PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU

FACULTAD DE CIENCIAS E INGENIERIA

SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA UNA INSTITUCION FINANCIERA

TESIS PARA OPTAR EL TÍTULO DE INGENIERO INFORMÁTICO

PRESENTADO POR:

MOISES ANTONIO VILLENA AGUILAR

LIMA – PERÚ

2006

DEDICATORIA

A mis padres Carolina y Francis por su incansable e ilimitado apoyo y amor incondicional a lo largo de toda mi vida de estudiante, y por ser hoy lo que soy gracias a ellos.
A mi hermano Gerardo por su inmenso amor y apoyo en todos los aspectos de mi vida.
A mi enamorada Susana por su amor sin fronteras y por su constante ánimo en concluir exitosamente este trabajo.

AGRADECIMIENTOS

Al Ingeniero Manuel Tupia por su apoyo y asesoría en la presente tesis y en mi desarrollo de asesor académico en la universidad.

Al Ingeniero Bruno Fernández por su valioso apoyo en el desarrollo del presente trabajo.

Al Ingeniero Carmen Quiroz por su valioso apoyo en mi desarrollo de asesor académico en la universidad

TABLA DE CONTENIDOS

RESUMEN

En la actualidad, las inversiones en seguridad que realizan las empresas se destinan cada vez menos a la compra de productos, destinando más bien parte de su presupuesto a la gestión de la seguridad de la información. El concepto de seguridad ha variado, acuñándose uno nuevo, el de seguridad gestionada, que va desplazando poco a poco al de “seguridad informática”. Las medidas que comienzan a tomar las empresas giran entorno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes: técnica, legal y organizativa, es decir, un planteamiento coherente de directivas, procedimientos y criterios que permiten desde la administración de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de información, la organización afín y sus infraestructuras.

Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que la seguridad absoluta no existe. Tomando lo anterior como punto de partida, una entidad puede adoptar algunas de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información,

La presente tesis ha realizado una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo relacionado a la Seguridad de Información.

I. INTRODUCCION

La información es el **principal activo** de toda organización según los más modernos paradigmas de la administración empresarial, pudiendo hacer su aparición de muchas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo, ilustrada en películas o hablada en conversaciones. En el ambiente de negocios competitivo de hoy, esa información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas, externas, accidentales o maliciosas para con la organización. Con el incremento del uso de nueva tecnología para almacenar, transmitir y recobrar información se han abierto canales para un mayor número y variedad de amenazas.

Se requiere establecer por tanto, un programa de gestión de seguridad de información dentro de cualquier tipo de organización. Es necesario asegurar la **confidencialidad, integridad, disponibilidad y auditabilidad** de la información vital para la corporación, el negocio y los clientes.

Una estrategia de gestión de la información es esencial para sobrevivir en el mercado actual. En la **Figura 1** se puede apreciar como los activos de información de una organización están rodeados de un complejo ambiente de objetos y amenazas que van desde simples virus de computadora hasta robos de la propiedad intelectual del negocio.

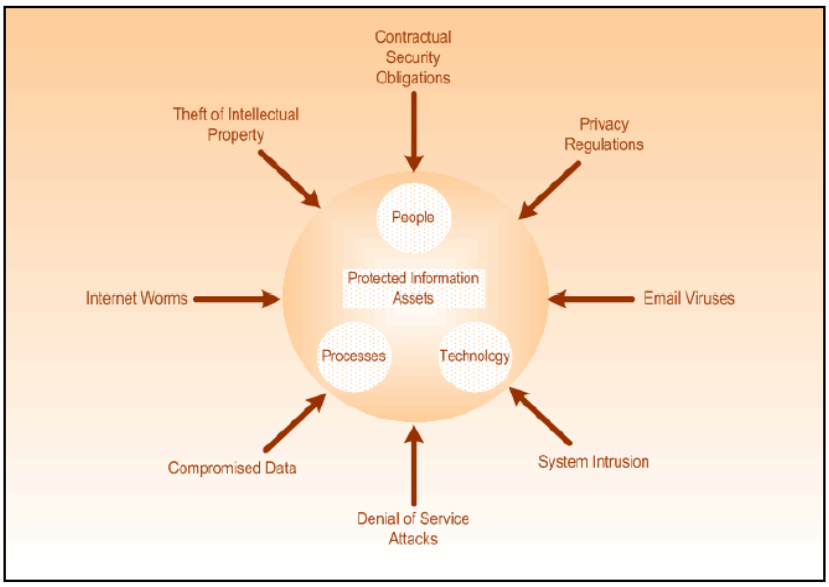

Figura 1. Activos de Información y su entorno [1]

II. OBJETIVOS Y ALCANCE

El objetivo de la presente tesis es establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado *modelo de sistema de gestión de seguridad de información* (SGSI) en una institución *financiera en el Perú*, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización.

En los dos de años de experiencia en consultaría para instituciones de micro finanzas, el autor de la presente tesis pudo constatar que a través de la adopción de las medidas adecuadas, un SGSI puede ayudar a una institución financiera a cumplir sus objetivos, protegiendo sus recursos financieros, sistemas, reputación, situación legal y otros bienes tanto tangibles como intangibles. De igual forma el autor de la presente tesis pudo observar que desafortunadamente, en ocasiones, se ve a un SGSI como una entidad complicada que dificulta la consecución de dichos objetivos, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo debe vérselo no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos.

Para este proyecto se tomara como referencia el modelo de seguridad de información de ***Mc Cumber*****,** por ser uno de los más influyentes, dado que abarca los principales estados de la información, características y medidas de seguridad. ***John R McCumber*** expuso en la decimocuarta edición de la ***National Computer Security Conference*** un modelo fácil y completo de seguridad, independiente del entorno, arquitectura o tecnología que gestiona la información. Su aplicación es universal y no está restringida por diferencias organizacionales. El modelo de tres dimensiones se convierte en un cubo con 27 celdillas como marco de actuación. **[2]**

El modelo se muestra en la siguiente figura:

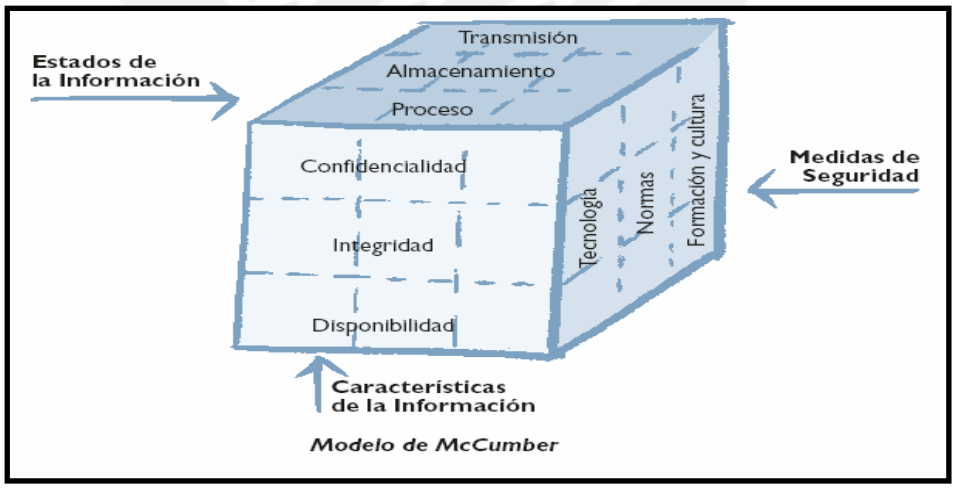

Figura 2. Modelo de Mc Cumber

A partir del modelo citado, la investigación cubrirá todos aquellos lineamientos a tener en cuenta en relación a estándares, normas, procedimientos y medidas tecnológicas que aseguren la confidencialidad, integridad, y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión. A esto se

le está agregando el aspecto de auditabilidad de la información (importante para la detección de accesos no autorizados a ella)

III. ESTADO DEL ARTE DEL PROBLEMA

En un mundo actual de constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado. Una efectiva administración sobre este tema es un aspecto de negocio y regulación, no sólo de tecnología.

A esto se suman las nuevas leyes y/o normas que van surgiendo **(Basilea II[1], Sarbanes Oxley[2])**, las cuales en un futuro cercano, impartirán lineamientos obligatorios sobre cómo las instituciones financieras del Perú deberán manejar su información, los controles internos que deberán asignarse e implementarse y el presupuesto que deberán destinar a la administración de los riesgos. **[6]**

La gestión de la seguridad de información deberá lidiar con estos aspectos de una manera proactiva y oportuna, para así poder ser considerada como efectiva, estando siempre alienada a los objetivos y estrategias de negocio de la organización. Por el momento la SBS viene exigiendo anualmente a las instituciones financieras, en oficios múltiples, información de gestión de sus seguros, alineados con los eventos establecidos por Basilea II.

1. JUSTIFICACION

Tomando como base lo expuesto surge la necesidad que toda institución financiera deba contar con un Sistema de Gestión de Seguridad de Información, el cual le permita administrar toda su información, garantizando los aspectos de confidencialidad, integridad, disponibilidad y auditabilidad que ésta debe cumplir.

Al mismo tiempo deberá permitir el cumplimiento de las normas vigentes de la Superintendencia de Banca y Seguros del Perú, la cual, en la actualidad y de manera paulatina, está adoptando las normas, leyes y estándares que imperan en Europa y Estados Unidos referentes a seguridad de información, control interno y cálculo de capital mínimo para riesgos, con la finalidad de implementarlos en las instituciones financieras del país en un futuro cercano. **[5]**

Hoy en día existen diferentes normas y estándares relacionados a la seguridad de información, que indican ***qué*** debe cumplir un adecuado SGSI, mas no señalan claramente el ***cómo*** lograrlo.

Se justifica así, la necesidad de un estudio centrado precisamente en analizar la manera implementar un adecuado SGSI a partir del análisis de las mejores prácticas y metodologías existentes.

---

[1] *Acuerdo de Basilea II establece estándares globales de administración de riesgos para instituciones financieras* **[3].**

[2] *Sarbanes Oxley Act del año 2002 (EEUU), establecido para recobrar la confianza de los inversores. Norma las certificaciones ejecutivas de los estados financieros como requerimiento permanente aplicable a todas las compañías que cotizan en la Bolsa de EEUU* **.[4][5]**

2. DEFINICIONES [6]

a. Información: es un activo, el cual, como cualquier otro activo de negocios, tiene valor para una organización y consecuentemente necesita ser protegido adecuadamente.

b. Tipos de Información: la información puede ser clasificada de diversas maneras, según la forma de comunicarse:

i. Impresa o escrita en papel
ii. Almacenada electrónicamente
iii. Transmitida por correo convencional o electrónicamente.
iv. Exhibida en videos corporativos
v. Hablada en reuniones

No importando la forma que tome la información, ésta deberá ser siempre protegida.

c. Seguridad de Información: Está caracterizada por la preservación de los siguientes aspectos

i. Confidencialidad: Asegurando que la información sea accesible solo por aquellos que están autorizados.
ii. Integridad: Salvaguardando la exactitud de la información en su procesamiento, así como su modificación autorizada.
iii. Disponibilidad: asegurando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea requerido.

d. Sistema de Gestión: Es un sistema para *establecer políticas* y objetivos de tal manera que se puedan cumplir estos últimos. Son usados por las organizaciones para diseñar sus políticas y para poner estas en funcionamiento a través de objetivos. Para ello se basa en:

i. Estructuras organizacionales
ii. Procesos sistemáticos y recursos asociados
iii. Metodologías de evaluación y medida.
iv. Revisión de procesos para asegurar que los problemas sean corregidos y las oportunidades para mejorarlos sean reconocidas e implementadas cuando sea necesario.

e. Sistema de Gestión de Seguridad de Información (SGSI): Es una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la Seguridad de la Información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad.

f. Objetivos de Control: Declaraciones de resultados deseados o propósitos a lograr. Proveen los lineamientos necesarios para delinear las políticas de manera clara y los controles necesarios.

3. MARCO DE REFERENCIA

A continuación se presentan ciertos aspectos importantes relacionados al tema de seguridad de información y su administración:

3.1 GOBIERNO DE TI

El Gobierno de TI es parte integral del ***Gobierno Corporativo***[3] y consiste en el liderazgo, estructura organizacional y procesos que aseguran que las Tecnologías de Información (TI) de una organización estén alineadas y acorde a las estrategias y objetivos de la misma. **[8][9][10]**

El gobierno de TI o llamado también *gobernabilidad de TI* es responsabilidad de la junta de directores y gerencia de una organización.

En medio de las responsabilidades del gobierno de TI como son establecer estrategias, administrar riesgos y medir desempeño, están los ***stakeholders***[4], los cuales conducen la organización y estrategia de TI.

Un factor primordial para el éxito de estas estructuras y procesos es una adecuada comunicación de todas las partes involucradas, basadas en relaciones constructivas, un lenguaje común y un compromiso compartido.

Las responsabilidades del gobierno de TI forman parte del gobierno corporativo y deben ser conducidas como cualquier otra estrategia. En términos más sencillos, el gobierno debe ser efectivo, transparente y medible.

El propósito del gobierno de TI es asegurar que el desempeño de las tecnologías de información cumpla con los siguientes objetivos **[9]**:

- Alineamiento de las tecnologías de información con los objetivos del negocio.
- Uso de las tecnologías de información para aprovechar las oportunidades y maximizar los beneficios.
- Uso responsable de los recursos de tecnología de información.

[3] *Se entiende por gobierno corporativo el conjunto de normas y reglas que regulan el proceso de toma de decisiones en una sociedad, así como también la organización y el ejercicio del poder en la sociedad anónima abierta* **[7]**

[4] *"StakeHolder" es usado para indicar cualquier persona que tiene una responsabilidad o una expectativa de las tecnologías de información en una organización.* **[11]**

- Adecuada administración de los riesgos de tecnología de información.

El gobierno de TI usualmente se da en distintas capas, con líderes de grupo recibiendo instrucciones de sus superiores, los cuales a su vez reportan a la gerencia de la organización.

Aquellos informes que den cuenta de un desvío de los objetivos establecidos son acompañados de las recomendaciones necesarias para corregirlas. Es importante mencionar que estos alcances no podrán ser efectivos al menos que las estrategias y objetivos hayan sido distribuidos a manera de cascada por toda la organización. En la Figura 3 se presenta conceptualmente la interacción entre los objetivos y actividades de TI desde una perspectiva de gobierno de TI, la cual puede ser aplicada a distintas capas dentro de la organización.

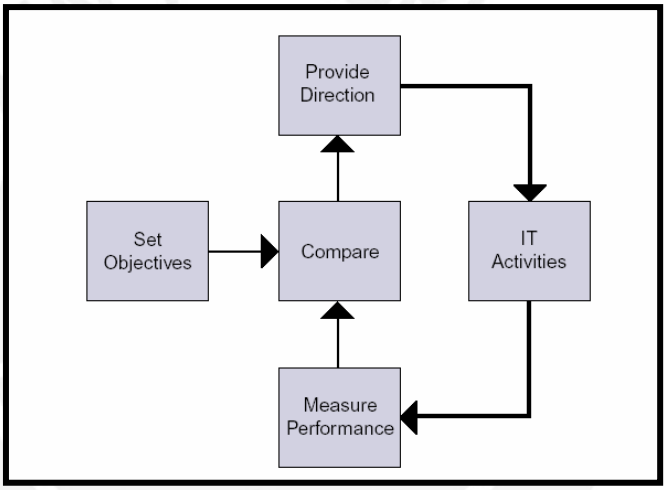

Figura 3. Interacción de objetivos y actividades de TI [12]

Como respuesta a las instrucciones recibidas, las funciones de TI necesitan enfocarse en:

- Maximizar los beneficios incrementando una adecuada automatización, haciendo más efectiva a una organización.
- Disminuir costos haciendo más eficiente a una organización.
- Administrar los riesgos de tecnología de información.

La infraestructura del gobierno de TI puede ser complementado de acuerdo a como lo indica la siguiente figura.

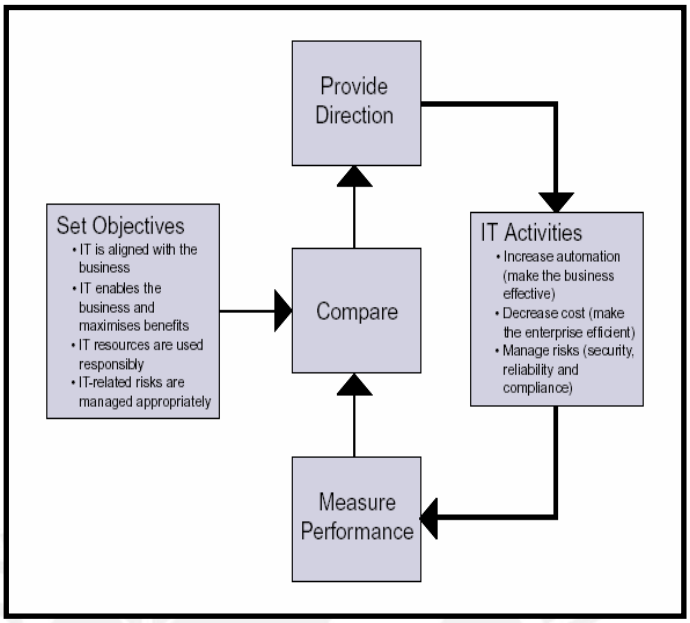

Figura 4. Infraestructura del Gobierno de TI [12]

Adicionalmente a las responsabilidades ya mencionadas del gobierno de TI, podemos agregar las siguientes:

- Tomar en cuenta el valor que encierran los "*stakeholders*" cuando se establezca una estrategia.
- Llevar por una buena dirección los procesos que implementan la estrategia.
- Asegurar que los procesos brinden resultados mensurables.
- Estar informado de los resultados e incentivar su mejora.
- Adoptar las acciones necesarias en función de los resultados que se obtengan.

En la Figura 5 se puede apreciar lo anteriormente expuesto.

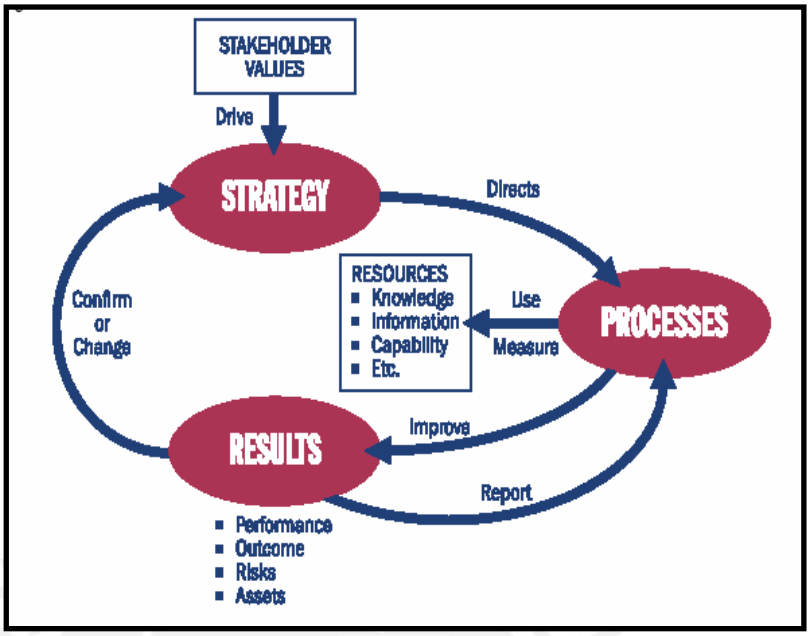

Figura 5. Responsabilidades del Gobierno de TI [13]

Siendo el alineamiento de las tecnologías de información con los objetivos del negocio un factor muy importante, la gerencia debe transmitir estos objetivos y la estrategia en cascada hacia la organización, haciendo que llegue a los empleados de todos los niveles. En la Figura 6 se puede visualizar lo expuesto.

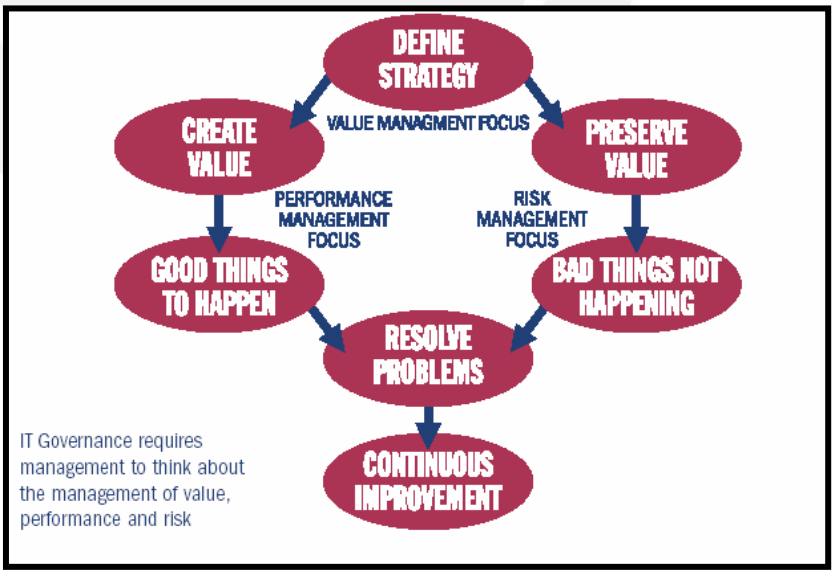

Figura 6. Rol de la Gerencia [13]

Es importante mencionar que un gran porcentaje de los valores de mercado de las empresas está atravesando por una transición desde lo tangible (inventarios, instalaciones, etc.) hacia lo intangible (información, conocimiento, experiencia, reputación, patentes, etc.). Muchos de estos activos tienen su soporte en las tecnologías de información. De esta manera una organización se vuelve vulnerable y frágil si su valor emana de aspectos conceptuales distintos de lo físico. Es así como un buen gobierno de TI se vuelve muy importante en dar soporte e implementar los objetivos del negocio.

A esto se agregan los riesgos a los que están expuestos los negocios en el mundo globalizado de hoy. Esto obliga a que la administración de las tecnologías de información sea efectiva y transparente.

El Gobierno de TI cubre los siguientes aspectos:

- Valor derivado de las tecnologías de información
- Administración de riesgos
- Alineamiento del negocio
- Administración de recursos
- Medida del desempeño

En la Figura 7 se observan los aspectos anteriormente mencionados

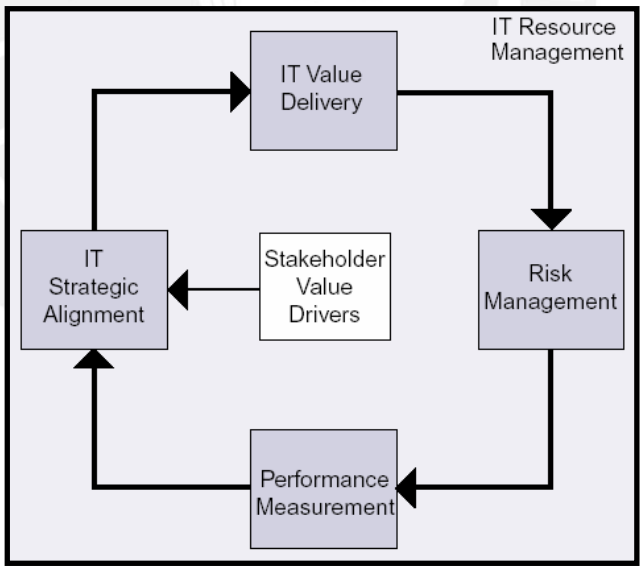

Figura 7 Áreas principales de un Gobierno de TI [14]

El Gobierno de TI es a su vez un proceso en el que la estrategia de TI conduce los procesos, los cuales obtienen los recursos necesarios para ejecutar sus responsabilidades.

Los procesos de TI generan reportes que permiten medir el desempeño, riesgos controlados y aceptados, recursos consumidos. Estos reportes confirmarán si la estrategia está siendo desarrollada de la manera más apropiada o brindarán indicaciones de que la estrategia necesita ser redireccionada. Estos procesos se pueden apreciar en la Figura 8.

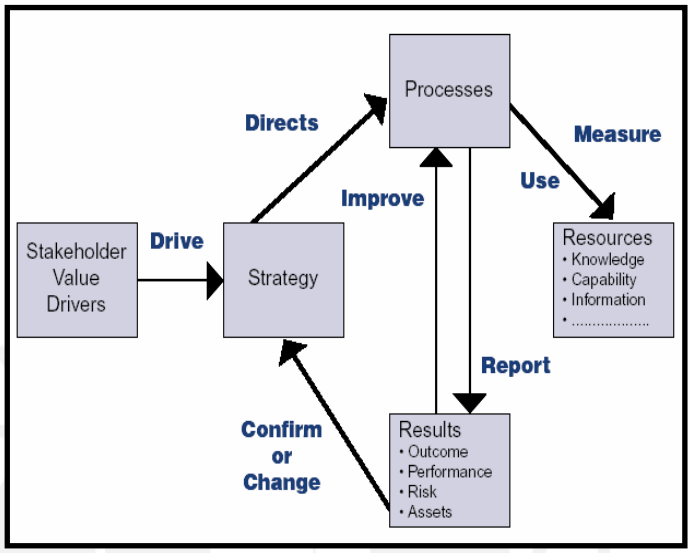

Figura 8. Procesos de un Gobierno de TI [14]

La gestión de seguridad de la información es un proceso clave en el gobierno corporativo. El gobierno de TI representa el liderazgo, estructuras organizacionales, procesos de negocio, que en conjunto aseguran que los activos de información de una organización den soporte y aseguren las estrategias y objetivos. Un Sistema de Gestión de Seguridad de Información (SGSI) es vital para el éxito de estas metas.

Dado que en la actualidad existen un gran número de modelos, estándares y normas internacionales relacionados a la gestión de seguridad de información, tomaremos como base una clasificación realizada por el ***IT Governance Institute***. En la Figura 9 podemos apreciar dicha clasificación, la cual tomó como base los aspectos de metodología, detalle de controles, controles de alto nivel, principios de seguridad y componentes de administración y gestión.

Security Guidance	Areas of Security Focus				
	Management Programme Components	Security Principles	High-level Security Controls	Detailed Control Practices	Model or Methodology
BS 7799			X		X
CobiT[1]			X	X	X
SSE-CMM					X
GAISP		X			
ISF		X	X	X	
ISO/IEC 13335	X	X	X	X	
ISO/TR 13569	X			X	
ISO/IEC 15408				X	X
ISO/IEC 17799				X	
ITIL			X		X
NIST 800-12	X	X	X		
NIST 800-14		X	X		
NIST 800-18			X		X
NIST 800-53				X	
OCTAVE		X	X	X	X
OECD		X			
Open Group					

Figura 9: Clasificación de documentos relacionado a seguridad de información [15]

Para fines de un Sistema de Gestión de Seguridad de Información es importante realizar un análisis y diagnóstico previo de la organización siguiendo una metodología adecuada, la cual permita luego establecer objetivos de seguridad a un nivel general y su implementación en controles específicos.

De acuerdo a esto y teniendo como base la clasificación mostrada en la Figura 9 se hará un análisis de los aspectos más importantes que nos puede brindar COBIT, BS7799, ISO 17799. Junto con este análisis, se procederá a realizar una revisión del estándar australiano AS/NZS 4360:2004 para aspectos de administración de riesgos, el cual forma parte primordial dentro de un SGSI.

3.2 BS 7799

Desarrollado por el British Standards Institute (Reino Unido) en el año de 1995. Ampliamente aceptado y utilizado como base para elaborar otros estándares de seguridad de información, incluyendo el ISO 17799.

Está organizado en diez secciones, cubriendo cada una un área distinta (aspectos organizacionales, aspectos técnicos, aspectos de instalaciones). En la Figura 10 se pueden apreciar las secciones del BS 7799.

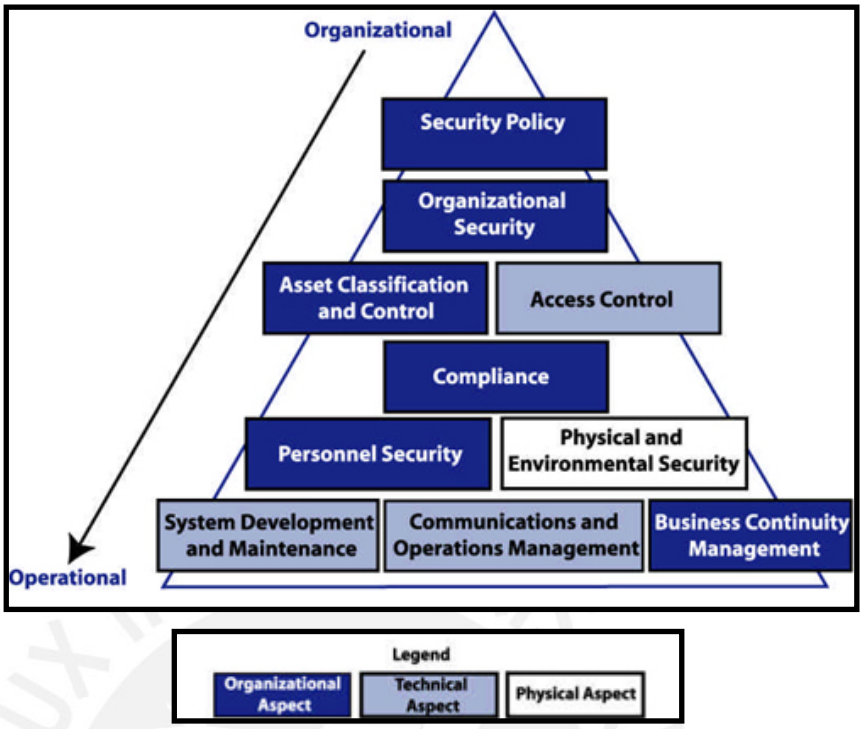

Figura 10 Secciones del BS 7799 [16]

Se puede apreciar a partir de la leyenda las distintas secciones del BS 7799, empezando por los aspectos organizacionales, hasta llegar a los aspectos operacionales.

La versión actual del estándar tiene dos partes

- *BS7799-1: 1999 Information Security Management. Code of Practice for Information Security Management*: es una guía que contiene consejos y recomendaciones para asegurar la seguridad de información de una organización de acuerdo a diez campos de aplicación.
- *BS7799-2: 1999 Information Security Management Specification for Information Security Management Systems:* consiste en recomendaciones para establecer un efectivo Sistema de Administración de Seguridad de Información (ISMS).

Este estándar cubre las necesidades de organizaciones de todo tipo, privadas y públicas. Será de gran interés para cualquier organización que almacene información confidencial en sistemas internos o externos, y que dependa de éstos para el normal desarrollo de sus operaciones.

En la Figura 11 se puede observar el grado de exposición de un sistema de información y el riesgo asociado. En el caso de una institución financiera, que es un servicio financiero, se puede apreciar que es **alto**.

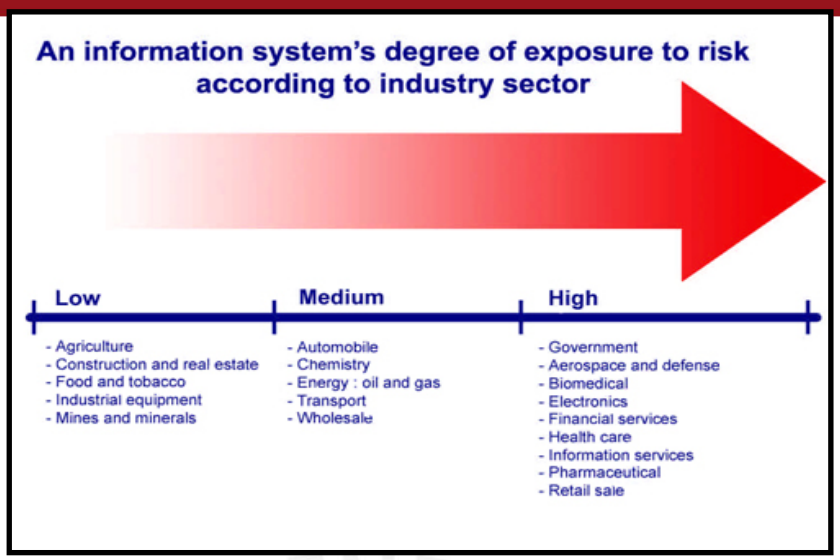

Figura 11 Grado de exposición de un sistema de información [17]

Por tanto, podemos observar que este estándar encierra aspectos importantes para el SGSI que estamos planteando para una institución financiera, más aún si como sabemos el riesgo de los sistemas de información de este tipo de instituciones es alto.

3.3 ISO 17799

El enorme éxito que tuvo el estándar BS 7799 hizo que hoy en día sea aceptado internacionalmente y publicado como ISO 17799.

Es importante mencionar que el estándar ISO 17799 no está destinado a ser usado como una normativa de administración de calidad a diferencia del ISO 9000.

Esencialmente el ISO 17799 es un estándar de seguridad, centrado principalmente en requerimientos de control y dividido en diez secciones. En la Figura 12 se aprecian las secciones del ISO 17799, las cuales reflejan claramente la influencia del BS 7799.

Figura 12. Secciones del ISO 17799 [18]

A continuación se describe cada sección y las acciones involucradas para asegurar el cumplimiento de sus objetivos:

- **Políticas de Seguridad**: la administración define en sus políticas de seguridad una dirección estratégica para la seguridad de la información y demuestra su respaldo y compromiso. Una política de seguridad documentada y aplicada es el núcleo vital para la aplicación de un ISMS[5]

- **Organización de la seguridad**: La organización de la seguridad significa principios y procedimientos para administrar la seguridad de la información. Los principales objetivos de esta sección son:

    - Administrar la seguridad de la información dentro de la organización
    - Mantener la seguridad de la información de la organización cuando es posible acceder a ella mediante elementos externos, como resultado de algunas facilidades brindadas.
    - Mantener la seguridad de la información de la organización cuando la responsabilidad de su procesamiento se ha encargado a un ente externo.

- **Clasificación y Control de Activos**: para proteger activos de información primero se debe elaborar un inventario de todos los activos de información dentro de la organización para así clasificarlos por grado de importancia, y en función a ello asignar acciones de protección a los mismos. Por tanto el principal objetivo de esta sección es:

[5] *Information Security Management System*

- Mantener la apropiada protección de los activos corporativos y asegurar que los activos de información reciban el apropiado nivel de protección.

- **Seguridad de Personal**: se intenta reducir los riesgos por errores humanos, robo, fraude o abuso de facilidades. El entrenamiento del personal es vital para el adecuado entendimiento de la seguridad de la información, promoviendo un comportamiento adecuado. Por tanto, los principales objetivos de esta sección son:

  - Asegurar que los usuarios estén alerta de las amenazas de la seguridad de la información.
  - Equipamiento adecuado de los usuarios para respaldar las políticas de seguridad de la organización en el curso de un normal desarrollo de trabajo.
  - Minimizar los daños frente a incidentes de seguridad, fallas, etc., buscando aprender de ellos.

- **Seguridad Física y Ambiental**: áreas seguras previenen accesos no autorizados, daños, interferencia en las premisas de negocios. Además protegen de pérdidas de activos de información, y finalmente de interrupciones propias del negocio. Por lo tanto el principal objetivo de esta sección es:

  - Prevenir el robo de información

- **Administración computacional y de redes:** los principales objetivos de esta sección son:

  - Asegurar un procesamiento de información seguro
  - Mitigar las fallas de sistema.
  - Proteger la integridad del software y la información relacionada al mismo.
  - Asegurar la disponibilidad e integridad del procesamiento de información y los servicios de comunicación.
  - Proteger la seguridad de información en las redes y su infraestructura
  - Prevenir daños a los activos de información y asegurar la continuidad de los procesos de negocio.
  - Prevenir la pérdida, modificación y uso indebido de la información que es compartida entre organizaciones.

- **Control de acceso a los sistemas:** los principales objetivos de esta sección son:

  - Controlar el acceso a la información.
  - Prevenir accesos no autorizados a los sistemas de información.
  - Asegurar la protección de los servicios de red.
  - Prevenir accesos no autorizados a las computadoras.
  - Detectar actividades no autorizadas.
  - Asegurar la seguridad de información cuando se usa tecnología móvil y demás facilidades de red.

- **Desarrollo y Mantenimiento de Sistemas:** los principales objetivos de esta sección son:
  - Asegurar qué criterios de seguridad se tienen en cuenta al momento del desarrollo de sistemas.
  - Prevenir la pérdida, modificación o mal uso de la data de los usuarios en las aplicaciones de sistemas.
  - Proteger la confidencialidad, autenticidad e integridad de la información.
  - Asegurar que los proyectos de TI y sus actividades relacionadas sean conducidas de manera segura.

- **Administración de Continuidad de Negocios:** esta sección señala las acciones correctivas y preventivas que deben tomarse en cuenta para hacer frente a interrupciones que afecten las actividades de negocio y para proteger los procesos críticos de negocio de los efectos, fallas o desastres mayores.

- **Cumplimiento de requerimientos legales:** esta sección busca reducir las brechas que pudieran existir en cuanto a obligaciones contractuales y regulatorias. Asimismo se busca cumplir con las políticas y estándares previamente establecidos por el ente regulador.

3.4 COBIT

Es una herramienta para la administración de las tecnologías de información. Fue desarrollada por ISACA como un estándar para la seguridad de la tecnología de información y buenas prácticas de control.

Está orientado a la gestión, auditoria de sistemas, control y seguridad. Define lo que es necesario hacer para implementar una efectiva estructura de control.

Permite atender las brechas entre los riesgos del negocio, necesidades de control y aspectos de tecnología. Brinda además, buenas prácticas a través de una plataforma de ***dominios*** y ***procesos*** y presenta actividades en una estructura lógica y administrativa.

La gestión y administración de una organización debe garantizar que exista una plataforma de control interno que dé soporte a los procesos de negocio. COBIT se concentra en los requerimientos del negocio relacionados a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información que fluye en la organización.

COBIT maneja el control desde el punto de vista de políticas, estructuras organizacionales y procedimientos. En cuanto a la administración y gestión, estas son manejadas desde la perspectiva del gobierno corporativo, es decir, señalando los lineamientos para que todos los individuos involucrados en la administración, uso, diseño, desarrollo y mantenimiento de los sistemas de información cumplan con los objetivos del negocio. Se maneja también, el concepto de ***objetivo de control*** el cual estable un propósito a ser cumplido implementando procedimientos de control dentro de una actividad particular de tecnologías de información.

Existen actualmente otros modelos de control como el ***COSO*** (USA), ***Cadbury*** (Reino Unido), ***CoCo*** (Canada) y ***King*** (Sudáfrica), los cuales están concentrados exclusivamente en el control, sin proveer un modelo claro para dar soporte a los procesos de negocio. El propósito de **COBIT** es cubrir esta brecha brindando una base para el cumplimiento de los objetivos de negocio con la adecuada gestión de la tecnología de información.

Su objetivo principal es el desarrollo de políticas claras y buenas prácticas para la seguridad y control de la tecnología de información para organizaciones comerciales, gubernamentales, y financieras entre otras. El desarrollo de COBIT está centrado en objetivos de control desde la perspectiva de los objetivos de negocio. A esto se agregan objetivos de control con fines de auditoria.

COBIT se compone de:

- **Guías de Administración (Management Guidelines):** para asegurar una organización exitosa, se debe administrar efectivamente la unión entre los procesos de negocios y los sistemas de información. Las guías de administración consisten en:
    - ***Modelos de Maduración (Maturity Models),*** que ayudan a determinar las fases y niveles esperados de control, comparándolos con normas actuales.
    - ***Factores Críticos de Éxito (Critical Success Factors),*** para identificar las acciones más importantes para alcanzar el control sobre los procesos de tecnología de información.
    - ***Indicadores Clave de Cumplimiento (Key Goal Indicators),*** para definir niveles objetivo de desempeño.
    - ***Indicadores Clave de Desempeño,*** para medir si un proceso de control de tecnología está cumpliendo con su objetivo.

- **Resumen Ejecutivo (Executive Summary)*:*** específicamente diseñado para ejecutivos y administradores, consiste en una explicación de los conceptos y principios claves de COBIT. Se incluye una síntesis de la plataforma o *Framework,* la cual muestra un detalle más amplio de los conceptos y principios, a la vez que se identifican los dominios (*Planeamiento y Organización, Adquisición e Implementación, Entrega y Soporte, Monitoreo*) y procesos de tecnología.

- **Plataforma (Framework)**: una organización exitosa está construida sobre una sólida plataforma de datos e información. La plataforma explica cómo los procesos de tecnología de información entregan la información que el negocio necesita para cumplir con sus objetivos. Esta entrega es controlada por medio de 34 controles de alto nivel, uno por cada proceso de tecnología, contenidos en cuatro dominios. La plataforma identifica cual de los siete criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y fiabilidad) y cual de los recursos de tecnología (personas, aplicaciones, tecnología, instalaciones y datos) son importantes para que los procesos de tecnología brinden un soporte completo a los objetivos de negocio.

- **Objetivos de Control (Control Objectives)**: la clave para mantener la rentabilidad en un ambiente tecnológicamente cambiante es medir qué tan bien se puede mantener el control. Los objetivos de control de COBIT brindan lo necesario para delinear una política clara y buenas prácticas para controles de tecnología de información. Se incluyen los aspectos óptimos o resultados deseados que deben alcanzarse, implementando alguno de los 318 objetivos de control específicos detallados, a través de los 34 procesos de tecnología de información.

- **Guías de Auditoria (Audit Guidelines)**: para cumplir con los objetivos trazados, periódicamente deben auditarse los procedimientos. Las guías de auditoria sugieren actividades que pueden desarrollarse para cada uno de los 34 objetivos de control de alto nivel, controlando de esta manera el riesgo asociado en caso no se cumpla con alguno.

- **Herramientas de implementación (Implementation Tool Set):** contiene herramientas para diagnóstico de controles de tecnología, aspectos de gestión de conocimiento, guías de implementación, preguntas frecuentes, casos de estudio de organizaciones que actualmente emplean COBIT, y presentaciones que pueden emplearse para introducir el COBIT en las organizaciones. Estas herramientas están diseñadas para facilitar la implementación del COBIT, mostrar lecciones aprendidas de organizaciones que rápida y exitosamente aplicaron COBIT en sus ambientes de trabajo.

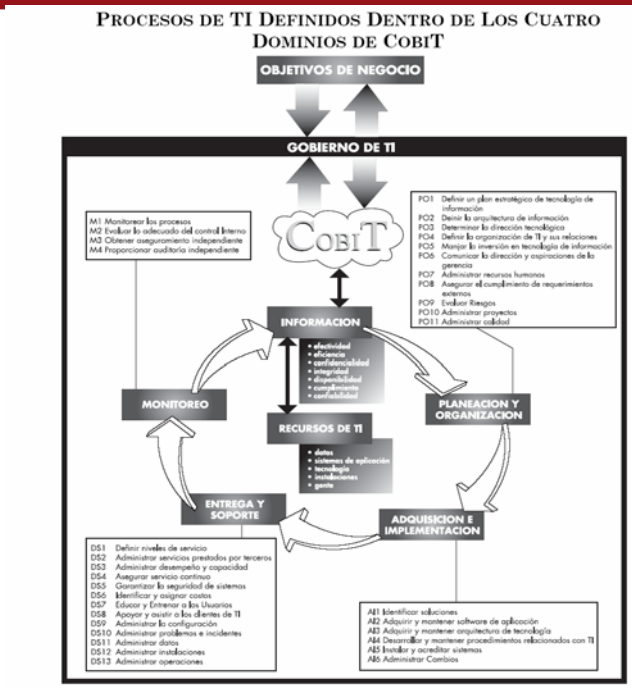

Figura 13 Dominios de Cobit [19]

3.5 AS/NZS 4360:2004

Desarrollado por el comité Australiano/Neo Zelandés OB/7. La primera edición de este estándar fue desarrollada en el año 1995. Brinda una guía genérica para la **administración de riesgos**. Puede ser aplicado a una variedad distinta de actividades, decisiones u operaciones de cualquier organización pública o privada.

Especifica los elementos del proceso de administración de riesgos, siendo genérico e independiente de cualquier industria o sector. El diseño e implementación de un sistema de administración de riesgo dependerá de las necesidades de cada organización, sus objetivos particulares, sus productos, servicios y procesos.

Debe aplicarse en todas las etapas de vida de una actividad, función, proyecto, producto o activo. El mayor beneficio es obtenido cuando se aplica desde el inicio.

El objetivo del estándar es brindar una guía que permita, tanto a las organizaciones públicas o privadas, grupos o individuos, alcanzar lo siguiente:

- Una base confiable y rigurosa para el planeamiento y toma de decisiones.
- Efectiva identificación de oportunidades y amenazas.
- Administración proactiva antes que reactiva.
- Mejor distribución y uso de los recursos.
- Confianza de los "*stakeholders*".
- Cumplimiento con aspectos regulatorios cuando esto aplique.
- Mejor Gobierno Corporativo.

A continuación se presentan algunas definiciones importantes a tener en cuenta en relación a la administración de riesgos, dentro de estas son:

- *Consecuencia*: impacto de un evento.
- *Control*: proceso, política, dispositivo, práctica o cualquier otra acción que actúa para minimizar un riesgo o ampliar oportunidades.
- *Evaluación de controles*: revisión sistemática de los procesos para asegurar que los controles continúen siendo efectivos y apropiados. La periodicidad de la evaluación de los controles la establece cada organización de acuerdo a la naturaleza de sus negocios y/o objetivos.
- *Evento*: ocurrencia de un conjunto particular de circunstancias. El evento puede tener una sola ocurrencia o convertirse en una cadena.
- *Frecuencia*: medida del número de ocurrencias por unidad de tiempo.
- *Amenaza*: fuente potencial de algún daño o desperfecto.
- *Probabilidad*: usada como una descripción general de la frecuencia de ocurrencia. Puede expresarse cualitativamente o cuantitativamente.
- *Pérdida*: cualquier consecuencia negativa o efecto adverso, financiero o de otro tipo que daña a la organización. El daño a la imagen de la organización puede incluirse como una pérdida.
- *Monitoreo*: consiste en la verificación, supervisión del progreso de una actividad, acción o sistema con la finalidad de identificar cambios en el desempeño, de acuerdo a los niveles previamente establecidos.
- *Organización*: grupo de personas e instalaciones, con responsabilidades, autoridad y relaciones.
- *Riesgo*: posibilidad de que ocurra algo que pueda tener algún tipo de impacto en los objetivos de una organización. Generalmente es expresado en términos de un evento o circunstancia y las consecuencias que puede producir.
- *Riesgo Residual*: es el riesgo que permanece luego de haber implementado un control o tratamiento.
- *Análisis de Riesgos*: proceso sistemático que consiste en entender la naturaleza de los riesgos y deducir su nivel.

- *Administración de Riesgos*: consiste en el proceso de identificación, análisis y evaluación de riesgos.
- *Eliminación de riesgo*: decisión que se toma en función a la situación que presenta el origen del riesgo.
- *Criterios para un riesgo*: términos de referencia que son tomados en cuenta al evaluar un riesgo. Se refiere a costos y beneficios asociados, requerimientos legales y regulatorios, requerimientos de usuarios, etc.
- *Evaluación de riesgos*: proceso de comparar los niveles de riesgo con los criterios previamente establecidos.
- *Identificación de riesgos*: proceso para determinar qué, dónde, cuándo, por qué y cómo podría ocurrir algo.
- *Proceso de Administración de riesgos*: aplicación sistemática de políticas, procedimientos y prácticas en las tareas de comunicación, establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos.
- *Plataforma para la administración de riesgos*: conjunto de elementos que forman parte del sistema de gestión de una organización en relación a la administración de riesgos. Estos elementos pueden incluir planeamiento estratégico, estrategias, toma de decisiones y cualquier proceso o práctica que maneje los riesgos.
- *Retención del riesgo*: intencionalmente o sin intención retener la responsabilidad por las pérdidas, o la carga financiera de las pérdidas dentro de la organización. La retención del riesgo también incluye los riesgos que no han sido identificados.
- *Compartir el riesgo*: se comparte el riesgo con un tercero fuera de la organización. Generalmente se habla de transferir el riesgo, y lo usual es a través de seguros.
- *Tratamiento de riesgos*: proceso de selección e implementación de medidas o controles para atenuar el impacto negativo de un riesgo.

Los principales elementos en el proceso de administración de riesgos son:

- **Establecer el contexto**: referido a la estrategia, organización y administración de riesgos en el cual tendrá lugar el resto del proceso. Se deben establecer aquellos criterios o métricas contra los cuales se evaluarán los riesgos.
- **Identificar riesgos**: se deben identificar los riesgos que se pretenda gestionar. Para ello debe efectuarse un análisis de los principales procesos de negocio de la organización, en especial, de aquellos que pueden catalogarse como los más críticos para el normal funcionamiento de la organización. Es importante detectar todas aquellas vulnerabilidades a las que está expuesta la organización, para luego identificar aquellas amenazas que pueden aprovecharlas.

- **Analizar los riesgos**: se identifican los controles implementados para atenuar los riesgos, con la finalidad de establecer si continúan funcionando de manera adecuada. Como parte del análisis deben evaluarse las probabilidades de ocurrencia y los impactos de cada uno de los riesgos para luego establecer su nivel y esto permita realizar una priorización.
- **Evaluar riesgos**: se comparan los niveles de riesgo obtenidos contra las métricas o criterios preestablecidos. Cada organización de acuerdo a sus objetivos y políticas decidirán el orden de atención de los mismos, usando como base el nivel obtenido a partir de las métricas.
- **Tratar riesgos**: en relación a aquellos riesgos que tengan un nivel bajo o aceptable, estos se atenderán con procedimientos de rutina normales dentro de los procesos de negocio de la organización. Para los riesgos con un mayor nivel, se deben desarrollar e implementar medidas que logren en lo posible ponerlos en nivel aceptable para la organización.
- **Monitoreo y revisión**: se debe realizar periódicamente una medición del desempeño de los controles implementados, pues podría darse el caso que en algún momento éstos necesiten ser mejorados, complementados o incluso cambiados.
- **Comunicar y Consultar**: se debe mantener una comunicación constante con los dueños de los procesos de negocio en una organización, pues finalmente ellos son los más indicados para dar un juicio de los controles implementados para tratar los riesgos a los que se ven expuestos.

En la Figura 14 se muestra gráficamente el proceso de administración de riesgos

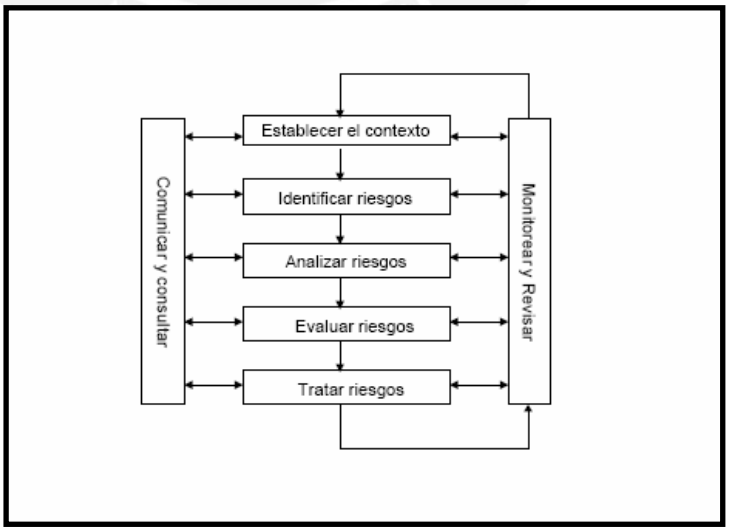

Figura 14. Proceso de Administración de Riesgos [20]

En relación a la administración de riesgos se presentan algunos tipos de éstos a los que se ven expuestos la mayoría de organizaciones. De acuerdo al tipo de organización, uno o más de los siguientes riesgos pueden presentarse:

- **Riesgo Estratégico**: Se asocia con la forma en que se administra la organización. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la organización por parte de la alta gerencia.
- **Riesgos Operativos**: Comprende los riesgos relacionados tanto con la parte operativa como técnica de la organización, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la organización, la desarticulación entre dependencias lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
- **Riesgos de Control**: Están directamente relacionados con inadecuados o inexistentes puntos de control y en otros casos, con puntos de control obsoletos, inoperantes o poco efectivos.
- **Riesgos Financieros**: Se relacionan con el manejo de los recursos de la organización que incluye, la ejecución presupuestal, elaboración de los estados financieros, pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada organización. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda organización.
- **Riesgos de Cumplimiento**: Se asocian con la capacidad de la organización para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la los entes reguladores.
- **Riesgos de Tecnología**: Se asocia con la capacidad de la organización para satisfacer sus necesidades actuales y futuras, así como para soportar el cumplimiento de su misión a través de su tecnología disponible.

El análisis de riesgos se puede desarrollar en distintos niveles de detalle dependiendo del tipo de riesgo, propósito del análisis, y sobretodo de la disponibilidad de información, datos y recursos. El análisis puede ser cualitativo, semi-cuantitativo, cuantitativo, o una combinación de estos dependiendo de las circunstancias. El orden de complejidad y costos de análisis, en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. En la práctica el análisis cualitativo es usado con frecuencia para obtener un esquema general de los riesgos a los que está expuesta una organización. A partir de este punto, si se desea entrar en detalles, se utilizará el análisis cuantitativo, siendo necesario contar con datos históricos correctamente cuantificados. Esto puede lograrse implementando las llamadas base de datos de pérdidas.[6]

[6] *Registro de eventos que produjeron una pérdida cuantificable generalmente en término monetarios. Se registra el evento, los activos tangibles o intangibles afectados y las medidas que se adoptaron.* **[21]**

Daremos a continuación algunos lineamientos en relación a los tipos de análisis de riesgos mencionados:

- **Análisis Cualitativo**: emplea palabras para describir la magnitud de las potenciales consecuencias y probabilidad de ocurrencia de las mismas. Las escalas a emplearse pueden ser adaptadas de acuerdo a las circunstancias, y pueden emplearse distintas descripciones según el tipo de riesgo. Las escalas más frecuentes en uso son las probabilidades y consecuencias bajos, medios y altos. La combinación de los pares nos dan como resultado el nivel de riesgo.

  El análisis cualitativo puede ser usado como:
  - Una primera actividad de reconocimiento de riesgos a los que está expuesta una organización. Este primer reconocimiento constituirá la base para un posterior análisis más detallado.
  - Apoyo en la toma de decisiones
  - Alternativa cuando no se cuenta con datos numéricos históricos o recursos suficientes para un análisis cuantitativo.

- **Análisis Semi-Cuantitativo**: En este tipo de análisis se busca ampliar la escala del análisis cualitativo, asignando valores numéricos iniciales, con cierta aproximación. Esto sentará una mejor base para el análisis cuantitativo, en el cual los valores numéricos serán más exactos. Es importante asignar con cuidado los valores a las probabilidades de ocurrencia de los eventos de riesgo, pues esto puede dar resultados inexactos, los cuales no reflejen la verdadera situación de los niveles de riesgo de la organización.

- **Análisis Cualitativo**: Este análisis emplea valores numéricos (a diferencia de escalas descriptivas usadas en el análisis cualitativo y semi-cualitativo) tanto para las probabilidades e impactos, empleando datos de varias fuentes (base de datos de pérdida por ejemplo). La precisión del análisis dependerá mucho de la exactitud y veracidad de los datos obtenidos de las fuentes que se consulten. Los impactos de los riesgos generalmente se expresarán en términos monetarios. En algunas oportunidades quizás se obtendrán distintos valores en el análisis para un sólo evento, esto de acuerdo a cómo ha ido variando el tiempo.

La forma en como se expresen las probabilidades e impactos y cómo se combinen para obtener un nivel de riesgo podrá variar de acuerdo al tipo de éste y del propósito del análisis de riesgos. Para obtener un mejor acercamiento a la metodología de administración de riesgos expuesta, es importante la lectura detallada del estándar australiano AS/NZS 4360:2004.

IV. ANALISIS Y DISCUSION

Se plantea un esquema de gestión de seguridad de información en función de cinco dominios, los cuales corresponderán a los temas vistos en el marco de referencia.

1. Gobierno de Seguridad de Información

Se busca establecer y mantener una plataforma de gestión que asegure que las estrategias de seguridad de información estén alineadas con las estrategias de negocio de la institución financiera y consistente con las normas regulatorias que exige la *Superintendencia de Banca, Seguros y AFP del Perú*

Para este punto del modelo se debe tener en cuenta lo expuesto en el marco de referencia, en el punto de Gobierno de TI. Se expusieron los lineamientos que deben tomarse como base para un adecuado Gobierno de TI, el cual está inmerso en el esquema de seguridad de información que se plantea. Cada institución financiera debe adaptar esos lineamientos a su realidad como un paso a implementar su gestión de seguridad de información.

A través del Gobierno de Seguridad de Información se busca desarrollar un sistema a través del cual las instituciones financieras puedan controlar e integrar la seguridad de información en un contexto de la tecnología de información y planeamiento de negocios.

El Gobierno de Seguridad de Información comprende el desarrollo e integración de una estructura administrativa y de organización, con reporte de los procesos que abarcan todos los aspectos de un programa de seguridad exitoso, lo cual permitirá una administración de negocios efectiva, y que a su vez administre y gestione los riesgos relacionados.

Las principales tareas que se deben desarrollar dentro de un Gobierno de Seguridad de Información son:

- Desarrollar una estrategia de seguridad de información que le dé soporte a la estrategia de negocios y a la dirección de la empresa.
- Obtener el apoyo y compromiso de las altas gerencias de la institución financiera.
- Definir claramente los roles y responsabilidades en lo relacionado a la seguridad de información dentro de la institución financiera.
- Establecer canales de comunicación que brinden soporte a las actividades de gobierno de seguridad de información.
- Identificar las actuales normas a las que se encuentra sujeta la institución financiera, evaluando la manera como pueden afectar la gestión de la seguridad de información.

- Elaborar una política de seguridad de información para la institución financiera.
- Desarrollo de normas y procedimientos que den soporte a las políticas de seguridad de información.
- Desarrollar un análisis de costo-beneficio adecuado para futuros programas de inversión en seguridad de información.

De esta manera el Gobierno de Seguridad de Información se convierte en una serie de actividades que buscan asegurar que los activos de información cuenten con un nivel de protección acorde con el valor y riesgo que significan para la institución financiera en caso se vean comprometidos por algún evento.
La gestión de seguridad de información efectiva abarca aspectos de negocio, legales y normativos **no sólo de tecnología**.

Para que la seguridad de información sea efectiva debe direccionar los procesos íntegramente. Es muy poco beneficioso si un sistema seguro es usado para actividades fraudulentas. Para asegurar que todos los elementos relevantes de seguridad sean conducidos en una estrategia de seguridad organizacional, las secciones del ***ISO 17799*** vistas en el marco de referencia pueden ser útiles como plataforma base. Normas y procedimientos se deben desarrollar como ya se mencionó, para atender cada punto de este estándar.

Cuando un Gobierno de Seguridad de Información es apropiadamente implementado debe dar como resultado:

✓ *Alineamiento estratégico:*
  - Requerimientos de seguridad implementados de acuerdo a las necesidades del negocio, los cuales brindan una guía de lo que debe realizarse y una medida de cuando se logró.
  - Soluciones de seguridad a la medida de los procesos del negocio, las cuales toman en cuenta la cultura, estilo de administración, tecnología y estructura de la organización.
  - Inversiones en seguridad de información alienadas con la estrategia del negocio, con un perfil de riesgo bien definido.

✓ *Entrega de Valor:*
  - Un conjunto de prácticas estándar de seguridad, requerimientos base de seguridad que siguen prácticas adecuadas y proporcionales al riesgo.
  - Esfuerzos distribuidos y proporcionales en áreas con mayor impacto y beneficio para el negocio.
  - Soluciones completas que abarcan toda la organización, procesos y tecnología basados en un entendimiento total del negocio de la organización.
  - Un continuo mejoramiento de la cultura basado en el entendimiento de que la seguridad es un proceso, no un evento.

- ✓ *Administración de Riesgos:*
  - Entendimiento colectivo del perfil de riesgo de la organización en relación a sus amenazas y vulnerabilidades.
  - Conocimiento de las prioridades en la administración de riesgos basadas en las consecuencias potenciales.
  - Suficiente mitigación de riesgos, con consecuencias aceptables del riesgo residual[7] resultante.
  - Entendimiento del riesgo residual y sus consecuencias.

- ✓ *Medida del Desempeño:*
  - Conjunto de métricas definidas y aceptadas, las cuales se encuentran apropiadamente alineadas con el negocio.
  - Proceso de medición que ayudará a identificar brechas y brindará retroalimentación del progreso que se vaya obteniendo.
  - Aseguramiento independiente brindado por evaluaciones y auditorias externas.

En un número creciente de situaciones, los activos digitales comprometen la mayor parte del valor de una organización. Debe existir un esfuerzo por reconocer esta situación y priorizar la protección de estos activos.

A continuación se detallan las principales tareas que se deben desarrollar para un gobierno de seguridad de información:

1.1 Estrategia de Seguridad de Información:

El desarrollo de una estrategia de seguridad de información como soporte para la estrategia de negocios es una tarea vital para una institución financiera, dado el volumen de información que maneja de sus clientes. Su desarrollo debe realizarse por el *administrador de seguridad de información,* el cual tendrá un papel primordial en el gobierno de seguridad de información. Las prácticas prudentes de negocio requieren que los procesos de tecnología de información se hallen alineados con los procesos de negocios de la cadena de valor de la institución financiera, así como con sus objetivos.
De esta manera la seguridad de información se convierte en parte integral del gobierno corporativo que debe poseer toda institución financiera.

Un ***conjunto de objetivos de seguridad, procesos, herramientas y técnicas*** constituyen conjuntamente una estrategia de seguridad. Una buena estrategia debe mitigar los riesgos, brindar soporte a los objetivos de negocio y maximizar el valor entregado a los usuarios; a su vez busca el cumplimiento de las normativas reguladoras contractuales propias de una institución financiera.

7 Riesgo que persiste luego de la implementación de controles **[22]**

Además, una estrategia de seguridad debe combinar, de la mejor manera, prácticas de seguridad en cada proceso y área de negocio de la institución financiera. Debe considerar capas de nivel de control. De igual manera, la capacitación y educación es primordial en la estrategia, pues la seguridad es a menudo débil al *nivel del usuario final:* es en este nivel que se deben desarrollar metodologías y procesos que permitan a las políticas, estándares y procedimientos ser fáciles de seguir, implementar y monitorear.

Una propuesta de seguridad en capas de nivel de control se presenta en la Figura 15, definiéndose lo que cada capa busca controlar:

Defensas en contra de compromiso de los sistemas	Políticas, Estándares, Procedimientos y Tecnología
Prevención	**Autenticación** **Autorización** **Encriptamiento** **Firewalls** **Etiquetado/ manipuleo/retención** **Administración** **Seguridad Física** **Prevención de Intrusos** **Escaneo permanente de virus** **Seguridad Personal** **Capacitación**
Contención	**Autorización** **Privacidad de información** **Firewalls/ seguridad de dominios** **Segmentación de redes** **Seguridad Física**
Detección/notificación	**Monitoreo** **Métricas** **Auditoria** **Detección de intrusos** **Detección de virus**
Reacción	**Respuesta ante incidentes** **Política/procedimiento de cambios** **Mecanismos adicionales de seguridad** **Nuevos/mejores controles**
Recolección de evidencias/ Rastreo de eventos	**Auditoria** **Monitoreo/ Gestión** **No Repudio** **Análisis Forense**
Recuperación/ Restitución	**Respaldos** **Continuidad de Negocios/ Plan de Recuperación de Desastres**

Figura 15. Seguridad de Capas de Nivel de Control

Los elementos que se pueden incluir en una estrategia de seguridad son:

- ✓ *Enlaces con la estrategia de negocio*: todas las decisiones deben ser filtradas en el modelo de negocios de la institución financiera. Si este modelo no existe, se debe desarrollar y validar. De no contarse con los fondos necesarios para desarrollar este modelo, se deben realizar inversiones mínimas aceptables en seguridad, basadas en prácticas que direccionen los riesgos. Es imprescindible la participación de la administración a nivel gerencial.

- ✓ *Mejores prácticas:* pueden no ser proporcionales al riesgo. Para ello debe realizarse una medida apropiada del valor de activos que quiere protegerse, y analizar si las medidas que se tomen no son más costosas que los mismos activos.

- ✓ *Políticas:* deben ser formales, mas aún siendo esto normado por el ente regulador de instituciones financieras. Todas las políticas y procedimientos deben documentarse, comunicados y actualizados con la regularidad apropiada. Como mínimo una política debe contemplar los siguientes aspectos:

    - Política de acceso a información.
    - Política de acceso a aplicaciones.
    - Política de acceso a redes.
    - Política de software.
    - Política de privacidad.
    - Política de clasificación y posesión de información.
    - Política de manejo de incidentes.
    - Política de accesos remotos.
    - Política de diseño y desarrollo de sistemas.
    - Política de evaluación y análisis de riesgos.
    - Política de entrenamiento y capacitación.
    - Política respaldos y recuperación.
    - Política de administración de cambios.
    - Política de seguridad personal.
    - Política de seguridad física.
    - Política de marcado, manipuleo y retención de información.
    - Política de documentación.
    - Políticas para estándares, creación de procedimientos (aprobación y mantenimiento).

- ✓ *Estándares:* deben desarrollarse para proporcionar las métricas necesarias que evalúen si un procedimiento o práctica particular cumple con las políticas establecidas. Cada política puede incluir un número determinado de estándares necesarios para varias actividades. A su vez los estándares son importantes para los propósitos de brindar una base para la auditoria de sistemas.

- ✓ *Autenticación:* es el proceso de establecer la identidad de un usuario de un sistema de información. Existen tres formas de autenticación:

    - Lo que uno *sabe (por ejemplo un password).*
    - Lo que uno *tiene (por ejemplo un token).*
    - Lo que uno *es (por ejemplo la biometría).*

  Algunos mecanismos adoptan o combinan algunos de estos componentes para mejorar la autenticación.

- ✓ *Administración:* gestionar y administrar todas las actividades requieren un esfuerzo significativo. Una función efectiva de seguridad requiere una adecuada administración de sus políticas de privacidad, autenticación, autorización y recuperación de procesos. La seguridad debe considerarse en distintas fases de tiempo como una herramienta, metodología, técnica o proceso. Es por ello la necesidad de desarrollar métricas que midan la efectividad de los procedimientos administrativos.

- ✓ *Recuperación:* Es imperativo que una organización no reduzca la efectividad y eficiencia de estrategia de seguridad recortando las inversiones en planeamiento de recuperación de negocios y sistemas. Es necesario realizar pruebas dos veces al año, tal como lo norma el ente regulador para todas las instituciones financieras. De estas pruebas se puede comprobar si alguna política o procedimiento viene respondiendo de acuerdo a lo esperado.

- ✓ *Servicios de Soporte*: es complicado contar con un personal de seguridad que cumpla con todos los requerimientos para las numerosas actividades y proyectos. Por esta razón la institución financiera podría necesitar apoyo externo. “Outsourcing” en cualquier actividad de negocio, en especial de seguridad, introduce un riesgo adicional que debe ser evaluado durante la decisión previa a tomar personal externo.

- ✓ *Tecnología:* existen muchas tecnologías con los mecanismos de seguridad necesarios para una estrategia exitosa. Entre ellas se puede citar:

    - Tecnología Firewall.
    - Tecnología de intrusión y detección de intrusos.
    - Tecnología antivirus.
    - Tecnología biométrica.
    - Tecnología de encriptamiento.
    - Tecnología de acceso remoto.
    - Tecnología de firmas digitales.
    - Tecnología EDI y EFT.
    - Tecnología VPN.
    - Tecnología SET.
    - Tecnología forense.

  El uso e interrelación de mecanismos de seguridad deben ser definidos por una arquitectura de seguridad que implemente los requerimientos de las políticas previamente establecidas.

1.2 Compromiso de la Administración Gerencial

Obtener el compromiso de la alta administración gerencial como respaldo a la seguridad de información de la institución financiera es imperativo para el éxito de sus actividades. Al igual que otras actividades, sin este compromiso, las actividades relacionadas con la seguridad de información inevitablemente fallarán. Cualquier iniciativa que afecte a tantas personas y tantos procesos de negocio no puede tener éxito sin el soporte y respaldo de la administración gerencial.

Es imperativo que la administración gerencial vea a la seguridad de información como un tema muy serio y brinde los recursos apropiados. Es ella la que debe aprobar la estrategia de seguridad planteada. Para ello, el administrador de seguridad de información debe capacitar a los ejecutivos gerenciales en temas de alto nivel relacionados a la seguridad de información. Los ejecutivos estarán en una mejor posición para apoyar las iniciativas de seguridad de información si son capacitados en la forma cómo sistemas de información críticos pueden afectar el negocio en caso fallen.

La administración gerencial debe tener un compromiso en los siguientes aspectos:

- ✓ Implementando altos estándares de gobierno corporativo.
- ✓ Tratando a la seguridad de información como un aspecto crítico del negocio y creando un ambiente positivo de seguridad.
- ✓ Demostrando a los agentes externos que la institución financiera trata a la seguridad de información de manera profesional.
- ✓ Implantando principios fundamentales, tales como asumir una importante responsabilidad por la seguridad de información, implementando controles que sean proporcionales al riesgo y señalando responsabilidades individuales.

La administración gerencial debe demostrar su compromiso con la seguridad de información de la siguiente manera:

- ✓ Involucrándose directamente en decisiones de alto nivel relacionadas a la seguridad de información, tal como la política de seguridad de información de la institución financiera.
- ✓ Ejerciendo un control a alto nivel.
- ✓ Destinando recursos necesarios para la seguridad de información.
- ✓ Revisando periódicamente la efectividad de la seguridad de información.

1.3 Roles y Responsabilidades

Asegurar que las definiciones de los roles y responsabilidades dentro de la institución incluyan actividades de gestión de seguridad de información es vital para el éxito de éstas. Es importante que se encuentren claramente definidas en el manual de organización y funciones.

En toda institución financiera, los roles y responsabilidades deben asegurar los siguientes aspectos:

- ✓ La línea de reporte debe direccionar a un ejecutivo de alto nivel. Mientras mayor sea el nivel del ejecutivo, será más conveniente pues tendrá la influencia necesaria para asegurar que sus administrados implementen la seguridad de información.
- ✓ Debe existir un esfuerzo coordinado entre el personal de sistemas, redes, recursos humanos, operaciones, auditoria interna, departamento legal y otro grupo que se considere necesario.

- ✓ Trabajo con consultores externos en auditorias externas.
- ✓ Identificación de objetivos de protección consistentes con el plan estratégico institucional.
- ✓ Identificación de elementos clave de seguridad.
- ✓ Políticas, estándares y procedimientos globales sean desarrollados e implementados para asegurar el mantenimiento de la seguridad.
- ✓ Implementación de planes para productos de seguridad sean siempre coordinados.
- ✓ Identificación de controles de seguridad apropiados.
- ✓ Gestión apropiada de incidentes de seguridad.
- ✓ Implementación coordinada de los controles con el personal de administración de procesos.
- ✓ Contar con asesoría externa para la seguridad física.
- ✓ Contar con sitios alternos de negocio, operativos y probados.
- ✓ Inducciones en temas de seguridad para nuevos empleados brindadas por el departamento de.
- ✓ Todos los planes de capacitación sean implementados de tal forma que incluyan sesiones para todos los niveles del negocio, incluyendo ejecutivos, técnicos, analistas, consultores, personal de soporte, etc.
- ✓ Desarrollo de procedimientos que integren la seguridad de información en cada unidad de negocio.

Para el caso de una institución financiera, cualquiera sea su tamaño, es importante contar con un *departamento de seguridad de información* integrado por personal capacitado en las siguientes áreas:

- ✓ Administración de seguridad lógica.
- ✓ Desarrollo de políticas.
- ✓ Arquitectura de seguridad.
- ✓ Investigación.
- ✓ Evaluación
- ✓ Auditoria

Se plantea como mínimo *seis personas* quienes estarían sujetas a diversos factores, de acuerdo a las posibilidades y políticas de la institución financiera.

1.4 Canales de Comunicación

Establecer canales de comunicación y reporte brinda un soporte al gobierno de seguridad de información, asegurando el buen desempeño de sus actividades El administrador de seguridad de información debería reportar directamente a un ejecutivo con nivel gerencial. Se debe evitar potenciales conflictos de interés. Las métricas de efectividad de un programa de seguridad de información deben establecerse y reportarse con una periodicidad regular.

Reportar en base a métricas es simplemente reportar algo que es **medible**, siendo lo más importante **definirlas**.

Con la finalidad de emplear una metodología de reportes en base a métricas, el administrador de seguridad de información debe identificarlas de acuerdo a la realidad de la institución financiera, además de relacionarlas con la seguridad integral de información de la institución, y buscar una manera de medirlas.

En la Figura 16 se presentan algunas métricas que pueden dar una base para desarrollar otras de acuerdo a la realidad de la institución financiera. Se mencionan sus ventajas y desventajas, haciendo notar que ninguna de ellas por sí sola brinda información directa acerca de la solidez del gobierno de seguridad de información.

Métrica	Ventajas	Desventajas
Vulnerabilidades de Sistemas	Identifica las vulnerabilidades reales de un sistema que pueden ser explotadas	No tiene en cuenta la accesibilidad del sistema, y por tanto el riesgo de que la vulnerabilidad realmente afecte a la institución financiera.
Violación a las políticas de configuración	Identifica cómo los administradores configuran los sistemas	No identifica el potencial para una penetración exitosa.
Ataques bloqueados (Firewalls o IDS[8])	Identifica lo que se ha intentado hacer con la institución financiera, con alguna información referida a la amenaza.	No indica las verdaderas vulnerabilidades y no puede diferenciar entre un ataque real y una prueba.
Número de empleados en un programa de capacitación	Identifica que tan bien los empleados siguen las directivas en el curso de capacitación.	No muestra si los empleados ponen en práctica lo aprendido.
Intentos fallidos de acceso a sistemas o archivos electrónicos.	Identifica una potencial amenaza	No toma en cuenta accidentes o errores.
Número de incidentes de seguridad	Identifica aspectos de seguridad actuales	Sólo identifica incidentes conocidos

Figura 16. Ventajas y Desventajas de algunas métricas

[8] *IDS: Sistema de Detección de Intrusos*

El reporte de las métricas debe enfocarse en **tendencias**, no sólo en números. La razón de esto es que el administrador de seguridad de información va esquematizando "instantáneas" de la organización y su progreso en el tiempo. Lo que debe ser relevante es que el gobierno de seguridad de información vaya mejorando su postura dentro de la institución financiera. Esto no quiere decir que los números sean menos importantes, pues deben leerse y usarse de acuerdo al contexto en el que encuentren.

La comunicación a todo el personal ayuda a asegurar que la seguridad de información sea conocida por toda la institución financiera. Para ello deben implementarse canales de comunicación, entre los cuales puede incluirse reuniones gerenciales, comités de seguridad de información, etc. Este tipo de información se puede lograr mediante publicaciones internas, publicaciones por una intranet, capacitación permanente, clases formales, etc.

Finalmente, el administrador de seguridad de información debe interactuar con otras instituciones financieras en temas afines a la seguridad de información. En la actualidad esto se viene dando a través de la Asociación de Bancos del Perú (ASBANC), en el comité mensual de riesgo operacional, donde se tratan temas de seguridad de información.

1.5 Normas Regulatorias y Legales

Una de las tareas del administrador de seguridad de información es identificar los aspectos regulativos y legales actuales a los que está sujeta una institución financiera en temas relativos a la seguridad de información. Estos se encuentran documentados en una resolución y una circular de la SBS:

- ✓ **Resolución S.B.S. Nº 006-2002**: reglamento para la administración de riesgos de operación[9].
- ✓ **Circular NºG-105-2002:** señala criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información. Es un documento complementario de la Resolución S.B.S N° 006-2002, y en su artículo 5 menciona los aspectos de administración de seguridad de información necesarios para una institución financiera.

[9] *La posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.***[23]**

La seguridad de información constituye por tanto en uno de los aspectos críticos en la pérdida financiera de la institución, como parte de la definición de riesgo operacional. Se encuentra inevitablemente interrelacionada con temas de privacidad, propiedad intelectual y leyes contractuales. Cualquier esfuerzo para diseñar e implementar una efectiva política de seguridad de información debe realizarse sobre la base de un conocimiento de los requerimientos legales y sus restricciones.

1.6 Políticas de Seguridad de Información

La tarea de establecer y mantener las políticas de seguridad de información corresponde al administrador de seguridad de información, quien debe implementar procesos para lograr ello. La institución financiera debe asegurar que estas políticas sean parte integral de su administración. Se deben considerar como "*documentos vivientes*" que deben ser revisados con regularidad para asegurar se mantengan actualizados ante cualquier cambio (tecnológico, organizacional, de procesos, etc.) en la institución financiera.

Se debe formalizar la periodicidad de revisión de las políticas y los criterios para dicha revisión. A partir de acá, los estándares se revisan y modifican para direccionar los cambios en las políticas. Los procedimientos y guías se derivan de las políticas de seguridad.

Las políticas de seguridad de información sirven a varios propósitos, estableciendo primariamente lo que está o no permitido. Además éstas deben alinearse apropiadamente a los objetivos de negocio. Algunos métodos para lograr este último propósito se citan a continuación:

- ✓ Determinar si las inversiones en seguridad de información son proporcionales o no con el perfil de riesgo de la institución y los objetivos de negocios.
- ✓ Determinar la clasificación de la información requerida para la institución, con la finalidad de implementar las políticas necesarias.
- ✓ Determinar si las políticas de seguridad han sido adecuadamente diseñadas, implementadas y reforzadas para proteger la información de la institución.

Los enunciados de las políticas deben ser lo suficientemente genéricos de manera que no sea necesario cambiarlos con mucha frecuencia; ni se presten a interpretaciones ambiguas. No es apropiado tener políticas que sean tan específicas que tengan que ser reformuladas cada vez que cambia la tecnología.

Las políticas deben centrarse en las necesidades del negocio y deberían dar respuesta a preguntas clave como:

- ✓ ¿Qué información se administrará?
- ✓ ¿Qué tan importante es la información para las operaciones críticas?
- ✓ ¿Qué tan confidencial es la información?
- ✓ ¿Qué tan importante es la integridad de la información?
- ✓ ¿Cómo puede accederse a la información?
- ✓ ¿Qué controles deben implementarse para la gestión de la información?
- ✓ ¿Cuál es el nivel de riesgo aceptable para la institución?

Un *programa de seguridad de información integral* puede incluir los siguientes elementos esenciales:

- ✓ Políticas: Enunciados de alto nivel en concepto y extensión.
- ✓ Estándares: Métricas o procesos usados para determinar si los procedimientos cumplen con los requerimientos de las políticas. Generalmente un estándar debe brindar los parámetros y límites suficientes de tal manera que un procedimiento no ambiguo cumpla con los requerimientos de una política relevante. Deben cambiar en la medida que los requerimientos y tecnología lo hagan.
- ✓ Procedimientos: Contienen pasos detallados necesarios para cumplir tareas específicas. Deben contener las salidas esperadas y mostrar las condiciones necesarias para la adecuada ejecución del procedimiento. Asimismo deben contener los pasos necesarios para resultados inesperados. Deben ser exactos y no ambiguos.
- ✓ Guías: Contienen información que ayudarán en la ejecución de los procedimientos. Pueden incluir sugerencias y ejemplos, explicaciones de los procedimientos, información de apoyo, herramientas que se pueden usar, etc.

En la Figura 17 se muestra la jerarquía de políticas, estándares y procedimientos.

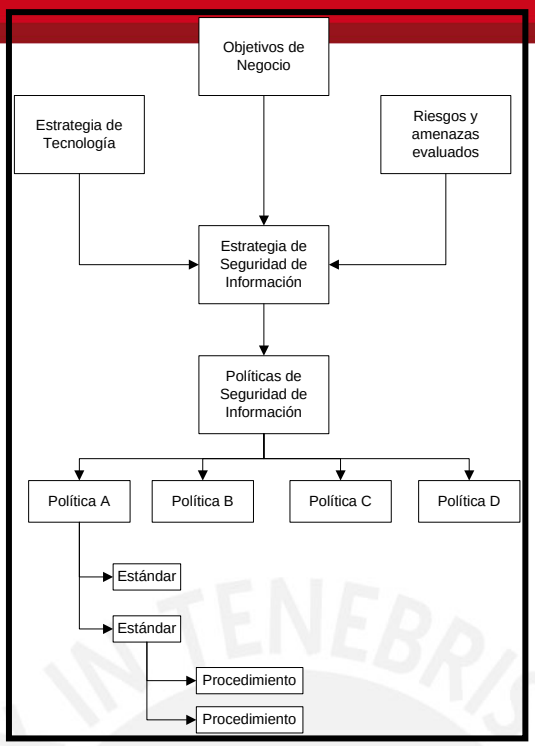

Figura 17 Jerarquía de políticas, estándares y procedimientos

1.7 Procedimientos y Guías

El desarrollo de procedimientos y guías que den soporte a las políticas de seguridad de información son responsabilidad del administrador de seguridad de información. Estándares técnicos y no técnicos deben desarrollarse para asegurar que los procedimientos cumplan con los requerimientos de las políticas. Algunos ejemplos de estándares se pueden nombrar:

- ✓ Estándares de passwords.
- ✓ Estándares de encriptación.
- ✓ Estándares de respaldos y retención.
- ✓ Estándares de políticas y procedimientos.
- ✓ Estándares de configuración de firewalls.
- ✓ Estándares de dominios de seguridad.

Algunos ejemplos de procedimientos técnicos y guías que pueden desarrollarse son:

- ✓ Respaldo y recuperación.
- ✓ Administración de privilegios.
- ✓ Reforzamiento del no cumplimiento con políticas (por ejemplo auditoria e detección de intrusos)
- ✓ Monitoreo automatizado del cumplimiento de políticas.
- ✓ Reforzamiento de la seguridad en las redes.
- ✓ Configuración de sistemas operativos.

Algunos ejemplos de procedimientos y guías no técnicos que pueden desarrollarse son:

- ✓ Procedimientos de revisión.
- ✓ Procedimientos de autorización.
- ✓ Procedimientos de aceptación de riesgos.
- ✓ Procedimientos de respuesta a incidentes.

1.8 Análisis de Valor

Las instituciones financieras a menudo justifican las inversiones en base a evaluación de proyectos. Por el contrario, para el caso de los proyectos de seguridad, el sustento es la verificación de evitar los riesgos específicos y cumplir los requerimientos del órgano regulador

El valor de evadir riesgos específicos puede sustentarse estimando las potenciales pérdidas en las que se incurre por un evento determinado, multiplicado por la probabilidad de que ocurra en un año. Este resultado es conocido como las pérdidas esperadas anuales (ALE[10]). El costo de un programa de seguridad para impedir un evento puede compararse luego en un análisis de costo-beneficio o como un retorno de inversión ROI[11].

Debe notarse que la experiencia en instituciones financieras muestra que el ROI no es usado, o que no es considerado como un buen indicador para justificar programas de seguridad. Esto es especialmente cierto para programas implementados por un tema normativo y/o regulatorio.

Los cálculos basados en el ROI para temas de seguridad de información han tenido poco desarrollo. Sin embargo, grupos de investigación en tres universidades norteamericanas han desarrollado fórmulas robustas y demostrables para datos en el retorno de inversión en seguridad *ROSI*[12].
Equipos de investigación de la Universidad de Idazo, del Instituto de Tecnología de Massachussets, y de la Universidad Carnie Mellon han desarrollado e investigado cálculos para el ROSI, los cuales pueden ser integrados por el administrador de seguridad de información al negocio de las instituciones financieras.

El análisis ROI puede enfocarse en tres potenciales tipos de beneficio:

- ✓ Ahorro en donde el ROI financiero pueda ser claramente identificado y cuantificado en términos de ahorro en costos. Por ejemplo en la administración automatizada o en otras herramientas que brindan beneficios cuantificables. Esto debe estar sustentado por la correspondiente información.

10 Término en inglés para "Annual Loss Expectation"
11 Término en inglés para "Return On Investment"
12 Término en inglés para "Return On Security Investment"

- ✓ Reducción cuantificable a la exposición del riesgo. Ejemplos pueden incluir la reducción de la probabilidad de ciertos tipos de brechas en la seguridad.

- ✓ Beneficios cualitativos que actualmente no son cuantificables en términos financieros pero que pueden definirse en términos cualitativos. Como ejemplos se pueden mencionar niveles altos de integridad de la información almacenada o circulando por la red, respuesta rápida y efectiva a incidentes de seguridad, o niveles altos de seguridad a través de capacitación del personal. Todos estos beneficios tienen consecuencias financieras que podrían ser difícilmente cuantificadas.

Con el análisis completo, el costo de implementar los procedimientos de seguridad de información, incluyendo la infraestructura que dará el soporte, debe ser cuantificado y revisado.

Un ejemplo de ROSI proveniente de los investigadores de Idaho es la fórmula para calcular el ROI para detección de intrusos en un sistema de defensa:

(R-E) + T= ALE

T es el costo de una herramienta de detección de intrusos
E es el dinero que se ahorra por detener las intrusiones a través del uso de la herramienta.
R es el costo anual para la recuperación de cualquier número de intrusiones.

Para determinar el ROSI, se debe restar del costo anual de intrusión lo que la institución financiera espera perder en un año (ALE).

Otro ejemplo para el cálculo del ALE es:

SLE x ARO= ALE

SLE[13] es la expectativa única de pérdida
ARO[14] es el rango de ocurrencia anualizado

13 Término en inglés para "Single Loss Expectancy"
14 Término en inglés para "Annualized Rate of Ocurrente"

2. Administración de Riesgos

De acuerdo a lo expuesto en el marco de referencia, podemos concluir que el objetivo de la administración de riesgos es identificar, cuantificar y administrar los riesgos asociados a la seguridad de información, con el fin de cumplir con los objetivos de negocio.

Se puede mencionar cinco tareas principales dentro del proceso de administración de riesgos:

- ✓ Desarrollo de un proceso sistemático, analítico y continuo de administración de riesgos.
- ✓ Garantizar que la identificación de riesgos, su análisis y mitigación, se encuentren integrados al ciclo de vida de los procesos de negocio.
- ✓ Aplicar metodologías de análisis e identificación de riesgos.
- ✓ Definición de estrategias para mitigar los riesgos a niveles aceptables para la institución financiera.
- ✓ Reportar cambios significativos en el riesgo a la gerencia, para tomar las decisiones que sean necesarias.

La administración de riesgos es un proceso que asegura que el impacto de las amenazas al explotar las distintas vulnerabilidades se encuentren en un nivel aceptado para la organización, incluyendo los costos asociados. A este nivel, esto se obtiene balanceando la exposición al riesgo con la implementación de controles de distintos tipos, sean por ejemplo administrativos o tecnológicos.

Para el caso de una institución financiera, generalmente el riesgo es la probabilidad de que un evento o transacción produzca pérdida monetaria, daño a la imagen, su personal y a sus activos. Se puede resumir el concepto en la siguiente ecuación:

Riesgo Total= Amenazas x Vulnerabilidad x Valor del Activo

El riesgo es parte de la vida diaria de una institución financiera y por tanto es poco práctico pretender eliminarlo, por lo que todas poseen un nivel de riesgo que aceptan. Una forma para establecer el nivel aceptable de riesgo es determinando un punto óptimo donde los costos de las pérdidas se sopesen con el costo de los controles. Algunas estrategias que pueden adoptar las instituciones financieras para tal fin son:

- ✓ Dar fin a la actividad que origina el riesgo.
- ✓ Transferir el riesgo.
- ✓ Reducir el riesgo empleando mecanismos de control.
- ✓ Aceptar el riesgo.

Es importante que una institución financiera cuente con un perfil de riesgo de su negocio. No existen modelos completos pero el dividir de manera lógica las áreas de riesgo de la organización, facilita el poder concentrarse en estrategias y decisiones para administrarlos. Asimismo permite desarrollar e implementar medidas que sean relevantes y económicamente convenientes.

Para desarrollar un programa de administración de riesgos, se debe emplear y adaptar un modelo referencial. En el marco de referencia se expone el estándar australiano ***AS/NZS 4360:2004***, el cual en la actualidad es el más conocido y difundido en administración de riesgos.

Empleando ***COBIT*** y su plataforma para el análisis de riesgos, se puede valorar los activos, evaluar sus vulnerabilidades, amenazas, riesgos, para luego aplicar medidas de control que dejen un riesgo residual, al cual luego se le puede aplicar un plan de acción.

La valoración de los activos suele ser compleja, por tanto debe realizarse de manera cuidadosa, pues a partir de ella se determinarán las medidas de control para cada activo en particular.

El primer paso de este proceso suele ser la identificación y clasificación de los recursos de información. La clasificación busca obtener el nivel de sensibilidad de los activos, siendo generalmente una tarea compleja. Se puede emplear como criterio de clasificación el costo de reemplazo de un activo: esto se aplica especialmente a los activos tangibles (hardware por lo general).

La valoración de datos e información se convierte en un aspecto bastante subjetivo. Por tanto es importante que la valoración incluya siempre como criterio el daño producto de la exposición de información a riesgos con niveles no aceptables para la institución financiera.

Algunos ejemplos típicos de activos asociados con información y tecnología son:

- ✓ Información y datos.
- ✓ Hardware.
- ✓ Software.
- ✓ Servicios.
- ✓ Documentos.
- ✓ Personal.

Algunos ejemplos típicos de amenazas son:

- ✓ Errores.
- ✓ Accidentes.
- ✓ Daño malicioso.
- ✓ Eventos naturales (terremotos por ejemplo).
- ✓ Fraude.
- ✓ Robo.
- ✓ Fallas de equipos y/o software.
- ✓ Pérdida de servicios (energía eléctrica por ejemplo).

Mientras que algunos ejemplos de vulnerabilidades son:

- ✓ Software defectuoso.
- ✓ Equipos configurados erróneamente.
- ✓ Diseño de red equivocado.
- ✓ Personal insuficiente.
- ✓ Tecnología no probada.
- ✓ Transmisión de información en medios inseguros.

El punto clave en la administración de riesgos es la mitigación o proceso de tratamiento (cómo el riesgo evaluado es tratado en la organización) En la Figura 18 se muestra el proceso de tratamiento de riesgos sugerido por el estándar AS/NZS 4360:2004:

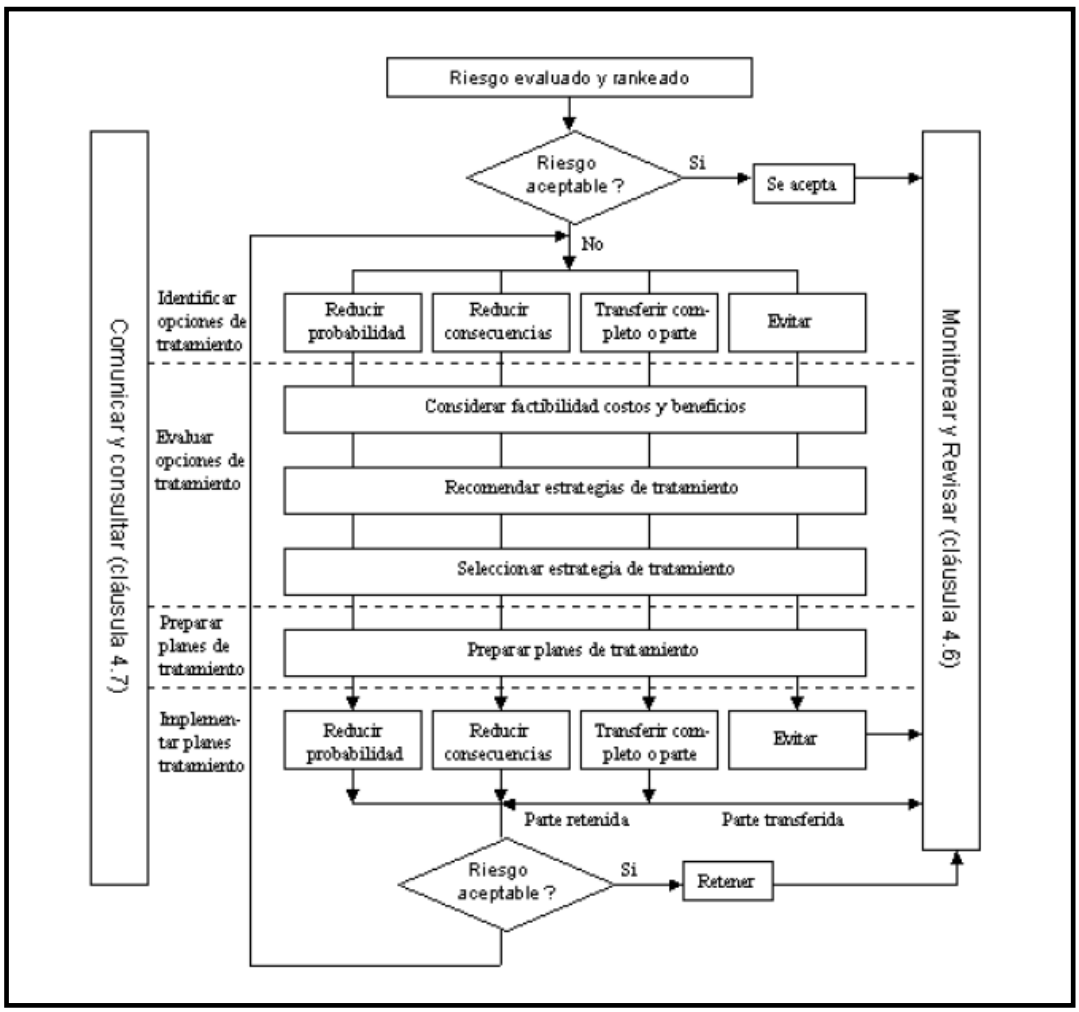

Figura 18. Proceso de Tratamiento de Riesgos según el AS/NZS 4360:2004 [24]

Los elementos de control que deben ser considerados pueden ser preventivos o detectivos, manuales o automatizados.

En resumen, el proceso de administración de riesgos consiste en **tomar decisiones de negocio**. El impacto de ataques y el nivel de riesgo aceptable para situaciones específicas, se convierten en una decisión fundamental de acuerdo a políticas de la organización.

2.1 Proceso de Administración de Riesgos

Los procesos deben ser diseñados de tal manera que puedan ser monitoreados en cuanto a su seguridad.

Las instituciones financieras usualmente deben usar algunas de las siguientes técnicas en este proceso:

- ✓ Identificar el perfil de riesgo de la organización.
- ✓ Entender y documentar la naturaleza y extensión de los riesgos a los que está expuesta la institución.
- ✓ Identificar prioridades en la administración de riesgos, lo cual se obtiene mediante la:
  - Identificación de la probabilidad de ocurrencia de las amenazas.
  - Identificación del valor cuantitativo (monetario) y cualitativo (efecto) de la información o recurso crítico.
  - Determinación del impacto en el negocio si la vulnerabilidad es explotada con éxito.

Se debe tener un entendimiento preciso de las necesidades de **confidencialidad, integridad y disponibilidad** de los recursos de información. Es necesario tener un conocimiento en detalle de los procesos de negocio y determinar qué recursos de información son críticos para cada línea de negocio en una institución financiera. Esta información se puede obtener en charlas con los dueños de cada proceso de negocio, documentación de procesos, y charlas con los gerentes de área. No se podrá definir adecuadamente que tan críticos son los recursos hasta que no se tenga detalle de los procesos de negocios a los que dan soporte.

2.2 Integración en el Ciclo de Vida de los Procesos

Asegurar que la identificación de riesgos, análisis y actividades de mitigación estén integradas en el ciclo de vida de los procesos, es un tarea importante en la gestión de seguridad de información.

Desde que los recursos de información van cambiando, surgen nuevas vulnerabilidades, lo cual implica una variación en el riesgo asociado. Por ello, es necesario realizar un seguimiento a estos cambios para adoptar las medidas necesarias en caso el riesgo tienda a aumentar.

Cada institución financiera debe implementar procedimientos de gestión de cambios en los recursos de información para mantener siempre controlado el nivel de riesgo expuesto de los mismos. Es recomendable que estos procedimientos sean clasificados por línea de negocio y/o áreas dentro de la organización.

Integrando la identificación de riesgos, análisis y actividades de mitigación en ciclo de vida de los procesos, se estará asegurando que la información crítica sea adecuadamente protegida. Este es un aspecto proactivo, que permitirá planear e implementar políticas de seguridad y procedimientos alineados con los objetivos de negocio y objetivos de la institución financiera.

Debido a que la administración de riesgos es un proceso continuo, éste debe ser visto como un **ciclo de vida**. Al aplicar una administración de riesgos basada en ciclos de vida, se optimizan costos, lo que una evaluación total de riesgos no permitiría. Por el contrario, las actualizaciones permiten la evaluación de riesgos y su administración, como un proceso periódico.

2.3 Identificación de Riesgos y Métodos de Análisis

La identificación de riesgos y métodos de análisis permiten un diseño e implementación de estrategias para mitigar la exposición al riesgo de la información más crítica de la institución financiera.

Los métodos de identificación de riesgos deben incluir:

- ✓ Examinar los recursos de información de todas las áreas de la institución financiera, de manera sistemática y objetiva.
- ✓ Una actitud proactiva antes que reactiva.
- ✓ Sintetizar todas las fuentes de riesgo para la información, tanto internas como externas a la institución financiera.

Un primer paso es realizar un mapeo de riesgos o una evaluación macro de las amenazas más importantes para la institución financiera. Se debe reiterar que esta actividad debe realizarse de **manera continua**.

Una gran variedad de riesgos pueden ser identificados, por lo que es necesario establecer qué riesgos serán objetivos de administración. Para esto se pueden revisar los tipos de riesgo dados en la sección de Administración de Riesgos del Marco de Referencia.

Métodos técnicos que incluyan el uso de software, so posibles de emplearse para identificar y hacer seguimiento a los riesgos. Para la aplicación de un análisis de riesgos y métodos de identificación, se debe preparar un plan de acción detallado, definir requerimientos de recursos, y establecer un presupuesto que permita desarrollar las tareas más importantes.

2.4 Mitigación de Riesgos

Cuando los riesgos que amenazan una institución financiera han sido identificados y **priorizados,** se plantean las estrategias de seguridad y se priorizan las opciones para mitigarlos. Los controles incluyen:

- ✓ Controles preventivos, para reducir las vulnerabilidades y hacer que un ataque fracase o reducir el impacto del mismo.
- ✓ Controles correctivos para reducir el impacto.
- ✓ Controles detectivos, para descubrir ataques anticipadamente, y aplicar los controles preventivos o correctivos.

Existen herramientas y procesos diversos para mitigar los riesgos dentro de la organización de una institución financiera. Debe hacerse un balanceo entre las opciones disponibles y lo que la institución financiera está dispuesta a aceptar. Para esto se consideran los costos e impactos en la institución financiera, siempre garantizando que los procesos de negocios no se vean afectados**. El costo de un control nunca debe exceder el beneficio esperado.**

Ejemplos para mitigar riesgos podrían incluir:

- ✓ Medidas de seguridad en aplicaciones.
- ✓ Seguridad física.
- ✓ Controles de acceso lógico.
- ✓ Controles de acceso a las redes.
- ✓ Firewalls.
- ✓ Sistema de Detección y Prevención de Intrusos.
- ✓ Procesos de administración de crisis.
- ✓ Seguridad inalámbrica.
- ✓ Encriptación.
- ✓ Antivirus

2.5 Cambios Significativos en los Riesgos

Es de primordial importancia reportar cambios significativos en los riesgos a los responsables de la gestión de seguridad de información en una institución financiera. A medida que ocurren cambios, la evaluación de riesgos debe ser actualizada para asegurar su efectividad y eficiencia.

Para administrar adecuadamente los riesgos, es necesaria una adecuada documentación. Las decisiones en relación a la documentación y su extensión implicarán costos y beneficios. La política de administración de riesgos debe definir la documentación que sea necesaria.

Específicamente en cada etapa del proceso, la documentación debe incluir:

- ✓ Objetivos.
- ✓ Audiencia.
- ✓ Recursos de Información.
- ✓ Decisiones.

El documento de políticas de administración de riesgos puede incluir información como:

- ✓ Objetivos de la política para administrar los riesgos.
- ✓ Relación entre la política de administración de riesgos, la estrategia de la institución financiera y los planes de negocio.
- ✓ Extensión y rango de aspectos a los cuales aplica la política.
- ✓ Guía para catalogar riesgos aceptables para la institución financiera.
- ✓ Responsables de la administración de riesgos.
- ✓ Nivel de documentación requerido.
- ✓ Plan de revisión de la política de administración de riesgos.

Una documentación típica de administración de riesgos debe incluir como mínimo lo siguiente:

- ✓ Un registro por riesgo: asimismo, para cada riesgo identificado registrar lo siguiente:
  - o Fuente de origen del riesgo.
  - o Naturaleza del riesgo.
  - o Controles existentes.
  - o Consecuencias y probabilidad de ocurrencia.
  - o Nivel de riesgo inicial.
  - o Vulnerabilidad a factores internos y externos.
- ✓ Un plan de mitigación y acciones para los riesgos, detallando lo siguiente:
  - o Identificación del responsable de la implementación del plan.
  - o Recursos a utilizarse.
  - o Presupuesto asignado.
  - o Cronograma de implementación.
  - o Detalle de controles.
  - o Frecuencia de revisión.
- ✓ Documentos de monitoreo y auditoria, que deben incluir:
  - o Resultados de revisiones y auditorias, y otros procedimientos de revisión.
  - o Seguimiento a recomendaciones e implementaciones.

3. Administración de un Programa de Seguridad de Información

El objetivo en la administración de un programa de seguridad de información es diseñar, desarrollar y gestionar lo necesario para implementar una plataforma de gobierno de seguridad de información.

Existen nueve tareas que comprenden la administración del programa:

- ✓ Creación y mantenimiento de planes para implementar una plataforma de seguridad de información.
- ✓ Desarrollo de conceptos base de seguridad de información.
- ✓ Desarrollo procedimientos y guías que aseguren que los procesos de negocio direccionen los riesgos de seguridad de información.
- ✓ Desarrollo de procedimientos y guías para las actividades relacionadas a la infraestructura tecnológica, que aseguren el cumplimiento con las políticas de seguridad de información.
- ✓ Integración de los requerimientos del programa de seguridad de información dentro del ciclo de vida de las actividades de la institución financiera.
- ✓ Desarrollo de metodologías para cumplir con los requerimientos de las políticas de seguridad de información, los mismos que tienen un impacto en usuarios finales.
- ✓ Promoción de responsabilidades en los dueños de los procesos de negocios y demás usuarios, en la administración de riesgos de seguridad de información.
- ✓ Establecimiento de métricas para la administración de la plataforma de seguridad de información.
- ✓ Aseguramiento de que los recursos internos y externos para la seguridad de información hayan sido identificados y apropiadamente gestionados.

3.1 Creación y Mantenimiento de Planes

La creación y mantenimiento de planes para la implementación de una plataforma de gobierno de seguridad de información es crítica para el éxito de un programa de seguridad. El plan se desarrolla para:

- ✓ Definir la plataforma.
- ✓ Obtener la aprobación de la plataforma de la alta gerencia.
- ✓ Implementar la plataforma de gobierno de seguridad de información.
- ✓ Monitorear el progreso y realizar los cambios que sean necesarios.

El plan debe especificar las responsabilidades en las tareas y establecer un cronograma para completarlas. Dependiendo del tamaño de la institución financiera, el administrador de seguridad de información puede ser el responsable de la gran mayoría de las tareas. En instituciones financieras más grandes, el administrador de seguridad de información puede delegar algunas de ellas.

El administrador de seguridad de información debe conducir primeramente un análisis de riesgos que identifique los niveles críticos de los recursos de información, así como las amenazas y vulnerabilidades relevantes de cada uno. Debe desarrollarse una **matriz** para establecer los recursos de información a proteger. Esto permitirá tener un plan más completo y actualizable. Los cambios realizados durante la etapa de desarrollo e implementación son menos costosos y más efectivos que los que se realizan después que el programa de seguridad esté en funcionamiento.

Desarrollar e implementar un plan de seguridad implica distintas variables, grupos participantes y variadas tareas. Consecuentemente, es indispensable contar con habilidades de gestión de proyectos y herramientas efectivas para el éxito del programa.

Si una institución financiera no cuenta con un puesto que dé soporte a la administración de proyectos, se deben emplear técnicas generales de administración de proyectos, tales como establecer objetivos, medir los progresos, hacer seguimiento a las fechas límite, y asignar responsabilidades.

La implementación de un programa de seguridad debe ser analizada para estimar los niveles de esfuerzo necesarios y recursos requeridos para desarrollar cada tarea. Como mínimo, para cada tarea debe considerarse lo siguiente:

- ✓ Horas hombre de acuerdo a la especialidad (por ejemplo analistas, programadores, etc.).
- ✓ Equipamiento necesario (por ejemplo luces adicionales, puertas de seguridad, lector de tarjetas, etc.)
- ✓ Requerimientos de hardware y software (por ejemplo firewalls, sistemas de detección de intrusos, pruebas de penetración, herramientas de monitoreo, etc.).
- ✓ Requerimientos de capacitación.

Habiendo establecido un cronograma de trabajo estimado para todas las tareas, se debe plantear un presupuesto, el cual consistirá en:

- ✓ Obtención de un nivel estimado de esfuerzo necesario fase a fase, así como los recursos necesarios para cada una.
- ✓ Expresar de manera aproximada el esfuerzo en horas hombre.

Lo que sigue es la programación de tareas, las cuales pueden organizarse de acuerdo a lo siguiente:

- ✓ Fecha más temprana de inicio: considerando la secuencia lógica entre tareas, tratando en lo posible de llevar a cabo tareas paralelas.
- ✓ Fecha más tardía de conclusión: considerando las horas estimadas por tarea, disponibilidad de personal, y demás recursos, permitiendo fechas no operativas (feriados, fines de semana, etc.).

3.2 Conceptos Base de Seguridad de Información

El desarrollo de conceptos base de seguridad de información ayuda a definir un nivel aceptable mínimo de seguridad, que será implementado para proteger los recursos de información, de acuerdo con los respectivos niveles de criticidad. Previo a la definición de estos conceptos bases, debe establecerse una política de seguridad de información, asignación de niveles de criticidad para los recursos de información, y evaluación de riesgo del entorno en el que se hallan éstos.

El administrador de seguridad de información emplea estos conceptos bases de seguridad para decidir qué medidas adicionales deben ser implementadas para cumplir con las políticas previamente establecidas. Las medidas de seguridad deben direccionar al personal, instalaciones, control operacionales y técnicos, incluyendo procedimientos.

Dos fuentes de conceptos bases de seguridad de información son los establecidos en el **ISO 17799** y el **BS7799**, vistos en el marco de referencia.

3.3 Procesos de Negocio

Los procesos de negocio se dan día a día. Un programa de seguridad efectivo es aquel en el cual la seguridad es considerada en cada proceso. Es primordial establecer programas de capacitación que aseguren el conocimiento del personal en temas de seguridad dentro del ciclo de vida de los procesos de negocio.

El personal responsable de la generación y uso de información relacionada a procesos de negocio es el más calificado para desarrollar prioridades, e identificar qué riesgos e impactos ocurrirían si los recursos de la institución financiera se perdieran o corrompieran. El administrador de seguridad de información debe coordinar esfuerzos de seguridad con esfuerzos de negocio. Esto para asegurar que la seguridad de información "conviva" con las necesidades de negocio, y que es posible diseñar e implementar procedimientos de seguridad.

El administrador de seguridad de información puede cumplir todo lo señalado, teniendo reuniones periódicas con los dueños de negocio de la institución financiera, y documentando esto en las guías de seguridad de información, que luego serán aceptadas y respaldadas por la alta gerencia.

3.4 Actividades relacionadas a la infraestructura tecnológica

Los procedimientos para las actividades de la infraestructura tecnológica son desarrollados para asegurar el cumplimiento con las políticas de seguridad de información. Existen varias definiciones e implementaciones para la infraestructura tecnológica, dependiendo de los objetivos de negocio de una institución financiera. **COBIT**, discutido en el marco de referencia, brinda un esquema que puede ser tomado en cuenta Sin embargo, existen componentes generalmente aceptados en una infraestructura de tecnología, que incluyen:

- ✓ Procesos
- ✓ Infraestructura
- ✓ Plataforma
- ✓ Red

Cada componente tiene requerimientos de confidencialidad, integridad, disponibilidad y auditabilidad. El administrador de seguridad de información debe considerar estos requerimientos para cada componente, no sólo individualmente, sino de manera colectiva, usándolos para determinar los controles que sean necesarios, adecuando las políticas de seguridad para proteger la información de la institución financiera.

A continuación se presentan los controles mínimos necesarios para cumplir con una política básica de seguridad de información:

- ✓ Control de procesos: Las políticas de seguridad de información y la administración de seguridad de información son controles esenciales para los procesos. Son la base para un programa de seguridad de información, y críticos para la infraestructura de tecnología.
- ✓ Control de instalaciones: Tienen por finalidad restringir el acceso a las áreas donde se procesa información confidencial y otros recursos tangibles de información, como por ejemplo el hardware. Entre los métodos para mantener al personal no autorizado lejos de áreas restringidas se incluyen el uso de diferentes dispositivos electrónicos (smart cards, cámaras de seguridad, sensores, etc.). Estos controles igualmente tienen por finalidad prevenir y/o mitigar daños a las instalaciones u otros recursos tangibles, causados por eventos naturales o tecnológicos.

- ✓ Control de personal: Se basan en las personas midiendo el nivel de confianza e integridad de quienes se encuentran ubicados en puestos claves dentro de la institución financiera, en especial el nuevo personal.
- ✓ Control en las plataformas: Se basa en la tecnología que incluye características de seguridad implementadas en los sistemas operativos, las aplicaciones, sistemas de detección de intrusos, etc.
- ✓ Control en la red: Se centran en dispositivos de seguridad tales como firewalls, ruteadores, switches, acceso remoto, y cualquier otro dispositivo que monitorea y restringe la información que viaja por las redes.

3.5 Actividades en el ciclo de vida de la institución financiera

Al integrar un programa de seguridad de información en las actividades del ciclo de vida de la institución financiera se asegura su efectividad. A través de programas de capacitación y educación, así como el establecimiento de políticas de seguridad de información, el administrador de seguridad de información puede implantar la seguridad en cada fase del ciclo de vida de negocios de la institución financiera.

La protección de los recursos de información de una institución financiera debe ser considerada en toda actividad dentro de los procesos de negocio. El administrador de seguridad de información, teniendo un conocimiento en detalle de cada proceso de negocio, podrá elaborar un eficiente y efectivo programa de seguridad de información.

El diseño e implementación de un programa de seguridad debe considerar la seguridad en el ciclo de vida de desarrollo de los sistemas. Una institución financiera puede emplear cualquier metodología, ello dependerá de dónde y cómo se considere la seguridad, y de los procesos de negocio de cada institución.

La metodología más empleada es la tradicional SDLC[15] que de manera resumida se compone de las siguientes fases:

- ✓ Viabilidad: Se determinan los beneficios estratégicos de implementación de un sistema, así como la identificación y cuantificación de los costos asociados. Igualmente se establecen cronogramas de trabajo preliminares.
- ✓ Requerimientos: Se define el problema o la necesidad que debe ser atendida, así como la funcionalidad y requerimientos del nuevo sistema. Es imprescindible la participación del usuario final en esta etapa. El sistema puede desarrollarse de manera interna o a través de un proveedor, siendo necesario en este último caso un adecuado y documentado proceso de adquisición.

15 Del inglés System Development Life Cycle

- ✓ Diseño: En base a los requerimientos definidos, se establecerán especificaciones que describan las partes del nuevo sistema y la forma como interactuarán, se implementarán, qué hardware y software se necesitará, requerimientos de red, etc. Además se establecerá un proceso formal de control de cambios para tomar en cuenta nuevos requerimientos que pudieran darse a lo largo del proceso de desarrollo.
- ✓ Desarrollo: Empleando las especificaciones del diseño, se empezará con la programación y formalización del soporte operacional de los procesos del sistema. En esta etapa ocurren distintos niveles de prueba, para validar y verificar lo que se viene desarrollando.
- ✓ Implementación: Se establecerá la operación del nuevo sistema con la aprobación de los usuarios finales. El sistema puede pasar por un proceso de certificación y acreditación para evaluar su efectividad en la mitigación de riesgos a un nivel aceptable. De la misma manera se evaluará si el sistema cumple con los objetivos previamente establecidos y si cuenta con un nivel apropiado de control.

Es imprescindible que el administrador de seguridad de información participe en todas las fases descritas para identificar los requerimientos de seguridad a fin de mantener los riesgos a un nivel aceptable.

3.6 Impacto en los Usuarios Finales

Los requerimientos de las políticas de seguridad deben ser diseñados teniendo en cuenta la autorización de acceso de los usuarios finales a recursos de información. Si los procesos de negocios se ven adversamente afectados por la implementación de procedimientos de seguridad, el administrador de seguridad de información debe justificar el impacto.

3.7 Responsabilidad

Promover la responsabilidad de los dueños de procesos de negocios y demás usuarios en la administración de los riesgos de seguridad de información es un desafío para la gestión de seguridad de información. Los dueños de los procesos de negocios son los que mejor entienden las necesidades de la institución, y además son los que mejor pueden evaluar el impacto en la misma, pues finalmente son los responsables de cumplir los objetivos de negocio.

El administrador de seguridad de información debe reunirse con los dueños de los procesos de negocios para discutir su responsabilidad en los riesgos de seguridad de información.

Esto un proceso de educación; el administrador de seguridad de información comunica cómo la seguridad de la institución financiera puede asistir a un dueño de procesos de negocio en la administración de los riesgos de seguridad de información.

Adicionalmente si alguno de los dueños de procesos de negocio no desea realizar cambios en los sistemas o aplicaciones para reforzar la seguridad, es imperativo que firmen la aceptación de los riesgos implicados, aceptando las consecuencias de los mismos.

3.8 Métricas

Establecer métricas para administrar la plataforma de seguridad de información permite gestionar adecuadamente la seguridad, midiendo de manera más precisa el desempeño de la misma.

El administrador de seguridad de información debe saber como medir el nivel de riesgo de los sistemas y redes, para a partir de ello implementar los controles más adecuados.

El mayor problema muchas veces es qué debe ser medido y cómo medirlo. Las métricas, tales como el número de ataques en contra de un sistema, o el número de virus que infectan un servidor, son algunos ejemplos.

Se puede tomar como modelo en el establecimiento de métricas el ***SSE-CMM***[16], para medir la evolución de los procesos de la organización.

3.9 Recursos Internos y Externos para la Seguridad de Información

Asegurar que los recursos internos y externos de seguridad de información sean identificados, apropiados y gestionados es una tarea obligatoria en las actividades de seguridad.

Se deben aprovechar todos los recursos con los que la institución financiera cuenta, los cuales incluyen recursos internos tales como servicios brindados por proveedores y consultores.

Entre los recursos externos se pueden mencionar el monitoreo remoto de firewalls, detección de intrusos, etc.

El administrador de seguridad de información es responsable de la administración de estos recursos, lo que incluye cumplir con las expectativas de desempeño de los mismos en comparación a los objetivos trazados.

16 Del inglés Systems Security Engineering Capability Maturity Model

Se vuelve de vital importancia contar con un proceso de administración de incidentes, el cual entre a tallar ante cualquier evento de seguridad, para atenderlo rápidamente, brindando la protección de los recursos de información de la institución financiera.

4. Gestión de la Seguridad de Información

Las principales tareas a desarrollar son:

- ✓ Asegurar que las reglas para el uso de los sistemas de información estén alineadas con las políticas de seguridad de información.
- ✓ Asegurar que los procedimientos administrativos para los sistemas de información estén alineados con las políticas de seguridad de información.
- ✓ Asegurar que los proveedores de servicios sigan las políticas de seguridad de información de la institución financiera.
- ✓ Asegurar que la seguridad de la información no se vea comprometida en el proceso de administración de cambios.
- ✓ Asegurar que las evaluaciones de vulnerabilidades midan la efectividad de los controles implementados.
- ✓ Asegurar que los aspectos que no cumplan las normas sean atendidos oportunamente.
- ✓ Asegurar que el desarrollo de actividades de seguridad de información puedan influenciar en la cultura y comportamiento del personal de la institución financiera.

4.1 Reglas de uso para los Sistemas de Información

Asegurar que las reglas de uso de los sistemas de información cumplan con las políticas de seguridad de información, garantiza una buena gestión de seguridad en la institución financiera.

Los aspectos a tomar en cuenta incluyen la identificación de la importancia de los activos de información, la necesidad de seguridad, definición de la sensibilidad y criticidad de los mismos, su confidencialidad, integridad y disponibilidad.

Las políticas deben ser consistentes y mapeadas con algún estándar, tal como el ***ISO/IEC 17799*** visto en el marco de referencia. Este estándar puede servir como checklist para asegurar que todos los tópicos de seguridad sean cubiertos.

Debe tenerse en cuenta que el diseño de una estrategia de seguridad puede ser el vehículo mas importante para contar con la participación de la alta gerencia de la institución financiera, obteniendo consenso y soporte para el programa de seguridad, necesarios si se desean políticas de seguridad efectivas.

4.2 Procedimientos Administrativos para Sistemas de Información

Al contar con una política aprobada por la alta gerencia, con los roles y responsabilidades asignados, se torna imprescindible contar con procedimientos y estándares de gestión.

Estos procedimientos se desarrollan para definir los pasos mínimos necesarios para desarrollar bases de seguridad, métricas, y requerimientos específicos de los sistemas.

Es crítico que el administrador de seguridad de información trabaje y coordine de cerca con los administradores de sistemas operativos, aplicativos, redes y correo, para asegurar de esta manera que los procedimientos administrativos cumplan con las políticas de seguridad de información.

Los procedimientos administrativos pueden abarcar en algunos casos los pasos necesarios para las solicitudes, autorizaciones, creación de usuarios, y su revisión periódica, transferencias y terminación. Estos procedimientos pueden ser desarrollados manualmente o de manera automatizada; sin embargo cada proceso debe cumplir con los estándares de seguridad, asegurando el cumplimiento de las políticas de seguridad de la institución.

4.3 Proveedores Externos

Las instituciones financieras a menudo cuentan con servicios brindados por departamentos, divisiones, y proveedores externos. El administrador de seguridad de información debe tomar las medidas necesarias para garantizar que los proveedores acaten las políticas de seguridad de información de la institución. Se vuelve necesario contar con controles que minimicen el riesgo al que se ve expuesta la institución financiera frente a proveedores externos, que acceden de manera directa o indirecta a información de la misma.

El administrador de seguridad de información debe comunicar a los proveedores de las políticas de seguridad de la institución, y obtener de ellos un acuerdo escrito de confidencialidad, dado que la mayoría de veces la información confidencial se puede ver expuesta. Generalmente este aspecto, así como otros niveles de servicio se establecen en un contrato firmado entre el proveedor y la institución financiera.

4.4 Uso de métricas para medir, monitorear y reportar

El empleo de métricas para medir, monitorear y reportar la efectividad y eficiencia de los controles de seguridad de información, así como las políticas de seguridad de información es una tarea continua que debe desarrollar el administrador de seguridad de información en una institución financiera. Adicionalmente, el monitoreo permite realizar los cambios que sean necesarios, dado que los sistemas de información y recursos de información constantemente cambian.

Por lo expuesto, la herramienta más efectiva para gestionar el programa de seguridad es *el empleo de métricas*. El administrador de seguridad de información debe contar con una metodología formal para medir la efectividad del programa de seguridad.

En el diseño de métricas, una buena base debe ser establecida. Buenas métricas deben ser específicas, medibles, alcanzables, repetitivas y dependientes del tiempo. Luego, las métricas pueden ser usadas para medir el progreso.

El administrador de seguridad de información debe contar con un proceso de revisión periódica de las métricas, reportándose cualquier actividad inusual. Un plan de acción para reaccionar a estas actividades debe ser desarrollado.

4.5 Gestión de Cambios

El administrador de seguridad de información debe implementar mecanismos de control en donde la seguridad sea considerada en cada proceso de cambio que efectúe la institución financiera. La seguridad debe ser monitoreada y mantenida constantemente, en la medida que nuevas vulnerabilidades pueden ser introducidas en los sistemas, como resultado de cambios y/o actualizaciones.

Un riesgo común es el desarrollo o implementación de una nueva aplicación que accede la red. Si la red no cumple con los requerimientos de seguridad de la institución financiera, surgen nuevos riesgos para los recursos de información.

A medida que se realizan cambios en los sistemas y procesos en el tiempo, existe a menudo una tendencia a que los controles de seguridad se vuelvan menos efectivos. Por ello, el administrador de seguridad de información debe tener participación activa en los cambios, para asegurar que no surjan nuevas vulnerabilidades. Del mismo modo es importante mantener actualizados los controles de seguridad como resultado de los cambios.

4.6 Evaluación de Vulnerabilidades

La evaluación de vulnerabilidades es una de las herramientas vital en la medición de la efectividad del programa de seguridad de información.

La evaluación de vulnerabilidades típicamente incluye:

- ✓ Revisión de controles de seguridad para determinar si existen vulnerabilidades.
- ✓ Prueba de controles en curso para determinar su efectividad.
- ✓ Pruebas de penetración para localizar vulnerabilidades.
- ✓ Desarrollo de recomendaciones para reducir las vulnerabilidades y mejorar la seguridad.
- ✓ Seguimiento de los progresos.
- ✓ Debilidades en los sistemas operativos.
- ✓ Deficiencias en las redes.
- ✓ Aplicaciones (incluyendo bases de datos, aplicaciones web, correo, etc.).

En algunas ocasiones es recomendable contratar los servicios de terceros para realizar estas evaluaciones. Esto brinda un punto de vista independiente y objetivo de las posibles vulnerabilidades que enfrenta la institución financiera. Estas evaluaciones deben incluir recomendaciones para mitigar las vulnerabilidades detectadas.

Las evaluaciones de vulnerabilidades son útiles para determinar las debilidades en un sistema, pero es importante tener en mente que la mayoría de veces existirá una amenaza que explote una vulnerabilidad y causará un impacto.

4.7 Aspectos de no cumplimiento

Para asegurar que aspectos de no cumplimiento sean resueltos de manera oportuna, el administrador de seguridad de información debe emplear procesos específicos. Dependiendo en qué tan significativo sea el riesgo, varios puntos de vista podrían aplicarse. Dependerá del administrador de seguridad de información emplear la mejor alternativa. Si un aspecto de no cumplimiento encierra un riesgo serio, es obvio que la resolución debe ser rápida.

Generalmente se lleva una bitácora de estos aspectos de no cumplimiento, registrando las responsabilidades asignadas. Estos aspectos pueden ser identificados por medio de distintos mecanismos tales como:

- ✓ Monitoreo.
- ✓ Reportes de auditoria.
- ✓ Revisiones de seguridad.
- ✓ Escaneo de vulnerabilidades.

4.8 Cultura, Comportamiento y Educación en Seguridad de Información

La capacitación y educación en temas de seguridad puede influencia en la cultura y comportamiento del personal. Se vuelve un factor crítico para el éxito de un programa de seguridad.

Esta educación y capacitación incluye varios aspectos, desde especialización del personal de seguridad, a habilidades generales por todo el resto del personal de la institución financiera.

La institución financiera debe tener conocimiento claro de su cultura, la actitud de las personas responsables de la seguridad de información. El proceso de educación y capacitación debe ser un proceso continuo, teniendo el administrador de seguridad la responsabilidad de que sea desarrollado de la mejor manera.

5. Administración de Respuestas a Incidentes

Las principales tareas a desarrollar son:

- ✓ Desarrollar e implementar procesos para detectar, identificar y analizar eventos relacionados con la seguridad.
- ✓ Desarrollar planes de respuesta y recuperación que incluyan la organización, entrenamiento y equipamiento de equipos.
- ✓ Pruebas periódicas de los planes de respuesta y recuperación.
- ✓ Asegurar la ejecución los planes de respuesta y recuperación.
- ✓ Establecer procedimientos de documentación para un evento, como base para un posterior análisis forense.
- ✓ Administrar revisiones posteriores a los eventos, identificando las causas y acciones correctivas.

5.1 Procesos para detectar, identificar y analizar eventos de seguridad

La identificación de un incidente no es una ciencia exacta: existen metodologías que pueden usarse para identificar los incidentes, pero cuando algo ocurre sólo una vez es a menudo complicado identificar el evento como una deficiencia de seguridad o problema de sistema.

Se define un incidente como un evento que causa algún nivel de interrupción a los procesos normales de negocio, y que es precipitado generalmente por un individuo, de manera maliciosa o accidental.

Dada esta definición, algunos incidentes que pueden categorizarse como de seguridad son:

- ✓ Intrusiones en las computadoras o intentos de intrusión.
- ✓ Ataques de denegación de servicio.
- ✓ Acceso a información de manera no autorizada.

Algunos incidentes son muy obvios. Pero desafortunadamente no todos los incidentes son fácilmente identificables. Por ello usualmente existen indicios característicos cuando un verdadero incidente de seguridad ha ocurrido. Estos indicios pueden encontrarse en:

- ✓ Archivos de Log (de firewalls, ruteadores, sistemas, IDS[17], etc.).
- ✓ Tráfico de red.
- ✓ Configuraciones del sistema.

Los sistemas en sí son a menudo la mejor fuente para obtener información acerca de un potencial incidente de seguridad. Es complicado poder ocultar por completo la evidencia de una intrusión de un sistema comprometido. El atacante usualmente hará cambios al sistema que de alguna manera puede ser detectado.

Por lo general un incidente de seguridad será identificado por los usuarios finales. En ese caso, el primer llamado es al área de help desk de la institución financiera (la gran mayoría de instituciones cuentan con esta área): si el personal de dicha área está capacitado en incidentes de seguridad, podrán asistir al administrador de seguridad de información en la identificación de estos incidentes. Por lo anterior es importante que el personal de ésta área este debidamente capacitado. En caso sea necesaria ayuda más especializada, el personal de help desk debe recabar la siguiente información:

[17] *Del ingles Intrusion Detection System*

- ✓ Nombre del usuario que reportó el incidente.
- ✓ Fecha y hora del reporte de incidente:
- ✓ Fecha y hora en la que inició con las indicaciones.
- ✓ Tipo de indicaciones que se brindó.
- ✓ Tipo de sistemas afectados (incluidos los sistemas operativos y hardware relacionado).
- ✓ Ubicación del sistema (si es posible la dirección IP).
- ✓ Informar si el evento sigue en curso o tuvo una actuación momentánea.
- ✓ Acciones que tomó el usuario previo al reporte del incidente.
- ✓ Acciones que tomó el área help desk al tomar conocimiento del incidente.

Si se sospecha de un incidente de seguridad, el área de help desk debe recomendar al usuario final dejar el sistema y esperar por indicaciones. Luego se comunica al administrador de seguridad de información para que tomen las medidas necesarias de acuerdo al tipo de evento.

5.2 Desarrollo de Planes de Respuesta y Recuperación

Desastres de toda naturaleza y magnitud pueden ocurrir en una institución financiera. Debido a la gran dependencia de la infraestructura tecnológica, se vuelve esencial que se desarrollen y mantengan planes de respuesta y recuperación. Este plan se derivará de las políticas y procedimientos existente, con los roles y responsabilidades para su preparación, ejecución y recuperación de distintos tipos de desastres.

Como se mencionó en la sección de Gobierno de Seguridad de Información, las instituciones financieras están reguladas para el tema de seguridad de información por la **Circular NºG-105-2002,** en donde se establece la necesidad de contar con un Plan de Continuidad de Negocios. Asimismo es recomendable contar con un Plan de Recuperación de Desastres, como complemento del primero.

Para el desarrollo de los planes de respuesta y recuperación se deben tener en cuenta como mínimo los siguientes aspectos, los cuales se deben implementar de acuerdo a las políticas y tamaño de la institución financiera:

- ✓ Contar con un buen inventario de hardware y software, debidamente clasificado en función a su criticidad para los procesos de negocio.
- ✓ Contar con un diagrama de conectividad de redes apropiado y actualizado.
- ✓ Contar con un cuestionario que permita la obtener información relevante de los sistemas que dan soporte a los procesos críticos de negocio.

- ✓ Contar con una matriz documentada con los sistemas críticos para los procesos de negocios y sus tiempos mínimos permitidos para estar fuera de funcionamiento.
- ✓ Contar con una matriz con los desastres potenciales, su impacto, y su probabilidad aproximada de ocurrencia.
- ✓ Contar con los costos de varias alternativas de recuperación para los procesos de negocios más críticos.
- ✓ Contar con un conjunto de recomendaciones que pueden ser presentadas a la alta gerencia para gestionar de la mejor manera la recuperación de un desastre.
- ✓ Contar con equipos de recuperación de desastre, divididos de acuerdo a los procesos de negocio e infraestructura tecnológica más críticos.
- ✓ Establecer las responsabilidades de cada miembro de los equipos de recuperación.
- ✓ Contar con procedimientos documentados y actualizados para la recuperación de desastres.
- ✓ Contar con centros de procesamiento alternos y ubicaciones alternativas para continuar con los procesos de negocios más críticos.
- ✓ Realizar frecuentemente pruebas de los planes, para medir su efectividad y detectar cualquier cambio o actualización necesaria.

5.3 Documentación

La documentación es vital para la respuesta a incidentes. Esto significa que en la medida que se documente los procedimientos y políticas antes de un incidente, durante y después, se podrá manejar y atender de la mejor manera a un incidente. Las medidas a tomar se mencionan a continuación:

- ✓ **Antes del incidente**: es claro que no se puede documentar los detalles de un incidente antes que ocurra. Pero se puede documentar los criterios que permitan manejar un incidente, así como las políticas y procedimientos que ayudarán cuando la institución financiera enfrente el inicio de un incidente.
- ✓ **Durante un incidente**: cuando un incidente está ocurriendo, lo primero es informarlo al administrador de seguridad de información, quien de acuerdo a la naturaleza del incidente lo reportará a la alta gerencia, o aplicará las medidas necesarias para contrarrestarlo, informando posteriormente de su ocurrencia. Es un momento importante para mantener una adecuada documentación del incidente, tomando nota de cada paso que se dio para su resolución. Esta documentación posteriormente sirve de base para la elaboración de reportes que detallen el incidente.

- ✓ **Después del incidente**: cuando el incidente ha terminado, se elabora un reporte o reportes con detalles del mismo. El propósito de estos reportes es mostrar lo que pasó y como se puede prevenir que no ocurra nuevamente en el futuro. Esto significa la mayoría de veces la actualización y/o cambio de controles de seguridad. Además se muestran por lo general conclusiones, teniendo claro que jamás se nombran las personas que tienen la responsabilidad de la ocurrencia del incidente, para no perder indicios importantes en un posterior análisis forense.

6. Conclusiones

De acuerdo a lo expuesto en la presente tesis, para implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el **apoyo y soporte de la alta gerencia**, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera. Al demostrarles lo importante que es la protección de la información para los procesos de negocio, se debe esperar de la alta gerencia su participación continua.

Contando con el apoyo de la alta gerencia se ha dado el primer gran paso. Este apoyo luego se debe transmitir a los dueños de procesos de negocio más importantes de la institución financiera, que generalmente son jefes de áreas. Dándoles a conocer la importancia de la seguridad de información en los procesos que manejan, se espera el apoyo de todo el personal a su cargo. Es recién en este punto donde entran a tallar todos los lineamientos del modelo de gestión expuesto, el cual se reflejará en las políticas, normas, estándares y procedimientos de seguridad, soportados por la tecnología de información de la institución. No necesariamente la tecnología de información por sí sola garantiza la seguridad de información. Se vuelve imperativo gestionarla de acuerdo siempre a los objetivos de negocio.De nada sirve contar con los últimos adelantos tecnológicos, si no se da la importancia debida a la protección de la información, la cual se verá reflejada en el cumplimiento de todas las políticas de seguridad de información, siempre actualizadas de acuerdo a los cambios constantes en los negocios propios de una institución financiera.

REFERENCIAS BIBLIOGRAFICAS

[1] D. Sullivan *The Definite Guide to Security Management.* Computer Associates pp 1, 2004.

[2] *La Seguridad de Información*, publicación editada por el Grupo Ibermática, Nº 93, pp. 5 Abril 2000.

[3] *Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision,* pp 1, 2003

[4] *The Impact of Sarbanes-Oxley on IT and Corporate Governance,* Whitepaper 2005, www.serena.com

[5] *Sarbanes-Oxley and IT Management* de Marvin Waschke, Whitepaper Computer Associates, 2004

[6] *ISO/IEC 17799 Code of Practice for Information Security Management*, Primera Edición 2000 www.isostandards.com

[7] *IT Governance Regulation – A Latin American Perspective* de Leonidas Anzola, Information Systems Control Journal, Volume 2, pp. 21, 2005.

[8] *Enterprise Governance and the Role of IT,* de Stacey Hamaker, Information Systems Control Journal, Volume 6, pp 27, 2005.

[9] *Board Briefing on IT Governance Second Edition,* pp 10-11, 2003.

[10] *IT and Enterprise Governance,* de Michael J.A. Parkinson y Nicolas J. Baker, Information Systems Control Journal, Volume 3, pp 17, 2005.

[11] *Una propuesta para mejorar las prácticas de Gobierno Corporativo en el Perú,* de Alejandro Indacochea, CENTRUM, Pontificia Universidad Católica Del Perú., http://centrum.pucp.edu.pe/docentes/AIndacochea_Libros/documentos_publicados/Gobierno_Corporativo.pdf.

[12] *Board Briefing on IT Governance Second Edition,* pp 12, 2003 http://www.itgi.org/template_ITGI.cfm?Section=Recent_Publications&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=10617

[13] *IT Governance Executive Summary,* Whitepaper IT Governance Institute, 2004 http://www.itgi.org/template_ITGI.cfm?Section=Recent_Publications&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=10617

[14] *Board Briefing on IT Governance Second Edition,* pp 20-21, 2003 http://www.itgi.org/template_ITGI.cfm?Section=Recent_Publications&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=10617

[15] *Information Security Harmonisation - Clasification of Global Guidance*-IT Governance Institute ISBN 1-933284-05-6 2005

[16] *BS7799-ISO 17799 Security Standards for a better Information Security Management*
http://www.bs7799-iso17799.com/whatis7799.html

[17] *BS7799-ISO 17799 Security Standards for a better Information Security Management*
http://www.bs7799-iso17799.com/whobs-7799.html

[18] *Leveraging ISO 17799 to Achieve Security Management Best Practices* de Evan Tegethoff
http://www.forsythe.com/Forsythe/itriskman/security/security_leveragingiso.jsp

[19] *Cobit Control Objectives 3erd Edition,* ISACA 2000
http://www.isaca.org/Template.cfm?Section=Downloads5&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742#COBIT

[20] *AS/NZS 4360:2004 Estándar Australiano para Administración de Riesgos* pp 9 2004
http://www.standards.com.au/shop/Script/Details.asp?DocN=AS564557616854

[21] *Glosario de Términos Técnicos*-Bradesco, pp1
http://200.189.182.180/uploads/conteudo/4105/11_Glossario.pdf

[22] *AS/NZS 4360:2004 Estándar Australiano para Administración de Riesgos* pp 5 2004
http://www.standards.com.au/shop/Script/Details.asp?DocN=AS564557616854

[23] *Superintendencia de Banca, Seguros y AFP*
http://www.sbs.gob.pe/PortalSBS/Normatividad/CompendioNormas.asp?s=1

[24] *AS/NZS 4360:2004 Estándar Australiano para Administración de Riesgos* pp 17 2004
http://www.standards.com.au/shop/Script/Details.asp?DocN=AS564557616854