso: Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo. Es cualquier actividad que utiliza recursos, y que se gestiona para permitir que los elementos de entrada se transformen en resultados.

Proceso crítico: Es todo proceso vital para la organización, establecido en términos de impactos financieros y operacionales.

Recursos del sistema: Son los activos proteger del sistema informático de la organización.

Registros: Son documentos que sirven como evidencia para demostrar a terceros que un requisito del Sistema de Gestión de Seguridad de la Información sea cumplido.

Responsable de la información: Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones.

Riesgo: Es la probabilidad de que la amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. Es la probabilidad de que la amenaza llegue acaecer por la existencia de una vulnerabilidad. Es la probabilidad de que una amenaza explote a una vulnerabilidad.

Riesgo legal: Es la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una institución del sistema financiero, derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones.

Riesgo residual: Es el riesgo remanente después del tratamiento del riesgo

SBS: Superintendencia de Bancos y Seguros.

Seguridad de la información: Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella. Es la preservación de la confidencialidad, integridad y disponibilidad de la información, adicionalmente pueden involucrarse otras propiedades, tales como autenticidad, responsabilidad, no repudio y confiabilidad.

Seguridades lógicas: Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Es la parte del sistema de gestión global, basado en un enfoque del riesgo del negocio, para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura de la organización, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Tecnología de la información: Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros.

Transferencia electrónica de información: Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros.

Tratamiento del riesgo: Es el proceso de selección e implantación de medidas para modificar el riesgo, estas medidas pueden ser, evitarlo, transferirlo, reducirlo, o asumirlo.
Una política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo como propósito, proteger la información, los recursos y la reputación de la misma.

Valoración del riesgo: Es el proceso de comparar el riesgo estimado contar los criterios de riesgo dados para determinar la significación del riesgo.

Vulnerabilidad: Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir perdidas a la organización. Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. Es una situación creada por la falta de uno o varios controles, con la que la amenaza pudiera afectar al entorno informático.