FACULTAD DE POSGRADOS

FORMULACIÓN DE UNA PROPUESTA PARA UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DE LA INDUSTRIA BANCARIA EN EL SECTOR PRIVADO

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de Información

Profesor Guía

MBA. Jaime Augusto Vinueza Trujillo

Autora

María Cristina Landázuri Benalcázar

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Jaime Augusto Vinueza Trujillo
Master in Business Administration
Mención en Finanzas y Marketing
CI: 1716028509

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Katalina del Rocío Coronel Hoyos
Magíster en Gerencia de Tecnologías de la Información
C.I: 1711000016

DECLARACIÓN DE AUTORÍA DEL MAESTRANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

María Cristina Landázuri Benalcázar

CI: 1719390641

AGRADECIMIENTOS

Agradezco a Dios por darme el ánimo, la fuerza y las posibilidades de seguir creciendo profesionalmente y alcanzar esta meta tan anhelada.

A mi familia que son mi motor y mi motivación de cada día, sin su apoyo no lo hubiera logrado.

A las autoridades y docentes de la Universidad de las Américas por todo el conocimiento compartido y las enseñanzas brindadas.

Gracias a mis compañeros por todas las experiencias vividas y su valiosa amistad.

DEDICATORIA

A mis padres maravillosos, mi pequeña sobrina hermosa, mi valiosa hermana y mi precioso Jonás

Los quiero tanto.

A todas las personas que me brindaron su ayuda y apoyo para lograr esta meta.

RESUMEN

En la actualidad la industria Bancaria en el Ecuador ha encaminado sus esfuerzos en proveer sistemas de información prácticos y accesibles a sus clientes adaptándose así a los avances tecnológicos de la época, sin embargo se ha evidenciado también, un crecimiento proporcional de amenazas y ataques informáticos que no solo ponen en riesgo los sistemas de información sino la estabilidad de una entidad, por tanto, el concepto de valor de la información como el activo más importante se ha convertido en el objetivo fundamental de las entidades bancarias, de ahí su importancia de establecer un esquema metodológico y procesos documentados para su adecuada gestión.

Un Sistema de Gestión de Seguridad de la Información (SGSI) según la ISO 27001 se basa en la preservación de la confidencialidad, integridad y disponibilidad de la información, mediante una gestión de riesgos que garantice que éstos sean conocidos, asumidos, gestionados y minimizados por la organización.

El presente proyecto plantea un modelo de sistema de gestión de seguridad de la información (SGSI) para entidades de la vertical bancaria del sector privado en el Ecuador basándose en las mejores prácticas y principios de las normas ISO, y de marcos de referencia como COBIT y COSO.

Se realiza un análisis de la problemática actual con el manejo de información y los requerimientos legales y normativos que son de carácter obligatorio para las entidades de la industria bancaria en el Ecuador y que son regulados por los entes de control, en base a estos requerimientos se propone la implementación de controles determinados en la norma ISO 27001.

Una vez determinado los requerimientos se procede a explicar y proponer un esquema o metodología para el desarrollo del SGSI en la fase de “Planeación” que incluye entregables como políticas, análisis de riesgos, clasificación de activos, plan de tratamiento de riesgos, etc. utilizando el modelo de mejora continua PDCA (Plan, do, check, act) conocido como “Ciclo de Deming”, en su

equivalencia en español es Planificar, hacer, verificar y actuar (PHVA), el cual establece un proceso cíclico de mejora continua en la cual se basa esta propuesta.

Para finalizar se plantea modelos y estructuras de medición para evaluar el rendimiento de la seguridad de la información y de la eficacia del SGSI.

ABSTRACT

Nowadays, banking industry in Ecuador has directed its efforts towards providing practical and accessible information systems to its clients, adapting itself to the technological advances of time. However, there has been a proportional increase in threats and computer attacks that, not only endanger the information systems but also the stability of the entity as a whole; therefore, the concept of value of information as the most important asset has become the fundamental objective of banking entities, hence the importance of establishing a methodological scheme and documented processes for its proper management.

An ISO 27001 Information Security Management System (ISMS) is based on the preservation of information confidentiality, integrity and availability, by means of a risk management process that ensures they are known, assumed, managed and minimized by the organization.

The following project proposes a model of information security management system (ISMS) for private sector banking entities in Ecuador based on best practices and principles of ISO standards, and frameworks such as COBIT for IT governance and COSO for internal control.

An analysis has been carried out taking into account current issues with information handling and legal and regulatory requirements which are mandatory for banking industry entities in Ecuador and therefore regulated by the financial authority; the proposed controls for implementation are determined in ISO 27001 and based on those requirements.

Once all requirements have been determined, there is an explanation and a proposal on a scheme or methodology for the ISMS seen on "Planning" phase, which includes information such as policies, risk analysis, asset classification, a risk treatment plan, etc. using the PDCA (Plan, do, check, act) model of improvement known as the "Deming Cycle", or translated into Spanish Planificar, hacer, verificar y actuar (PHVA), that establishes a cyclical process of continuous improvement in which the cited proposal is based.

Finally, there are suggestions on models and measurement structures intended to evaluate the information security performance and ISMS effectiveness.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

De acuerdo al boletín # 42 “el crecimiento de la economía ecuatoriana se ha dado en gran medida por el aporte de varios sectores productivos, entre las cuales se destaca el rol de la banca privada como agente dinamizador del sistema financiero nacional” (Asociación de Bancos Privados del Ecuador, 2014).

La Banca privada ha efectuado una fuerte inversión en los últimos años en proyectos que provean bienestar, seguridad y satisfacción al cliente como son la banca móvil, banca en línea, cobros móviles, banca telefónica (Call Center), cajeros automáticos, autoservicio, etc. Todos estos servicios se encuentran apalancados con altos estándares relacionados a la seguridad de la Información, lo cual ha permitido incluir un mayor número de ecuatorianos a la red de servicios financieros.

En el sector bancario, los sistemas de información permiten la articulación de las dinámicas productivas y se convierten en elementos fundamentales para responder frente a cambios y satisfacer los requerimientos legales y normativos del entorno, más aun cuando las transformaciones que se han producido en las últimos años se fundamentan en el valor de la información y el conocimiento como la materia prima para alcanzar mayor productividad en la gestión.

El objetivo del uso de la información para las instituciones del sistema financiero del Ecuador ha cambiado de perspectiva en los últimos años, dado que la información se ha convertido en el activo más importante para una empresa que pertenece a esta industria.

La seguridad de esta gran cantidad de información se convierte en un factor esencial en el desarrollo del negocio bancario, es un elemento indispensable para garantizar confianza en el uso de las tecnologías de información no solo para las entidades bancarias sino en general para la nueva sociedad digital; es por esto que el término CDO (*Chief Data Officer*) Oficial corporativo de datos, se lo ha denominado como un rol estratégico y clave en la nueva era de los

negocios inteligentes. El desafío de las empresas en la actualidad se basa en cómo generar mayor competitividad a través de buena información, esto implica entre otras cosas tener datos correctos de los clientes, protegerlos, mantenerlos actualizados, enriquecer los datos con los que se cuenta y además tener la facultad de monetizar esa información. Todo esto es viable si existen métodos y sistemas estructurados, y de fácil manejo apalancados en una gestión eficiente que garantice su vigencia y su funcionalidad.

Actuando bajo estos lineamientos, la Junta Bancaria del Ecuador ha establecido la resolución JB-2012-2148 para las instituciones del Sistema Financiero en la cual se establecen medidas de seguridad en la tecnología de información. En el artículo 2, numeral 2.33 se determina que:

“Calidad de la información.- es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella” (Superintendencia de Bancos y Seguros, 2014). Adicionalmente en el numeral 4.3.5.4 del mismo documento se establece lo siguiente: “El envío de información de sus clientes relacionada con al menos números de cuentas y tarjetas, debe ser realizado bajo condiciones de seguridad de la Información” (Superintendencia de Bancos y Seguros, 2014).

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye la ISO 27001. La seguridad de la información, según esta norma, “consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización” (Portal de ISO 27001 en español, 2012). “El propósito de un SGSI es, por tanto, garantizar que los riesgos de seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una manera documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios” (Portal de ISO 27001 en español, 2012).

En los últimos años se ha hecho evidente el aumento de las amenazas y ataques efectuados a la información de una manera proporcional a los avances tecnológicos; de acuerdo a un estudio efectuado por la compañía de seguridad

informática ESET en enero del 2015, indica que en los últimos 5 años se han reportado el 70% de todos los casos de fuga de información que ocurrieron desde el 2004, la cantidad de registros filtrados en los últimos dos años es casi igual al 90% de la cantidad de habitantes de Latinoamérica, lo cual sería como si en el último par de años se hubiera visto filtrada información sensible de 9 de cada 10 habitantes de la región. Las empresas financieras se encuentran dentro del grupo de empresas con mayor número de ataques (70%) (Amaya, 2015).

En el mes de mayo del presente año se vivió uno de los ataques de crimen cibernético más fuertes que se han perpetrado en los últimos años, el ya famoso virus *Wanna Cry (ransomware)* que afectó a 200.000 computadoras en todo el mundo, colocándose con fecha 15 de mayo al Ecuador en el tercer lugar de los países Latinoamericanos con mayor registro de infecciones del virus, debajo de México y Brasil, incluso se conoce que una institución financiera de nuestro país fue víctima del virus; otras cifras alarmantes vienen de las amenazas externas por ejemplo el 93% de casos de phishing (emails) contienen re direccionamientos hacia algún virus de tipo ransomware, en el 2016 se ha incrementado a un 250% más de sitios web de phishing, $3.100 millones de pérdidas se registran por afectación de emails corporativos y un 97% de los usuarios no pueden identificar emails de tipo phishing.

Se identificó que la propagación del virus se lo hace por medio de 3 vectores que son: correo electrónico, conexión a una red inalámbrica, y mediante *worms* (gusanos) de red, el atacante incluso puede llegar a tener permisos de administrador de un equipo, inhibir aplicativos e infectar toda una red. Microsoft pidió a los gobiernos de todo el mundo ver dicho ataque como una llamada de atención sobre sus métodos de acumulación de vulnerabilidades y la falta de estrategias para una protección adecuada de la información, de ahí la importancia de establecer un esquema de gestión de la seguridad de la información basado no solo en herramientas de prevención sino en todo un conjunto de políticas, procesos y procedimientos que se encuentren alineados a los objetivos del negocio.

Aún en nuestro medio no se ha creado una adecuada conciencia del riesgo que implica el no contar con una planificación, ejecución, monitoreo y mejora continua de un conjunto de controles que permitan reducir el riesgo de sufrir incidentes de seguridad de la información; de ahí la importancia de contar con un sistema de gestión estructurado, sistemático y acorde a las regulaciones gubernamentales para la seguridad de la información.
El presente estudio pretende abordar dicha necesidad de la industria bancaria y aportar con soluciones estratégicas que sean viables y sustentables en el tiempo.

Justificación:
Contribuir con un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para empresas de la industria Bancaria del sector privado; dicho sistema se constituirá en una herramienta estratégica que permitirá gestionar el activo prioritario de una empresa como es la información, reduciendo el riesgo de pérdida de la misma y generando confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

“El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades” (Portal de ISO 27001 en español, 2012), son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

De acuerdo a un estudio efectuado por la firma de seguridad informática Kaspersky, “más del 80% de los códigos maliciosos son desarrollados con el fin de robar información bancaria” (AeTecno, 2012) y existen ataques a diario a los sistemas web de las entidades financieras. “Los costos relacionados con delitos informáticos pueden ir desde un aumento en la inversión en sistemas y personal de seguridad, hasta la cobertura de indemnizaciones, campañas de imagen, pérdida de competitividad en el mercado, entre otros” (El Espectador, 2012).

De acuerdo con el estudio de ciberdelito desarrollado por el Registro de Direcciones de Internet para América Latina y Caribe (Lacnic), el phishing o robo de datos personales significa pérdidas anuales por unos US$93 mil millones de dólares, y afecta a unos 2.500 bancos que operan en la región, en tanto los robos a cuentas de clientes suman otros US$761 millones de dólares (Segu.Info, 2012).

El nivel de seguridad alcanzado por medios técnicos no es suficiente en sí para garantizar una seguridad razonable, por tanto, la aplicación de un sistema de gestión en donde se desarrollen procedimientos y políticas que se encuentren alineados a los objetivos del negocio permitirá mantener un nivel de exposición siempre menor al nivel de riesgo que la empresa ha decidido asumir.

Objetivos:

Objetivo General:
Proponer un modelo de Sistema de Gestión de Seguridad de la Información para empresas de la industria bancaria en el sector privado.

Objetivos Específicos:

- Efectuar un análisis del estado actual de los riesgos en la gestión de seguridad de la información en términos generales y posteriormente de forma específica en la industria de la banca en el sector privado.
- Identificar y analizar los requerimientos de seguridad de la Información para la industria bancaria, en base al cumplimiento normativo nacional e internacional.
- Formular un SGSI, aplicable a la industria de la banca del sector privado en base al uso combinado de estándares existentes en el medio y considerando las mejores prácticas y marcos de referencia de la industria.
- Evaluar la aplicabilidad de la propuesta para un modelo de Sistema de Gestión de Seguridad de la Información dentro de los cuatro aspectos fundamentales: legal, económico, operacional y organizacional.
- Formular un plan de monitoreo continuo y control del SGSI, que permita garantizar que los controles, procesos y procedimientos cumplan con los objetivos planteados.

Alcance

El presente trabajo tiene como objetivo establecer un modelo para un Sistema de Gestión de Seguridad de la información que incorpore estándares internacionales y normativas gubernamentales, que soporte los procesos y los objetivos de la industria bancaria en el sector privado del Ecuador.

Se realizará la evaluación de los riesgos de seguridad de la información asociados a la banca privada, mediante un análisis general de la situación actual de la información y de su importancia en esta industria.

Se determinará una metodología para la evaluación de estos riesgos, la cual permitirá identificarlos, clasificarlos y gestionarlos de manera que constituyan un nivel de exposición siempre menor al nivel de riesgo que la empresa ha decidido asumir.

Se identificarán los activos principales de información para la industria de la banca en la actualidad de acuerdo a la criticidad y administración.

Con los requerimientos de seguridad de la información establecidos para este tipo de industria en el Ecuador, se aplicarán los esquemas de gestión de la seguridad de acuerdo a la norma ISO 27001 y la ISO 27002, para la adecuada gestión de procesos de seguridad conforme al marco de referencia COBIT y las mejores prácticas de seguridad; como resultado se propone un modelo para un sistema de gestión de seguridad de la información que abarque las necesidades actuales de la industria bancaria sin dejar de lado el crecimiento e innovación tecnológica a la cual está inmersa dicha industria.

Finalmente se realizará una evaluación de la aplicación de la propuesta en los siguientes aspectos: legal, organizacional, operacional y económico determinando la vialidad del proyecto y justificando la inversión requerida para esta solución.

Con esta evaluación se determinará un plan de monitoreo para el sistema de gestión que sea sustentable en el tiempo y a los cambios tecnológicos.

1. Capítulo I: Marco teórico

A continuación, un detalle de los principales conceptos para la realización de esta propuesta:

1.1 Que es un SGSI

"SGSI es la abreviatura utilizada para referirse a un *Sistema de Gestión de la Seguridad de la Información"* (Portal de ISO 27001 en español, 2012). ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*. EL SGSI es el concepto central sobre el que se construye la ISO 27001. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración (Portal de ISO 27001 en español, 2012).

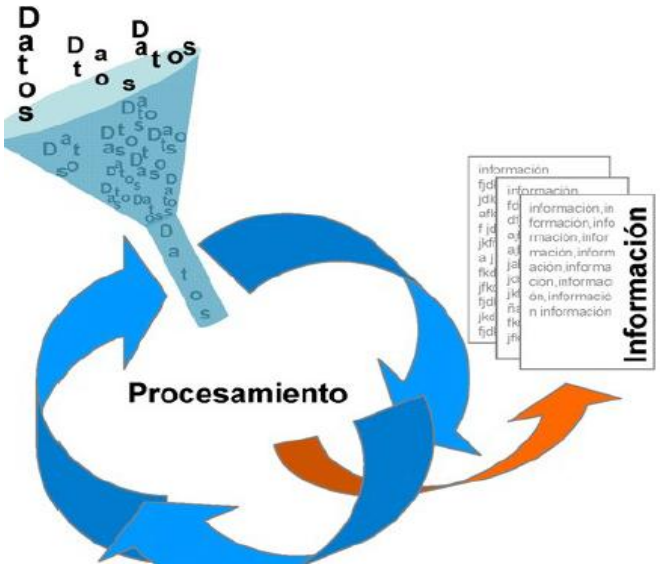


Figura 1. Un SGSI

Tomado de (Portal de ISO 27001 en español, 2012)

1.2 Fundamentos

Un SGSI debe garantizar que la seguridad de la información es gestionada correctamente en base a los siguientes principios:

- Confidencialidad: la información no puede estar disponible, ni puede ser revelada a personas, entidades o procedimientos no permitidos.
- Integridad: mantener la integridad, exactitud y completitud de la información.
- Disponibilidad: uso, utilización y acceso de la información y los sistemas de generación de la misma por personas, entidades, procesos o procedimientos cuando sea requerido.

Una vez conocido el ciclo de vida de la información se debe adoptar un proceso metódico, ordenado y documentado desde un enfoque orientado a riesgos, este proceso es el que constituye un SGSI (Portal de ISO 27001 en español, 2012).

1.2.1 La información

“Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información tiene una estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno” (Perea, 2016).

1.2.2 Sistema de Información

Según Murdick (1998) un sistema de información es aquel sistema que “examina y recupera los datos provenientes del ambiente que captura los datos a partir de las transacciones y operaciones efectuadas dentro de la empresa que filtra, organiza y selecciona los datos y los presenta en forma de información a los gerentes, proporcionándoles los medios para generar la información” (Subero, 2000) .

1.2.3 Seguridad de la Información

La seguridad de la información, según ISO 27001, consiste en la “preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización” (Portal de ISO 27001 en español, 2012) .Es necesario considerar otras definiciones

importantes al momento de hablar de seguridad de la información y son los siguientes:

- Activo.- recurso del sistema de información necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- Activo de Información.- es todo aquello que se genera, procesa o almacena y que posee valor a una organización.
- Amenaza.- es un evento que puede desencadenar en un incidente de seguridad en la organización, produciendo daños o pérdidas en los activos.
- Ataque.- Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- Control.- proceso mediante el cual la administración verifica si lo que ocurre concuerda con lo que se supone debe ocurrir. Adicionalmente un control permite que se realicen los ajustes o correcciones necesarias en caso de detectar eventos que se escapan a la naturaleza del proceso.
- Gestión de activos.- acción que busca proteger los activos de información de una organización mediante el control de acceso a cada uno de ellos.
- Impacto.- Cambio adverso en el nivel de los objetivos del negocio logrados.
- Oficial de Seguridad.- persona encargada de administrar, implementar, actualizar y monitorear el SGSI.
- Políticas de Seguridad.- busca establecer reglas para proporcionar dirección gerencial y el soporte para la seguridad de la información.
- Riesgo.- es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia.
- Riesgo Aceptable.- es el riesgo propio del proceso o actividad que no supone un perjuicio grave y que de acuerdo a los criterios del negocio puede ser asumido.
- Riesgo Residual.- es el riesgo que permanece una vez que se han aplicado los controles necesarios para minimizar el riesgo inicial.

- Riesgo de la Seguridad de la Información.- Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- Comunicación del riesgo.- Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.
- Estimación del riesgo.- Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- Identificación del riesgo.- Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- Reducción del riesgo.- Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- Retención del riesgo.- Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- Transferencia del riesgo.- Compartir con otra de las partes la pérdida o la ganancia de un riesgo.
- Vulnerabilidad.- Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.
- Mínimo Privilegio.- principio que establece que las entidades, individuos o procesos tengan habilitado el derecho de acceso o modificación únicamente a la información que necesitan de forma exclusiva para cumplir con las funciones.
- Confidencialidad.- característica de la información que determina la disponibilidad para el uso o visualización exclusiva de los individuos, entidades o procesos que se encuentran autorizados, conforme al principio del mínimo privilegio.
- Integridad.- propiedad de la información que determina exactitud, completitud y validez de acuerdo a los valores y expectativas determinadas por la empresa y las entidades de control.
- Disponibilidad.- característica de la información que determina el acceso a su uso cuando sea requerido por un individuo, proceso o entidad

autorizada. El aseguramiento de esta propiedad ayuda a minimizar la posibilidad de interrupción de los procesos del negocio para preservar la continuidad de las operaciones.

- Matriz RACI.- esquema de asignación sugerida del nivel de responsabilidad para prácticas de proceso a diferentes roles y estructuras.

1.3 Sistemas de GSI (Gestión de seguridad de la información)

De acuerdo a la norma ISO 27001 el sistema de gestión de la seguridad de la información conserva la confidencialidad, integridad y disponibilidad de la información al aplicar un proceso de gestión de riesgos y les entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada. A continuación, una descripción de los estándares y normativas aplicadas en este proyecto en la gestión de la seguridad de la información:

1.4 ISO (International Organization for Standardization)

Es una federación mundial de organismos nacionales de normalización alrededor de 160 países, trabajan a nivel de Comités Técnicos, tienen al menos 19,000 estándares publicados desde 1947 (creación), 1951 (publicación).

Trabaja en función a 8 principios de gestión:

1. Orientación al cliente
2. Liderazgo
3. Participación del personal
4. Enfoque de procesos
5. Enfoque de sistemas de gestión
6. Mejora continua
7. Enfoque de mejora continua.
8. Relación con el proveedor.

Los estándares ISO son aplicables a cualquier tipo y tamaño de empresa (Balaguer, 2013).

En los últimos años ha existido un incremento considerable de la demanda en las empresas por implementar un sistema de gestión basado en estándares. La ISO 27001 se ha transformado a nivel mundial en la norma principal para el conocimiento de la seguridad de la información y muchas organizaciones han optado por certificar su cumplimiento; en el siguiente gráfico (Figura 2) se muestra el incremento en certificados desde el año 2007 hasta el 2012:

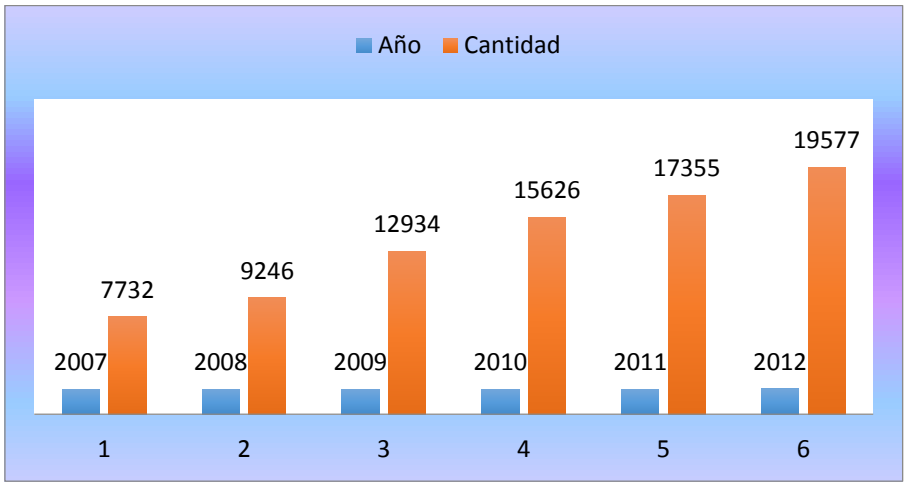


Figura 2. Certificados Otorgados por Año

Tomado de (Academy, 2013)

1.4.1 Estructura del estándar ISO 27001

Los anexos de la ISO 27001 incluyen información relevante sobre lo que se debe considerar para gestionar la seguridad de la información. En la versión ISO/IEC 27001:2013 se incluye la nueva estructura del Anexo A, en donde se agrega 3 dominios de control, los cuales incluyen un total de 14 cláusulas de control de seguridad que contienen a un total de 35 categorías principales de seguridad y 114 controles (Trejo, 2013).

La nueva estructura contiene 10 secciones en donde a partir del 4to paso se inicia la planeación de la gestión de un SGSI. En la figura 3 se muestran los pasos efectuados en la fase de planeación del SGSI con sus principales actividades.

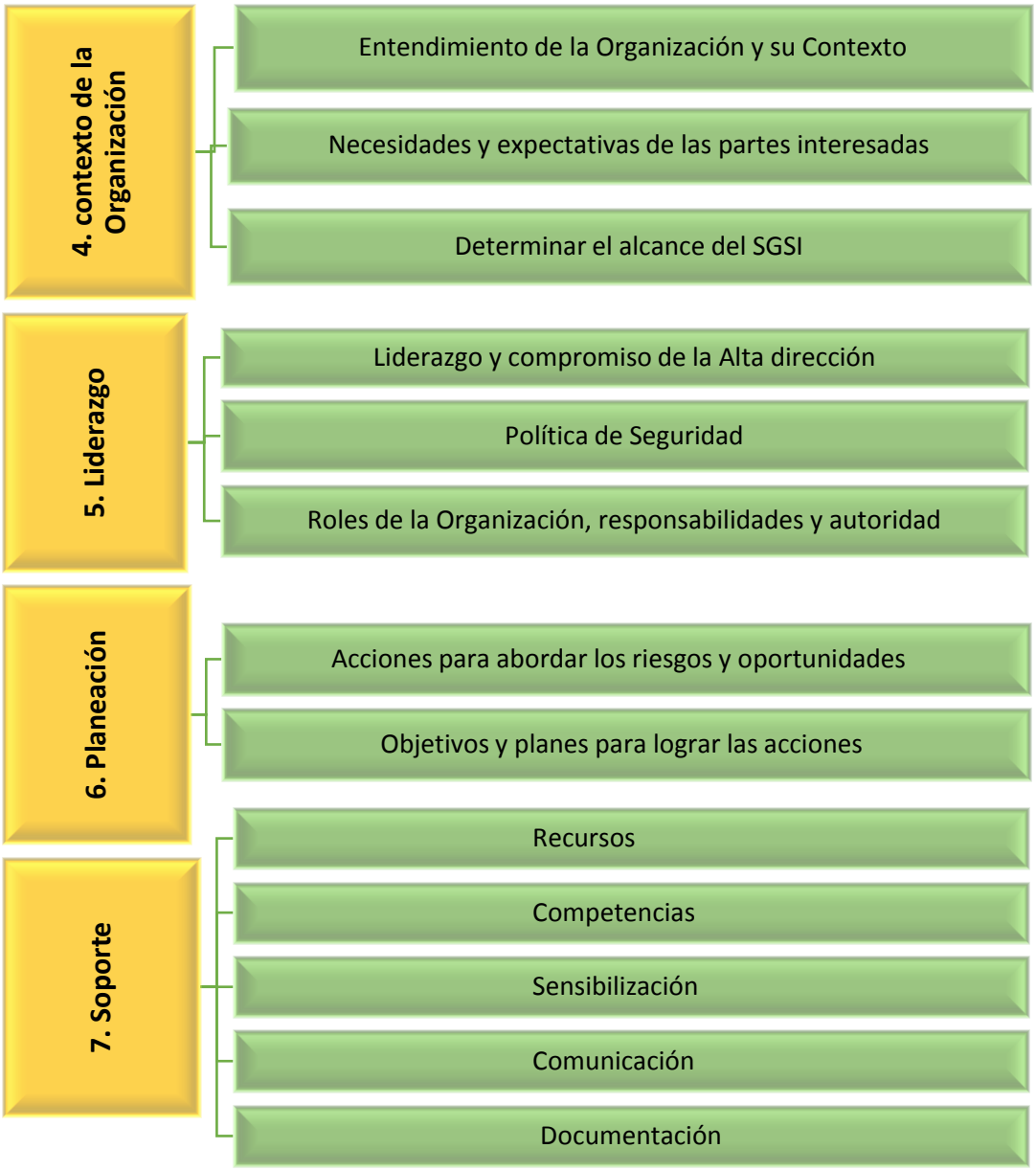
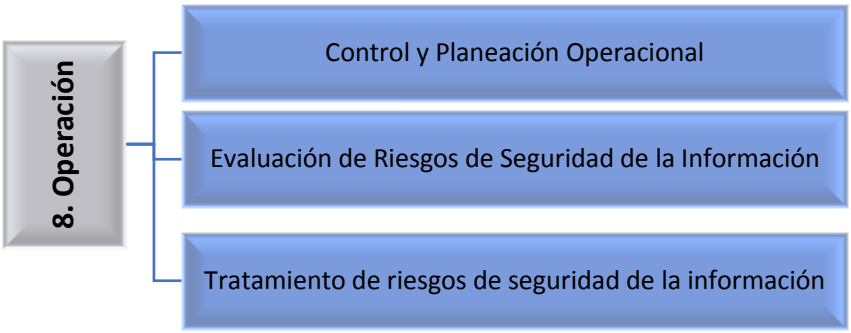


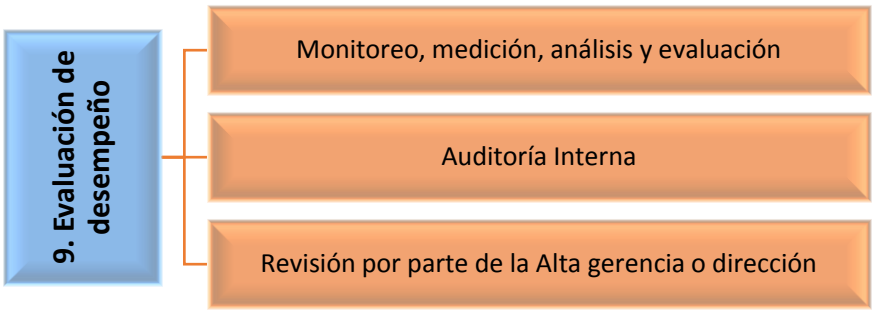
Figura 3. Estructura de la ISO 27001 para la fase de planeación

En la figura 4 se muestran los pasos a efectuar para las fases “Hacer”, “Verificar” y “Actuar”.

Fase Do (Hacer):



Fase Check (Verificar):



Fase Act (Actuar):

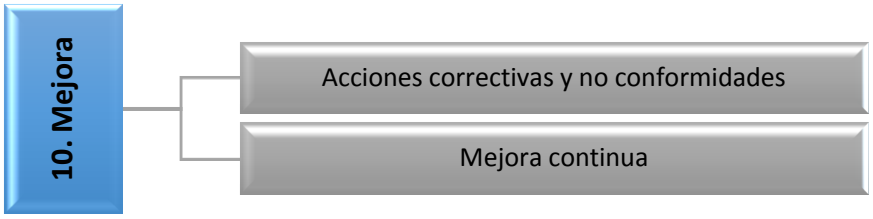


Figura 4. Estructura de la ISO 27001 para las fases “Hacer”, “Verificar” y “Actuar”

En el sección 3.1 Requisitos Generales, se detalla cada una de las secciones de la norma y sus principales actividades como un requerimiento para el establecimiento de un SGSI.

1.4.1.1 Anexos

El “Anexo A – Referencia de objetivos y controles” respecto de la versión anterior aumenta de 11 a 14 dominios o categorías, en la figura 5 se presenta la lista de objetivos de control detallados en el Anexo A los cuales están alineados con aquellos controles detallados en la norma ISO/IEC 27002:2013, cláusulas 5 a la 18.

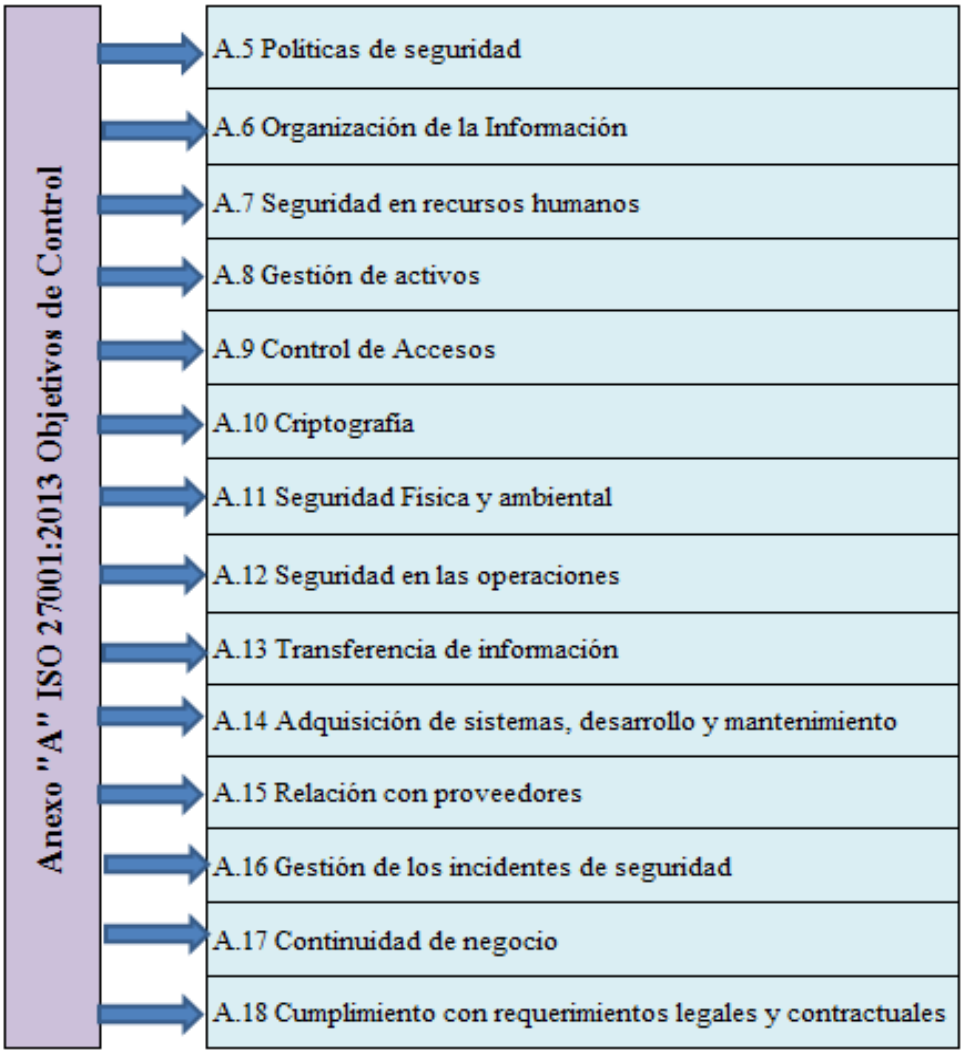


Figura 5. Anexo “A” Objetivos de Control
Tomado de (Trejo, 2013)

1.4.2 Descripción de los documentos y entregables de la aplicación del SGSI

La siguiente lista detalla la cantidad mínima de documentos requeridos por la revisión 2013 de la norma ISO/IEC 27001.

Tabla 1.

Lista de Documentación obligatoria requerida por ISO/IEC 27001

DOCUMENTOS	CAPÍTULO DE ISO 27001:2013
Alcance del SGSI	4.3
Políticas y Objetivos de Seguridad de la Información	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento del Riesgo	6.1.3 e), 6.2
Informe sobre evaluación y tratamiento del riesgos	8.2, 8.3
Definición de funciones y responsabilidades de seguridad.	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1

Tomado de (Academy 27001, 2014).

La siguiente lista detalla los registros mínimos requeridos por la revisión 2013 de la norma ISO/IEC 27001.

Tabla 2.

Lista de Registros mínimos requeridos por ISO/IEC 27001

REGISTROS	CAPÍTULO DE ISO 27001:2013
Registros de Capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de Supervisión y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2

REGISTROS	CAPÍTULO DE ISO 27001:2013
Resultados de la revisión por parte de la dirección	9.3
Resultados de acciones correctivas	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4.3

Tomado de (Academy 27001, 2014)

A continuación en la figura 6 se sintetiza los aspectos principales de la norma ISO mencionada en la sección 7 en la cual se basa esta propuesta:

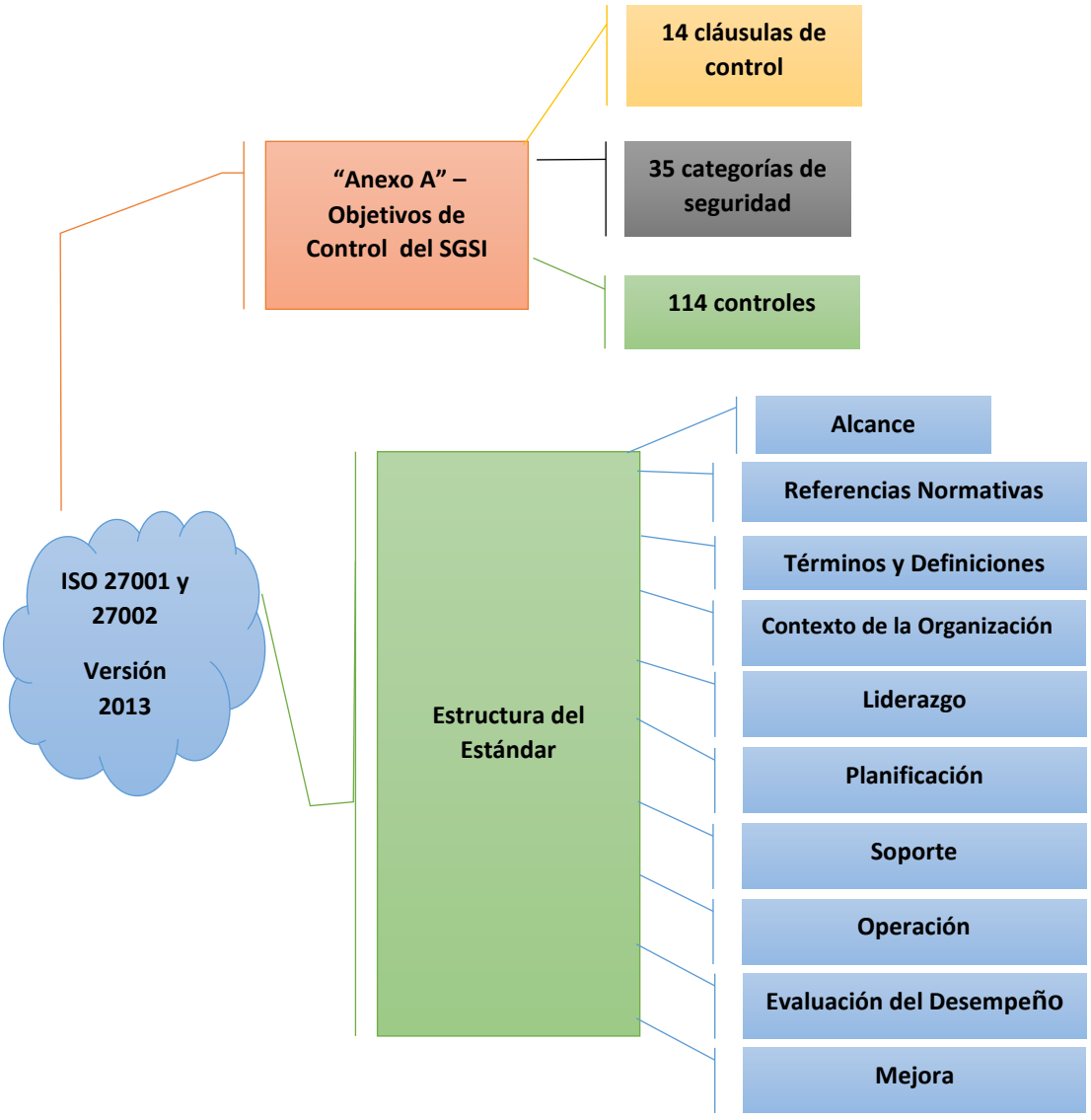


Figura 6. Síntesis estructura de la norma ISO 27001:2013

1.5 COBIT (Control objectives for information and related technology)

COBIT es un framework o marco de trabajo que presenta un conjunto de herramientas de soporte del gobierno de TI que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio. Describen como los procesos de TI entregan la información que el negocio necesita para lograr sus objetivos (ISACA, 2012). COBIT define dos conceptos fundamentales:

- Control: “Son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos de negocio serán alcanzados y que eventos no deseables serán prevenidos, detectados y corregidos” (ISACA, 2012).
- Objetivo de Control en TI: “propósito que se desea alcanzar implementando procedimientos de control en una actividad en particular” (ISACA, 2012).

1.5.1 Los Procesos de COBIT 5

COBIT 5 suministra un marco de referencia a las organizaciones para el logro de objetivos y entrega de valor, mediante un Gobierno y Gestión de TI empresarial prácticos. COBIT ha evolucionado en su desde el año 1996 con un enfoque de auditoría hacia un enfoque en el año 2012 de gobierno corporativo de TI (Ver Figura 7).

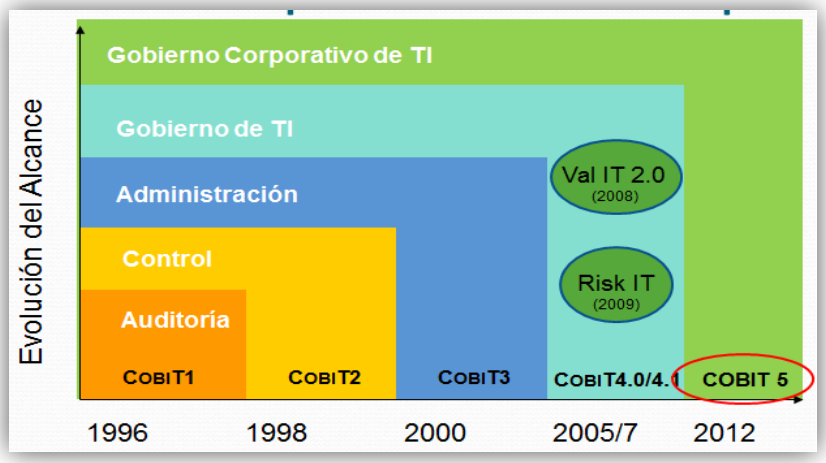


Figura 7. Evolución del Alcance de COBIT

Adaptado de (ISACA, 2012)

La Figura 8 muestra el detalle de los 37 procesos de gestión y gobierno de COBIT5

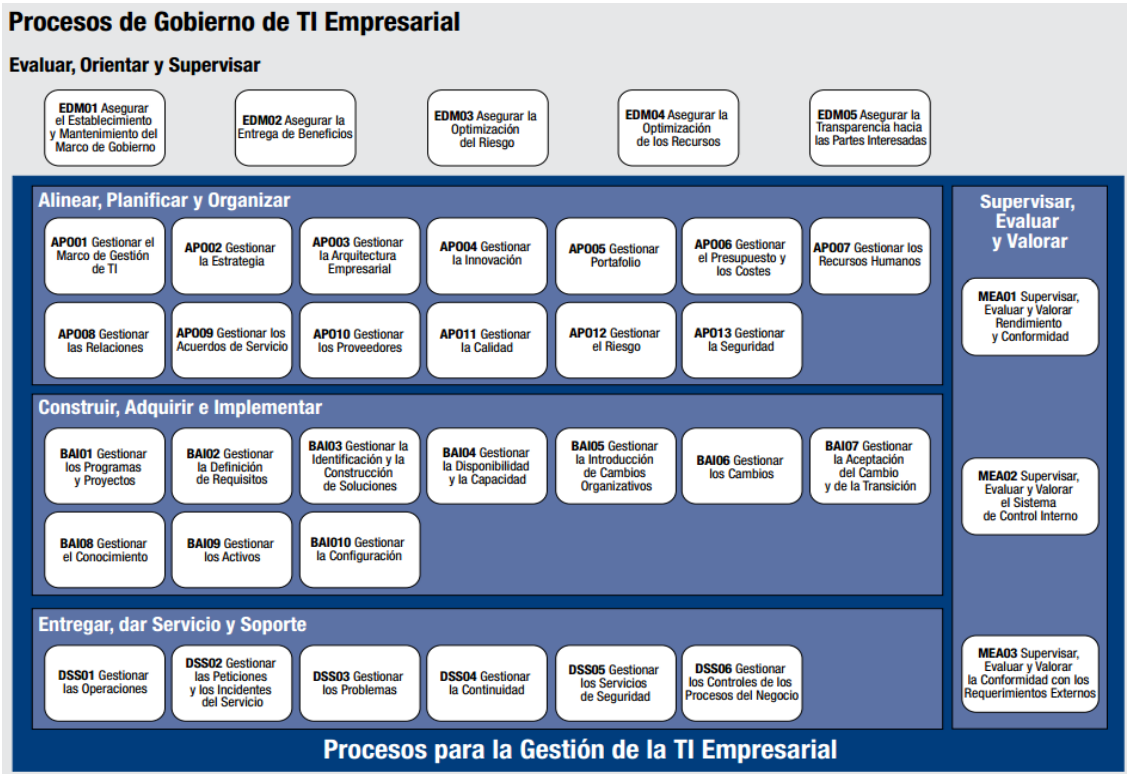


Figura 8. Procesos de COBIT 5

Tomado de (ISACA, 2012)

1.5.2 Relación con otros estándares y normas

COBIT 5 se alinea con los últimos estándares y marcos de referencia usados en el mundo empresarial (Ver Figura 9):

- Empresas: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000.
- Relacionados con TI: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOOK/PRINCE2, CMMI.

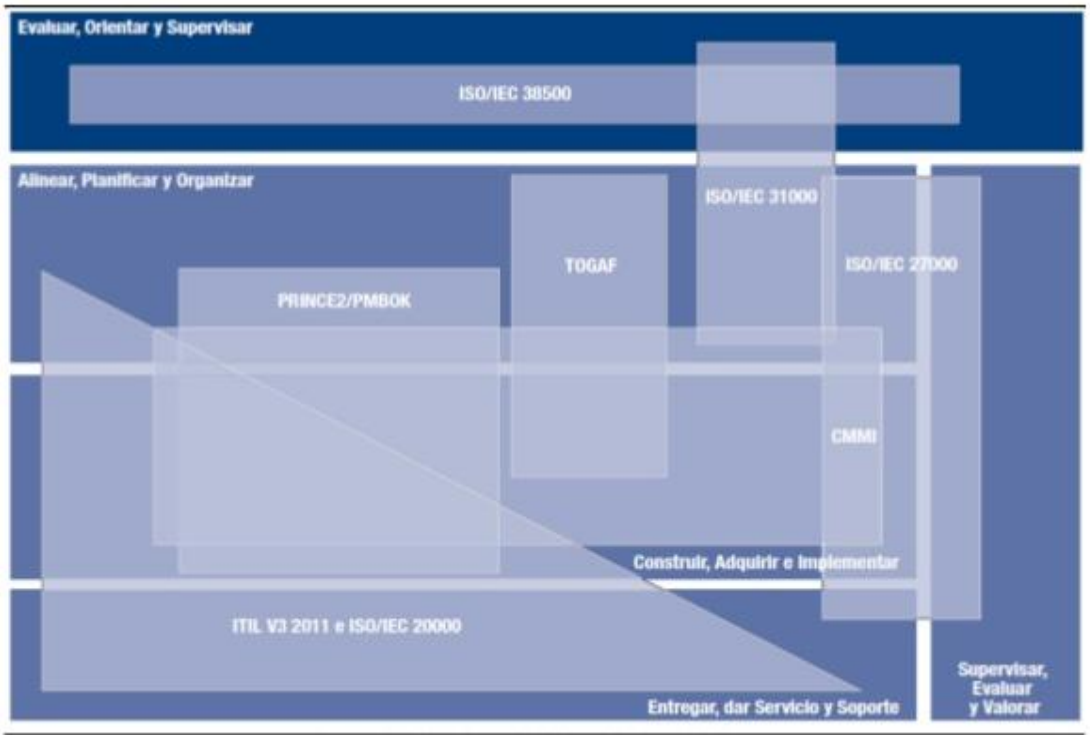


Figura 9. Relación de COBIT con otros estándares
Tomado de (ISACA, 2012)

Los procesos de COBIT que se ajustan a los requerimientos de un SGSI o se complementan con lo ya establecido en el estándar ISO 27001:2013, son los siguientes:

1. Proceso APO13 (Gestionar la Seguridad)

Área: Gestión

Dominio: Alinear, Planificar y Organizar

"Definir, operar y supervisar un sistema para la gestión de la seguridad de la información" (ISACA, 2012):

- ✓ APO13.01 Establecer y mantener un SGSI.
- ✓ APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
- ✓ APO13.03 Supervisar y revisar el SGSI.

2. Proceso DSS05 (Gestionar los Servicios de Seguridad)

Área: Gestión

Dominio: Entrega, Servicio y Soporte

"Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Las metas de este proceso son las siguientes" (ISACA, 2012):

- ✓ DSS05.01 Proteger contra software malicioso.
- ✓ DSS05.02 Gestionar la seguridad de la red y las conexiones.
- ✓ DSS05.03 Gestionar la seguridad de los puestos de usuario final.
- ✓ DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
- ✓ DSS05.05 Gestionar el acceso físico a los activos de TI.
- ✓ DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
- ✓ DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

A continuación, se presenta un resumen de las principales normas, marcos de referencia, marco de trabajo etc., utilizados en este trabajo:

Tabla 3.

Resumen normas, marcos de referencia utilizados

Norma / Marco de referencia	Título de la norma	Versión actual	Emitida por	Descripción
ISO/IEC 27001:2013	Tecnología de la información Sistemas de gestión de la Seguridad de la información – Requisitos	2013-10-25 Segunda edición	Organización Internacional de Normalización (ISO)	Proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información.

Norma / Marco de referencia	Título de la norma	Versión actual	Emitida por	Descripción
ISO/IEC 27002:2013	Tecnología de la Información" – Técnicas de Seguridad – Código de prácticas para los controles de seguridad de la información	2013-10-01 Segunda edición	Organización Internacional de Normalización (ISO)	Establece un catálogo de buenas prácticas que determina, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de los riesgos.
ISO/IEC 27004:2009 y 27004:2016	Tecnología de la Información – Técnicas de Seguridad – Administración de la seguridad de la información, monitoreo, medición, análisis y evaluación	2016-12-15 Segunda Edición	Organización Internacional de Normalización (ISO)	Proporciona directrices para ayudar a las organizaciones a evaluar el desempeño de la seguridad de la información y la eficacia de un sistema de gestión de la seguridad de la información para cumplir con los requisitos de ISO / IEC 27001: 2013.
ISO/IEC 27005:2009	Tecnología de la Información - Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información	2008 – 06	Organización Internacional de Normalización (ISO)	Proporciona directrices para la gestión del riesgo de la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de Seguridad de la Información.
COBIT 5	Marco de Negocio para el gobierno y la gestión de las Tecnologías de la Información de la Empresa	10/ Abril / 2012 Sexta Edición	ISACA (Asociación global sin ánimo de lucro de 140.000 profesionales en 180 países)	COBIT 5 es un marco de referencia que permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

Norma / Marco de referencia	Título de la norma	Versión actual	Emitida por	Descripción
COSO	Committee of Sponsoring Org anizations de la Treadway Commission (COSO) El Comité de Organizaciones Patrocinadoras de la Comisión Treadway	2013 Quinta Edición	Comisión Treadway Organización Voluntaria del sector privado, establecida en Estados Unidos	El Informe C.O.S.O. es un documento que especifica un modelo común de control interno con el cual las organizaciones pueden implantar, gestionar y evaluar sus sistemas de control interno para asegurar que éstos se mantengan funcionales, eficaces y eficientes.

1.6 Metodología de implantación de un SGSI

Para la implantación de un sistema de Gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PDCA (Plan, do, check, act) conocido como “Ciclo de Deming” en su equivalencia en español es Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo puede ser utilizado como un gestor de calidad y de servicios con el objetivo de afinarlos y mantener un proceso de mejora continua o permanente. A continuación se detallan las actividades y objetivos de cada uno de los pasos o fases del ciclo PDCA aplicado a un sistema de gestión de la Seguridad de la Información:

1.6.1 Planificar

En esta fase se debe definir el alcance de un SGSI, como por ejemplo los términos de negocio, la estructura organizacional, los procesos relevantes, los activos y la tecnología que mantiene. Adicionalmente en esta fase se establece la política de seguridad de la información y se determina la metodología de evaluación del riesgo y todos los requisitos que tenga la organización.

Es importante evaluar los controles que la organización mantiene actualmente y su efectividad, ya que esto determinará los controles primarios que deben ser considerados en la implementación (ISOTools Excellence, 2015).

1.6.2 Hacer

En esta fase se debe definir e implementar un plan de tratamiento de riesgos, que debe contar con los recursos, prioridades y responsabilidades para alcanzar los objetivos de control definidos para mitigar los riesgos. Adicionalmente se debe definir un sistema de medición que permita conseguir los resultados esperados de cada objetivo y sean comparables a la hora de medir la eficacia de los controles y por último se gestionan también los programas de concienciación al personal (ISOTools Excellence, 2015).

1.6.3 Verificar

En la fase de verificación la organización debe orientar los esfuerzos en establecer procedimientos de monitoreo y revisión que permitan identificar posibles errores en los resultados obtenidos producto de la implementación de controles de seguridad y el procesamiento propio de la información.
En la fase de verificación también se revisa la efectividad del SGSI basado en lo determinado por la norma ISO 27001 (ISOTools Excellence, 2015).

1.6.4 Actuar

En la fase “Actuar” la organización debe implementar las mejoras identificadas en el SGSI y ejecutar acciones preventivas y correctivas para una adecuada gestión del SGSI, adicionalmente se comunican las acciones y posibles mejoras a las partes interesadas, dichas mejoras deben ser concordantes con los objetivos establecidos en la organización (ISOTools Excellence, 2015).

1.7 Niveles de madurez para el proceso de seguridad de la información

El propósito de un modelo de madurez es el de evaluar la seguridad y sus procesos en una organización y determinar el grado de implementación y desarrollo en el que se encuentra y mediante los resultados obtenidos establecer estrategias que permitan pasar a un grado de madurez óptimo. A continuación, se presenta en la figura 10 un esquema de evaluación de la madurez basado en el modelo CMMI y en la Norma ISO/IEC 17799.

Figura 10. Niveles de Madurez

Adaptado de (Paez, 2015)

Como consecuencia de una iniciativa por mejorar la seguridad de la información con la dirección del marco COBIT, una entidad bancaria de Medio Oriente (HDFC Bank) y su grupo de seguridad de la información (ISG) ha definido 8 atributos deseables para los componentes de la seguridad de la información, adicionalmente se definen los requerimientos necesarios para ubicarse en cada nivel de madurez. El modelo de madurez se basa en el modelo definido en COBIT 4.1 y se encuentra adaptado hacia los parámetros de cumplimiento de un sistema de gestión de seguridad (ISACA, 2014). A continuación, en la tabla 4 se presenta el modelo de madurez con sus componentes para evaluar un sistema de gestión:

Tabla 4.

Modelo de Madurez de la Seguridad de la Información

Columna 1	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Inicial	**En desarrollo**	**Definido**	**Gestionado**	**Optimizado**
Política	Ausencia de política	Política limitada	Política integral definida y publicada	Política publicada e implementada de manera uniforme	Revisión y mejora continuas de la política
Roles y responsabilidades	Roles y responsabilidades no definidos	Roles parcialmente definidos	Roles y responsabilidades bien determinados y definidos	Roles y responsabilidades definidos y ejecutados	Roles y responsabilidades revisados de manera continua
Automatización	Manual	Semiautomatizada	Automatizada	Automatizada y completamente operativa	Actualización permanente de la automatización
Alcance	No implementado	Cobertura limitada	Activos críticos	Completo	Revisión periódica del alcance para garantizar la cobertura total
Eficacia	N/A	Baja	Media	Alta	Muy alta
Gestión de incidentes	Sin seguimiento	Visibilidad limitada	Seguimiento de incidentes críticos	Seguimiento y cierre de todos los incidentes	RCA aplicado a todos los incidentes y solucionados
Medición	Sin medición	Medición limitada	Mediciones integrales definidas	Medido y revisado de forma periódica	Criterios de medición revisados periódicamente
Informes	Sin informes	Informes limitados	Informes definidos	Informes enviados a la alta dirección y revisados	Requerimientos de informes periódicamente revisados y actualizados

Tomado de (ISACA, 2014)

2. Capítulo II: Análisis de la situación actual del manejo de información en la industria de la banca

Durante años la industria de la Banca ha ofrecido servicios y productos con una visión hacia el mercado y sus clientes. En la actualidad las exigencias han sido mayores. Una de las principales preocupaciones que actualmente poseen los Sistemas de Información en la industria bancaria, es proporcionar la información necesaria que exige tanto el negocio corporativo como el de consumo. Por tanto, existe una necesidad de orientar y personalizar los servicios hacia un grupo de clientes más exigentes y que aporten como valor agregado la seguridad de su información y los servicios atados a sus necesidades.

Los sistemas de información actuales han sido desarrollados de tal manera que no permiten cubrir con toda la demanda de información y seguridad que un cliente requiere. El artículo "*Los sistemas de información en las entidades bancarias"* menciona que: "Se observa la falta de información uniforme acerca de la situación integral de todos los productos y servicios que tiene un cliente desde un único punto del sistema, como uno de los principales problemas actuales. Asimismo, es frecuente observar entidades que no poseen en forma integrada la totalidad de sus sistemas periféricos con el sistema central de procesamiento, provocando muchas veces la disponibilidad de datos incompletos e incoherentes de un mismo cliente. Asimismo, entre otros aspectos se destacan las crecientes exigencias normativas a nivel nacional e internacional, las presiones del entorno por minimizar el riesgo crediticio y de inversión, así como también el crecimiento de la competencia de mercado" (Díaz, 2006).

Todos estos aspectos desencadenan una situación actual compleja para el futuro a mediano plazo de los sistemas de soporte al negocio bancario.

La información y su consecuente manejo es fundamental para la industria bancaria en el Ecuador y a nivel internacional; de ahí la importancia de establecer metodologías y procedimientos que permitan identificar posibles

riesgos que comprometan la seguridad de los usuarios y clientes. Un Sistema de Gestión de la información permite identificar riesgos potenciales y centrar los esfuerzos en estrategias de seguridad de la información.

En este capítulo se presenta un análisis de la situación actual de la información enfocada en la industria bancaria y la metodología utilizada para efectuar un análisis y medición de riesgos de información de acuerdo al enfoque mantenido en las normas ISO.

“El propósito de un SGSI es, por tanto, garantizar que los riesgos de seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una manera documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios” (ISO27001.es, 2012) .

Para asegurar que la organización alcance los objetivos de negocio deseados, se deberá enfocar el análisis buscando un balance adecuado entre el manejo de riesgos y los beneficios esperados. Para esto es necesario identificar las actividades más importantes que deben ser desarrolladas, identificar los procesos de principio a fin, establecer un esquema como un todo (forma integral) y determinar los criterios de administración del riesgo, si son mitigados o no.

En la Figura 11 se muestra las relaciones entre los diferentes factores que aumentan o disminuyen los riesgos.

Figura 11. Factores que aumentan o disminuyen los Riesgos

Tomado de (ISO27001.es, 2012)

Las amenazas aprovechan las vulnerabilidades en los sistemas lo que permite exponer a los activos de información los cuales se verían impactados si los riesgos se materializan. Los riesgos marcan requerimientos de seguridad, que imponen el establecimiento de controles, que de ser efectivos permiten proteger de las amenazas.

2.1 Cumplimiento normativo en el Ecuador

La Superintendencia de Bancos y Seguros (SBS) del Ecuador, mediante la resolución N° JB-2005-834 del 20 de octubre de 2005, emitió la norma “De la gestión del Riesgo Operativo”, la cual fue incorporada en el título X, capítulo V de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria y es de aplicación obligatoria para todas las instituciones financieras públicas y privadas. Esta norma tuvo algunas modificaciones, las cuales fueron plasmadas en las resoluciones N° JB-2008-1202, JB-2009-1491, JB-2011-1851, JB-2011-1983, JB-2012-2148 y por último

JB-2014-3066, las mismas que se fueron codificando en el capítulo V de la Gestión de Riesgo Operativo.

En el artículo 21 de la sección VII de la norma que hace referencia a la Seguridad de la Información, se menciona lo siguiente:

“Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos:

21.1 Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información”

Adicionalmente, en el artículo 22 se menciona lo siguiente:

“Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente:

22.1 Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:

22.1.1 Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado;

22.1.2 Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables;

22.1.3 Autorizar los cambios funcionales a las aplicaciones; y,

22.1.4 Monitorear el cumplimiento de los controles establecidos

22.2 Identificar y documentar los requerimientos mínimos de seguridad para cada tipo de información, con base en una evaluación de los riesgos que enfrenta la institución, aplicando la metodología de gestión de riesgo operativo de la entidad; y, con los controles de seguridad de la información;

22.3 Establecer procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios;

22.4 Mantener segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización;

22.5 Definir los procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e incluyan los cambios emergentes;

22.6 Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio;

22.7 Determinar los sistemas de control y autenticación tales como: sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica;

22.8 Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las instituciones deben definir y ejecutar planes de

acción sobre las vulnerabilidades detectadas;
22.9 Controles 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 malicioso;
22.10 Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros;
22.11 Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios;
22.12 Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;
22.13 Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades,
22.14 Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible;
22.15 Considerar en la definición de requerimientos para nuevos sistemas o mantenimiento, aquellos relacionados con la seguridad de la información;
22.16 Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución;
22.17 Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información; y,

22.18 Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fin de tomar acciones orientadas a mejorarlo" (Superintendencia de Bancos y Seguros, 2014).

Por tanto, el establecimiento de un SGSI actualmente es un requisito obligatorio en la industria bancaria en el Ecuador, y de ahí la importancia de que las instituciones del sistema financiero encaminen sus actividades hacia el cumplimiento de lo requerido en dicha normativa, y no sea un proceso estático sino que debe encontrarse en un ciclo de evaluación y mejora continua.

En la tabla 5 se muestra una síntesis de los artículos de la norma de Riesgo operativo establecida por el ente de control y determinado para cumplimiento obligatorio de las entidades financieras del Ecuador en el **ámbito de la gestión de la seguridad de la información**. Adicionalmente se efectuó un mapeo de dichos artículos con las 35 categorías de seguridad del Anexo "A" (objetivos de control) establecidas en la norma ISO 27001:2013. De esto se puede concluir que todos los requerimientos establecidos por la Superintendencia de Bancos se encuentran contemplados en los objetivos de control de la norma ISO. A continuación, se muestra el detalle:

Tabla 5.

Síntesis del requerimiento normativo vs los objetivos establecidos por la ISO 27002

ARTICULOS PARA EL CUMPLIMIENTO NORMATIVO EN EL ECUADOR		ISO 27002:2013
Art.	**Resumen del artículo de la norma de Riesgo Operativo de la SBS**	**Objetivo de Control relacionado**
21.1	Determinar funciones y responsables de la implementación y administración de un SGSI	A.6.1 Organización Interna
22.1	Disponer de un inventario de la información con propietarios y sus respectivas responsabilidades, clasificar la información en términos de su valor, autorizar los cambios funcionales y monitorear el cumplimiento de los controles	A.8.1 Responsabilidad por los activos A.8.2 Clasificación de la información
22.2	Identificar los requerimientos mínimos de seguridad en base a una evaluación de riesgos	A.8 Administración de Activos
22.3	Procedimientos de eliminación de la información crítica de forma segura	A.8.3 Manejo de los Medios
22.4	Mantener segregación de funciones y responsabilidades en la modificación de los activos de la organización	A.6.1 Organización Interna
22.5	Definir procedimientos de gestión de cambios en activos y su registro incluyendo cambios de tipo emergente.	A.12.1 Procedimientos operacionales y responsabilidades
22.6	Establecer procedimientos de afectación directa a las bases de datos que incluya el registro de los solicitantes, autorizadores y motivo	A.12.1 Procedimientos operacionales y responsabilidades
22.7	Determinar los sistemas de control y autenticación para evitar accesos no autorizados	A.12.2 Protección contra código malicioso
22.8	Gestionar la realización de auditorías de seguridad de la infraestructura tecnológica	A.18.2 Revisiones de seguridad de la información
22.9	Controles para detectar y evitar la instalación de software no autorizado	A.12.5 Control del Software de Operación
22.10	Medidas para proteger la información contenida en: medios de almacenamiento u otros	A.5.1 Orientación de la dirección para la seguridad de la información A.8.2 Clasificación de la información
22.11	Procedimiento para el control de accesos a la información, administración de derechos y perfiles para el registro, eliminación y modificación de la información	A.9.2 Gestión de acceso del usuario
22.12	Procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos no autorizados	A.9.1 Requisitos de Negocio para el control de acceso
22.13	Procedimientos para contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren cambios críticos	A.12.1 Procedimientos operacionales y responsabilidades
22.14	Aplicar técnicas de encriptación sobre información crítica o sensible	A.10.1 Controles Criptográficos
22.15	Considerar en la definición de requerimientos para nuevos sistemas aquellos relacionados con la seguridad de la información	A.6.1 Organización Interna
22.16	Establecer procedimientos de gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras
22.17	Definir un sistema de registros históricos que permitan verificar el cumplimiento de políticas, procedimientos, procesos y controles	A.18.2 Revisiones de seguridad de la información
22.18	Evaluar periódicamente el desempeño del sistema de gestión de la seguridad	A.18.2 Revisiones de seguridad de la información

2.2 La evaluación de riesgo según la norma ISO 27001:2013

La norma ISO 27001:2013 determina que la organización debe establecer un proceso para evaluar el riesgo, en donde se determinen los criterios para la aceptación y evaluación del riesgo de la seguridad.

Además la evaluación debe proporcionar resultados válidos y consistentes que estén asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información dentro del alcance establecido en el SGSI.

Una vez evaluados se debe identificar a los propietarios o responsables directos del riesgo, evaluar las posibles consecuencias y la probabilidad de su ocurrencia.

La Organización debe conservar la documentación que sustenta el proceso de evaluación de riesgo (ISO/IEC 27001, 2013).

2.3 Gestión, análisis y evaluación de riesgos de la Información

Las organizaciones hoy en día, en especial aquellas empresas que dependen de sus sistemas de información para garantizar transacciones seguras con sus clientes, enfrentan distintas amenazas que muchas veces llegan a explotar vulnerabilidades, por tanto, el riesgo se encuentra presente en toda actividad y se podrían ver comprometidos los pilares de la seguridad como son: la confidencialidad, integridad y disponibilidad de la información.

El riesgo puede incrementar cuando los objetivos difieren del desempeño esperado o cuando ocurren cambios en la organización.

Una definición clara de objetivos permite la identificación y evaluación de los riesgos relacionados, por tanto, los objetivos deben contar con las características “SMART” y ser establecidos en todos los niveles de la organización (COSO, 2013).

S = Específico,

M = Medible,

A = Alcanzable,

R = Relevante y

T= Temporal

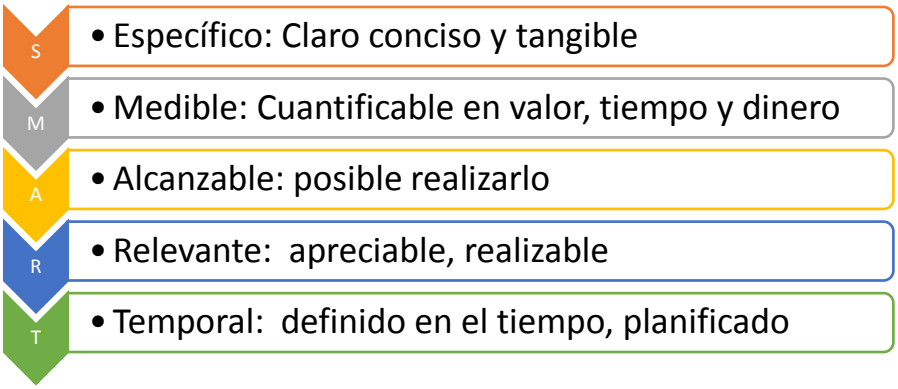


Figura 12. Características de los Objetivos Smart
Adaptado de (T.Doran, 2016)

Al operar dentro de un rango de tolerancia al riesgo se permite a la Dirección una mayor confianza de que la organización logrará sus objetivos.
La tolerancia al riesgo puede afectar el nivel de los recursos asignados para la consecución de los objetivos (COSO, 2013).
La Dirección deberá, en base a los objetivos estratégicos del negocio y la evaluación de riesgos, definir el apetito al riesgo, el cual es la cantidad de riesgo que la organización está dispuesta a asumir, y la tolerancia al riesgo es el nivel aceptable de variación del desempeño en relación con la consecución de los objetivos.
El análisis de riesgos es la base fundamental de un SGSI. Es la actividad que nos va a proporcionar resultados de dónde residen los problemas actuales o potenciales que requiere de atención inmediata para lograr un nivel esperado de seguridad. De acuerdo a la ISO 27001 el análisis de riesgos debe ser proporcionado a la naturaleza y valoración de los activos y de los riesgos a los que los activos se encuentran expuestos. La valoración del riesgo debe identificar las amenazas que pueden comprometer los activos, su vulnerabilidad e impacto en la organización, determinando el nivel del riesgo.

El proceso de evaluación del riesgo se lo debe iniciar una vez que se ha realizado la identificación de todos los activos de información comprendidos en el alcance determinado por la organización. La norma ISO 27001 exige efectuar de manera disciplinada y sistemática un análisis y evaluación del

riesgo de los activos identificados para determinar cuáles son aquellos que deben ser protegidos para mitigar su riesgo, y por tanto, obtener mediante la aplicación de controles el riesgo residual o nivel de riesgo aceptado por la empresa (ISO/IEC 27002, 2013)

La gestión del riesgo debe formar parte de todas las actividades del SGSI, y debe ser aplicado en la implementación y posteriormente en los procesos de mejora continua. El proceso de gestión del riesgo de la seguridad de la información puede ser aplicable a toda una organización o de ser el caso a una parte de ella (ISO/IEC 27005, 2009).

A continuación, se efectuará una descripción de los pasos a seguir para la gestión del riesgo.

2.3.1 Visión general del proceso de gestión del riesgo de la seguridad de la información

La gestión del riesgo de la seguridad de la información consta de las siguientes fases o procesos:

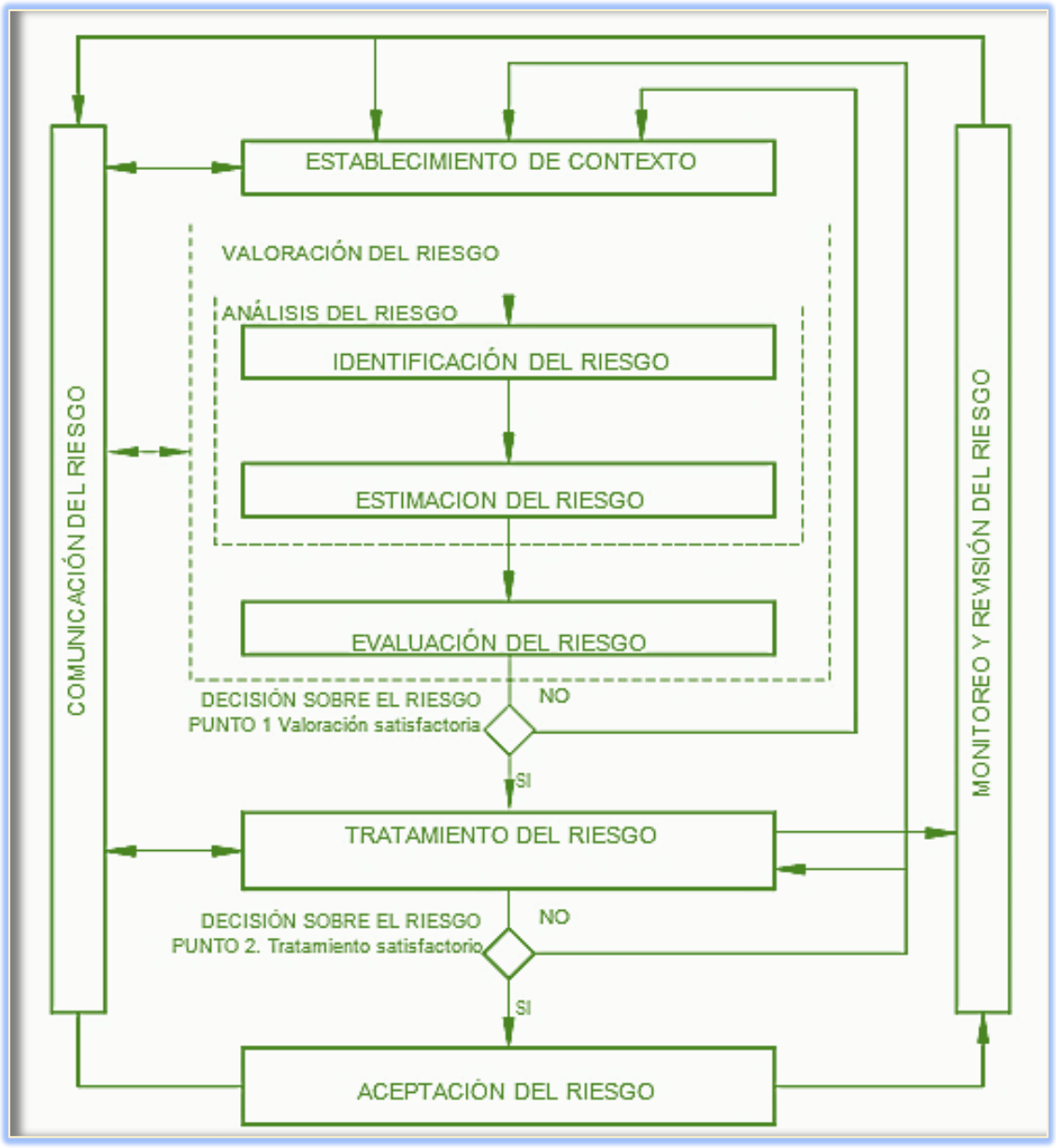


Figura 13. Proceso de Gestión del Riesgo de la Seguridad de la información

Tomado de (ISO/IEC 27005, 2009)

En la figura se ilustra el proceso para la gestión del riesgo que inicia con el establecimiento del contexto en donde se va a evaluar el riesgo y posteriormente se realiza la valoración; si la información es pertinente y suficiente para tomar una decisión sobre el riesgo se procede a determinar su, como se ve en la figura el proceso puede ser repetitivo para la valoración y el

tratamiento de riesgo, esto permitirá un nivel de detalle mayor en cada iteración y se obtendrá una valoración más precisa de los riesgos.

La aceptación del riesgo debe garantizar que los riesgos residuales son aceptados por la alta gerencia especialmente en aquellos en los cuales la implementación de un control no está considerada.

Es importante mencionar que los pasos para la gestión del riesgo: contextualización, valoración, tratamiento y aceptación forman parte de la fase de planificación del ciclo “PDCA” para la implementación de un SGSI, en la fase “Do” o hacer se implementa el plan de tratamiento del riesgo, en la fase “Check” o verificar se realiza un monitoreo y revisión permanente del riesgo y por último en la fase “Act” o actuar se efectúan mejoras del proceso de gestión del riesgo (ISO/IEC 27005, 2009). A continuación se explica de manera detallada cada uno de los pasos para la gestión del riesgo.

2.3.2 Establecimiento del Contexto

El establecimiento del contexto engloba determinar los criterios necesarios para la gestión del riesgo, así como su alcance, límites, etc., para establecer el contexto es válido tomar toda la información que fuese oportuna sobre la organización, algunos de los criterios que deben definirse son los siguientes:

2.3.2.1 Criterios de Evaluación del Riesgo

La norma ISO recomienda considerar los siguientes aspectos:

- El valor estratégico de la información
- La criticidad de los activos de información
- Los requisitos legales, normativos y contractuales
- La disponibilidad, confidencialidad e integridad para las operaciones.
- Los requerimientos de las partes interesadas y el impacto negativo en la imagen (ISO/IEC 27005, 2009).

2.3.2.2 Criterios de Impacto

El impacto del riesgo se debe especificar respecto del daño o costos que puede ocasionar a la entidad, la norma recomienda considerar los siguientes aspectos:

- Nivel de clasificación de los activos impactados
- Pérdida de la confidencialidad, integridad o disponibilidad
- Deterioro de operaciones
- Afectaciones al negocio o las finanzas
- Modificación de planificaciones
- Afectación a la imagen o reputación
- Incumplimiento de requerimientos legales, normativos o contractuales (ISO/IEC 27005, 2009).

2.3.2.3 Criterios de la aceptación del riesgo

La organización debe definir los criterios para la aceptación del riesgo que muchas veces dependen de los objetivos y decisiones estratégicas de la organización y de las partes interesadas. Se puede determinar una escala cuantitativa para establecer los niveles. La norma recomienda considerar los siguientes aspectos:

- Los criterios deben incluir los niveles del riesgo deseable que la organización está dispuesta aceptar.
- Los criterios podrían entenderse como la relación entre el beneficio esperado y el riesgo estimado.
- Los criterios pueden incluir ciertos requerimientos de tratamiento a futuro o por un tiempo definido (ISO/IEC 27005, 2009).

2.3.3 Valoración del Riesgo de la Seguridad de la Información

La valoración del riesgo permite obtener una calificación que puede ser cuantitativa o cualitativa del riesgo cuyo resultado proporciona información relevante para la toma de decisiones o la priorización de riesgos. La valoración del riesgo establece el valor de los activos de información, identificando amenazas y vulnerabilidades, identifica los controles y sus

efectos en el riesgo que ha sido identificado, analiza las posibles consecuencias y, por último, prioriza los riesgos resultantes respecto de los criterios de evaluación del riesgo establecidos (ISO/IEC 27005, 2009). La valoración de riesgos consta de las siguientes actividades:

2.3.3.1 Análisis del Riesgo

a. Identificación del Riesgo.- tiene como objetivo establecer las causas de una pérdida y por qué o cómo podría ocurrir, dentro de la identificación del riesgo se encuentran las siguientes actividades:

- **Identificación de los activos:** los activos de una organización deben considerarse e identificarse tomando en consideración todos los tipos de activos que pueden existir en una organización, cuáles son sus responsables o propietarios y deben ser descritos con un nivel de detalle adecuado. La determinación de los activos, su inventario y clasificación se amplía en el capítulo III literal 3.2 de este trabajo.

- **Identificación de las amenazas:** para identificar las amenazas a los activos de información se puede utilizar como un insumo el inventario de incidentes que mantenga una organización, catálogos o guías de amenazas y la información que puede proporcionar los propietarios o custodios del activo. Una amenaza de acuerdo a la ISO puede ser interna o externa, y ser generada de forma intencional o deliberada.

  A continuación se presenta en la tabla 6 algunos ejemplos de amenazas comunes, clasificadas de acuerdo a su origen en deliberadas, accidentales y ambientales de acuerdo a la norma ISO 27005.

Tabla 6.

Ejemplos de Amenazas

TIPO	AMENAZAS	ORIGEN		
		Accidentales	Deliberadas	Ambientales
Daño físico	Fuego	✓	✓	✓
	Daño por agua	✓	✓	✓
	Contaminación	✓	✓	✓
	Accidente importante	✓	✓	✓
	Destrucción del equipo o los medios	✓	✓	✓
	Polvo, corrosión, congelamiento	✓	✓	✓
Eventos naturales	Fenómenos climáticos			✓
	Fenómenos sísmicos			✓
	Fenómenos volcánicos			✓
	Fenómenos meteorológicos			✓
	Inundación			✓
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	✓	✓	
	Pérdida de suministro de energía	✓	✓	✓
	Falla en el equipo de telecomunicaciones	✓	✓	
Perturbación debida a la radiación	Radiación electromagnética	✓	✓	✓
	Radiación térmica	✓	✓	✓
	Impulsos electromagnéticos	✓	✓	✓
Compromiso de la información	Interceptación de señales de interferencia comprometedoras		✓	
	Espionaje remoto		✓	
	Escucha encubierta		✓	
	Hurto de medios o documentos		✓	
	Hurto de equipo		✓	
	Recuperación de medios reciclados o desechados		✓	
	Divulgación	✓	✓	
	Datos provenientes de fuentes no confiables	✓	✓	
	Manipulación con hardware		✓	
	Manipulación con software	✓	✓	
	Detección de la posición		✓	

TIPO	AMENAZAS	ORIGEN		
		Accidentales	Deliberadas	Ambientales
Fallas técnicas	Falla del equipo	✓		
	Mal funcionamiento del equipo	✓		
	Saturación del sistema de información	✓	✓	
	Mal funcionamiento del software	✓		
	Incumplimiento en el mantenimiento del sistema de información	✓	✓	
Acciones no autorizadas	Uso no autorizado del equipo		✓	
	Copia fraudulenta del software		✓	
	Uso de software falso o copiado	✓	✓	
	Corrupción de los datos		✓	
	Procesamiento ilegal de los datos		✓	
Compromiso de las funciones	Error en el uso	✓		
	Abuso de derechos	✓	✓	
	Falsificación de derechos		✓	
	Negación de acciones		✓	
	Incumplimiento en la disponibilidad del personal	✓	✓	✓

Adaptado de (ISO/IEC 27005, 2009)

- **Identificación de los controles existentes:** Es importante identificar los controles que existen o se encuentran implementados en la organización, esto permitirá definir los riesgos que no requieren de un control o también si el control es efectivo o requiere de un nuevo diseño o de un control complementario. Si el control no se encuentra adecuadamente definido o su funcionamiento no es el óptimo puede generar vulnerabilidades. Una manera en la cual se puede estimar la eficacia del control es validando si está reduciendo la probabilidad de ocurrencia o la factibilidad para explotar alguna vulnerabilidad o también si el impacto es menor, los cuales son los dos factores (impacto, probabilidad) que determinan el riesgo. Como resultado se debería obtener un listado de controles existentes y planificados, su avance o implementación y el activo al cual están protegiendo (ISO/IEC 27005, 2009).

- **Identificación de las vulnerabilidades:** como un input para identificar las vulnerabilidades se puede utilizar la lista de amenazas, los activos y los controles implementados o existentes. Las vulnerabilidades pueden estar presentes en varias instancias como por ejemplo en: procesos, tecnología (hardware y software), personas, entes externos, etc. La vulnerabilidad no causa un daño o impacto por sí sola, debe existir una amenaza que explote dicha vulnerabilidad, de no existir dicha amenaza podría no requerir la implementación de un control. Se debe considerar también, que un control que no es efectivo o se encuentra incorrectamente implementado puede convertirse en una vulnerabilidad (ISO/IEC 27005, 2009).

  En el anexo 1 se muestran algunos ejemplos de vulnerabilidades y posibles amenazas que podrían explotar dichas vulnerabilidades.

- **Identificación de las consecuencias:** se debe evaluar las posibles consecuencias que podría sufrir un activo al encontrarse comprometida su integridad, confidencialidad y disponibilidad, por tanto se deben identificar los posibles escenarios en donde se hagan presentes los incidentes de seguridad que describe a la amenaza que explota una o varias vulnerabilidades. Para poder determinar la importancia o impacto del escenario se debe considerar los criterios establecidos en los puntos 2.3.1.1 en el establecimiento del contexto. Como resultado de este análisis se debe obtener una lista de escenarios de incidentes con sus consecuencias en los activos y los procesos de negocio (ISO/IEC 27005, 2009).

b. **Estimación del Riesgo.-** La estimación del riesgo puede ser cualitativa o cuantitativa dependiendo del nivel de detalle y de las circunstancias en que se conozcan las vulnerabilidades y los incidentes. Un análisis cualitativo se utiliza generalmente para obtener una visión general y amplia del riesgo, posteriormente se realiza una evaluación cuantitativa para obtener un nivel más específico de estimación del riesgo. Las

estimaciones y la forma de análisis deben ser congruentes con los criterios de evaluación que se han establecido. Para una estimación cualitativa pueden utilizarse adjetivos como alta, media o baja para determinar sus consecuencias o la probabilidad de ocurrencia; si bien esta metodología es de fácil comprensión, muchas veces puede resultar un tanto subjetiva, en cambio para la estimación cuantitativa se utilizan valores numéricos para describir tanto el impacto como la probabilidad. Una desventaja de este método generalmente puede darse en la falta de información de los datos en los cuales esté basado la calificación (ISO/IEC 27005, 2009).

- **Valoración de las consecuencias:** en esta actividad se evalúa el impacto de las consecuencias en el negocio que son producto de posibles incidentes en la seguridad de la información. El valor del impacto puede ser mostrado de forma cualitativa o cuantitativa siempre que proporcione información para la toma de decisiones. La valoración de acuerdo a la norma ISO 27005 se determina utilizando dos medidas:
  - "El valor de reemplazo del activo
  - Las consecuencias para el negocio por la pérdida o compromiso de los activos (ISO/IEC 27005, 2009)".

- **Valoración de los incidentes**: en esta actividad se evalúa la probabilidad de los escenarios de incidentes y el impacto al negocio en caso que sucedieran. Para valorar los incidentes se debería tomar en cuenta la frecuencia de ocurrencia de la amenaza y la factibilidad de explotación de las vulnerabilidades.

- **Nivel de estimación del riesgo:** la estimación del riesgo resulta de una combinación de la probabilidad de ocurrencia de un escenario y sus consecuencias o impacto al negocio asignando valores que pueden ser de índole cualitativa o cuantitativa.

2.3.3.2 Evaluación del Riesgo

En la evaluación se efectúa una comparación de los niveles de riesgo versus los criterios definidos en el establecimiento del contexto de la evaluación del riesgo y su aceptación. Generalmente las determinaciones se basan en el nivel de aceptación o tolerancia al riesgo, sin embargo es importante también considerar el impacto, probabilidad y la identificación y análisis del riesgo. Cuando existen varios grupos de riesgos en un nivel “bajo o medio” podrían convertirse en riesgos altos que deben ser considerados y requieran de tratamiento (ISO/IEC 27005, 2009). Para la evaluación del riesgo es importante considerar:

- La importancia de un criterio para la organización.- por ejemplo para una entidad de la vertical bancaria es imprescindible que los riesgos sean evaluados en base a la preservación de la confidencialidad, integridad y disponibilidad de la información, siendo los pilares necesarios que las entidades deben garantizar a sus clientes.
- La relevancia de los procesos o procedimientos del negocio, por ejemplo para una entidad de la vertical bancaria se deberían abordar los procesos relacionados con la gestión de productos y servicios en: la apertura e instrumentación, gestión comercial, administración transacciones / requerimientos y gestión de soporte.

A continuación se presenta un método para valorar los riesgos basados en la norma ISO, que combina aspectos cualitativos y cuantitativos dependiendo de su definición:

Se va a considerar una valoración cuantitativa del activo en una escala de 0 a 4 cuando el caso permita la aplicación de criterios numéricos, existirán casos como la preservación de la vida humana la cual no es posible realizar una valoración cuantitativa.

Se determinará la probabilidad de la ocurrencia de la amenaza estableciendo cuestionarios que afecten a los grupos de activos donde la amenaza se hace presente, cada respuesta añade un valor o puntaje, que posteriormente se acumularán y serán comparados con los rangos establecidos, la escala determinada para el nivel de ocurrencia de la amenaza quedaría en **alto,**

medio y bajo y así mismo para la facilidad de explotación de la vulnerabilidad.

Tabla 7.

Matriz con valores predefinidos para la relación entre el valor del activo, la probabilidad de ocurrencia y la facilidad de explotación

	Probabilidad de ocurrencia - Amenaza	**Baja**			**Media**			**Alta**		
	Facilidad de explotación	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Valor del activo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Adaptado de (ISO/IEC 27005, 2009)

En el ejemplo de la tabla 7 se determina una estimación cuantitativa en base al valor del activo, evaluando la probabilidad de ocurrencia de la amenaza versus la facilidad de explotación de la vulnerabilidad, por tanto si un activo tiene un valor para la organización de “4” en base a criterios de seguridad de la información, la amenaza es “media” y la facilidad de explotación de la vulnerabilidad es “alta”, la medida del riesgo sería de 7.

Una vez que se tiene una medida de riesgo pertinente, se determina la estimación del riesgo que como se dijo anteriormente resulta de la combinación de la probabilidad de ocurrencia por el impacto esperado en el negocio. “La probabilidad de un escenario de incidente está dada por una amenaza que explota una vulnerabilidad con una probabilidad determinada” (ISO/IEC 27005, 2009). En la siguiente tabla se muestra dicha probabilidad en base al impacto en el negocio determinado por el escenario del incidente:

Tabla 8.

Estimación del Riesgo en base al impacto y a la probabilidad

	Probabilidad del escenario de incidente	Muy baja (muy improbable)	Baja (improbable)	Media (Posible)	Alta (Probables)	Muy alta (Frecuente)
Impacto en el negocio	Muy baja	0	1	2	3	4
	Baja	1	2	3	4	5
	Media	2	3	4	5	6
	Alta	3	4	5	6	7
	Muy alta	4	5	6	7	8

Adaptado de (ISO/IEC 27005, 2009)

Tabla 9.

Valoración del nivel de riesgo

NIVEL	SIMBOLOGÍA	RANGO
BAJO	A	De 0 - 2
MEDIO	M	De 3 - 5
ALTO	B	De 6 a 8

Adaptado de (ISO/IEC 27005, 2009)

Del análisis se obtiene un mapa de calor en el cual las valoraciones de riesgo que se encuentran en verde corresponden a un riesgo bajo (0 a 2), las puntuaciones en celeste a un riesgo medio (3 a 5) y las puntuaciones en naranja a un riesgo alto (6 a 8). La decisión para la gestión del riesgo se encontrará determinada por el nivel de tolerancia al riesgo que la organización se encuentra dispuesta aceptar.

2.4 Tratamiento del riesgo de la seguridad de la información

Existen 4 acciones para gestionar el tratamiento del riesgo de la seguridad de la información y son: i) reducir el riesgo, ii) aceptar el riesgo, iii) evitar el riesgo y iv) transferir el riesgo. La siguiente figura detalla la gestión del tratamiento del riesgo dentro de un SGSI:

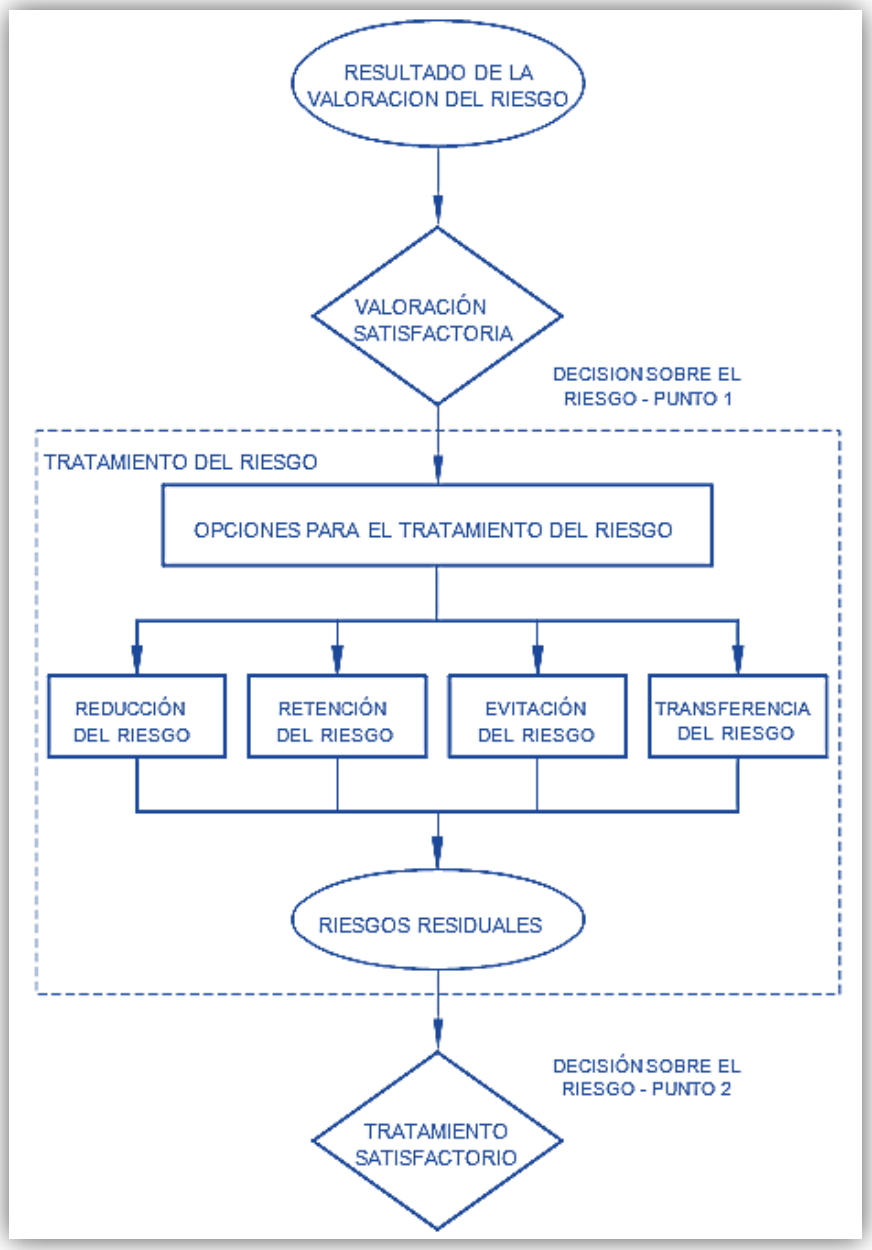


Figura 14. Gestión del Tratamiento del Riesgo

Tomado de (ISO/IEC 27005, 2009)

Es posible realizar más de una acción al momento de gestionar un riesgo, es decir se podría aplicar controles que reduzcan la probabilidad y el impacto del riesgo y transferir el riesgo residual a un tercero. El plan de tratamiento de riesgo debe identificar claramente el orden prioritario para la implementación de cada tratamiento, dicho orden puede ser establecido en base a la clasificación del riesgo y a un estudio de costo y beneficio, es responsabilidad

de la alta gerencia establecer concordancia entre los costos de implementación de controles y el presupuesto (ISO/IEC 27005, 2009).

Posterior a determinar el plan de tratamiento de los riesgos se debe evaluar el riesgo que permanece a pesar de la aplicación de los controles (riesgo residual), se lo puede efectuar con una iteración nueva de la valoración del riesgo comparando con los efectos esperados del tratamiento.

2.4.1 Reducir el riesgo

Dicha acción determina que el riesgo debe reducirse mediante la selección e implementación de controles, de tal manera que el riesgo residual se pueda considerar aceptable para la organización (ISO/IEC 27005, 2009).

2.4.2 Aceptar el riesgo

Dicha acción determina que de acuerdo a la evaluación del riesgo la organización acepta el riesgo. Por tanto si el nivel del riesgo cumple con los criterios establecidos no es requerida la implementación de criterios adicionales (ISO/IEC 27005, 2009).

2.4.3 Evitar el riesgo

Dicha acción significa que la organización decide evitar el riesgo mediante la omisión de alguna actividad, proceso, etc. o mediante la modificación de condiciones sobre las que se realiza una actividad. Cuando el riesgo es considerado alto o extremo y las acciones para controlarlo no son factibles en presupuesto o recursos se puede evaluar o considerar evitar el riesgo (ISO/IEC 27005, 2009).

2.4.4 Transferir el riesgo

La acción de transferir el riesgo comprende una decisión para compartir con terceros el riesgo, por tanto se puede contratar servicios con externos cuya función será la de gestionar o monitorear el proceso o sistema en donde se encuentre el riesgo y tomar decisiones frente a un posible ataque. Es importante considerar que se puede transferir la administración del riesgo, más

no es posible transferir la responsabilidad del impacto en caso de suscitarse un incidente (ISO/IEC 27005, 2009).

2.5 Aceptación del riesgo de la seguridad de la información

Es necesario que se registre de manera formal la decisión de aceptar el riesgo y las respectivas responsabilidades. Los responsables deberán revisar y aprobar los planes individuales para el tratamiento del riesgo y verificar el riesgo remanente o residual. Pueden existir ocasiones en los cuales los responsables acepten riesgos que no cumplan con los criterios de aceptación definidos, dichos casos deben encontrarse con la justificación respectiva y encontrarse documentados (ISO/IEC 27005, 2009).

2.6 La implementación de Controles

En la versión ISO/IEC 27002:2013 se incluyen 114 controles, los cuales se encuentran divididos en los siguientes objetivos:

- Políticas de seguridad de la información
- Controles operacionales

A cada punto de control se le debe asociar un rango o factor determinado. La organización debe decidir qué tipo de rango se requiere para evaluar el control que necesita, teniendo en cuenta que los controles de carácter preventivo son más eficaces que los correctivos.
El concepto de control en esta norma se debe considerar como un conjunto de medidas, acciones y/o documentos que permiten cubrir o auditar ciertos riesgos (ISO/IEC 27002, 2013).

2.7 Enunciado de aplicabilidad

De acuerdo a la norma ISO 27001 un enunciado de aplicabilidad es un documento en el cual deben documentarse los objetivos de control y los controles seleccionados, así como las razones para su selección. También debe registrarse la exclusión de cualquier objetivo de control y controles enumerados en el Anexo A.

Según lo expresado por la 27001 Academy (2011) “La declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información. El objetivo del documento es definir cuáles de los 114 controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 son los que usted implementará y para los controles que correspondan, cómo se realizará su implementación” (Kosutic, ISO 27001/ISO 22301 Base de conocimientos, 2015).

Dicho enunciado sirve para mostrar a terceros la racionalidad al haber seleccionado los objetivos de control y los controles para mitigar o disminuir los riesgos encontrados.

3. Capítulo III: Identificación de los requerimientos para la gestión de la seguridad de la información

La ISO/IEC 27001 menciona la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una entidad.

Además menciona que para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia el resultado de un proceso constituye directamente la entrada del proceso siguiente.

La aplicación de un sistema de procesos dentro de una organización, con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un “enfoque basado en procesos” (Turmero, 2014).

“El enfoque basado en procesos para la gestión de la seguridad de la información presentada en la norma ISO/IEC 27001, estimula a sus usuarios en la importancia de:

a) Comprender los requisitos de seguridad de la información del negocio y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;

b) Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;
c) El seguimiento y revisión del desempeño y eficacia del SGSI, y;
d) La mejora continua basada en la medición de objetivos" (ISO/IEC 27001, 2013).

Para el desarrollo de esta tesis se adoptará el modelo de mejora continua "Planificar-Hacer-Verificar-Actuar" para estructurar todos los procesos del SGSI; a pesar de que en la última versión de la norma se elimina el "enfoque a procesos" se adoptará dicho modelo puesto que la gestión en seguridad engloba un conjunto de procesos que a su vez ejecutan actividades encaminadas a resultados.

La Figura 15 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas y mediante las acciones y procesos requeridos obtiene resultados de seguridad de la información que cumplen dichos requisitos y expectativas.

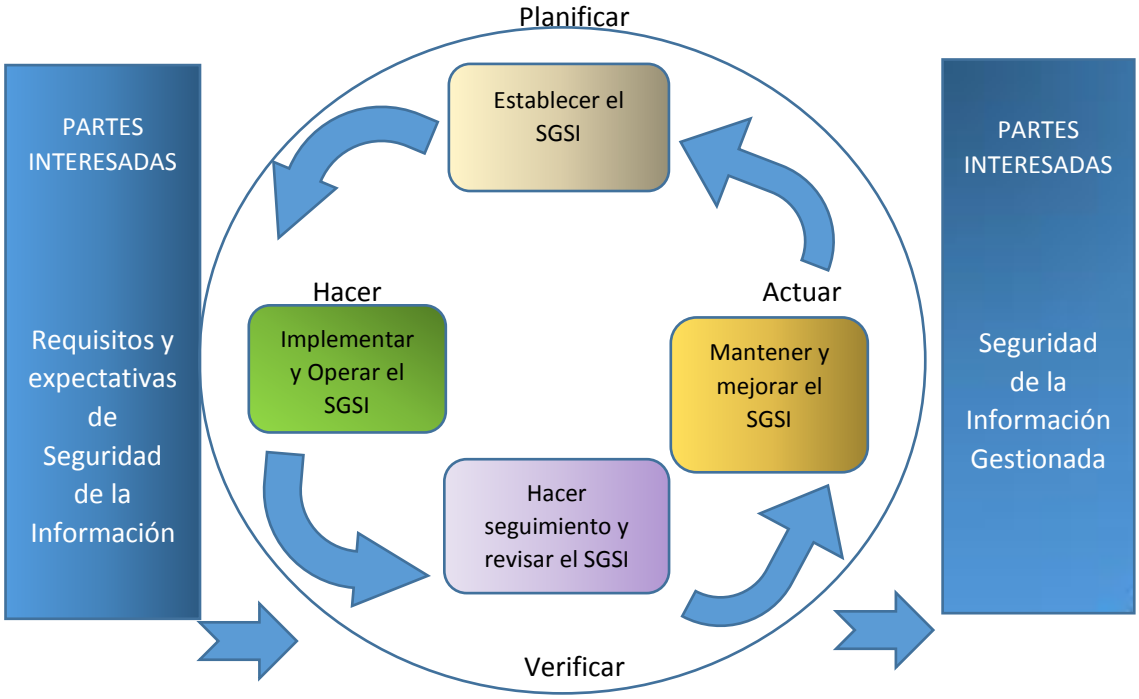


Figura 15. Modelo PHVA aplicado a los procesos de SGSI

Adaptado de (Oficina de Seguridad para las redes informáticas, 2013)

Un ejemplo de un requisito de seguridad sería que los ataques efectuados a la seguridad de la información no causen daño económico severo a una organización.

Un ejemplo de una expectativa de seguridad podría ser que si ocurre un incidente de seguridad, como por ejemplo un ataque al sitio Web de la organización, exista el suficiente recurso humano con capacitación en los procedimientos apropiados que minimice el impacto.

La siguiente tabla muestra los objetivos generales de cada fase de la implementación de un SGSI conforme el modelo PHVA (Planificar, Hacer, Verificar y Actuar).

Tabla 10.

Objetivos de las fases de la implementación de un SGSI con la metodología PHVA

Planificar (Establecer el SGSI).	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de una organización
Hacer (Implementar y operar el SGSI)	Implementar y Operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (Hacer seguimiento y revisar el SGSI)	Evaluar y, en donde sea aplicable, medir el rendimiento del proceso contra la política, sus objetivos y experiencia práctica e informar los resultados a la dirección para gestionar su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y de revisión de gestión u otra información relevante, para lograr la mejora continua del SGSI.

Adaptado de (Oficina de Seguridad para las redes informáticas, 2013)

3.1 Requisitos Generales

Los requisitos que establece la norma ISO para la implementación de un SGSI pretenden ser de carácter genérico y aplicable a todo tipo de organización,

independiente de su estructura, tipo de servicio, etc. Cuando una entidad ha determinado su conformidad con la normativa, no es aceptable la eliminación de cualquier requisito. Cuando se exceptúa la implementación de algún control que mitiga un riesgo identificado en la entidad, es necesario justificar y obtener evidencia necesaria para garantizar que el riesgo ha sido asumido por la entidad o considerado en el apetito de riesgo de la organización (ISO/IEC 27001, 2013).

“La organización debe establecer, implementar, mantener y mejorar un SGSI documentado, en el contexto de las actividades del negocio y de los riesgos que enfrenta” (ISO/IEC 27001, 2013).

Es necesario que el Sistema de Gestión de Seguridad de la Información sea constituido como parte de los procesos de la entidad y que la seguridad en la información forme parte de los requerimientos al momento de diseñar procesos, establecer controles o sistemas de información.

A continuación, se resume los requisitos para la implementación de un SGSI en base a la norma ISO 27001:2013, haciendo énfasis en aquellos requerimientos imprescindibles para las organizaciones pertenecientes a la industria bancaria. Para ciertos requisitos se explicará de forma detallada en el capítulo IV en la propuesta del modelo de implementación para un SGSI.

3.1.1 Conforme al Contexto de la Organización

i) La entidad debe identificar las situaciones tanto internas como externas que podrían afectar la capacidad para lograr los resultados al momento de implementar un SGSI y que son relevantes para el cumplimiento de los objetivos.
ii) La entidad debe identificar a las partes interesadas que son oportunas para la implementación de un SGSI así como sus requerimientos, los cuales podrían incluir entre otros, requisitos legales o regulatorios, obligaciones con proveedores, etc.
iii) La entidad debe determinar el alcance que tendrá el SGSI, estableciendo los límites y el ámbito de aplicabilidad del sistema de gestión,

considerando lo establecido en el punto (i) y (ii), adicionalmente debe identificar las dependencias entre actividades relacionadas con otras organizaciones y a nivel interno (ISO/IEC 27001, 2013).

3.1.2 Conforme al Liderazgo

3.1.2.1 Liderazgo y compromiso

La alta gerencia debe asumir un compromiso respecto de la implementación del SGSI considerando lo siguiente:

i) Asegurando el desarrollo y cumplimiento de la política de seguridad de la información y que sus objetivos sean acordes con la estrategia de la entidad.
ii) Garantizando la integración de los requerimientos del SGSI a los procesos del negocio.
iii) Garantizando la disponibilidad de los recursos necesarios para el establecimiento del SGSI.
iv) Fomentar en la entidad la importancia de la gestión de seguridad y del cumplimiento de los requerimientos de un SGSI.
v) Garantizar que el SGSI alcance los logros planificados.
vi) El apoyo permanente al personal involucrado.
vii) Impulsar procesos de mejora continua

3.1.2.2 Política

La alta gerencia debe establecer una política de seguridad de la información que se encuentre acorde a los objetivos estratégicos de la organización, que proporcione un esquema de trabajo basado en los objetivos para preservar la seguridad de la información, que incluya además el compromiso para cumplir con los requerimientos aplicables y los relacionados a la mejora continua.

La política de seguridad de la información debe ser formalizada, documentada y difundida para su cumplimiento a nivel interno, el detalle y propuesta para el establecimiento de la política de seguridad se encuentra expresado en el punto 4.4 de este documento.

3.1.2.3 Respecto de los roles organizacionales, responsabilidades y autoridades

La alta gerencia debe garantizar que los roles y responsabilidades de los involucrados en el desarrollo de un SGSI, estén establecidos y sean comunicados. Adicionalmente deberá asignar responsabilidades para comunicar acerca del desempeño del SGSI (ISO/IEC 27001, 2013).

3.1.3 Conforme a la Planificación

3.1.3.1 Acciones para abordar los riesgos y las oportunidades

Cuando la entidad planifica la implementación de un SGSI debe considerar los asuntos mencionados en el punto 3.1.1, de los cuales se podrá obtener información sobre los posibles riesgos u oportunidades que deben ser atendidas. Por tanto es fundamental que se determine las acciones para abordar dichos riesgos y se determine procesos que permitan evaluar su eficacia.

Evaluación de riesgo de la Seguridad de la Información

La entidad debe establecer un proceso para la evaluación del riesgo que establezca lo siguiente:

i) Los criterios de riesgo de la seguridad de la información, garantizando que dichas evaluaciones proporcionan resultados medibles, sólidos y comparables, etc.
ii) El proceso de evaluación del riesgo debe identificar aquellos riesgos en los cuales se vean comprometidas la confidencialidad, integridad o disponibilidad de la información, así como la identificación del propietario del riesgo.
iii) Posterior a la identificación se debe analizar los riesgos y sus posibles consecuencias, determinando la probabilidad de ocurrencia y los niveles de riesgo.
iv) Por último se evalúa el riesgo comparando los resultados con los criterios definidos (ISO/IEC 27001, 2013).

Tratamiento de riesgo de la Seguridad de la Información

La entidad debe establecer un proceso para el tratamiento de riesgo de la seguridad de la información en donde se determine lo siguiente:

i) Las acciones apropiadas considerando los resultados de la evaluación del riesgo
ii) Establecer o diseñar los controles necesarios para implementar el tratamiento de riesgo y compararlos con los establecidos en la norma.
iii) Generar la declaración de aplicabilidad de los controles requeridos y además las justificaciones en caso de asumir el riesgo.
iv) Establecer el plan de tratamiento del riesgo y gestionar las aprobaciones correspondientes (propietario del riesgo).

Es importante mencionar que el plan de tratamiento de riesgo debe encontrarse documentado y disponible para las partes interesadas (ISO/IEC 27001, 2013).

3.1.3.2 Objetivos de seguridad de la información y planificación para lograrlos

Los objetivos de seguridad de la información deben encontrarse alineados a la política de seguridad de la entidad, deben ser medibles, difundidos y actualizados de manera periódica. Adicionalmente al definirlos se deben considerar los requisitos de seguridad de la información y los resultados obtenidos del análisis del riesgo.

Para lograr el cumplimiento de los objetivos la entidad debe establecer entre otros los recursos que necesita, las acciones que se realizarán, los responsables, el tiempo y como se medirán o evaluarán los resultados (ISO/IEC 27001, 2013).

3.1.4 Apoyo o Soporte

3.1.4.1 Recursos

La entidad debe proporcionar los recursos requeridos para todas las fases de implementación del SGSI.

3.1.4.2 Competencias

La entidad debe establecer las competencias mínimas con las que debe contar el personal perteneciente a la organización para que no se vea afectada la gestión del SGSI; de ser necesario establecer acciones encaminadas a proveer de las competencias requeridas. Estas acciones deben ser gestionadas por el área de Talento humano o gestión del recurso humano en cada entidad.

3.1.4.3 Conocimiento

El personal perteneciente a la entidad u organización debe tener pleno conocimiento de la política de seguridad, de su participación en el desempeño o eficacia del SGSI y las consecuencias del incumplimiento de los mismos.

3.1.4.4 Comunicación

La entidad debe establecer los parámetros de comunicación pertinentes con la gestión del SGSI en donde se incluya el tema a comunicar, el periodo, a quien reportar y los procesos afectados.

3.1.4.5 Información documentada

Un SGSI debe contar con información documentada de acuerdo a lo establecido por la norma ISO 27001 así como también con información considerada necesaria por la organización. La información mantenida puede variar de acuerdo al tipo de organización, su tamaño, sus procesos, su estructura, etc. (ISO/IEC 27001, 2013) .

- Creación y actualización

Cuando se crea o actualiza la documentación de un SGSI, la entidad debe asegurar la identificación clara y descriptiva del documento, debe contar con un formato establecido y con las revisiones y aprobaciones requeridas y suficientes.

- Control de la Información documentada

La documentación de un SGSI debe ser revisada y controlada para garantizar que sea apropiada, que se encuentre disponible y que mantenga los controles de seguridad requeridos contra el uso inadecuado o perdido de integridad.

Para el control de la documentación la norma recomienda establecer procesos de distribución, acceso y recuperación de la información, almacenamiento adecuado y conservación, mantener un control de cambios o versionamiento y esquemas de disposición o retención de la información.

Es importante mencionar que el acceso a la información estará determinado por la clasificación con la que se le designe al documento conforme el levantamiento de activos que se realiza como parte del proceso de implementación del SGSI (ISO/IEC 27001, 2013).

3.1.5 Operación

3.1.5.1 Control y planificación Operacional

Toda entidad que se encuentre en proceso de implementar un SGSI debe planificar los procesos que le llevaran a cumplir con los requisitos de seguridad de la información. La entidad debe conservar la documentación pertinente y controlar los cambios planificados y los no planificados así como asegurar el control de los procesos que son externalizados (ISO/IEC 27001, 2013).

3.1.5.2 Evaluación y tratamiento de riesgo de la seguridad de la información

La entidad debe realizar evaluaciones al riesgo de forma periódica o cuando ocurran eventos significativos que involucren a la seguridad de la información, tomando en consideración los criterios definidos en el punto 3.1.3.1.

La entidad debe implementar el plan para el tratamiento de los riesgos y mantener la documentación de los resultados obtenidos (ISO/IEC 27001, 2013).

3.1.6 Sobre la evaluación del desempeño

3.1.6.1 Monitoreo, medición, análisis y evaluación

La entidad debe evaluar la efectividad y desempeño del SGSI, para esto es necesario determinar que se requiere medir y los métodos que se aplicarán. Los métodos seleccionados deben generar resultados que sean comparables para considerarlos aplicables.

Se debe definir la periodicidad de medición y monitoreo, el responsable de la actividad, cuando se deben revisar los resultados y quien debe efectuar dicho análisis. El esquema de monitoreo y medición para el presente trabajo se base en la norma ISO 27004:2016 y se detalla en el capítulo VI.

3.1.6.2 Auditoría Interna

La entidad debe llevar a cabo auditorías de forma periódica y planificada en donde se proporcionará información relacionada al cumplimiento de la norma respecto de todos los requisitos establecidos para su implementación.

Se deben elaborar programas de auditoría que mantengan la periodicidad, los métodos, responsabilidades y los informes resultantes de la evaluación, adicionalmente se deberá considerar lo siguiente:

- Determinar los criterios y el alcance de la auditoría
- Seleccionar al personal apropiado e independiente para realizar la evaluación
- Garantizar que los resultados de las auditorías son remitidos a la alta dirección
- Mantener toda evidencia y documentación producto de la revisión realizada (ISO/IEC 27001, 2013).

3.1.6.3 Revisión de gestión

La alta gerencia debe realizar revisiones periódicas y planificadas al SGSI para determinar y garantizar su eficiencia y efectividad.

Las revisiones deben considerar entre otros, el avance o estado de las actividades, los cambios en la organización ya sea de carácter interno o externo, las opiniones acerca del desempeño del SGSI que pueden incluir no

conformidades, resultados del monitoreo, resultados de las auditorías, etc. Además se debe considerar los resultados de la evaluación del riesgo, el estatus del plan de tratamiento del riesgo y las oportunidades de mejora (ISO/IEC 27001, 2013).

3.1.7 Mejora

3.1.7.1 Respecto de las no conformidades y acciones correctivas

Cuando se da una no conformidad en la entidad se debe establecer las acciones correspondientes para controlar, corregir y confrontar las consecuencias.

Evaluar la no conformidad de tal manera que se pueda identificar su causa raíz y de esta manera evitar situaciones similares a futuro. Se debe evaluar la efectividad de las acciones correctivas y de ser necesario se realizarán cambios al sistema de gestión de la seguridad de la información.

Las acciones correctivas deben estar encaminadas a cubrir los efectos de las no conformidades identificadas, es importante documentar toda la información resultante de dichas evaluaciones o mejoras.

La entidad debe realizar los esfuerzos necesarios para mejorar de manera continua la eficacia, efectividad y capacidad del SGSI (ISO/IEC 27001, 2013).

A continuación, en la tabla 11 se presenta un esquema de los requisitos generales para cada fase de la gestión de un SGSI:

Tabla 11.

Mapa conceptual de los requerimientos generales para la gestión de un SGSI en base a la ISO 27001

REQUERIMIENTOS PARA LA IMPLEMENTACIÓN DE UN SGSI				
FASES	**Establecimiento del SGSI**	**Implementación y Operación del SGSI**	**Seguimiento y Revisión del SGSI**	**Mantenimiento y Mejora del SGSI**
ACTIVIDADES	1.- Definición del Alcance	1.- Formular Plan para el tratamiento del riesgo	1.- Ejecutar procedimientos de seguimiento y revisión	1.- Implementar mejoras identificadas
	2.- Definición de la Política de SGSI	2.- Implementar el plan de tratamiento del riesgo	2.- Emprender revisiones sobre la eficacia del SGSI	2.- Emprender acciones correctivas y preventivas
	3.- Definir el enfoque para la valoración del riesgo	3.- Implementar los controles seleccionados	3.- Medir la eficacia de los controles	3.- Comunicar las acciones y mejoras a las partes interesadas
	4.- Identificar los riesgos	4.- Definición de la medición de la eficacia de los controles	4.- Revisar las valoraciones de los riesgos a intervalos planificados	4.- Asegurar que las mejoras alcancen los objetivos propuestos
	5.- Analizar y evaluar los riesgos	5.- Implementar programas de formación	5.- Realizar auditorías internas del SGSI	
	6.- Identificar el tratamiento del riesgo	6.- Gestionar la operación del SGSI	6.- Emprender una revisión del SGSI realizada por la Dirección	
	7. - Seleccionar los objetivos de control	7.-Gestionar los recursos del SGSI	7.- Actualizar los planes de seguridad	
	8.-Obtener la aprobación de la Dirección	8.- Implementar procedimientos y otros controles para la gestión de incidentes de seguridad	8.- Registrar acciones y eventos de alto impacto	
	9.- Obtener la autorización para la implantación			
	10.- Elaborar la declaración de aplicabilidad			

Adaptado de (ISO/IEC 27001, 2013)

A continuación, en la figura 16 se presenta una síntesis de la gestión y las responsabilidades de la Dirección requeridas para una implementación y mejora continua de un SGSI:

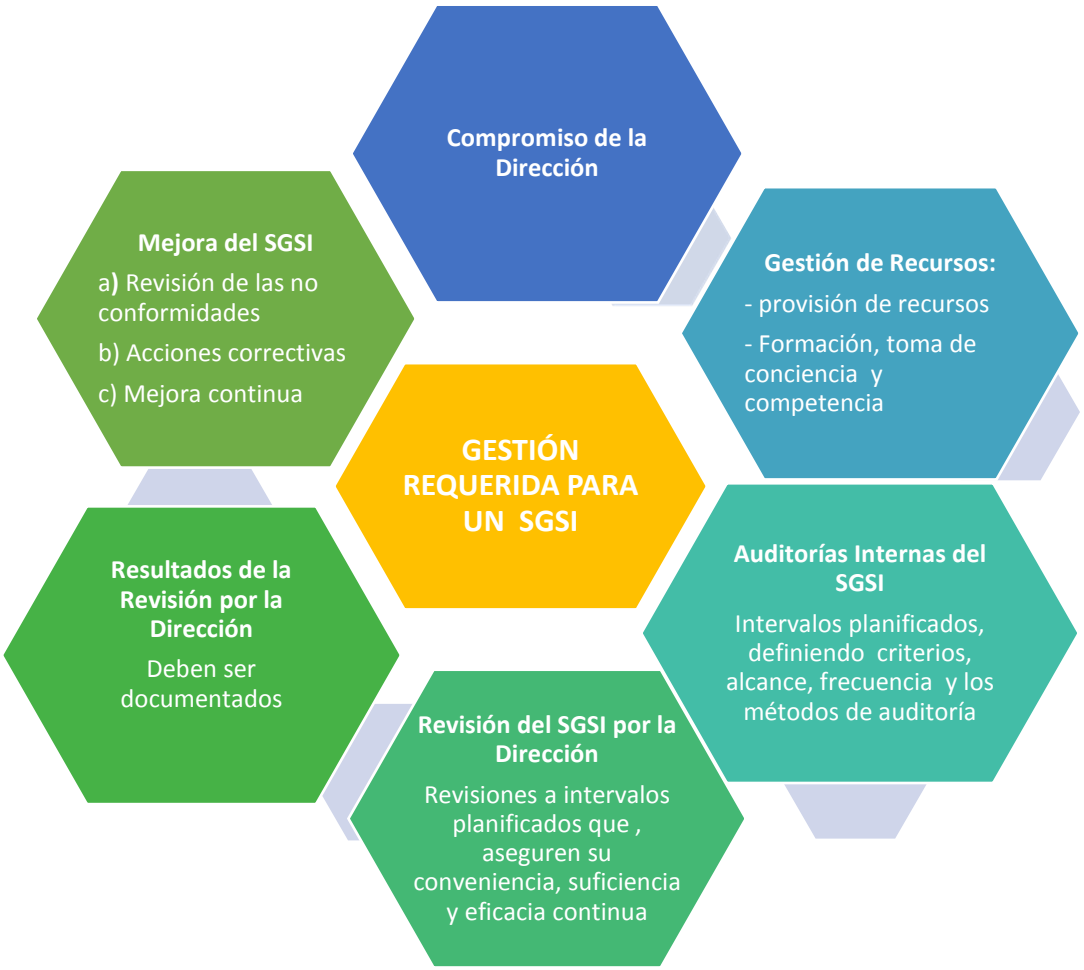


Figura 16. Síntesis de la gestión requerida para un SGSI

3.2 Identificación y clasificación de los activos de información

Dentro de los requerimientos para el establecimiento de un SGSI se encuentra la realización del análisis de riesgos de seguridad de la información para lo cual es necesario establecer un inventario de activos de información que mantiene la organización. Un activo en relación con la seguridad de la información se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización (Portal de ISO 27001 en español, 2012).

La norma ISO 27001 nos dice que todos los activos de información deben ser identificados de una forma clara y se tiene que mantener un inventario de los mismos.

El inventario de activos junto con su clasificación debe ser validado y revisado de manera anual por el área de Seguridad de la Información de la organización, y servirá para la definición de los activos que deben ser protegidos y en los cuales se deben aplicar los controles pertinentes. Cada uno de los activos mencionados va a tener un responsable que va a realizar el mantenimiento de su seguridad, aunque puede que éste no la gestione. A continuación, se describe los roles y responsabilidades que deben establecerse para el levantamiento y clasificación de los activos.

3.2.1 Roles y Responsabilidades

3.2.1.1 Propietario de Información

Persona a la que, por su cargo y/o responsabilidad la organización reconoce como responsable de la información que gestiona y de los procesos del negocio a su cargo. Es responsable de establecer el nivel de confidencialidad, disponibilidad e integridad de los activos de información de los que es propietario, adicionalmente es responsable de la definición de los accesos hacia esta información.

3.2.1.2 Custodio de la Información

Corresponde al colaborador que tiene control o posesión física o lógica de la información sea esta información propiedad de la organización o de terceros.

3.2.1.3 Usuarios

Los usuarios son todos los colaboradores de la organización o terceras partes que requieren acceder a la información. Los usuarios serán responsables de conocer y cumplir las definiciones de seguridad sobre los datos que acceden.
Adicionalmente cada usuario deberá:

a) Clasificar toda información generada por el usuario,

b) Reportar situaciones de incumplimiento al propietario de la información.

3.2.1.4 Inventario y activos de Información

La información y los activos de información deben ser identificados, inventariados y deben tener asignado un propietario de dicha información que será el encargado de rendir cuentas sobre el activo.

Cada activo o grupo de activos de una organización deben ser claramente identificados y documentados. Existen dos clases de activos de acuerdo a la norma ISO que son los activos primarios (procesos del negocio) y los activos de soporte que son aquellos de los cuales dependen los activos primarios. En la siguiente tabla se muestran los tipos de activos primarios que pueden existir.

Tabla 12.

Tipos de activos primarios

Activo	Ejemplo
Procesos o Subprocesos y actividades del Negocio	-Procesos que son necesarios para el cumplimiento de la misión de la entidad. - Procesos que si sufren algún cambio afectarían a la entidad -Procesos necesarios para el cumplimiento contractual, normativo o legal.
De información	-Información importante para el cumplimiento de los objetivos y la misión de la entidad -Información personal o privada -Información estratégica -Información cuyo proceso de obtención implica costos y tiempo.

Adaptado de (ISO/IEC 27005, 2009)

A continuación se describe los tipos de activos de soporte que pueden existir, dichos activos pueden tener vulnerabilidades que serán explotadas por amenazas, en donde el objetivo es perjudicar al activo primario (ISO/IEC 27005, 2009).

Tabla 13.

Tipos de activos de soporte

Tipo	Detalle	Ejemplos
Hardware	Son los elementos físicos que sirven para dar soporte a los procesos	Servidores Computadoras Impresoras Discos externos CD-ROM Documentación
Software	Son los programas que permiten el funcionamiento o procesamiento de datos	Software de servicio Programas que constituyen la base operativa del computador Software de escritorio Software de mensajería
Red	Estos activos comprenden los dispositivos de telecomunicaciones que permiten conectar equipos remotos físicos o sistemas de información	Medios y soportes – red pública Switches Routers Adaptador de Ethernet
Personas	Personas que se encuentran involucradas en el sistema de información	Alta gerencia Usuarios Líderes de proyectos Personal operativo Desarrolladores
Ubicación	Comprende los sitios o lugares que contienen el alcance del activo	Instalaciones de oficinas o agencias Edificaciones Servicios y medios
Organización	Comprende la estructura organizacional de la entidad y los procedimientos que controlan dicha estructura	Autoridades Áreas de la organización y sus funciones La organización de un proyecto Proveedores/contratistas

Adaptado de (ISO/IEC 27005, 2009)

3.2.1.5 Criterios de Valoración de los activos

Para valorar los activos se debe tener en cuenta los siguientes aspectos:

a) Disponibilidad.- la importancia de la ausencia o funcionamiento del activo.

b) Integridad.- Se debe responder a la pregunta de qué repercusiones tendría la alteración del activo.

c) Confidencialidad.- Se debe responder a la pregunta del riesgo o repercusión de un acceso no autorizado hacia el activo.

3.2.1.6 Clasificación del nivel de confidencialidad

En la tabla 14 se presenta una propuesta para clasificar los activos de información de acuerdo a su nivel de confidencialidad.

El sistema de clasificación de la información propuesto consta de cuatro niveles, donde cada nivel refleja el grado de confidencialidad de la información respecto al acceso y/o divulgación de la misma. Los niveles de clasificación tienen por objeto establecer criterios para proteger la información y están basados en la capacidad para describir el posible daño a una entidad en este caso para una organización perteneciente a la vertical bancaria.

Tabla 14.

Clasificación de los activos por su confidencialidad

CLASIFICACION	DESCRIPCIÓN
Información Restringida	Es la información con mayor nivel de confidencialidad y reserva para una organización, esta información está destinada únicamente para uso interno exclusivo de un grupo de personas de una organización. La pérdida, modificación o divulgación de este tipo de información resulta en una pérdida significativa de la posición competitiva o en el daño de la imagen de la organización. Ejemplo: Usuarios y contraseñas balances financieros, indicadores estratégicos, etc.
Información Confidencial	Esta tipo de información tiene un grado menor de sensibilidad que la información restringida pero igualmente su acceso será restringido. La pérdida, modificación o divulgación no autorizada de este tipo de información puede resultar en una pérdida o daño a la organización. La protección específica de este tipo de información es requerida por regulaciones o leyes. Dicha información solo puede ser accedida por aquellas personas que lo requieran para el ejercicio de sus funciones. Ejemplo: información confidencial de clientes.

CLASIFICACION	DESCRIPCIÓN
Información para uso interno	Esta clasificación aplicará a información de uso exclusivamente interno y que sirva para la operación de la Organización, pero no de acceso público. La divulgación o utilización no autorizada de esta información tendrá un impacto menor en la organización o imagen de la misma. Ejemplo: Políticas, directrices, manuales, procedimientos, etc.
Información de uso público	La información que se ubica en esta categoría podrá ser expuesta al público y no requiere de controles adicionales a los asociados con la protección de autoría. El acceso a este tipo de información no representa riesgo ni impacto para la organización. Ejemplo campañas publicitarias, promociones, servicios, etc.

Adaptado de (Área de Seguridad BI, 2016)

3.2.1.7 Clasificación en base a la disponibilidad de los activos de Información

La importancia de la disponibilidad de los activos de información se fundamenta en el impacto que tendría que los datos no sean accesibles para las operaciones diarias y la continuidad de los procesos de una organización. Para esta propuesta se considerarán los siguientes niveles de disponibilidad:

Tabla 15.

Niveles de disponibilidad de los activos de Información

CLASIFICACION	DETALLE
Extrema	Los activos que se encuentran en esta categoría afectan a procesos u operaciones que son determinantes para la normal operación del negocio y que no pueden ser ejecutadas en tiempo diferido. Su disponibilidad es vital para la organización. Si falla el proceso asociado al activo dicho suceso afectará a la imagen de la organización.
Alta	Los activos que se encuentran en esta categoría afectan a procesos u operaciones que poseen una relevancia importante para la ejecución de las funciones y actividades de la organización. La falta o no disponibilidad del activo de información impacta negativamente a la Entidad.

CLASIFICACION	DETALLE
Media	Los activos que se encuentran en esta categoría afectan a procesos u operaciones de negocio que si bien son considerados importantes, en caso de un contingente o falla podrán ser ejecutados de forma manual o en tiempo diferido hasta que la falla sea solucionada. La falta o no disponibilidad impacta negativamente no solo el proceso evaluado sino podría afectar a otros procesos.
Baja	Impacta negativamente de manera leve al proceso, no implica una interrupción en los procesos relevantes y esenciales para la normal operación de la empresa.

Adaptado de (Área de Seguridad BI, 2016)

3.2.1.8 Clasificación en base a la integridad de los activos de Información

En este parámetro la información será clasificada a nivel de integridad tomando como referencia el impacto que tendría la pérdida de exactitud y completitud de la información, como por ejemplo fallas en los sistemas de información, en las aplicaciones, en equipos, etc. Para esta propuesta se determinan los siguientes niveles de integridad:

Tabla 16.

Niveles de integridad de los activos de Información

CLASIFICACIÓN	DETALLE
Extrema	Cualquier falla o afectación a la integridad de los activos que se encuentran en esta categoría produce un impacto severo en la operatividad de la organización y podría generar sanciones, multas y pérdida severa de la imagen corporativa.
Alta	Un fallo o afectación a la integridad de los activos que se encuentran en esta categoría puede implicar un impacto negativo que puede ser de índole legal o económica, retraso en los procesos o funciones y una pérdida de imagen severa.
Media	Un fallo o afectación a la integridad de los activos que se encuentran en esta categoría puede resultar en un impacto negativo medio de índole legal o económica, retraso en los procesos o pérdida moderada de la imagen a nivel interno.
Baja	Un fallo o afectación a la integridad de los activos que se encuentran en esta categoría puede impactar negativamente de manera leve al proceso, no implica pérdida de imagen a nivel externo o interno.

Adaptado de (Área de Seguridad BI, 2016)

En el capítulo IV – Elaboración de la propuesta del modelo de SGSI, se muestra la valoración resultante aplicando los criterios definidos en este capítulo.

4. Capítulo IV: Elaboración de la propuesta del modelo de SGSI

La determinación de implementar un SGSI debe ser parte de una decisión a nivel estratégico de una organización en donde se involucre a todo el personal y cuente con el apoyo permanente de la Alta Dirección, siendo este aspecto fundamental para poder lograr los objetivos planteados.

De acuerdo a lo mencionado por el Instituto Nacional de Tecnologías de la Comunicación de España “el diseño de un SGSI dependerá de los objetivos y necesidades de la empresa, así como de su estructura. Estos elementos son los que van a definir el alcance de la implantación del sistema, es decir, las áreas que van a verse involucradas en el cambio. En ocasiones, no es necesario un sistema que implique a toda la organización, puede ser que sea sólo necesario en un departamento, una sede en concreto o un área de negocio. El tiempo de implantación del sistema de gestión de seguridad de la información varía en función del tamaño de la empresa, el estado inicial de la seguridad de la información y los recursos destinados a ello, pero podríamos estimar que su duración es de entre seis meses y un año para evitar que quede obsoleto, esto depende también del ámbito, tamaño y complejidad de la organización. La empresa debe contar con una estructura organizativa, así como de recursos necesarios, entre otras cosas, para llevar a cabo la implantación del SGSI” (Instituto Nacional de Tecnologías de la Comunicación, 2014). Para el presente trabajo se realiza la propuesta y formulación de los documentos y procesos establecidos para la fase de Planificación de la metodología de gestión de un SGSI aplicado para empresas de la industria bancaria con el objetivo de establecer una guía o referente de implementación. Adicionalmente se incluyen modelos de medición de resultados y del nivel de implementación del SGSI en base a lo mencionado en la normativa ISO 27004 Medición de la Seguridad de la Información.

4.1 Aplicación de la metodología de desarrollo e implementación de un SGSI

Para el caso de esta propuesta se establece como metodología de implantación de un SGSI el ciclo PDCA (Planificar, Hacer, Verificar y Actuar), el cual está dividido en cuatro fases en donde, finalizada la última y analizados sus resultados se vuelve a comenzar de nuevo en la primera. En la figura 17 se muestra el modelo con las actividades asociadas a cada una de las etapas:

Figura 17. Etapas Ciclo de Deming – Actividades de Implementación

Adaptado de (Delgado, 2014)

4.2 Determinación del alcance

Lo primero que se debe considerar al momento de establecer o formular un modelo de Sistema de Gestión de Seguridad de la Información es determinar el ámbito o alcance en el que se va aplicar el SGSI, el cual deberá ser viable y manejable para la organización, no es aconsejable abarcar todos los procesos o áreas si no se cuentan con los recursos materiales o humanos para ello. Por tanto, para las empresas de la industria bancaria en el sector privado del Ecuador que son el objetivo de este trabajo, el alcance del SGSI estará encaminado a las necesidades y objetivos del negocio de esta vertical, siendo la protección de la información de los clientes la necesidad principal de la industria bancaria, un SGSI debe estar encaminado a la preservación y aseguramiento de la confidencialidad, integridad y disponibilidad de la información. Los lineamientos deben establecer las bases para la implementación de medidas y controles que permitan a la empresa gestionar adecuadamente los riesgos que afectan a la información, así como a los activos de información relacionados.

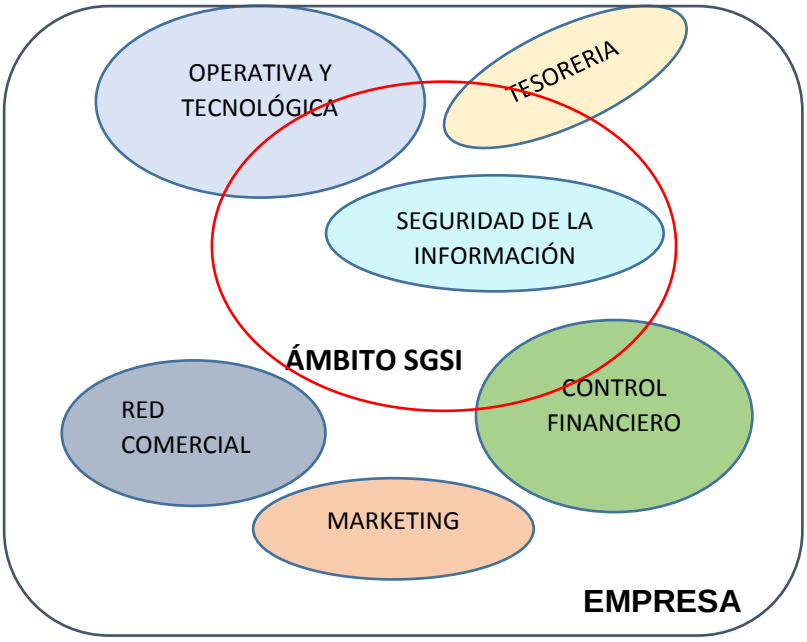


Figura 18. Ejemplo del establecimiento del ámbito SGSI

Por tanto, el alcance de un SGSI debe ser aplicado a toda la información que se administre en los procesos y operaciones de la empresa sea la información

de entrada, sustento o producto de dichos procesos y operaciones, aplica además a todos los activos en los cuales reside la información.

La implementación de un SGSI debe desarrollarse acorde a lo mencionado en la normativa ISO 27001:2013 en su literal 4.3 en el cual se determina que “la organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance. Al determinar este alcance, la organización debe considerar:

a) los asuntos externos e internos que comprende la organización y su contexto.
b) Los requerimientos, necesidades y expectativas de las partes interesadas.
c) Interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones” (ISO/IEC 27001, 2013).

La definición del alcance del sistema de gestión de la seguridad de la información es responsabilidad de la alta dirección con el asesoramiento del equipo de trabajo que se ha destinado al proyecto, adicionalmente se recomienda constituir un comité de seguridad que se encuentre liderado por la Gerencia del área de Seguridad de la Información y como entes participantes a los gerentes o subgerentes de las áreas involucradas.

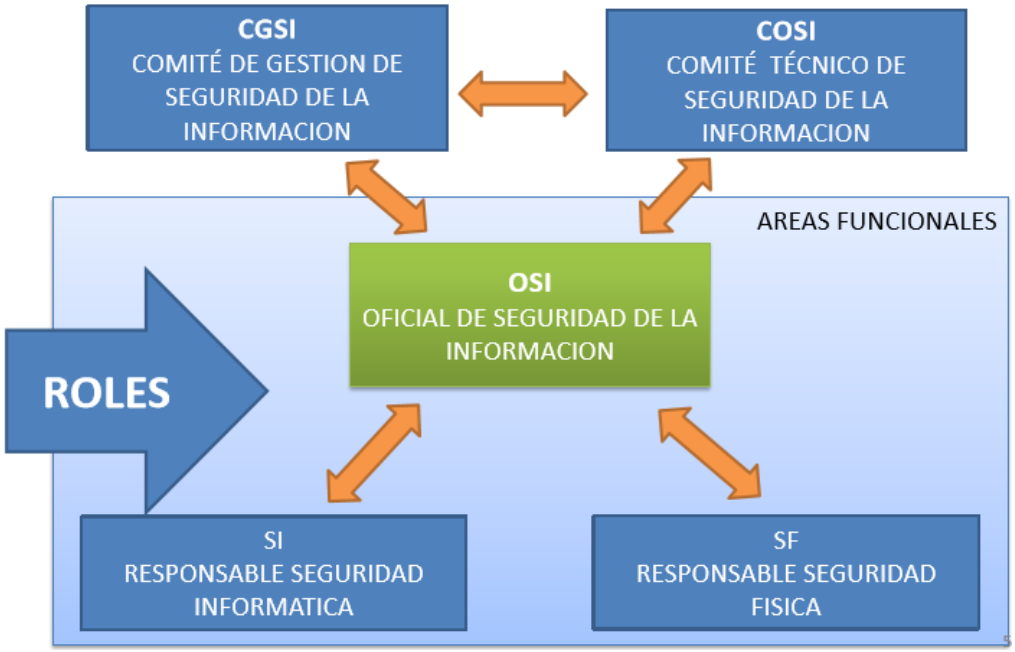


Figura 19. Responsabilidades en la gestión de la Seguridad

Adaptado de (Delgado, 2014)

Las funciones del Comité de Gestión de Seguridad de la Información son las siguientes:

- Comunicar la situación organizacional sobre la gestión de seguridad de la información.
- Designar y proponer la selección de un Oficial de Seguridad de la Información (OSI).
- Elegir a los miembros del Comité Técnico de Seguridad de la Información (COSI).
- Participar del proceso de implementación y mejora continua del Sistema de Gestión Seguridad de la Información (SGSI) (Delgado, 2014).

4.3.1 Aspectos a considerar para determinar el alcance en una empresa de la industria bancaria

Para determinar el ámbito de aplicación de un SGSI es importante identificar aquellos procesos críticos y esenciales para la continuidad del negocio, si la empresa cuenta con un análisis de impacto del Negocio (BIA), este podría

considerarse un insumo inicial para la determinación del mismo. Adicionalmente se debe analizar lo siguiente:

- Las diferentes líneas de negocio de la institución financiera; qué productos ofrece, cual es el proceso Core de la organización, cuál es su cliente objetivo.
- Modelo o estructura organizacional de la empresa, gestión por procesos, productos o funciones.
- Posicionamiento de la empresa, presencia a nivel nacional o internacional, porcentaje de presencia a nivel del sistema financiero nacional.
- Si se cuenta con un levantamiento de activos de la información en la organización.

4.3.2 Metodología para determinar el alcance del SGSI

Se propone la Metodología de las Elipses como herramienta de identificación de los componentes de cada proceso y las interfaces con otros procesos en la organización y con entidades externas a la empresa, el método se basa en:

1. Visualizar con precisión inicialmente los distintos subprocesos que componen el alcance, esto se debe determinar en la elipse concéntrica y posteriormente con los usuarios y dueños de estos procesos determinar cuáles son los activos de información vitales para la empresa.
2. Identificar en la elipse intermedia las distintas interacciones que los subprocesos de la elipse concéntrica tienen con los otros procesos de la organización, posteriormente se debe identificar con los dueños de los procesos los activos de información involucrados en los procesos.
3. En la elipse externa se identifican aquellas organizaciones extrínsecas a la organización que pueden tener interacción con los subprocesos identificados en la elipse concéntrica, las flechas indican dicha interacción (Alexander, 2014).

A continuación, se presenta un ejemplo sobre la aplicación de esta metodología en el proceso de generación de inversiones:

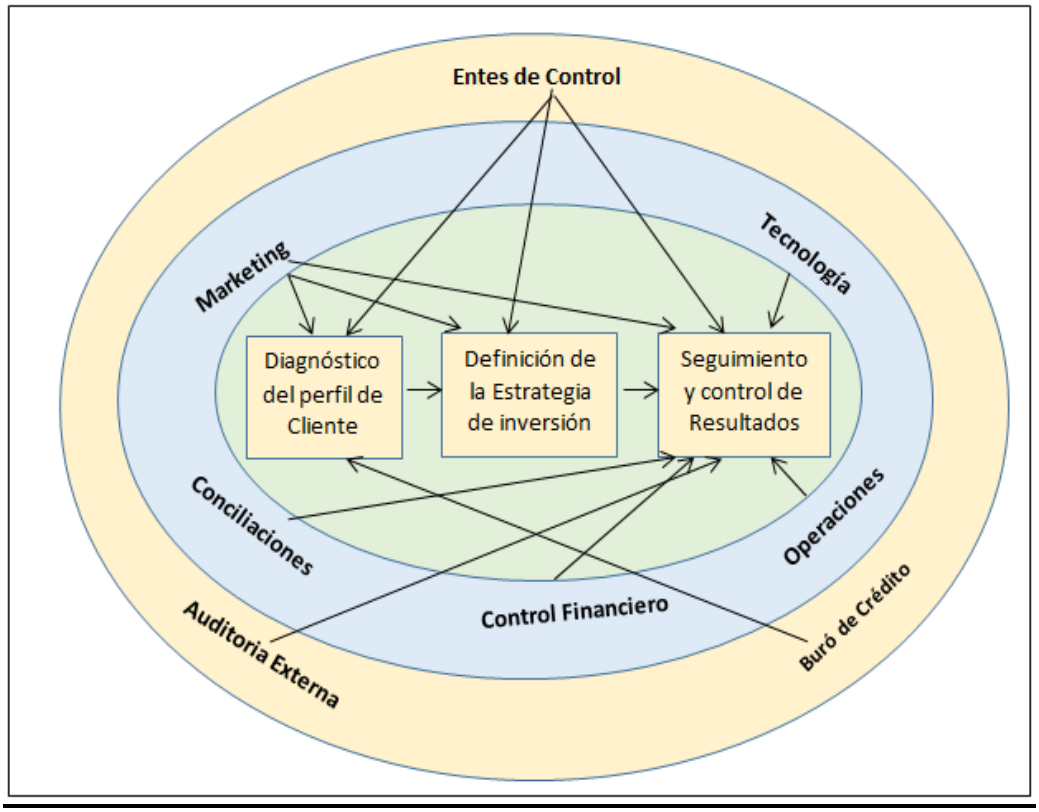


Figura 20. Ejemplo Metodología de las Elipses

Adaptado de (Alexander, 2014)

A continuación, en la figura 21 se presenta un diagrama que sintetiza los aspectos a considerar para determinar el alcance de un SGSI ya sea aplicando o no la metodología de las elipses:

Figura 21. Resumen de los pasos para la determinación del Alcance del SGSI

4.4 Definir la política de seguridad

La base de toda gestión de la información está en la definición de una política organizacional o política de seguridad de la información que se encuentre acorde a las características del negocio, requerimientos normativos, activos identificados, y la infraestructura tecnológica mantenida.

Si la organización no cuenta con una política de seguridad de la información, esta debe ser desarrollada en la fase de planificación del SGSI en base a las necesidades del sistema; de tal manera que la política guíe y encamine a la consecución de los objetivos de negocio.

La política de Seguridad de la información es el documento que determina el compromiso de la Alta Dirección con el SGSI y establece las bases para la implementación de medidas y controles que permitan una adecuada gestión de los riesgos de información.

La norma ISO 27001:2013 en su literal 5.2 menciona lo siguiente: “la alta dirección debe establecer una política de seguridad de la información que:

a) Es pertinente al objetivo de la organización;
b) Incluya los objetivos de seguridad de la información o que proporcione el marco de trabajo para establecer los objetivos de seguridad de la información;
c) Incluya un compromiso para satisfacer los requisitos aplicables, relacionados a la seguridad de la información y;
d) Incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información debe:

e) Estar disponible como información documentada;
f) Ser comunicada dentro de la organización; y
g) Estar disponible para las partes interesadas, según corresponda” (ISO/IEC 27001, 2013).

4.4.1 Estructura de la política de Seguridad de la Información

De acuerdo a lo requerido por la normativa, se ha formulado una referencia de cómo podría estructurarse la política de Seguridad de la Información, los elementos mínimos son los siguientes:

- ✓ **Objetivo**.- los objetivos de la política de Seguridad de la Información deben estar acorde a la estrategia, objetivos y metas del negocio y deben describir los lineamientos esperados de cumplimiento para la Organización.
- ✓ **Compromiso / acuerdo.-** establece los acuerdos y compromisos de cumplimiento de los lineamientos mencionados.
- ✓ **Alcance de la Política.-** establece el ámbito de aplicabilidad de la política.
- ✓ **Principios.-** se describen las normas generales relacionadas con la seguridad de la información, las cuales describen los comportamientos que deben seguirse dentro de la organización. Los principios se encuentran asociados a la cultura de la Organización, los requerimientos legales que deben cumplirse o que rigen a la industria relacionada o a los principios básicos de seguridad establecidos por las mejores prácticas. Los principios sin embargo pueden cambiar con el tiempo y los avances tecnológicos, por esto la importancia de una revisión como mínimo anual de la política.
- ✓ **Fecha de Vigencia / Periodo de Transición**
- ✓ **Políticas relacionadas / Procedimientos asociados.-** menciona a las políticas o procedimientos relacionados a los principios de la política en los cuales se detalla de manera más explícita el ámbito de alcance y al cual hace referencia.
- ✓ **Excepciones**.- situaciones expresamente puntuales en las cuales puede excepcionar un lineamiento de la política.
- ✓ **Glosario de términos**
- ✓ **Resumen de la política**
- ✓ **Desarrollo de la Política:**

- **Lineamientos o Marco de Gobierno**.- explicación respecto del marco o lineamientos a los cuales la política se encuentra asociada, ejemplo: la aplicación de directrices, procedimientos, estándares, etc. Se define adicionalmente la jerarquía de los documentos normativos internos y externos.
- **Roles, funciones y responsabilidades**.- determinación de las responsabilidades a nivel de la Alta Dirección, comités relacionados, la Gerencia de Seguridad de la Información, el área de Seguridad de la Información, los propietarios, custodios y usuarios de la información.
- **Políticas Generales.-** lineamientos que regirán la Seguridad de la información en la empresa.

✓ **Violaciones a la Política.-** describe las medidas o sanciones a tomarse en caso de incumplimiento o violación a los lineamientos de la política de seguridad de la información, estas declaraciones deben estar asociadas a la política general de ética y comportamiento de la organización.

✓ **Registro de Control de cambios**

✓ **Aprobación y fecha**

4.4.2 Aprobación de la Política de Seguridad de la Información

Es necesario no solamente que la política sea conocida y difundida, es necesario que exista la firma de aprobación por el rango más alto a nivel directivo, esto demostrará el compromiso que debe tener la alta gerencia en cuanto a la seguridad de la información y los lineamientos a cumplirse.

A continuación, en la figura 22 se muestra una síntesis de los componentes y aspectos con los que debe contar la política de seguridad de la información:

Figura 22. Síntesis de los componentes principales de la política de seguridad

4.5 Clasificación de los activos de información

4.5.1 Procedimiento para identificar, inventariar y clasificar los activos de información

De acuerdo a la norma ISO/IEC (27002) 17799:2005 – Código para la práctica de la gestión de la seguridad de la información que menciona lo siguiente:

- "Se debe clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.
- Las clasificaciones y los controles de protección asociados para la información, deben tomar en cuenta las necesidades comerciales de intercambiar o restringir información y los impactos comerciales asociados con dichas necesidades" (ISO/IEC 27002, 2013)

Por tanto, el objetivo de la clasificación de la información es la de establecer lineamientos y principios para preservar y asegurar la confidencialidad,

integridad y disponibilidad de los activos de información, clasificando la información según su criticidad e importancia para evitar pérdidas de tipo financieras, operativas y/o de la imagen corporativa.

4.5.1.1 Actividades del Procedimiento:

1. Identificar los roles y responsabilidades para las áreas involucradas en el proceso. El responsable de efectuar esta actividad en este caso será el área de seguridad de la información.
2. Capacitar a los responsables (propietarios de la información) sobre los criterios y el proceso a seguir para la identificación y clasificación de activos.
3. Identificar y definir los activos de información.- todos los responsables de procesos deben identificar cuáles y cuantos activos de información tienen bajo su responsabilidad y asignar un custodio responsable del mantenimiento de los controles apropiados.
4. Inventariar los activos de información con los datos mínimos requeridos y validar con el responsable del proceso. Los activos de información deben ser registrados en una matriz o inventario. En el anexo 2 se presenta un ejemplo del formato para un inventario de activos.

   A continuación en la tabla 17, se presenta una propuesta de la información mínima que debe contener el levantamiento o inventario de activos:

Tabla 17.

Estructura del inventario de activos

Dato	Descripción
Identificador del Activo	Código único que sirve para identificar al activo
Activo de información	Descripción del nombre del activo de información
Descripción del activo /Funcionalidad	Narrativa corta y descriptiva sobre el activo y su funcionalidad

Dato	Descripción
Propietario del activo	Persona a la que, por su cargo y/o responsabilidad la organización reconoce como responsable de la información que gestiona y de los procesos del negocio a su cargo. Es responsable de establecer el nivel de confidencialidad, disponibilidad e integridad de los activos de información de los que es propietario, adicionalmente es responsable de la definición de los accesos hacia esta información.
Custodio del activo	Corresponde al colaborador que tiene control o posesión física o lógica de la información, sea esta información propiedad de la organización o de terceros. Además, el custodio es la persona o grupo de personas que administra el activo al que se hace referencia.
Unidad de Información	Nombre de la unidad de información a la que pertenece el activo
Proceso	Nombre del proceso al cual pertenece el activo
Área / Departamento	Se especifica el nombre del área o departamento que genera o hace uso del activo.
Estado de Aprobación	Pendiente, en proceso o aprobado
Fecha Aprobación	Fecha en que fue aprobado
Fecha Modificación	Fecha en que fue modificado
Dependencia de Activos	Si mantiene el activo alguna dependencia con otro
Tipo de Activo	tangible, intangible estructura, intangible no estructurada
Activos de soporte	Descripción de los activos complementarios o de soporte que forman parte del activo, estos pueden ser de tipo: humano, hardware, software, dato, físico, etc.
Tipo de Almacenamiento	Ejemplo: Físico, digital
Período de almacenamiento	El tiempo establecido para almacenar la información del activo

Dato	Descripción
Lugar de almacenamiento	Se especifica el lugar físico en donde es almacenado o resguardado el activo, dependiendo del tipo de activo, tangible o intangible, el lugar de almacenamiento puede ser:
Considerado para Contingencia	Si el activo requiere de un proceso de contingencia

Adaptado de (Área de Seguridad BI, 2016)

5. **Valoración de los activos**.- de acuerdo a los pilares de seguridad de la información: i) confidencialidad, ii) disponibilidad e iii) integridad (ver capítulo III literal 3.2.1.6, 3.2.1.7, 3.2.1.8), para cada uno de estos pilares se evaluará el activo en los aspectos económico, legal, de imagen y operativa asignando una valoración numérica como se muestra en la tabla a continuación:

Tabla 18.

Aspectos para la valoración de un activo

Escala	Valor	Económica	Legal	Imagen	Operativa
Extremo	4	Costos altos de remediación	Afectación Legal o una posible multa o pérdida de categoría	Existe una pérdida importante en la marca, participación de mercado y reputación	Rigurosamente afectada la operatividad de los procesos, se requiere un tiempo alto de remediación
Alto	3	Costo significativo de remediación	Afectaciones económicas por observaciones y demandas	Existe una pérdida en la marca y su valor, participación de mercado, y una publicidad desfavorable	Se afecta la operatividad del proceso, tiempo medio de remediación.

Escala	Valor	Económica	Legal	Imagen	Operativa
Medio	2	Costo bajo de remediación	Demandas u observaciones que no implican afectación económica	Puede existir un impacto bajo o menor en el valor de la marca y en la reputación de la organización	Operatividad del proceso limitado, menor tiempo de remediación
Bajo o nulo	1	No genera pérdidas económicas	No implica consecuencias de tipo Legal.	No involucra una afectación a la imagen	No involucra afectación a la operatividad del proceso.

Adaptado (Área de Seguridad BI, 2016)

A continuación se presenta una guía de preguntas que se pueden efectuar para calificar y valorar el activo en base a los criterios de la tabla 19:

Tabla 19.

Guía de preguntas para valorar al activo

Aspecto	Consulta	Criterio
Económico	Si el activo que se gestiona a través del proceso/procedimiento no se encuentra disponible, ¿podría generar pérdidas económicas a la Institución?	**Disponibilidad**
Legal	Si el activo que se gestiona a través del proceso/procedimiento no se encuentra disponible, ¿podría generar sanciones legales de entes de control o demandas de externos a la Institución?	
Imagen	Si el activo que se gestiona a través del proceso/procedimiento no se encuentra disponible, ¿podría afectar la imagen de la Institución?	
Operativa	Si el activo que se gestiona a través del proceso/procedimiento no se encuentra disponible, ¿podría afectar la normal operatividad del proceso?	

Económico	Si el activo que se gestiona a través del proceso/procedimiento es modificado sin previa autorización, ¿podría generar pérdidas económicas a la Institución?	**Integridad**
Legal	Si el activo que se gestiona a través del proceso/procedimiento es modificado sin previa autorización, ¿podría generar sanciones legales de entes de control o demandas de externos a la Institución?	
Imagen	Si el activo que se gestiona a través del proceso/procedimiento es modificado sin previa autorización, ¿podría afectar la imagen de la Institución?	
Operativa	Si el activo que se gestiona a través del proceso/procedimiento es modificado sin previa autorización, ¿podría afectar la normal operatividad del proceso?	
Económico	Si la información confidencial asociada al activo es divulgada, ¿podría afectar a las decisiones de tipo económicas y estratégicas de la Institución?	**Confidencialidad**
Legal	Si la información confidencial asociada al activo es divulgada, ¿podría afectar el cumplimiento de normas y regulaciones legales o constituir demandas a la Institución?	
Imagen	Si la información confidencial asociada al activo es divulgada, ¿podría afectar a la imagen de la Institución?	
Operativa	Si la información confidencial asociada al activo es divulgada, ¿podría afectar al proceso operativo de la Institución?	

Adaptado de (Área de Seguridad BI, 2016)

6. Determinar el valor total del Activo.- el valor resultante para cada criterio de seguridad de la información (confidencialidad, integridad y disponibilidad) será el valor de impacto más alto en los aspectos: económico, legal, operativo o imagen.
7. Por último y de acuerdo al valor resultante de criticidad del activo se procede a clasificarlo en restringido, confidencial, uso interno o de uso público (ver punto 3.2.1.6, tabla 14)
8. Establecer una columna de observaciones o comentarios sobre el activo en caso de ser necesario.
9. Efectuar la difusión de la clasificación de los activos a las partes interesadas y determinar procesos de revisión periódica para una mejora continua.

A continuación en la tabla 20 se muestra un ejemplo sobre la valoración del activo:

Tabla 20.

Ejemplo Matriz de Valoración del Activo

Matriz de Valoración de Activos																			
Proceso: Gestionar Mesa de Ayuda					**Área: Soporte Tecnológico**														
Activo		**Valoración Resultante**			**CONFIDENCIALIDAD**					**INTEGRIDAD**					**DISPONIBILIDAD**				
Identificador del activo	**Nombre Activo**	**Valor**	**Clasifi**	**Escala**	**Oper**	**Ima.**	**Eco.**	**Leg.**	**Res.**	**Oper.**	**Ima.**	**Eco.**	**Leg.**	**Res.**	**Oper.**	**Ima.**	**Eco.**	**Leg**	**Res.**
AI_001_I	Inventario de requerimientos	**4**	**RESTRINGIDO**	**Extremo**	2	2	3	1	3	4	1	2	1	4	4	2	3	1	4
AI_002_I	Estadísticas de cumplimiento de SLA	**3**	**CONFIDENCIAL**	**Alto**	1	3	1	1	3	3	3	2	1	3	2	2	3	1	3
AI_003_I	Contrato con el proveedor del servicio	**4**	**RESTRINGIDO**	**Extremo**	1	2	2	2	2	1	3	3	4	4	3	1	3	3	3
AI_004_I	Procedimiento de gestión de servicios	**3**	**CONFIDENCIAL**	**Alto**	1	1	1	1	1	3	2	3	1	3	3	1	1	1	3
AI_005_I	Manual de usuario	**2**	**USO_INTERNO**	**Medio**	1	1	1	1	1	2	1	1	1	2	2	1	1	1	2
AI_006_I	Organigrama del equipo de Mesa de Ayuda	**1**	**PÚBLICO**	**Bajo**	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Adaptado de (Área de Seguridad BI, 2016)

4.5.2 La clasificación de la información como un requerimiento normativo para las organizaciones en la industria bancaria

La norma de riesgo operativo establecida mediante una resolución de la Superintendencia de Bancos (JB-2014-3066) establece en su artículo 22 que las organizaciones deben: “Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:

1. Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado;
2. Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables;
3. Autorizar los cambios funcionales a las aplicaciones; y,
4. Monitorear el cumplimiento de los controles establecidos” (Superintendencia de Bancos y Seguros, 2014).

Tomando en consideración que dicha clasificación es de carácter obligatorio para las entidades que son objeto de este estudio, se propone que la clasificación se la realice por fases y por procesos, es decir priorizando a los procesos que contienen la información sensible y fundamental para el negocio como una primera etapa. Esto se recomienda debido a la estructura y tamaño de este tipo de industria.

A continuación, en la figura 23 se presenta una síntesis sobre el proceso que deberían efectuar las entidades para realizar el inventario y clasificación de sus activos.

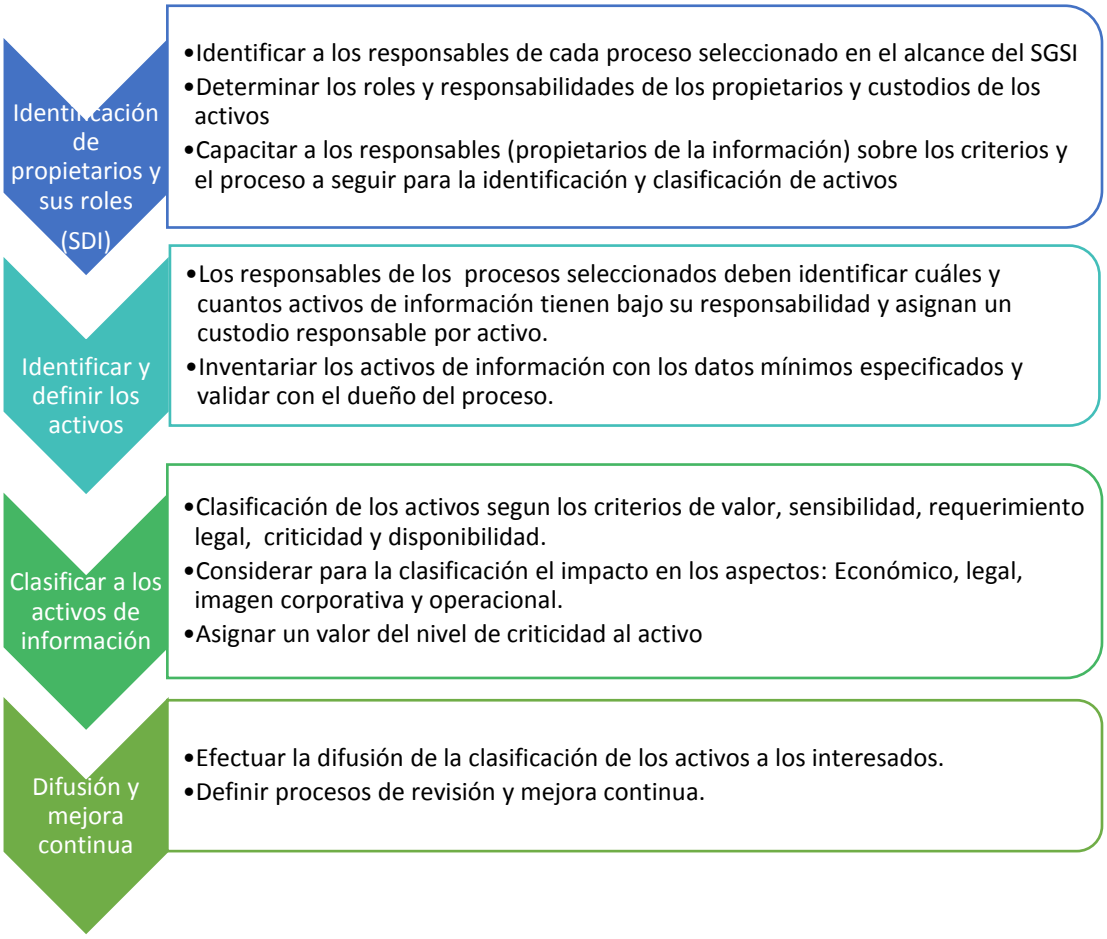


Figura 23. Metodología para la clasificación de activos de información

4.5.3 Factores claves de éxito para un proyecto de Clasificación de la Información

Para que un proyecto de Clasificación de la información sea exitoso ya sea una empresa de la vertical bancaria o de otro tipo es importante lograr sinergia en los siguientes aspectos:

- ✓ Participación activa, soporte, apoyo y compromiso permanente de la Alta Gerencia.
- ✓ Cumplimiento de los tiempos establecidos por cada responsable o propietario en la determinación de los activos de sus procesos asignados.
- ✓ Cumplimiento y retroalimentación del área de Seguridad de la Información sobre los criterios de clasificación a los involucrados.
- ✓ Monitoreo y seguimiento periódico del avance del proyecto.
- ✓ Comunicación permanente y efectiva entre los miembros del equipo.

4.5.4 Mejores prácticas o sugerencias para aplicar a la información

4.5.4.1 Información Digital:

Aquí se encuentra la información almacenada en cintas de seguridad, almacenamiento en la nube, discos duros, soportes físicos (DVD, CD), USB, discos portátiles.

Tabla 21.

Mejores prácticas – información Digital

Restringida / Confidencial	**Uso Interno**	**Pública**
-Para los medios de almacenamiento externos deben ser resguardados y el acceso al sitio debe ser limitado. -Todo respaldo de información que se encuentre en medios magnéticos debe cumplir con los requerimientos de seguridad establecidos por el dueño o propietario de la Información. -La información confidencial o restringida no debe ser compartida mediante correo electrónico personal o mediante las redes sociales, entre otros. -Para el acceso a la información no se podrá utilizar credenciales o usuarios que no pertenezcan al colaborador. -Asegurarse de que la información ha sido completamente eliminada de los medios magnéticos con los métodos apropiados.	Será utilizada únicamente para la operatoria normal de la empresa. No debe ser divulgada públicamente.	N/A

Adaptado de (Área de Seguridad BI, 2016)

4.5.4.2 Información Física:

Entre estos encontramos todo tipo de información impresa como manuales, procedimientos, informes, revisiones, papeles de trabajo, etc.

Tabla 22.

Mejores prácticas – información Física

Restringida / Confidencial	**Uso Interno**	**Pública**
-No mantener esta información a la vista de colaboradores no autorizados. -La información impresa debe ser retirada inmediatamente de las impresoras o puestos de trabajo. -Todo documento debe ser retirado del escritorio y asegurado en archivadores o gavetas cuando el colaborador no se encuentre en su sitio de trabajo. -La información crítica debe contener un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros (proveedores). -Al momento de eliminar los documentos se lo debe realizar con procesos definidos que garanticen la seguridad y eliminación total de la información	- Escritorio limpio. - Será utilizada únicamente para la operatoria normal de la empresa. -No debe ser divulgada públicamente.	N/A

Adaptado de (Área de Seguridad BI, 2016)

4.6 Seleccionar los objetivos de control

Conforme se mencionó en los primeros capítulos de este trabajo, la norma ISO 27001:2013 describe en su Anexo “A” los objetivos de control para un sistema de Gestión de la seguridad de la información, en total se tienen 144 controles que se encuentran divididos en 35 categorías de seguridad y 14 cláusulas de control.

La norma ISO 27002:2013 establece que: “La selección de los controles dependerá de las decisiones organizativas basadas en los criterios de aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque general de gestión de riesgos aplicados a la organización, y también estará sujeta a toda la legislación nacional e internacional pertinente” (ISO/IEC 27002,

2013), por tanto, para objeto de este análisis se procedió a seleccionar a los controles mínimos que deben ser considerados en una organización de la industria bancaria en el Ecuador, tomando como criterio de análisis la legislación nacional vigente.

Para determinar los controles mínimos que requiere cumplir la industria analizada, se tomaron las disposiciones establecidas por el ente de control (mencionado en el capítulo II) y se comparó con los 144 controles especificados en la norma ISO 27001 y 27002 para determinar su correspondencia y su aplicabilidad.

Es importante aclarar que los controles seleccionados en base a la normativa vigente, corresponden únicamente a los artículos **21 y 22 del capítulo V de la Administración y gestión de riesgos de la resolución JB-2014-3066** emitida por la Superintendencia de Bancos que abordan la responsabilidad del área de Seguridad de la información para la gestión de un SGSI, no obstante se debe recordar que dichos controles son los mínimos requeridos de acuerdo a la norma, pero que el cumplimiento de cada organización debe abarcar la completitud de la norma ISO 27001. A continuación, en la tabla 23 el detalle:

Tabla 23.

Controles mínimos y mandatorios para empresas de la industria Bancaria en el Ecuador

CONTROLES (ANEXO "A") OBLIGATORIOS PARA LA INDUSTRIA BANCARIA POR CUMPLIMIENTO NORMATIVO				
Objetivo de Control	**Categoría de Seguridad**	**#**	**Control**	**Detalle del Control**
A.5 Políticas de seguridad de la información	A.5.1 Orientación de la dirección para la seguridad de la información	A.5.1.1	Políticas para la seguridad de la información	"La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información"
A.6 Organización de la Seguridad de la Información	A.6.1 Organización Interna	A.6.1.1	Roles y responsabilidades de la seguridad de la información	"Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas"
		A.6.1.2	Segregación de Funciones	"Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos"
		A.6.1.5	Seguridad de la información en la gestión de proyecto	"Se debe abordar la seguridad de la información en la gestión de proyecto sin importar el tipo de proyecto"
A.8 Administración de Activos	A.8.1 Responsabilidad por los activos	A.8.1.1	Inventario de activos	"Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos"

CONTROLES (ANEXO "A") OBLIGATORIOS PARA LA INDUSTRIA BANCARIA POR CUMPLIMIENTO NORMATIVO				
Objetivo de Control	**Categoría de Seguridad**	**#**	**Control**	**Detalle del Control**
		A.8.1.2	Propiedad de los activos	"Los activos que se mantienen en inventario deben pertenecer a un dueño"
		A.8.1.3	Uso aceptable de los activos	"Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información"
	A.8.2 Clasificación de la Información	A.8.2.1	Clasificación de la información	"La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización"
		A.8.2.3	Manejo de activos	"Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización"
	A.8.3 Manejo de los medios	A.8.3.2	Eliminación de los medios	"Se deben eliminar los medios de información de forma segura y sin peligro usando procedimientos formales"
A.9 Control de Acceso	A.9.1 Requisitos de negocio para el control de acceso	A.9.1.1	Política de control de acceso	"Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información"
	A.9.2 Gestión de acceso del usuario	A.9.2.2	Asignación de acceso de usuario	"Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios a los sistemas y servicios"

CONTROLES (ANEXO "A") OBLIGATORIOS PARA LA INDUSTRIA BANCARIA POR CUMPLIMIENTO NORMATIVO				
Objetivo de Control	**Categoría de Seguridad**	**#**	**Control**	**Detalle del Control**
		A.9.2.5	Revisión de los derechos de acceso de usuario	"Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica"
	A.9.4 Control de acceso al sistema y aplicaciones	A.9.4.1	Restricción de acceso a la información	"Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones de acuerdo a la política de control de acceso"
A.10 Criptografía	A.10.1 Controles Criptográficos	A.10.1.1	Política sobre el uso de controles criptográficos	"Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información"
A.12 Seguridad de las operaciones	A.12.1 Procedimientos operacionales y responsabilidades	A.12.1.2	Gestión de cambios	"Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información"
	A.12.2 Protección contra código malicioso	A.12.2.1	Controles contra código malicioso	"Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios"
	A.12.4 Registro y Monitoreo	A.12.4.1	Registro de evento	"Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información"

CONTROLES (ANEXO "A") OBLIGATORIOS PARA LA INDUSTRIA BANCARIA POR CUMPLIMIENTO NORMATIVO				
Objetivo de Control	**Categoría de Seguridad**	**#**	**Control**	**Detalle del Control**
	A.12.5 Control del software de operación	A.12.5.1	Instalación del software en sistemas operacionales	"Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales"
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras	A.16.1. 1	Responsabilidades y procedimientos	"Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información"
		A.16.1.2	Informe de eventos de seguridad de la información	"Se deben informar lo antes posible los eventos de seguridad de la información mediante canales de gestión apropiados"
		A.16.1.5	Respuesta ante incidentes de seguridad de la información	"Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados"
A.18 Cumplimiento	A.18.2 Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la seguridad de la información	"El enfoque de la organización para la gestión de la seguridad de la información y su implementación se debe revisar en forma independiente a intervalos planificados o cuando ocurran cambios significativos"
		A.18.2.3	Verificación del cumplimiento técnico	"Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización"

4.7 Definición del plan de tratamiento del riesgo

Como se mencionó en el capítulo III de este documento, la organización debe: a) formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información; y b) implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades (ISO/IEC, 2006).

El objetivo del Plan de Tratamiento del riesgo es detallar las actividades que determinan como se van a implementar cada uno de los controles establecidos en la declaración o enunciado de aplicabilidad. Se requiere la aprobación por parte del Directorio de la institución financiera.

El marco de referencia COBIT 5 en su proceso APO13: “Gestionar la Seguridad” establece como práctica clave de gobierno la actividad: “Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información” en el cual determina que se debe: “Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio” (ISACA, 2012).

El plan debe establecer claramente los recursos, responsabilidades y prioridades que se derivan de la evaluación de riesgos.

4.7.1 Como establecer las responsabilidades para la definición y gestión del plan de tratamiento del riesgo.

El marco de referencia Cobit para el proceso APO 13 Gestionar la Seguridad, establece los roles y responsabilidades para cada práctica de gobierno, en donde se encuentra la actividad “Definir y gestionar un plan de tratamiento del

riesgo de seguridad de la información", la explicación de cada rol se presenta a continuación:

- **R (responsable).-** Hace referencia a los roles que se encargan de la actividad principal para completar la actividad y producir la salida esperada (ISACA, 2012).
- **A (responsable de que se haga)** [del inglés, accountable] ¿Quién rinde cuentas sobre el éxito de la tarea? Asigna la responsabilidad de consecución de la tarea. Se debe tener en cuenta que el rol mencionado es el nivel más bajo apropiado para rendir cuentas; hay por supuesto, más altos niveles de rendición de cuentas también. Para activar la potenciación de la empresa, la responsabilidad de rendir cuentas se descompone con la mayor granularidad posible (ISACA, 2012).
- **C (consultado).-** ¿Quién proporciona entradas? Estos roles que proporcionan entradas son clave. Se debe tener en cuenta que corresponde a los roles de responsable y de rendir cuentas obtener información de otras unidades o, también de, interesados externos. En cualquier caso, las entradas de estos roles enumerados deben ser consideradas y, si se requiere, tomar las medidas necesarias para que se escalen, incluyendo la información del propietario del proceso y/o del Comité de Dirección (ISACA, 2012).
- **I (informado).-** ¿Quién recibe la información? Estos son los roles que son informados de los logros y/o entregables de las tareas. Por supuesto, el rol del 'responsable de hacer' debe recibir siempre información apropiada para supervisar la tarea, al igual que los roles responsables del área de interés (ISACA, 2012).

En el anexo 3 se muestra la matriz RACI completa para el proceso APO13: "Gestionar la Seguridad" en donde se identifica los roles y responsabilidades en la definición y gestión del plan de tratamiento del Riesgo. En donde se puede observar que los responsables principales de ejecución de la actividad son: El CIO, el Gestor de Seguridad de la Información, y el Jefe de Administración de TI. Los resultados, logros o entregables deben ser

informados al Comité Estratégico (Desarrollo/Proyectos) y a la oficina de Gestión de Proyectos.

Por último, el responsable de que la tarea se complete será el Director de Seguridad de la Información o conocido como CISO. Existen varios cargos o roles que proporcionan entradas al proceso como son: Director General Ejecutivo, Director de Operaciones, propietarios de procesos, Comité de Riesgos, Auditoria, Cumplimiento normativo, Jefe de Desarrollo, Jefe de Arquitectura de Negocio, Jefe de Operaciones de TI, gestor de Servicios, Gestor de Continuidad, etc.

4.7.2 Actividades para la Gestión del Plan de Tratamiento del Riesgo según COBIT 5

De acuerdo a lo descrito en el marco de referencia COBIT 5, las actividades asociadas a la práctica clave de gestionar y definir un plan de tratamiento del riesgo son las siguientes:

1) Desarrollar un plan de tratamiento de riesgos que se encuentre acorde a los objetivos estratégicos de la empresa y que garantice que el plan contiene las soluciones de seguridad pertinentes, y que cuenta con los recursos y las definiciones de las responsabilidades para gestionar los riesgos.

2) Desarrollar un inventario de componentes o controles implementados para gestionar los riesgos.

3) Establecer casos de negocio pertinentes y adecuados para la implementación del plan de tratamiento de riesgos.

4) En base al plan de tratamiento de riesgos, establecer la entrega de información para el desarrollo de soluciones.

5) Establecer esquemas de medición de la efectividad de las actividades o prácticas de gestión y detallar los parámetros o forma de utilizar dichas mediciones.

6) Impulsar actividades para la capacitación y formación en seguridad de la información.

7) Establecer estrategias para integrar los procedimientos de seguridad de información que permitan detectar eventos adversos de seguridad y se logre una adecuada gestión y respuesta a incidentes (ISACA, 2012).

4.8 Propuesta para evaluar el nivel de implementación de un SGSI en la fase de planificación

Se propone un formato para evaluar el nivel de avance de la gestión de un Sistema de Seguridad de la Información en la etapa de Planificación (PLAN) de acuerdo al ciclo PDCA utilizado para esta propuesta. El formato puede ser modificado de acuerdo a las necesidades y requerimientos de cada organización; no obstante, sí deben considerarse todos los entregables mencionados.

En la matriz se incluyen los aspectos esenciales por cada uno de los pasos requeridos para una planeación de un SGSI que deben ser considerados en la etapa de planeación. Se proyecta un nivel de cumplimiento en base a 3 parámetros: implementado, parcialmente implementado y no implementado.

A continuación, en la Tabla 24 se muestra una plantilla de valoración del estado de implementación para la fase de planeación de un SGSI, en base al conocimiento adquirido en el desarrollo de este trabajo. Las respuestas corresponden a un ejemplo práctico en una entidad financiera.

Tabla 24.

Plantilla de evaluación del nivel de implementación de un SGSI en su fase de planeación

N°	Actividades a Considerar	Implementación		
		Si	Parcial	No
1. Definición del Alcance				
1	Se ha considerado los asuntos externos e internos que comprenden la organización y su contexto. Los requerimientos y necesidades de las partes interesadas. Se ha considerado aquellas interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.		1	
2	Se ha establecido un análisis de impacto del negocio (BIA), procesos críticos y esenciales para la continuidad del negocio.	1		
3	Se conoce claramente las líneas de negocio, productos o servicios que ofrece, el Core organizacional, cliente objetivo, estructura organizacional.		1	
4	Se ha efectuado un análisis del posicionamiento de la organización, presencia a nivel nacional e internacional.	1		
5	Se cuenta con un levantamiento de activos		1	
2. Definición de la Política de SGSI				
6	La política se encuentra documentada, disponible y es pertinente al objetivo estratégico de la Organización		1	
7	La política incluye los objetivos de seguridad de la información y proporciona el marco de trabajo, las responsabilidades, roles y funciones	1		
8	La política incluye un compromiso para satisfacer los requisitos aplicables relacionados a la seguridad de la información	1		
9	Incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información			1

N°	Actividades a Considerar	Implementación		
		Si	Parcial	No
3. Identificación y clasificación de activos				
10	Se han identificado los roles y responsabilidades para las áreas involucradas en el proceso y se ha efectuado la capacitación respectiva	1		
11	Se ha identificado y definido los activos de información por cada responsables o propietario	1		
12	Los activos han sido identificados y valorados conforme los aspectos de integridad, confidencialidad y disponibilidad de la información		1	
13	Se ha obtenido un nivel de clasificación del activo conforme su grado de confidencialidad			1
4. Definir el contexto del Riesgo.				
14	La metodología de valoración del riesgo es aplicable al SGSI y a los requerimientos reglamentarios, legales y de seguridad de la información del negocio.	1		
15	Se han definido los criterios de evaluación del riesgo, los criterios de impacto y los criterios de aceptación del riesgo.	1		
16	La metodología seleccionada para valoración de riesgos asegura que dichas valoraciones producen resultados comparables y reproducibles.		1	
5. Valoración del Riesgo				
17	Se han identificado los activos de información (punto 3), las posibles amenazas y los controles existentes.		1	
18	Se han identificado las vulnerabilidades y las posibles consecuencias que un activo podría sufrir al comprometer su integridad, disponibilidad o confidencialidad (posibles escenarios).		1	
19	Se ha obtenido un nivel de estimación del riesgo considerando el impacto y la probabilidad de los escenarios		1	
20	Se ha efectuado una evaluación del riesgo comparando los niveles de riesgo versus los criterios definidos en el contexto de evaluación del riesgo y su aceptación			1

N°	Actividades a Considerar	Implementación		
		Si	Parcial	No
6. Definir el tratamiento del Riesgo				
21	Se han establecido los criterios para gestionar el riesgo (reducir, aceptar, evitar o transferir)		1	
22	Se ha definido un plan de tratamiento de riesgo que identifique claramente el orden prioritario para la implementación de cada tratamiento			1
23	Se ha evaluado el riesgo residual, el cual permanece a pesar de la aplicación de los controles		1	
24	Se ha registrado formalmente la decisión de aceptación del riesgo y las respectivas responsabilidades.			1
7. Implementación de Controles				
25	Los objetivos de control y los controles se han seleccionado de manera que cumplan con los requisitos identificados en el proceso de valoración y tratamiento de riesgos.		1	
26	La selección de los objetivos tiene en cuenta los criterios para la aceptación de riesgos al igual que los requisitos legales, reglamentarios y contractuales.		1	
8. Elaborar la declaración de aplicabilidad				
27	La declaración incluye los objetivos de control y los controles seleccionados y las razones para su selección.	1		
28	La declaración incluye los objetivos de control y los controles implementados actualmente.			1
29	La declaración incluye la exclusión de cualquier objetivo de control y controles enumerados en el Anexo A y la justificación para su exclusión.		1	

N°	Actividades a Considerar	Implementación		
		Si	Parcial	No
9. Establecer el plan de Tratamiento de Riesgos				
30	El plan de tratamiento de riesgos incluye las actividades de implementación de todos los controles establecidos en el enunciado de aplicabilidad		1	
31	El plan detalle claramente por cada control los recursos, responsabilidades y prioridades que se derivan de la evaluación de riesgos.	1		
32	Se han identificado los roles y responsabilidades de los gestores del Plan		1	
33	El plan de Tratamiento de riesgos se encuentra alineado a los objetivos estratégicos del negocio			1
TOTAL		**10**	**16**	**7**
		30.30%	**48.48%**	**21.2 %**

De los resultados obtenidos se puede observar que un 30.30% conforme los parámetros establecidos se encuentra “implementado”, un 48.48% se encuentra parcialmente implementado y un 21.2% no está implementado o no se ha iniciado. Es importante mencionar que se requiere de un 100% de cumplimiento en todos los aspectos listados para poder asumir que la fase de Planeación de un SGSI está completa.

4.8.1 Análisis de Resultados

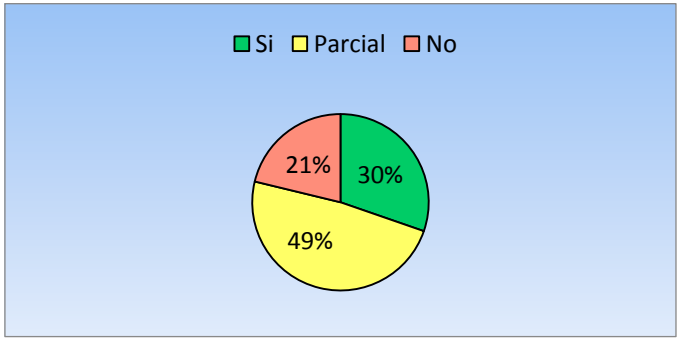
Del ejemplo práctico se obtiene los siguientes resultados:

Tabla 25.

Evaluación Preliminar

Concepto	1. Definición del Alcance	2. Definición de la Política de SGSI	3. Identificación y clasificación de activos	4. Definir el contexto del Riesgo	5. Valoración del Riesgo	6. Definir el tratamiento del Riesgo	7. Implementación de Controles	8. Elaborar la declaración de aplicabilidad	9. Establecer el plan de Tratamiento de Riesgos	**Total**
Si	2	2	2	2	0	0	0	1	1	10
Parcial	3	1	1	1	3	2	2	1	2	16
No	0	1	1	0	1	2	0	1	1	7
Total	5	4	4	3	4	4	2	3	4	**33**

En este gráfico se obtiene la sumatoria por cada paso / fase de acuerdo a la respuesta otorgada de implementación (Si, Parcial, No), en donde de acuerdo a los resultados y para efectos del ejercicio práctico se muestra una mayor tendencia en la "implementación parcial" con 16 registros que representa el 49%, en la siguiente figura se muestra el resultado:



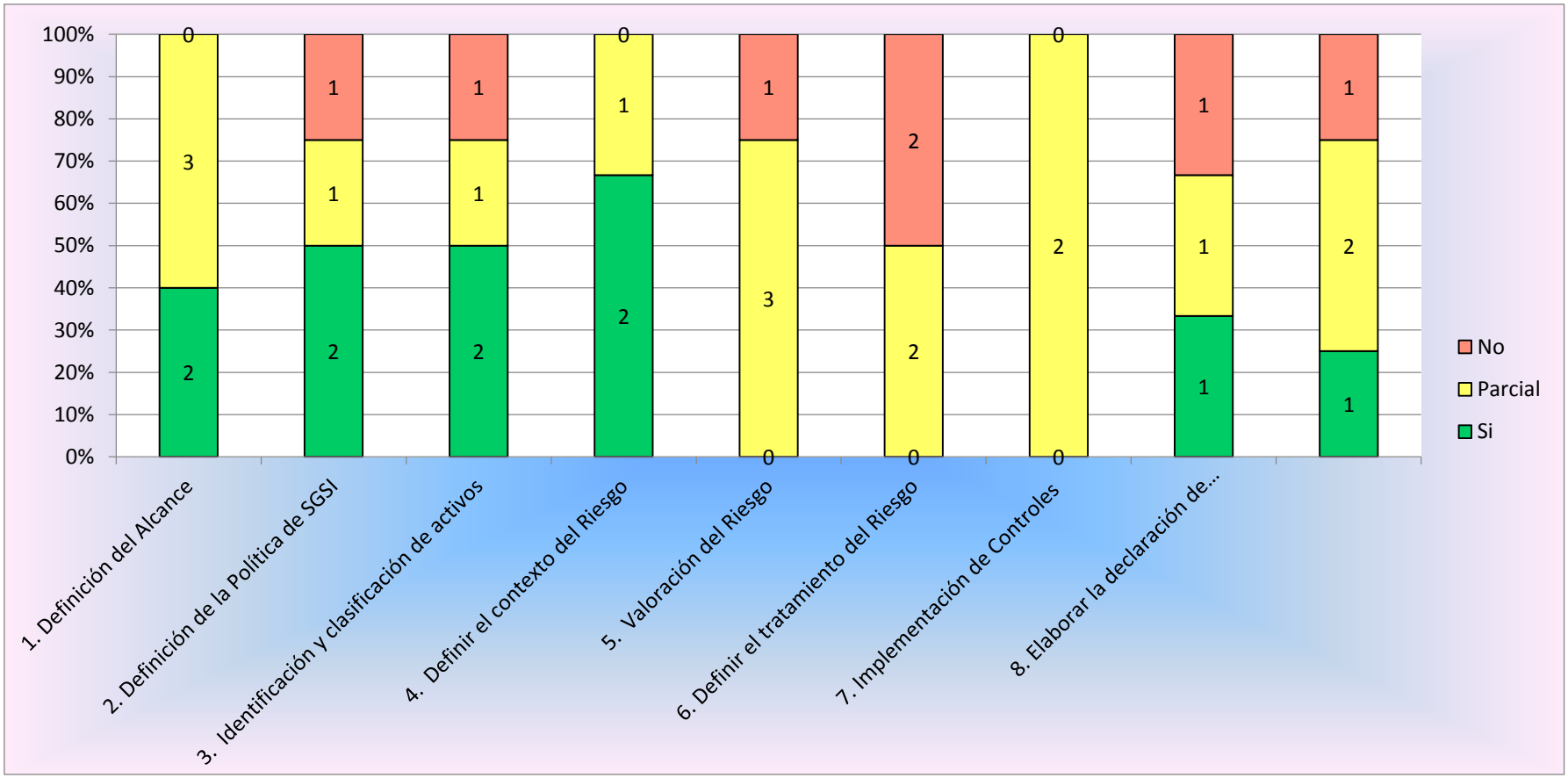


Figura 24. Resultados evaluación preliminar por fase

Evaluación Final

A continuación, en la tabla 26 se presenta los resultados finales consolidados entre lo implementado y lo pendiente (no implementado o parcialmente implementado) para poder determinar el estado real del SGSI. En la figura 25 se muestra la brecha existente entre lo esperado y el estatus actual. Se observa que en los aspectos de la definición de una política de seguridad y la identificación y clasificación de activos la entidad se encuentra mayormente encaminada al objetivo; no obstante, para el aspecto de la definición de controles requiere de acciones prioritarias para su avance e implementación.

Tabla 26.

Resultados finales

Estado	1. Definición del Alcance	2. Definición de la Política de SGSI	3. Identificación y clasificación de activos	4. Definir el contexto del Riesgo	5. Valoración del Riesgo	6. Definir el tratamiento del Riesgo	7. Implementación de Controles	8. Elaborar la declaración de aplicabilidad	9. Establecer el plan de Tratamiento de Riesgos	TOTAL
Implementado (si)	2	2	2	2	0	0	0	1	1	10
No Implementado (no, parcial)	3	2	2	1	4	4	2	2	3	23
Ponderación	10	10	10	10	10	10	10	10	10	**33**
Evaluación	4.00	5.00	5.00	6.67	0.00	0.00	0.00	3.33	2.50	

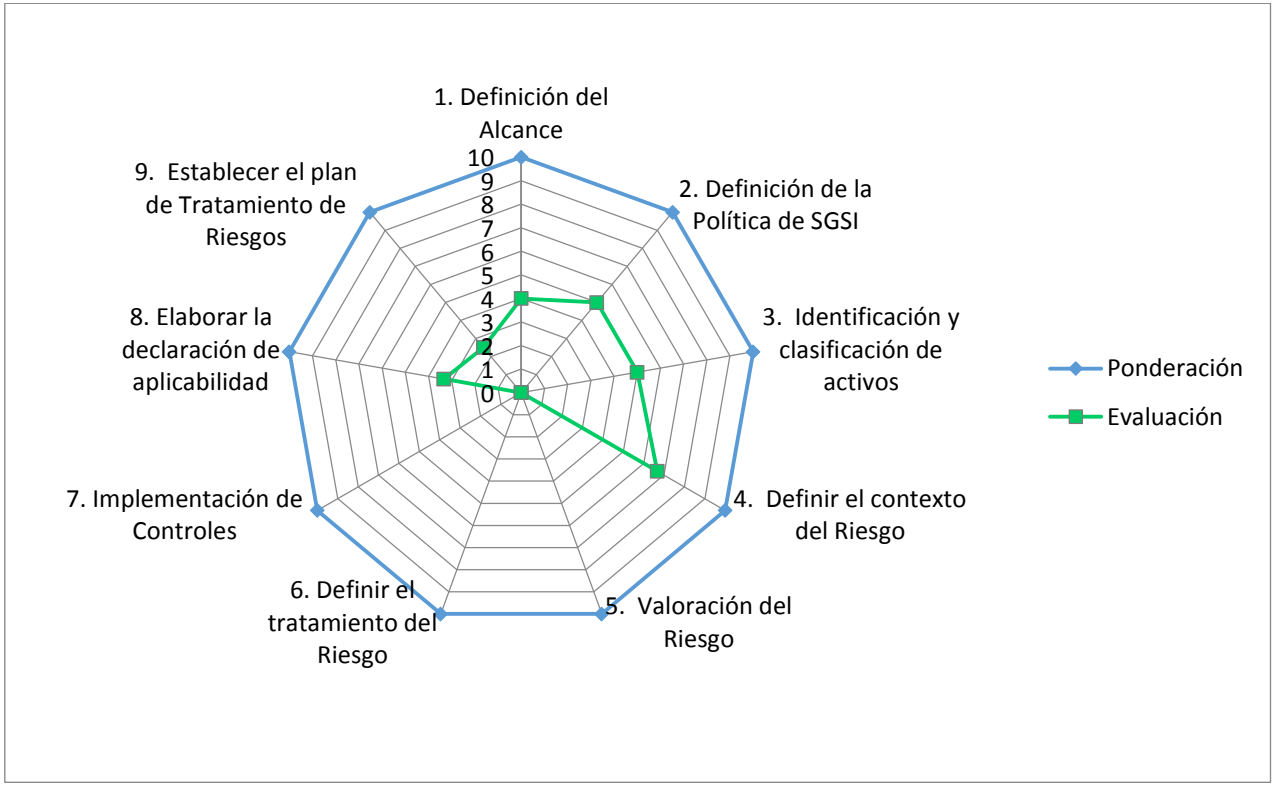


Figura 25. Brecha entre lo esperado y el avance actual

5. Capítulo V: Evaluación y análisis de la aplicación de la propuesta

5.1 Introducción:

En este capítulo se determinará y analizará la aplicación de la propuesta enunciada en los capítulos previos a este trabajo en varios ámbitos como son: Legal/normativo, económico, organizacional y operacional. La norma ISO 27001:2013 menciona que: “La adopción del Sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información de la organización está influenciada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y la estructura de la organización” (ISO/IEC 27001, 2013), por tanto, en este capítulo se analizará la factibilidad real de implementación en una organización de la industria bancaria frente a los requisitos mínimos necesarios para establecer un SGSI, así como sus posibles limitantes o restricciones al cumplimiento. El ideal no siempre puede ser aplicable en todos los casos, por esta razón toma importancia el concepto desde el cual se entiende a la aplicación de los requerimientos conforme a las necesidades, objetivos, tamaño y estructura de la organización.

5.2 En el aspecto legal y normativo

De acuerdo al documento publicado por Silvia Delgado Vera “Aplicación de los intereses pasivos y activos en el sistema bancario ecuatoriano y sus efectos macroeconómicos 2013”, establece que: “El marco legal del sistema financiero ecuatoriano lo constituye un conjunto de leyes, reglamentos, decretos, normas y resoluciones que regulan la actividad financiera y se establecen en herramientas y documentos especiales para regularizar el ahorro y la inversión de los diversos elementos para el desarrollo de la economía. Se conforma por:

- La Constitución Política del Ecuador.

- La ley General de instituciones del Sistema Financiero (a partir del 2 de septiembre de 2014 es reemplazada por el Código Orgánico Monetario y Financiero)

Nuestra Constitución en su Art. 308 dice: Las actividades financieras son un servicio de orden público, y podrán ejercerse, previa autorización del estado, de acuerdo con la ley.

La Constitución de la República del Ecuador, determina las normas generales de la actividad financiera a través de la Superintendencia de Bancos. La ejecución de la política crediticia y financiera también se ejercerá a través de la banca pública" (Vera, 2015).

"El código orgánico Monetario y Financiero tiene por objeto regular los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador. La Superintendencia de Bancos efectuará la vigilancia, auditoría, intervención, control y supervisión de las actividades financieras que ejercen las entidades públicas y privadas del Sistema Financiero Nacional, con el propósito de que estas actividades se sujeten al ordenamiento jurídico y atiendan al interés general" (Registro Oficial de la Asamblea Nacional, 2014).

Por tanto, siendo la Superintendencia de Bancos la encargada de la supervisión y control de dichas entidades, ha determinado el cumplimiento obligatorio de lineamientos de seguridad los cuales han sido detallados en el capítulo II, y se expresan mediante la resolución N° JB -2005-834 del 20 de Octubre de 2005 norma "De la gestión del Riesgo Operativo", y en su última modificación JB-2014-3066, las mismas que se fueron modificando en el capítulo V de la Gestión de Riesgo Operativo. En la sección VII de la norma que hace referencia a la Seguridad de la Información en el artículo 21 donde se menciona: *"Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya*" (Superintendencia de Bancos y Seguros,

2014), adicionalmente en el artículo 22 se menciona lo siguiente: "*Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información"* (Superintendencia de Bancos y Seguros, 2014).

Siendo esta norma de carácter obligatorio toma mayor relevancia la factibilidad y cumplimiento que cada organización debe establecer para gestionar un Sistema de Gestión de Seguridad de la Información y dar cumplimiento al mismo.

Respecto de limitantes en el ámbito legal no se encontraron artículos en la Constitución Política que se contrapongan a lo determinado por el ente de control; al contrario, una entidad de la vertical financiera se encuentra obligada a cumplir con los lineamientos de seguridad expresados en la norma de Riesgo Operativo citada anteriormente, caso contrario podrá ser objeto de sanción o multa para la institución.

5.3 En el aspecto económico

La implementación de un Sistema de Gestión de la Seguridad implica una serie de gastos de tipo económicos a la organización que están vinculados a la implementación de controles, sin embargo se debe considerar que frente a las amenazas actuales a las que se encuentra vulnerable las organizaciones del tipo de industria bancaria la cual es objeto de este estudio, por contener información de tipo sensible y confidencial de los clientes que puede derivar en acciones delictivas como fraude, robo de identidades, suplantación y por consecuencia afectaciones directas a la imagen de la organización y pérdidas económicas; por esto la importancia de adoptar el concepto de "inversión" y no de "gasto", ya que una gestión efectiva de la seguridad de la información permitirá evitar o minimizar impactos mayores provenientes de ataques o vulnerabilidades a los sistemas. Cuando la organización efectúa el análisis de sus riesgos tiene la capacidad de conocer el impacto económico de un fallo de la seguridad y la probabilidad de que pueda ocurrir.

El análisis de riesgos debe estar encaminado a cubrir las necesidades y requerimientos de seguridad de una organización, en donde se deberá considerar los recursos económicos y humanos con los que cuenta la organización. La inversión en seguridad tiene que ser correspondiente al riesgo.

Durante la fase de planeación de un SGSI es importante estimar los recursos económicos y humanos que van a ser requeridos para todas las fases de un SGSI desde su planeación hasta su mejora continua, de nada serviría que se realicen grandes esfuerzos en las etapas de planeación e implementación si no existe medición de resultados y procesos para la mejora continua.

Al ser una propuesta en general para la industria bancaria, no se puede tener una estimación de costos totales ya que el presupuesto dependerá de muchos aspectos como: la estructura de la organización, su tamaño, su nivel de madurez en gestión de la información, sus recursos humanos, etc.

A continuación, se describen algunos aspectos que deben ser considerados al momento de estimar un presupuesto para el desarrollo e implementación de un Sistema de Gestión de la Información:

5.3.1 Costos de asistencia externa

Las normas como la ISO 27001 proporcionan información de gran utilidad para el desarrollo e implementación de un SGSI, sin embargo, dicha información no siempre es suficiente para poder gestionar el alcance y desarrollo de un proyecto de seguridad. Se debe evaluar si la seguridad se implementará con soporte externo (proveedores, consultores) o con los recursos únicamente internos.

Si se implementa con recursos únicamente internos los costos serán menores pero el tiempo estimado será mayor y se requerirá de mayores horas de trabajo para cada recurso asignado. Por tanto, en base a la experiencia para esta propuesta se recomienda la implementación al menos de una primera fase con el soporte externo (consultores / proveedores).

Es importante recalcar que todo dependerá del presupuesto estimado que la Alta dirección ha determinado en sus objetivos estratégicos anuales.

5.3.2 Costo recurso humano interno

Tiempo del recurso interno en el involucramiento de los lineamientos, alcance y conocimiento de cada proceso dentro del alcance del SGSI, desarrollo de la documentación, capacitación interna, etc.

En la fase de planificación es importante estimar los tiempos del recurso interno, definir el porcentaje de tiempo de cada jornada de trabajo que se utilizará para la planificación y desarrollo del proyecto de implementación de un SGSI, se debe establecer acuerdos de comunicación para los entregables y para los niveles a los cuales se van a reportar los avances.

5.3.3 Costo en tecnología

Para la implementación de ciertos controles será necesaria la inversión de tecnología, como por ejemplo para el control A.8.3.2 de la categoría “Manejo de los medios”, la cual dice que: “Se deben eliminar los medios de forma segura y sin peligro cuando ya no se necesiten, usando procedimientos formales”, para este caso será muy probable la contratación de una empresa especializada en destrucción que garantice la eliminación con procedimientos formales y que garantice que la información eliminada no será recuperada por externos. Una inversión muy importante es la del proceso de continuidad del negocio, requiere de la implantación de sitios alternos de procesamiento para garantizar la disponibilidad y la continuidad de las operaciones.

5.3.4 Costos de capacitación

La implementación de la norma ISO 27001 implica cambios a las empresas no solo en sus procesos, documentación o procedimientos sino también en las capacidades y conocimientos de las personas, por tanto para poder

implementar un Sistema de Gestión de la información es necesario preparar al recurso humano que va a ejecutar los planes establecidos y esto involucra la adquisición de la norma, cursos, guías, etc.

5.3.5 Costo de certificación

Esto aplica para el caso en que la organización haya decidido ingresar al proceso de certificación de la norma, para difundir el cumplimiento de sus procesos de seguridad en la información de manera pública.

De acuerdo a lo mencionado por la "27001 Academy" en una de sus publicaciones, "la entidad de certificación tendrá que realizar una auditoría de certificación, cuyo costo dependerá de la cantidad de días/hombre que le demande hacer el trabajo: podrá ser desde menos de 10 días/hombre para empresas pequeñas hasta unas docenas de días/hombre para organizaciones más grandes. El costo del día/hombre depende del mercado local" (Kosutic D. , 2011).

Es importante mencionar que estos costos implican una inversión inicial, ya que se requiere cada cierto tiempo (3 años) efectuar una re-certificación, de lo contrario ya no se encontraría vigente.

5.4 En el aspecto organizacional

Como ya se mencionó previamente, los lineamientos de la norma ISO 27001 para la implementación de un SGSI son aplicables a cualquier tipo o estructura de una organización, es decir, de acuerdo a las necesidades y a los objetivos de una entidad se pueden adaptar los procesos y los requerimientos de la norma. Por tanto, no existen limitantes en el aspecto organizacional, lo que es importante recordar, es que el proceso de adaptación a un nuevo esquema y procesos de seguridad requiere como primer paso del apoyo y compromiso de la Alta Dirección para su implementación.

La implementación de un Sistema de Gestión de Seguridad de la Información se encuentra determinada por la estructura organizacional de cada empresa, sus objetivos, servicios, productos, etc. Para el caso de estudio, en las empresas de la vertical bancaria toma mayor relevancia su planificación e implementación por ser un requerimiento que involucra un cumplimiento regulatorio.

Se recomienda que un SGSI sea analizado e implementado priorizando en una primera fase aquellos departamentos o áreas en donde se gestiona la información Core o esencial para la normal operatividad de las funciones y procesos de la entidad.

Una estructura organizacional debe ser diseñada tomando en cuenta la capacidad del personal perteneciente a la entidad. A continuación, en la figura 26 se muestra un ejemplo de una estructura organizacional de un banco del Ecuador:

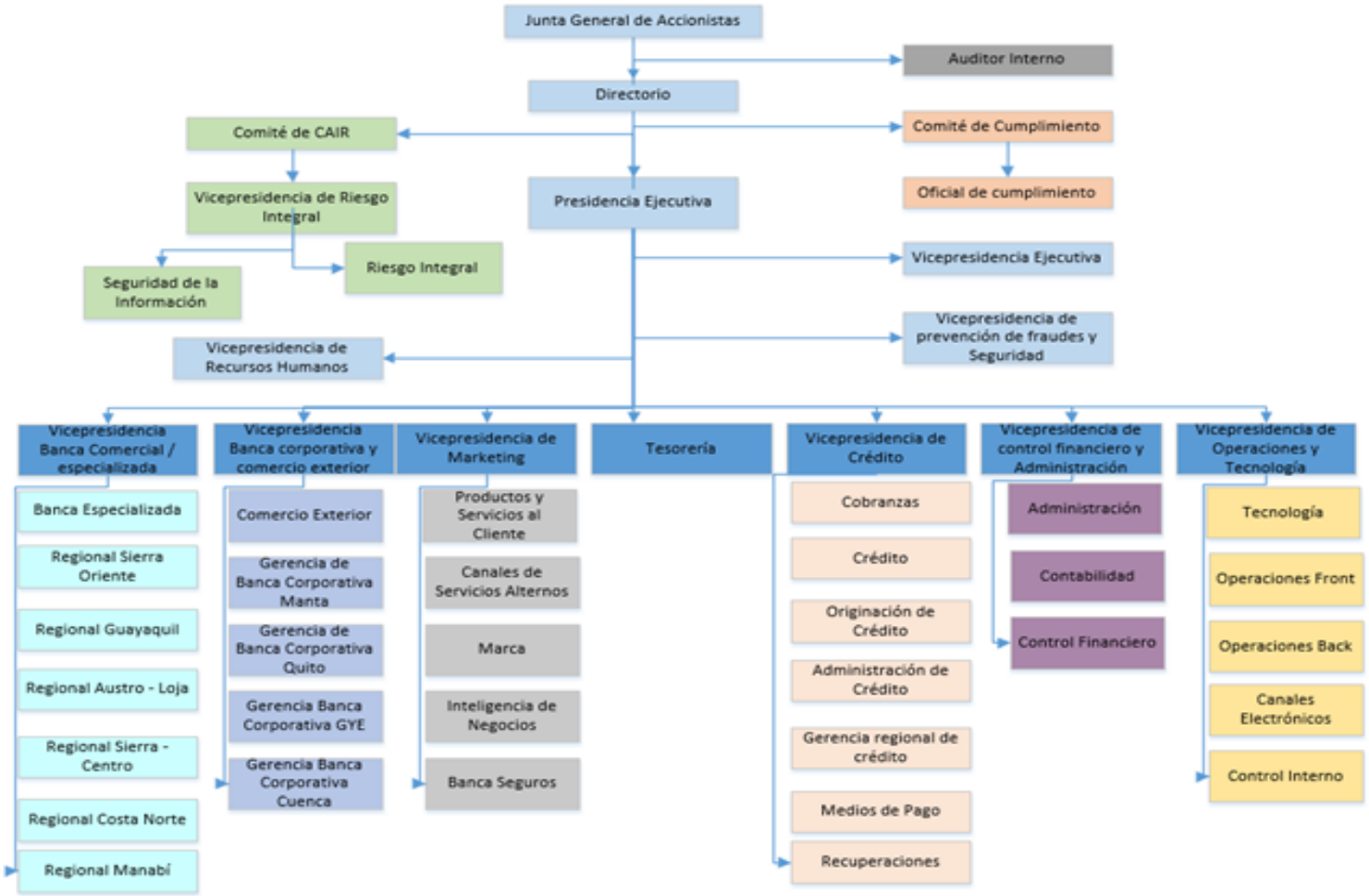


Figura 26. Estructura organizacional de un Banco del Ecuador

Fuente: Adaptado de (Portal interno BI, 2017)

5.5 En el aspecto operacional

La propuesta presentada se basa en un modelo de procesos denominado “Ciclo de Deming”: Planificar, Hacer, Verificar y Actuar (PHVA), dicho modelo se sustenta en un esquema de mejora continua la cual requiere de procesos de revisión periódica para lograr una adaptación a los cambios que pueda suscitarse en una organización, dentro del alcance que se ha definido para el SGSI, esto es un aspecto fundamental para lograr una eficacia operativa en todo el ciclo del modelo.

Si bien, el aspecto operativo es fundamental en una organización y aún más en una entidad bancaria por su tamaño y su orientación al servicio, se debe considerar que la base de toda gestión efectiva se encuentra en la determinación de los procedimientos claves y concisos que deben ser llevados a cabo por todos los involucrados. Los procedimientos son los documentos que van a ser generados en la fase de “implementación” de un Sistema de Gestión de la seguridad.

La ISO 27001:2013 en su numeral 8.1 “Control y planificación operacional” determina que: “la organización debe mantener la información documentada hasta que sea necesario y tener la certeza que los procesos se llevaron a cabo según lo planeado. La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no planificados, al tomar acciones para mitigar cualquier efecto adverso, según sea necesario” (ISO/IEC 27001, 2013), por tanto, los limitantes mayores que se ha encontrado en este aspecto pueden radicar en la falta de compromiso de los ejecutores o de una falta de planeación, documentación y capacitación de los mismos, siendo que este proceso es puramente colaborativo se requieren de dichos factores para su éxito. A continuación, en la figura 27 se presenta una síntesis del capítulo en la cual se resume los aspectos esenciales a considerar:

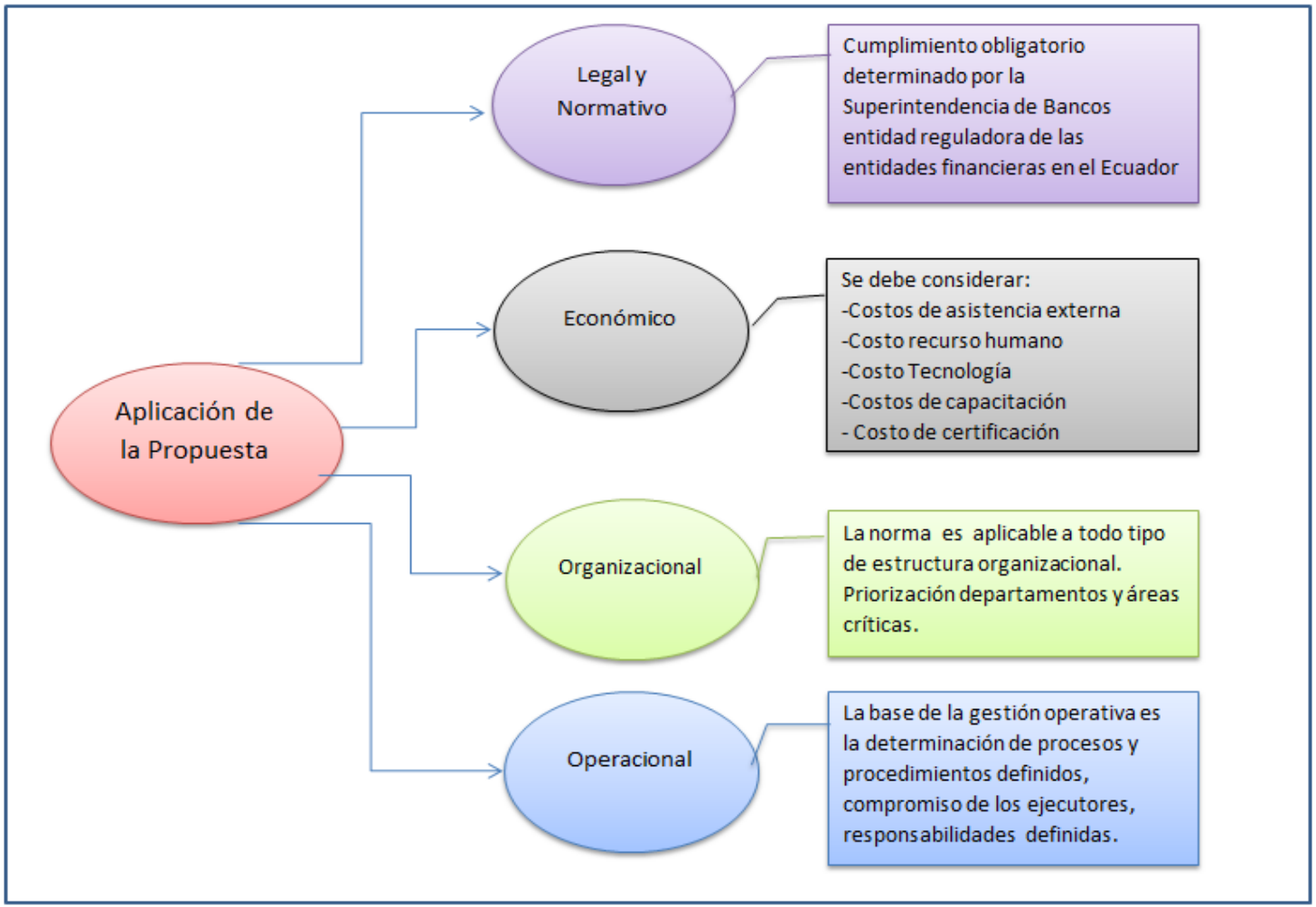


Figura 27. Síntesis del capítulo V – Análisis de la aplicación de la Propuesta

6. Capítulo VI: Formulación de un plan de monitoreo, medición y control del SGSI

6.1 Definición de la medición del cumplimiento del proceso

Una parte muy importante de la gestión de la Seguridad de la información es la medición o evaluación de los resultados. No se puede determinar la eficacia de un SGSI si no se puede medir el cumplimiento y los resultados.

Se requiere del uso de métricas las cuales serán de ayuda para el cumplimiento de los objetivos y para la evaluación de la eficacia de resultados. Además que proporcionan datos que reducirán costos ocasionados por problemas en su implementación.

Para evaluar el cumplimiento del proceso, el marco de referencia COBIT ha determinado métricas relacionadas a los objetivos que permiten obtener un grado de cumplimiento del proceso.

A continuación, se presenta en la tabla 27 la recopilación de algunas métricas para evaluar y medir el nivel de cumplimiento del proceso de gestión de la seguridad y de la implementación de un SGSI y que se basa en el marco de referencia COBIT 5 en procesos como el APO13 (Gestionar la Seguridad), DSS05 (Gestionar los servicios de Seguridad), APO12 (Gestionar el Riesgo), etc.

Tabla 27.

Ejemplo de métricas para evaluar el nivel de cumplimiento del SGSI

Meta u Objetivo	Métricas Relacionadas
Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	Número de roles de seguridad claves claramente definidos
	Número de incidentes relacionados con la seguridad
Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
	Nivel (%) de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa
	Número de soluciones de seguridad que se desvían del plan
Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	Número de servicios con alineamiento confirmado al plan de seguridad
	Número de incidentes de seguridad causados por la no observancia del plan de seguridad
	Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad
Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado
La gestión y tratamiento del Riesgo está implementado adecuadamente	Número y porcentaje de medidas que no reducen el riesgo residual
La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	Número y porcentaje de incidentes relacionados con accesos no autorizados a la información
La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final, al ingreso a la organización y durante el año
	Número y porcentaje de incidentes que impliquen dispositivos de usuario final

Tomado de (ISACA, 2012)

6.2 Objetivos de la medición de la seguridad de la información

De acuerdo a lo mencionado en la ISO/IEC 27004:2009 los objetivos de la medición de la seguridad de la información en relación con un SGSI incluyen lo siguiente:

a) “Evaluar la eficacia de los controles aplicados o grupos de controles.
b) Evaluar la eficacia de la aplicación SGSI.
c) Verificar el grado en el que se fijaron las necesidades de seguridad y saber si han sido cumplidas.
d) Facilitar la mejora del rendimiento de la seguridad de la información en cuanto a los riesgos de negocio de la organización global.
e) Proporcionar información para la revisión por parte de la dirección para facilitar la toma de decisiones relacionadas con el Sistema de Gestión de Seguridad de la Información y justificar la necesidad de mejora de la aplicación del SGSI” (ISO/IEC 27004, 2009).

A continuación, se ilustra las relaciones cíclicas de entradas y salidas de la medición de actividades en relación al ciclo PDCA, especificado en la ISO/IEC 27001.

Los números de cada figura representan sub-cláusulas relevantes de la ISO/IEC 27001:2005

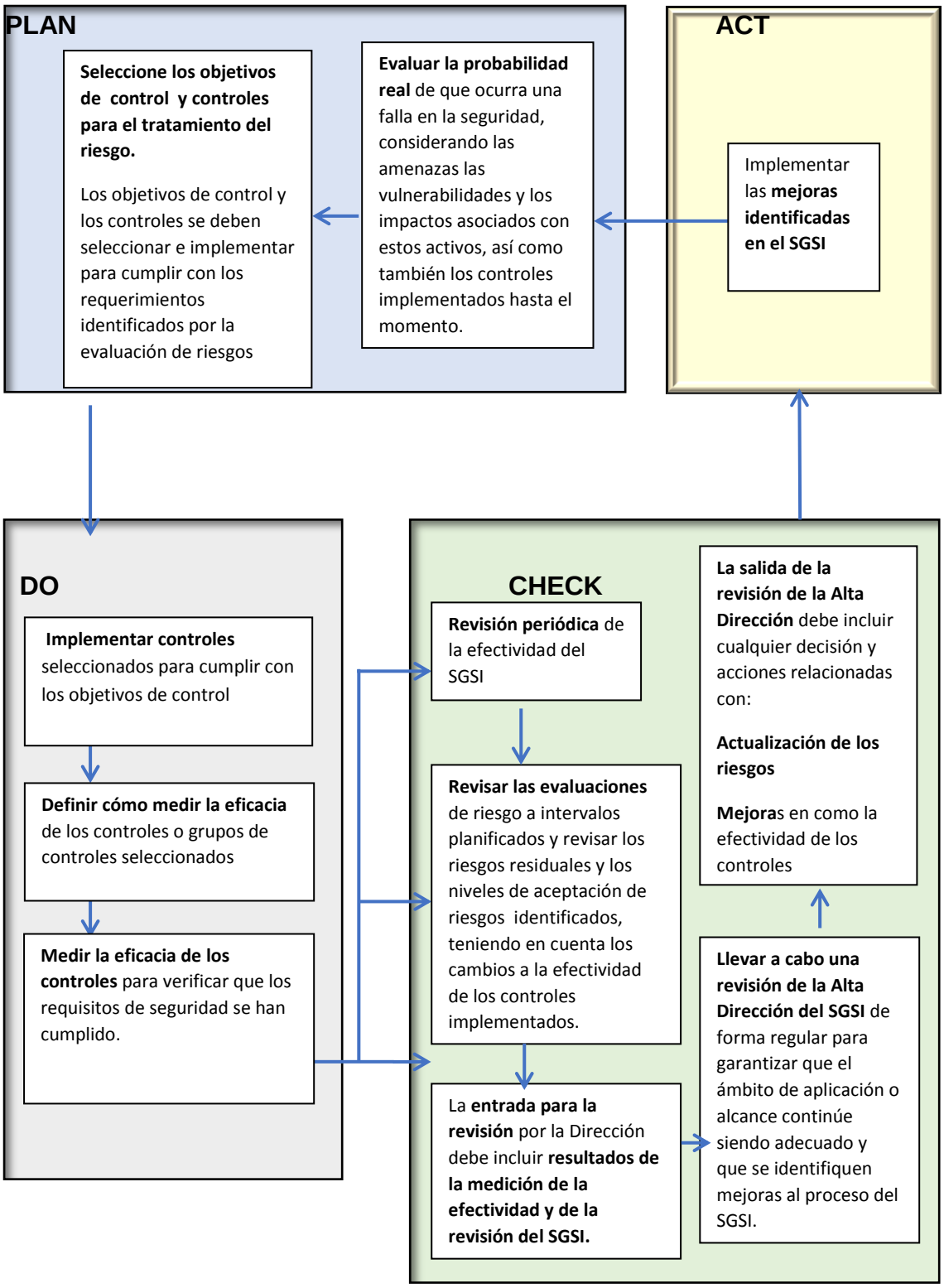


Figura 28. Entradas y salidas en el ciclo PDCA de la Gestión de Seguridad de la Información

Adaptado de (ISO/IEC 27004, 2009)

La organización deberá establecer los objetivos de medición basados en una serie de consideraciones:

a) El rol de la seguridad de la información en apoyo de actividades generales y de riesgos de la organización empresarial.
b) Los requisitos legales aplicables, reglamentarios y contractuales.
c) La estructura organizacional
d) Costos y beneficios de implementar medidas de seguridad de la información
e) Los criterios de riesgo de aceptación de la organización
f) La necesidad de comparar varios Sistemas de Gestión de Seguridad de la Información dentro la misma entidad.

6.3 Proceso para la medición de la eficacia de la seguridad de la información

La norma ISO/IEC 27004 proporciona orientación sobre la elaboración y utilización de parámetros y la medición, para evaluar la eficacia de un sistema de gestión de la información. Esto incluye entre otros la política, la administración del riesgo de seguridad de la información, objetivos de control, controles, procesos y procedimientos.

Apoyar al proceso de revisión, ayuda adicionalmente a determinar si alguno de los procesos del Sistema de Gestión de Seguridad de la Información o los controles implementados necesita cambios o mejoras. Se debe considerar que ninguna medición puede garantizar una seguridad total, no existe la seguridad absoluta.

La normativa se puede aplicar a cualquier tipo de organización y establece etapas con el objetivo de medir la eficacia de la seguridad de la información.

6.3.1 Etapas de medición de la eficacia de la seguridad de la información:

De acuerdo al blog especializado de SGSI las etapas aplicables de la medición son las siguientes:

1. **Selección procesos y objetos de medición.**

Las empresas deben definir lo que hay que medir y el alcance de la medida. Sólo se consideran en la medición los procesos bien documentados que son consistentes y repetibles. Objetos de medición puede ser el rendimiento de los controles o de procedimientos, el comportamiento del personal, etc.

2. **Definición de las líneas base.**

Los valores base que muestran el punto de referencia deben definirse para cada objeto que se está midiendo.

3. **Recopilación de datos.**

Los datos deben ser dimensionales precisos y oportunos. Se pueden emplear técnicas automáticas de obtención de datos para lograr una recolección estandarizada y presentar informes.

4. **Desarrollo del método de medición.**

Según ISO 27004, la secuencia lógica de operaciones se aplica en diversos atributos del objeto seleccionado para la medición. Se usan indicadores como fuentes de datos para mejorar el rendimiento de los programas de seguridad de la información (ISO/IEC 27004, 2016).

5. **Interpretación de los valores medidos.**

Mediante procesos y la tecnología para el análisis y la interpretación de los valores se deben identificar las brechas entre el valor inicial y el valor de medición real.

6. **Comunicación de los valores de medición.**

Los resultados de medición del SGSI se comunicarán a las partes interesadas. Se puede hacer en forma de gráficos, cuadros de mando operacionales, informes o boletines de noticias, etc. (Excellence, ISOTools, 2014).

6.4 Tipos de medidas

6.4.1 General:

La norma ISO/IEC 27004 en su versión 2016 menciona lo siguiente: El desempeño de las actividades planificadas y la efectividad de los resultados se pueden medir aplicando los dos siguientes tipos de medidas:

a) **medidas de desempeño:** medidas que expresan los resultados previstos en términos de las características de la actividad planificada, tales como la cuantificación de personal, logros de hitos o el grado en que se han implementado controles de seguridad de la información.
b) **medidas de efectividad:** medidas que expresan el efecto que la realización de las actividades planificadas tiene en los objetivos de seguridad de la información de las organizaciones.

Estas medidas pueden ser específicas de la organización, ya que cada organización tiene sus propios objetivos, políticas y requisitos específicos de seguridad de la información (ISO/IEC 27004, 2016).

6.4.2 Medidas de desempeño

La norma ISO/IEC 27004 menciona que las medidas de desempeño pueden utilizarse para demostrar el progreso en la implementación de los procesos del SGSI, procedimientos asociados y controles específicos de seguridad, mientras que la efectividad se refiere a la medida en que se han realizado las actividades planificadas y se han alcanzado los resultados previstos, las medidas de desempeño deberían referirse a la medida en que se han implementado los procesos y controles de seguridad de la información. Estas medidas ayudan a determinar si los procesos del SGSI y los controles de seguridad de la información se han implementado de acuerdo a lo especificado.

Las medidas de rendimiento utilizan datos que se pueden obtener de registros de asistencia, planes de proyectos, herramientas de escaneo automatizado y

otros medios comúnmente utilizados para documentar, registrar y monitorear las actividades del SGSI.

La recopilación, el análisis y la notificación de las medidas deberían automatizarse siempre que sea posible, a fin de reducir el costo y el esfuerzo requerido y el potencial error humano (ISO/IEC 27004, 2016).

6.4.3 Medidas de efectividad

La norma ISO/IEC 27004 menciona que las medidas de efectividad deben usarse para describir la efectividad y el impacto que las realizaciones del plan de tratamiento de riesgos del SGSI y los procesos y controles del SGSI tienen sobre los objetivos de seguridad de la información de la organización. Estas medidas deberían utilizarse para determinar si los procesos del SGSI y los controles de seguridad de la información están funcionando según lo previsto y lograr los resultados deseados. Dependiendo de esos objetivos, se pueden usar medidas de efectividad para cuantificar. Por ejemplo:

a) ahorro de costos producidos por el SGSI o los costos incurridos en el tratamiento de incidentes de seguridad
b) el grado de confianza del cliente
c) la consecución de otros objetivos de seguridad de la información.

La medida de efectividad puede ser creada combinando los datos obtenidos de las herramientas automatizadas de monitoreo y evaluación con datos obtenidos de forma manual sobre las actividades del SGSI. Para lograr esto, una organización debe tener una capacidad establecida para:

d) evaluar el grado en que los procesos, controles o grupos de controles del SGSI han sido implementados
e) recopilar datos de las herramientas automatizadas para el monitoreo y evaluación,
f) recopilar manualmente información de las actividades del SGSI;

g) normalizar y analizar datos procedentes de múltiples fuentes automatizadas y manuales; y
h) interpretar y reportar estos datos para la toma de decisiones (ISO/IEC 27004, 2016).

Ejemplificando lo dicho anteriormente, podemos medir el nivel de compromiso que mantiene la alta dirección con el desarrollo del SGSI, por tanto, una **medida de desempeño** será la asistencia a las revisiones periódicas y otras reuniones que puedan ser convocadas. El resultado previsto en este caso es la asistencia plena a todas las reuniones, la medida es simplemente cuántos asisten frente a cuántos deben asistir. Al principio, los resultados de estas medidas podrían indicar un déficit, sin embargo, con el tiempo, los resultados deben alcanzar y permanecer cerca de los objetivos previstos. En este punto, la organización debe comenzar a concentrar sus esfuerzos de medición en **medidas de efectividad**.

Después de que la mayoría de las medidas de rendimiento alcancen y permanezcan al 100%, la organización debe comenzar a concentrar sus esfuerzos de medición en medidas de efectividad. Estas medidas de eficacia combinan información sobre la realización del plan de tratamiento de riesgos con una variedad de información sobre los recursos y pueden aportar insumos al proceso de gestión de riesgos.
También pueden proporcionar la visión más directa sobre el valor de la seguridad de la información para la organización y pueden ser los que deberían ser de mayor interés para la alta dirección (ISO/IEC 27004, 2016).

6.5 Desarrollo del modelo o método de medición

El modelo de medición de la seguridad de la información de acuerdo a lo planteado en la norma ISO 27004 es una estructura que vincula una necesidad de información con los objetos de medición pertinentes y sus atributos. Los objetos de medición pueden incluir procesos, procedimientos, proyectos y recursos planificados o implementados (ISO/IEC 27004, 2009). El modelo de

medición de seguridad de la información describe cómo los atributos concernientes son cuantificados y convertidos en indicadores, los cuales proveen la base para la toma de decisiones (ISO/IEC 27004, 2009).

La figura 29 se presenta una adaptación de las relaciones claves en el modelo de medición de la seguridad de la información reformado en la norma ISO/IEC 27004 versión 2016:

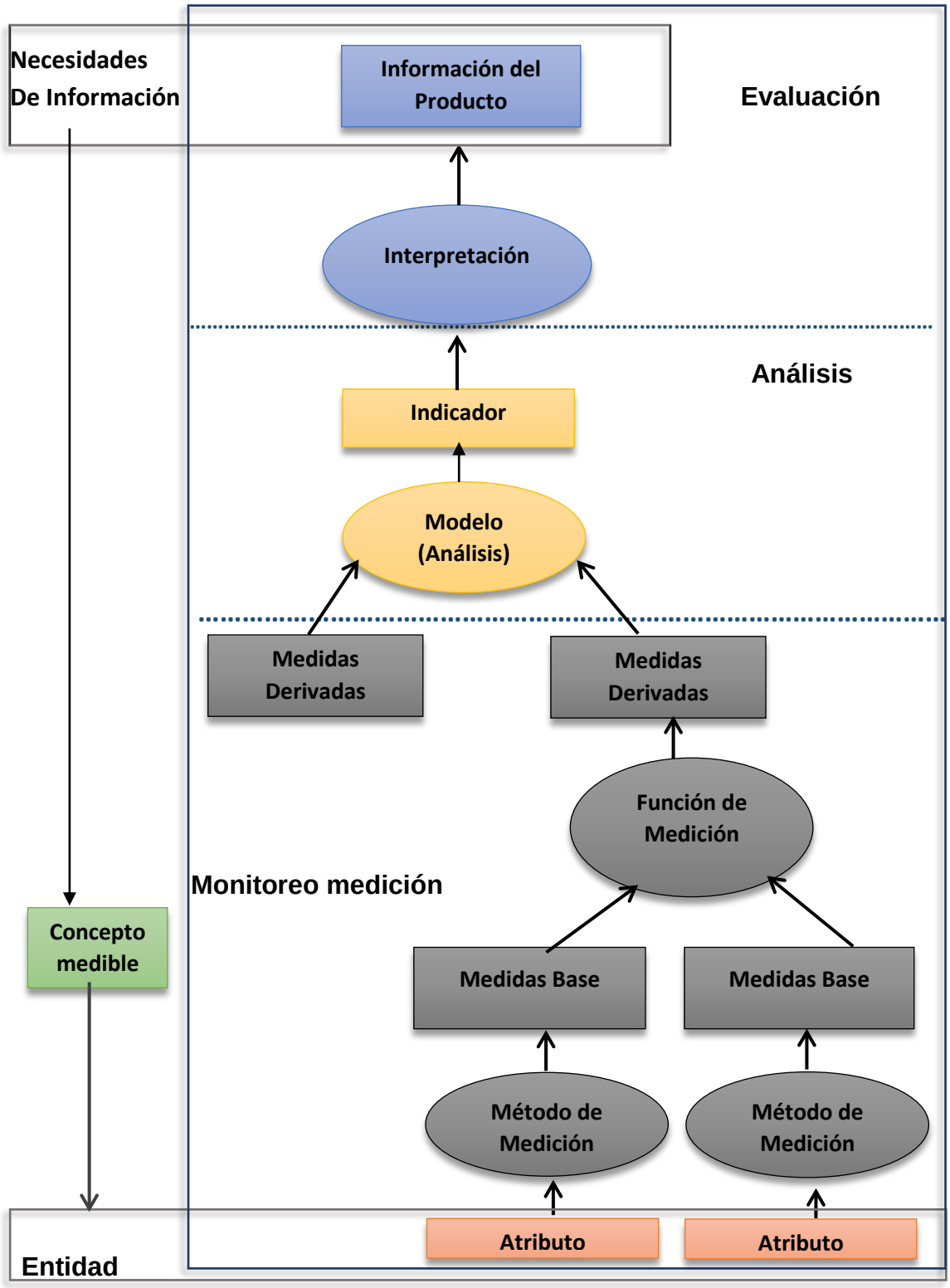


Figura 29. Relaciones claves en el modelo de medición de la información

Adaptado de (ISO/IEC 27004, 2016)

Para poder comprender el esquema de medición se describen a continuación el significado de los elementos del diagrama:

Atributo.- propiedad relevante para la necesidad de información.

Método de medición.- Operaciones que asignan o mapean un atributo a una escala.

Medida base.- Variable asignada a un valor, aplicando el método a un atributo.

Función de medición.- Algoritmo para combinar dos o más medidas base.

Medida derivada.- Variable asignada a un valor, aplicando la función de medición a dos o más valores de medidas base.

Modelo de Análisis.- Algoritmo para combinar medidas y criterios de decisión.

Indicador.- Variable asignada a un valor mediante la aplicación del modelo de análisis a la base y / o medidas derivadas.

Interpretación.- Explicación o detalle relacionado a la información cuantitativa en el indicador con las necesidades de información en el lenguaje de los usuarios de medición.

Producto de información.- el resultado del proceso de medición que satisface las necesidades de información.

6.5.1 Aplicación del modelo de medición

“Una medida base es la medida más simple que se puede obtener, esta resulta de la aplicación de métodos de medición sobre los atributos seleccionados de un objeto de medición. Un objeto de medición puede tener muchos atributos, de los cuales sólo algunos pueden tener valores útiles para ser asignados a una medida base.

Un método de medición es una secuencia lógica de operaciones utilizado para cuantificar un atributo con respecto a una escala específica, cuando se habla de operaciones estas pueden incluir, el conteo de ocurrencias o el paso de tiempo” (ISO/IEC 27004, 2009).

Un método de medición se puede aplicar a los atributos de un objeto de medición, los cuales pueden ser: rendimiento de los controles implementados, estado de los activos de información, conocimiento y comportamiento del personal frente a los lineamientos de seguridad de la información, grado de satisfacción de las partes interesadas, etc. Un método de medición puede utilizar objetos de medición y atributos de una variedad de fuentes como por ejemplo: resultados del análisis de riesgos, reportes de auditorías, reporte de incidentes, resultados de test penetration, etc. (ISO/IEC 27004, 2009).

A continuación en la tabla 28 se muestra un ejemplo de la aplicación del modelo de medición para el control A.8.1.1 Inventario de activos, el cual determina que: "Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos", el control pertenece al objetivo de control: A.8 Administración de activos y a la categoría: A.8.1 Responsabilidad por los activos.

Tabla 28.

Ejemplo de Medida base y método de medición

Objeto o Concepto medible (O)	Atributo (A)	Método de Medición (M)	Medidas Base (MB)
O.1 Definición del alcance de los activos de información	A.1 Activos identificados en el plan (O.1)	M.1 Contar la cantidad de procesos de la institución incluidos para el levantamiento de los activos	MB.1 Procesos levantados a la fecha
O.2 Plan de Capacitación al personal propietario y custodio de los activos de información	A.2 Personal identificado en el plan (O.2)	M.2 Contar la cantidad de personas programadas para recibir la capacitación	MB.2 Personal planificado a la fecha

La tabla 28 incluye un ejemplo de las relaciones entre un objeto o concepto medible de la gestión de un SGSI, un atributo, un método de medición y su medida base para medir los objetos establecidos por los controles implementados.

6.5.2 Medida derivada y función de medición

La medida derivada es una combinación de dos o más medidas base, por tanto una medida base puede servir como entrada para varias medidas derivadas.

Una función de medición es un cálculo utilizado para combinar medidas base que resulte de manera tal que permita obtener una medida derivada (ISO/IEC 27004, 2009).

“La función de medición puede involucrar una variedad de técnicas, tales como promediar las medidas base, aplicando ponderación a las medidas base, o asignando valores cualitativos a las medidas base. La función de medición puede combinar medidas base utilizando diferentes escalas, tales como resultados de evaluaciones porcentuales o cualitativas” (ISO/IEC 27004, 2009).

En la siguiente tabla se muestra con respecto al ejemplo de la tabla 28 la aplicación de la función de medición y la medida derivada obtenida:

Tabla 29.

Ejemplo de Medida derivada y Función de Medición

Medida Base (MB)	Función de Medición (F)	Medida Derivada (MD)
MB.1 Procesos identificados a la fecha	F.1 Dividir el número de procesos levantados a la fecha por el total de procesos existentes en una Organización.	MD.1 Progreso a la fecha (MB.1)
MB.2 Personal planificado a la fecha (A.2)	No contiene medida derivada, va directo al modelo de análisis →	

6.5.3 Indicadores y modelo analítico

“Un indicador es una medida que provee una estimación o valoración de atributos específicos derivados de un modelo analítico con respecto a necesidades de información definidas. Los indicadores se obtienen aplicando un modelo analítico a las medidas base y/o derivadas, y combinándolas con

los criterios de decisión. La escala y el método de medición afectan la elección de técnicas analíticas utilizadas para producir los indicadores" (ISO/IEC 27004, 2009).

En la tabla 30 se muestra para el ejemplo planteado las relaciones entre las medidas derivadas, el modelo analítico y los indicadores, para el desarrollo del modelo de medición.

Tabla 30.

Ejemplo de indicadores y el modelo analítico

Medida Derivada (MD)	Modelo Analítico (MA)	Indicador (I)
MD.1 Progreso a la fecha (MB.1) **De MB.2 – ver Tabla 31**	MA.1 (Dividir el progreso a la fecha MD.1) por los procesos existentes. Lo planificado a la fecha (MB.2) multiplicado por 100.	I.1 Estado expresado como una combinación de proporciones (MD.1 / MB.2 * 100)

6.5.4 Interpretación de los resultados

Los resultados de la medición se obtienen interpretando indicadores y tomando en consideración criterios de decisión.

Los criterios de decisión sirven para identificar las necesidades de una acción o actividad, así como también para establecer el nivel de confianza en los resultados. Los criterios de decisión se pueden aplicar a diversos indicadores como por ejemplo analizar tendencias, tiempos, etc. (ISO/IEC 27004, 2009).

La siguiente tabla muestra para el ejemplo planteado la relación entre los indicadores y su interpretación sobre los resultados obtenidos en el modelo de medición.

Tabla 31.

Ejemplo de relación entre el indicador y el análisis e interpretación de resultados

Indicador (I)	Interpretación de resultados (IR)
I.1 Estado expresado como una combinación de proporciones (MD.1 / MB.2 * 100)	IR.1 Los resultados obtenidos deberían encontrarse en un porcentaje entre: 90 y 100% para concluir la consecución esperada de cumplimiento del objetivo de control, de lo contrario será necesario establecer una planificación adicional para su cumplimiento.

6.6 Factores de éxito

De acuerdo a lo mencionado en la ISO/IEC 27004:2009 los siguientes son algunos de los factores que contribuyen al éxito del programa de medición de seguridad de la información y facilitan la continua mejora del SGSI:

1. Compromiso de la dirección con los recursos apropiados
2. Existencia de procesos y procedimientos del SGSI;
3. Un proceso repetible capaz de capturar y reportar datos significativos para proporcionar tendencias relevantes durante un período de tiempo;
4. Medidas cuantificables basadas en los objetivos del SGSI;
5. Datos fácilmente obtenibles que pueden utilizarse para la medición;
6. Evaluación de la eficacia del Programa de Medición de la Seguridad de la Información y aplicación de mejoras identificadas;
7. La recopilación periódica consistente, el análisis y la notificación de los datos de medición;
8. Utilización de los resultados de la medición por los *stakeholders* relevantes para identificar las necesidades de mejorar del SGSI
9. Aceptación de la retroalimentación sobre los resultados de medición de los *stakeholders* relevantes; y

10. Evaluaciones de la utilidad de los resultados de medición y la implementación de mejoras identificadas.

Una vez implementado con éxito, un Programa de Medición de la Seguridad de la Información puede:

a) Demostrar el cumplimiento de una organización con los requisitos legales o reglamentarios aplicables y las obligaciones contractuales;
b) Apoyar la identificación de problemas de seguridad de la información previamente no detectados o desconocidos;
c) Ayudar en la satisfacción de las necesidades de informes gerenciales cuando se establezcan medidas para actividades históricas y actuales; y
d) Ser utilizado como insumo en el proceso de gestión de riesgos de seguridad de la información, auditorías internas del SGSI y revisiones de gestión (ISO/IEC 27004, 2009).

A continuación, en la figura 30 se presenta una síntesis del capítulo VI en la cual se resumen las actividades y aspectos a considerar para un modelo de medición de seguridad de la información:

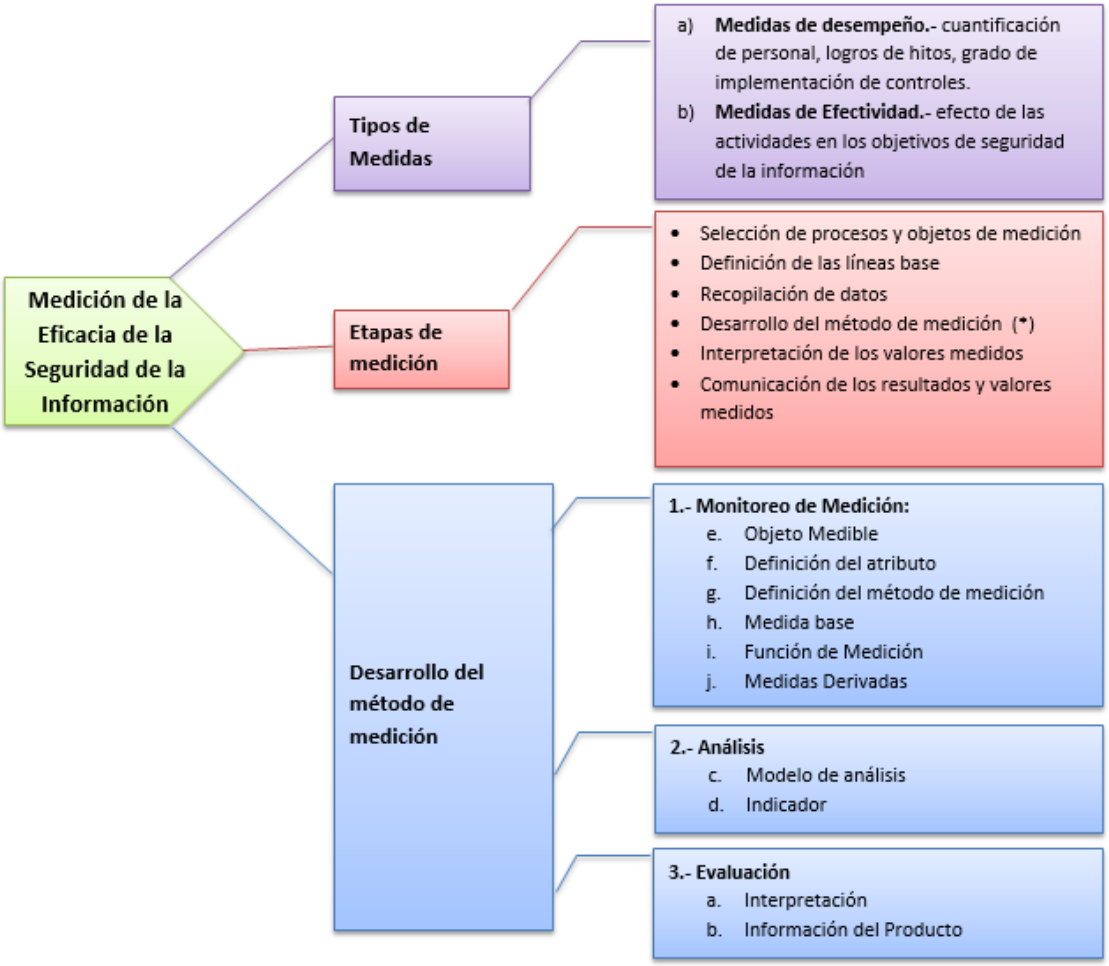


Figura 30. Síntesis del capítulo VI Medición de la Eficacia de la Seguridad de la Información

7. Conclusiones y Recomendaciones

7.1 Conclusiones

La implementación de un sistema de gestión de seguridad de la información debe ser parte de los objetivos estratégicos del negocio, difícilmente se podrán obtener los resultados esperados si el SGSI no apalanca la misión, visión y objetivos de la empresa, adicionalmente la definición de procesos en sí no son suficientes, se requiere del compromiso y la aceptación de la alta gerencia para lograr en el tiempo un sistema sostenible.

Para que un SGSI se constituya como tal, es necesario que la entidad implemente la totalidad de requerimientos que se mencionan en este documento, y especialmente para el caso de estudio (instituciones de la industria bancaria) se debe considerar los requerimientos normativos mínimos con los que deben cumplir las entidades, los cuales se encuentran apalancados en la norma ISO 27001.

Un aspecto importante que debe considerar toda entidad que se encuentre en proceso de implementación de un SGSI, es la determinación del alcance, es necesario analizar los asuntos internos y externos, requerimientos de las partes interesadas, procesos críticos, estructura organizacional, etc., no es necesario abarcar la totalidad de procesos y áreas de forma inicial, el SGSI es un sistema de mejora continua aplicable a pocos o muchos procesos y a cualquier tipo de entidad.

El establecimiento de un SGSI no es un proceso estático, debe encontrarse en un ciclo de evaluación y mejora continua, la cual se logra mediante la medición de objetivos y de la eficacia de los controles, por tanto, de nada serviría un gran trabajo y esfuerzo en las etapas de planeación e implementación si no se realiza auditorías y revisiones posteriores que permitan obtener resultados de la efectividad del proceso.

El análisis de los riesgos nos permite obtener como resultado un mapa de calor en base a los criterios de evaluación, de impacto y de aceptación del riesgo, en donde la Dirección de la entidad deberá establecer el apetito de riesgo o la tolerancia al riesgo que está dispuesta asumir, y de acuerdo a esta decisión se planteará el plan para el tratamiento del riesgo.

Cuando se realiza la clasificación de los activos de información, existe el riesgo de que la valoración se torne subjetiva debido a que la apreciación se encuentra atada al criterio del evaluador, es de vital importancia establecer umbrales o escalas que permitan eliminar dicha subjetividad sustentando las valoraciones en base a lineamientos o límites establecidos tanto para los aspectos operativos, legales, económicos y de imagen.

La base de toda gestión exitosa se encuentra en el compromiso y la responsabilidad de los involucrados y de la alta gerencia, para lograrlo es necesario generar la idea de una inversión, mas no de un costo innecesario a la organización, es importante recordar que el eslabón más débil en la cadena de vulnerabilidades son las personas y es ahí donde se debe iniciar la concientización de la seguridad.

7.2 Recomendaciones

Las entidades financieras deben incluir como parte de sus objetivos estratégicos el establecimiento, implementación y mejora de un sistema de gestión de la seguridad de la información, cimentando la importancia de dicho aspecto para los logros organizacionales.

Se recomienda evaluar la capacidad de la organización para implementar los requerimientos obligatorios y necesarios que establece un SGSI, se debe determinar y no subestimar los tiempos, presupuesto, recursos, limitantes, etc. que demanda el proceso de implementación de un SGSI en una organización.

Se recomienda a las entidades financieras y en general cualquier tipo de organización, establecer un alcance del SGSI que sea realista y viable de acuerdo a las capacidades de la organización, no es necesario abarcar la totalidad de procesos sino más bien enfocarse en aquello que requiere la organización y que forma parte del Core del negocio. Es importante recordar que el tiempo estimado de vigencia para un levantamiento de procesos para un SGSI es de 6 meses a 1 año, pasado este tiempo los cimientos del proceso pueden empezar a quedar obsoletos.

Se recomienda a las entidades financieras establecer esquemas de medición del sistema de gestión de seguridad de la información basados en la efectividad de los controles implementados y emprender un proceso continuo para su mejora.

Al gestionar los riesgos se recomienda a la alta gerencia establecer un equilibrio, de tal manera que se pueda controlar los riesgos a los cuales se encuentra inmersa una organización sin alterar los objetivos del negocio.

Se recomienda que en el proceso de levantamiento y clasificación de activos, se realice una capacitación previo a la valoración por parte de los custodios y propietarios de la información, sobre los criterios mediante los cuales se van a identificar a los activos y posteriormente a clasificar, determinar con las áreas especializadas los umbrales y límites que servirán para valorar los activos y eliminar en gran parte la subjetividad.

Establecer dentro de la planificación del área de seguridad de la información de la entidad, un cronograma de capacitaciones permanentes en el año acerca de los temas relevantes y principios de seguridad de la información como son: ingeniería social, escritorios limpios, política de seguridad de la información, seguridad de accesos, etc. que permita prevenir vulnerabilidades propias del desconocimiento de los empleados sobre la protección de la seguridad de la información.

REFERENCIAS

Academy 27001. (2014). Informe: Lista de documentación obligatoria requerida por ISO/IEC 27001. Recuperado el 10 de Febrero de 2016 de https://lciso27000.files.wordpress.com/2015/02/iso-27001-lista-documentacion-requerida.pdf

Academy, 2. (2013). Qué es norma ISO 27001. Recuperado el 3 de Octubre de 2016 de http://www.iso27001standard.com/es/que-es-iso-27001/

AeTecno. (2012). El espectador.com. Recuperado el 12 de Abril de 2016 de https://tecno.americaeconomia.com/articulos/segun-kaspersky-80-del-malware-busca-el-robo-de-informacion-bancaria

Alexander, A. G. (2014). ISO27001.es. Recuperado el 20 de Abril de 2016 de Análisis y Evaluación del Riesgo de Información: Un Caso en la Banca: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf

Amaya, C. G. (2015). WeliveSecurity. Recuperado el 22 de abril de 2016 de https://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion/

Área de Seguridad BI. (2016). Clasificación de la Información. Quito, Ecuador.

Asociación de Bancos Privados del Ecuador. (2014). Boletín informativo de la asociación de Bancos Privados del Ecuador. Recuperado el 20 de Marzo de 2016 from http://www.asobancos.org.ec/ABPE_INFORMA/42_2014.pdf

Balaguer, I. M. (2013). La nueva Versión ISO 27001:2013.

Consejo Superior de Administración Electrónica. (2012). Libro II Catálogo de Elementos. In C. S. Electrónica, MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (tercera ed., p. 75). Madrid .

COSO. (2013). Informe COSO (Quinta ed.).

Delgado, M. F. (2014). Taller de Implementación de la norma ISO 27001. Recuperado el 20 de Julio de 2016 de http://www.academia.edu/29923191/Taller_de_Implementaci%C3%B3n_de_la_norma_ISO_27001

Díaz, G. (2006). De Gerencia.com. Recuperado el 4 de Mayo de 2016 de http://www.degerencia.com/articulo/los_sistemas_de_informacion_en_las_entidades_bancarias_estrategias_escenarios_y_desafios_futuros

El Espectador. (2012). El espectador. Recuperado el 7 de Marzo de 2016 de http://www.elespectador.com/tecnologia/delitos-informaticos-causan-perdidas-millonarias-bancos-articulo-340755

Excellence, ISOTools. (2014). Blog Especializado en Sistemas de Gestión de Seguridad de la Información. Recuperado el 6 de Agosto de 2017 de http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/

Instituto Nacional de Tecnologías de la Comunicación. (2014). Implantación de un SGSI en la empresa. Recuperado el 18 de Julio de 2016 de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISACA. (2012). COBIT 5 (Sexta ed.).

ISACA. (2014). COBIT Focus Volumen 1. Recuperado el 5 de Abril de 2016 de https://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volumen-1-enero-de-2014.aspx

ISO. (2013). International Organization for Standardization. Recuperado el 11 de marzo de 2016 de https://www.iso.org/

ISO/IEC. (2006). Técnicas de Seguridad, Sistemas de Gestión de la seguridad de la Información (SGSI) Requisitos (Primera ed.).

ISO/IEC 27001. (2013). Norma NCH/ISO 27001 Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de la Seguridad de la Información - Requisitos (Segunda ed.). Chile.

ISO/IEC 27002. (2013). International Standard ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security controls (segunda ed.).

ISO/IEC 27004. (2009). International Standard ISO/IEC 27004 Information technology - Security techniques - Information security management - Measurement. In ISO/IEC.

ISO/IEC 27004. (2016). International Standard Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation (Segunda ed.).

ISO/IEC 27005. (2009). Norma Técnica NTEISO/IEC Ecuatoriana 27005 Tecnología de la información. Técnicas de seguridad. Gestión del Riesgo en la Seguridad de la Información. Ecuador.

ISO27001.es. (2012). Sistema de Gestión de la Seguridad de la Información. Recuperado el 21 de Marzo de 2016 de http://www.iso27000.es/download/doc_sgsi_all.pdf

ISOTools Excellence. (2015). Blog especializado en Sistemas de Gestión de Seguridad de la Información. Recuperado el 11 de Abril de 2016 de http://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Kosutic, D. (2011). 27001 Academy. Recuperado el 28 de Junio de 2017 de https://advisera.com/27001academy/es/blog/2011/02/08/cuanto-cuesta-la-implementacion-de-la-norma-iso-27001/

Kosutic, D. (2015). ISO 27001/ISO 22301 Base de conocimientos. Recuperado el 17 de Mayo de 2016 de

https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/

Oficina de Seguridad para las redes informáticas. (2013). Recuperado el 20 de Octubre de 2016 de http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Paez, C. (2015). Academia.edu. Recuperado el 18 de Marzo de 2016 de http://www.academia.edu/6744740/5._NIVELES_DE_MADUREZ_PARA_EL_PROCESO_DE_SEGURIDAD_DE

Perea, L. E. (2016). Desarrollo de Habilidades en el uso de las Tecnologías de la Información y la Comunicación.

Portal de ISO 27001 en español. (2012). ISO 27000.es. Recuperado el 16 de Abril de 2016 de http://www.iso27000.es/sgsi.html

Portal interno BI. (2017). Organigrama Banco Internacional. Quito, Ecuador.

Registro Oficial de la Asamblea Nacional. (2014). Código Orgánico Monetario y Financiero (Vol. segundo suplemento).

Segu.Info. (2012). Segu.Info Noticias sobre Seguridad de la Información. Recuperado el 4 de Mayo de 2016 de http://blog.segu-info.com.ar/2012/04/los-ataques-de-phishing-crecen-cerca-de.html

Subero, S. (2000). Monografías.com. Recuperado el 20 de Junio de 2016 de http://www.monografias.com/trabajos44/sistemas-administrativos/sistemas-administrativos.shtml

Superintendencia de Bancos y Seguros. (2014). Título X.- De la Gestión y Administración de Riesgos. In S. d. Seguros.

T.Doran, G. (2016). ObjetivosSmart 2.0. Recuperado el 13 de Marzo de 2016 de https://veritasonline.com.mx/objetivos-smart-2-0/

Trejo, G. (2013). Magazcitum. Recuperado el 15 de Mayo de 2016 de http://www.magazcitum.com.mx/?p=2397#.WXfossJK200

Turmero, I. J. (2014). Documentación del SGC: El enfoque basado en procesos. Recuperado el 10 de Junio de 2016 de http://www.monografiass.com/trabajos97/documentacion-del-sgc-enfoque-basado-procesos/documentacion-del-sgc-enfoque-basado-procesos.shtml

Vera, S. C. (2015). Eumed.net. Recuperado el 8 de Junio de 2017 de http://www.eumed.net/libros-gratis/2016/1502/index.htm

ANEXOS

Anexo 1. Ejemplos de vulnerabilidad por tipo de información con amenazas que pueden explotar dicha vulnerabilidad

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión	Abuso de los derechos
	(supervisión) de los derechos de acceso	
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones)	Abuso de los derechos
	Regulares	
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Tomado de (ISO/IEC 27005, 2009)

Anexo 2. Ejemplo formato de inventario de activos

En el Anexo se presenta un ejemplo del formato que puede ser utilizado para el registro e inventario de los activos de información.

TIPO DE DOCUMENTO: FORMATO	EMPRESA: (LOGO)	
TITULO: INVENTARIO DE ACTIVOS	FECHA DE ELABORACIÓN: MES / AÑO	NO. PAGINA: 1 DE 1

Id Activo	Área / Departamento	Proceso Asociado	Nombre Activo	Descripción	Activos Dependientes	Tipo Activo	Almacenamiento		Periodo Almacenamiento	Tiene Contingencia	Propietario	Custodio
							Digital	Físico				
1	Seguridad de la Información	Gestionar incidentes de Seguridad de la Información	Directriz de Control de Accesos	Directriz que mantiene los lineamientos para el control y generación de accesos a los distintos aplicativos de la organización	N/A	Activo de Información Tangible	Bodega 1, archivador 3	Disco D/Manuales y Directrices	Indefinido	NO	Gerente de Seguridad de la Información	Supervisor de Seguridad
2	Auditoria Interna	Mantener evidencia de las auditorias efectuadas	Papeles de trabajo	Documentación que contiene toda la evidencia, registros y papeles de trabajo fisico o lógico generado durante una revisión de auditoria	Herramienta /Aplicativo TeamMate	Activo de Información tangible e intangible	Archivo 1 auditoria	Disco Respaldo / Bases de Datos / Team Mate	Al menos 7 años	NO	Gerente de Auditoria Interna	Auditores Junior, Senior, Supervisores de Auditoria
3	Tecnologia - Infraestructura	Gestionar la infraestructura Tecnológica	Servidor de Aplicaciones	Equipo que realiza la función de servidor de aplicaciones	Servicio de Comunicaciones	Activo Fisico Tecnológico	N/A	Centro de Cómputo	Tiempo de vida útil del equipo	SI	Jefe de Infraestructura	Operadores del Centro de Cómputo
4	Servicios Financieros	Generar Captaciones	Certificados de depósitos	Instrumento financiero al portador, negociable, que se emite a la recepción de un depósito a plazo, representado por un titulo.	Solicitud de CID	Activo de Información Tangible	Archivador 1 / Servicios Finacieros	Servidor Compartido / Certificados	Al menos 7 años	NO	Jefe de Captaciones	Asesor de Servicios Financieros
5	Tecnologia	Administrar las Bases de Datos	Base de Datos MySQL	Repositorio de la información proveniente de la plataforma MySQL	Servidor de Base de Datos	Activo de Información Intangible	Servidor de Base de Datos	N/A	Al menos 7 años	SI	Jefe de Sistemas	Administrador de la Base de Datos
6	Tecnologia	Administrar la infraestructura lógica	Herramientas para desarrollo	Aplicativos para el desarrollo de software	Licencias del software	Activo de Software	N/A	Servidor de aplicaciones	N/A	SI	Jefe de Desarrollo	Analistas y Desarrolladores de Sistemas

Anexo 3. Matriz RACI (COBIT) Proceso Gestionar la Seguridad (APO13)

Se presenta el esquema de la matriz RACI de COBIT 5 en donde se identifica los roles y responsabilidades en la definición y gestión del plan de tratamiento del Riesgo.

Matriz RACI APO13																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de Negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
APO13.01 Establecer y Mantener un SGSI		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y Gestionar un plan de tratamiento del Riesgo de la seguridad de la Información		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Supervisar y revisar el SGSI					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Fuente: COBIT 5 – Procesos Catalizadores