GUÍA METODOLÓGICA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD EN INSTITUCIONES

Karina Miranda-Vásquez

Piura, agosto de 2013

Facultad de Ingeniería

Maestría en Dirección Estratégica en Tecnologías de la Información

Miranda, K. (2013). *Guía metodológica para implementar un sistema de gestión de seguridad en instituciones* (Tesis de máster en Dirección Estratégica de Tecnologías de la Información). Universidad de Piura. Facultad de Ingeniería. Piura, Perú.

UNIVERSIDAD DE PIURA

FACULTAD DE INGENIERIA

"Guía metodológica para implementar un sistema de gestión de seguridad en instituciones"

Tesis para optar el Grado de Máster en

Dirección Estratégica en Tecnologías de la Información

Karina Elena Miranda Vásquez

Asesor: Omar Hurtado Jara

Piura, Agosto 2013

- ✓ A Dios por haberme dado la vida para lograr mis objetivos, a mi amor y a mi familia por su apoyo permanente.

Prólogo

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La información es el principal activo de muchas organizaciones y precisa ser protegida adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio. En la actualidad, las empresas de cualquier tipo o sector de actividad se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de contingencias, las cuales pueden dañar considerablemente tanto los sistemas de información como la información procesada y almacenada.

Ante estas circunstancias, las organizaciones han de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, primando la protección de la información.

Para proteger la información de una manera coherente y eficaz es necesario implementar un Sistema de Gestión de Seguridad de la Información y TI (SGS). Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos del negocio, que permite asegurar la información frente a la pérdida de:
• Confidencialidad: sólo accederá a la información quien se encuentre autorizado.
• Integridad: la información será exacta y completa.
• Disponibilidad: los usuarios autorizados tendrán acceso a la información cuando lo requieran.

La seguridad total es inalcanzable, pero mediante el proceso de mejora continua del sistema de seguridad se puede conseguir un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran.

El establecimiento de una guía metodológica de gestión de la seguridad de la información clara y bien estructurada apoyará a las empresas que con sus propios recursos puedan desarrollar actividades como la planificación, diseño, operación y retroalimentación (mejora continua) de la seguridad, utilizando estándares internacionales como la Norma ISO 27002 e ITIL.

El objetivo de esta guía es desarrollar pautas básicas con algunos ejemplos para la implementación de un Sistema de gestión de Seguridad de la Información y TI (SGS) en organizaciones.

El presente trabajo lo he venido aplicando en las diferentes consultorías de seguridad de la información tanto en empresas del sector privadas de telecomunicaciones y sector público, lográndose en una de ellas la certificación ISO 27001.

Esta guía va dirigida a quienes requieran iniciar una gestión de seguridad en sus organizaciones, así como aquellos que requieran complementar y/o mejorar sus sistemas de gestión de seguridad de la información y TI (SGS) ya implementados.

Resumen

Existen estándares internacionales de seguridad dispuesto para su ejecución, pero muchas organizaciones fracasan en el intento de aplicarlo con rigurosidad, debido a que su personal de seguridad no interpreta adecuadamente las normas o tiene insuficiente conocimiento o falta de experiencia.

El uso de estándares no únicamente es tratar de cumplir con todo lo que se indica, sino necesariamente aplicar aquello que sea gestionado por la organización.

Se presenta una guía metodológica para la implementación de un sistema de gestión de seguridad basado en estándares internacionales referente a la gestión de seguridad y tecnologías de la información. En la cual se dan las pautas claves para la planificación, diseño, operación y retroalimentación de un sistema de gestión de seguridad.

Finalmente se presentan los factores críticos de éxito y conclusiones de esta guía metodológica que está orientada a instituciones sea privada o estatal y sirva en gran medida en la aplicación de controles de seguridad.

INDICE

Introducción

En el presente proyecto se pretende dar a las instituciones un enfoque sencillo y didáctico, basado en el conocimiento adquirido para implementar un sistema de gestión de seguridad, tomando como base estándares internacionales.

El primer capítulo proporciona los lineamientos básicos de la seguridad de la información, así como una descripción de cada norma y/o estándar donde esté relacionado los temas de seguridad de la información. Aquí mencionamos la importancia del porque implementar un sistema de gestión de seguridad, que es un gobierno de las tecnologías de información, que es el estándar ISO 27002 y una breve explicación de los dominios que comprende, que es ITIL y finalmente mencionamos otros estándares relacionados a la gestión de seguridad.

En el segundo capítulo, se presenta una breve descripción de las amenazas y vulnerabilidades que aquejan y/o puedan estar comprometidas las personas, familias, empresas y gobiernos debido a que de alguna forma utilizan medios para comunicarse a través del uso de las tecnologías de la información, sistemas de información, redes como por ejemplo: internet, teléfonos celulares, programas, correo electrónico, etc. Ello los expone y se ve necesario que se conozcan las diversas amenazas que existen y así prepararnos a fin de prevenir en caso de alguna vulnerabilidad. Mencionamos por ejemplo la brecha digital, amenazas cibernéticas, amenazas de interoperabilidad, amenazas humanas, infraestructura crítica, así como delitos informáticos, en éste último vemos las referencias a las leyes a nivel de Perú.

En el tercer capítulo se presenta el desarrollo de una guía metodológica para implementar un sistema de gestión de seguridad en cuatro fases: planificación, diseño, operación y retroalimentación. En cada una de las actividades que se desarrollan, especificamos los siguientes elementos: la entrada, desarrollo de la acción(es), quienes deberían participar y el elemento de salida. Se indican algunos ejemplos a fin de que se pueda comprender su desarrollo.

Finalmente se mencionan los principales factores críticos de éxito a tener en cuenta, así como las conclusiones y recomendaciones en base al desarrollo de este proyecto.

Capítulo 1:
Marco Teórico y Estado del Arte

1.1 Guía Metodológica

Es una herramienta metodológica que permite ordenar información o darle a los contenidos diferentes tratamientos para posibilitar el aprendizaje, presentados de manera clara, sintética, esquemática y práctica, a la vez que permitan dar una idea general de las diferentes fases o procesos que se llevan cabo para realizar un tema o actividad determinada.

La Guía Metodológica está integrada por actividades que entrelazan contenidos conceptuales para la autoformación presentados en el folleto de apoyo y procedimientos para la realización de actividades vivenciales y participativas, como sugerencias, para ser desarrolladas en procesos.

1.1.1 Componentes de la guía

En la primera parte se incluye una breve presentación incluyendo la introducción y los objetivos perseguidos por la guía, además del marco conceptual, el cual constituye un apoyo para refrescar los contenidos básicos - sirve también como material de consulta para las empresas que no cuentan con conocimientos anteriores sobre el tema.

En la segunda parte se hace una breve conceptualización de cada fase, la cual contiene aspectos temáticos metodológicos que se permitan adecuar a las necesidades de la población objetivo.

Cada fase se orienta a determinar los pasos a seguir para la realización de actividades en forma esquemática, lo cual presentan de manera resumida los contenidos, en un sentido teórico práctico.

Finalmente la presente guía contiene sugerencias o planteamientos necesarios para desarrollar la actividad y se deja propuesto un espacio para la participación y la puesta en marcha de la guía. A modo personal se puede dejar plasmado un glosario que recoja palabras claves utilizadas en los contenidos del tema.

1.2 ¿Qué es un Sistema de Gestión?

Un sistema de gestión de la seguridad es un enfoque gerencial para la seguridad.
Se trata de un sistemático, explícito y amplio proceso de gestión de riesgos sobre la seguridad.

Como con todos los sistemas de gestión, en un sistema de gestión de la seguridad se prevé la fijación de objetivos, planificación y medición del desempeño. Un sistema de gestión de la seguridad es parte de una organización. Se convierte en parte de la cultura, y de la forma en que realizamos un trabajo.

¿Por qué implementar un Sistema de Gestión de la Seguridad?

- Porque ayuda a una organización a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa.
- Por desestimar riesgos.
- Por la falta de contramedidas.
- Por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno.
- Por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información.
- Por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, entre otros.

Un Sistema de Gestión de la Seguridad de la Información implica que la organización ha estudiado los riesgos a los que está sometida toda su información, ha evaluado que nivel de riesgo asume, ha implementado controles (no sólo tecnológicos, sino también organizativos y legales) para aquellos riesgos que superan dicho nivel, ha documentado las políticas y procedimientos relacionados y ha entrado en un proceso continuo de revisión y mejora de todo el sistema.

1.3 Gobierno de las Tecnologías de Información

En el pasado considerar la función de TI (Tecnologías de Información) de una organización como una función meramente de soporte era una práctica común. Actualmente, la mayor parte de la inversión en infraestructura y nuevas aplicaciones de TI abarcan líneas y funciones de negocio, incluso algunas organizaciones llegan integrar a socios y clientes dentro de sus procesos internos.
Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de las tecnologías de información (TI) que la soportan, esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las “ciber-amenazas” y la guerra de la información.
- El coste de las inversiones actuales y futuras en información y en tecnología de información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa; así hay muchas organizaciones que reconocen los beneficios potenciales que la tecnología puede proporcionar, comprenden y administran los riesgos asociados con la implementación de nuevas tecnologías.

El principal objetivo de Gobierno TI es entender las cuestiones y la importancia estratégica TI para permitir a la organización que mantenga sus operaciones e implemente las estrategias necesarias para sus proyectos y actividades futuras.

El Gobierno TI provee las estructuras que unen los procesos TI, los recursos de TI y la información con las estrategias y los objetivos de la empresa. Además, el Gobierno TI integra buenas prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoriza el rendimiento de TI para asegurar que la información en la empresa y las tecnologías relacionadas soportan sus objetivos de negocio.

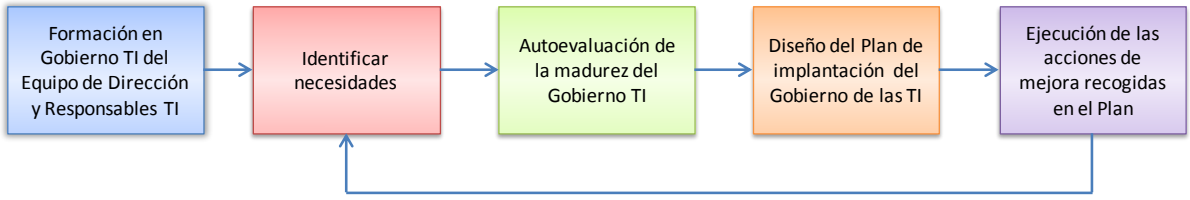
Cada implementación de gobierno TI se lleva a cabo en diferentes condiciones y circunstancias (entorno de Gobierno TI) determinados por factores tales como:

- Cultura de la organización
- Leyes y regulaciones vigentes tanto internas como externas
- Misión, visión y valores de la organización
- Roles y responsabilidades
- Intenciones estratégicas y tácticas de la organización

El proceso de implantación de gobierno TI asiste a los diferentes niveles de la organización con una detallada hoja de ruta que le ayuda en la implementación de sus necesidades de Gobierno TI.

La mencionada hoja de ruta es un primer paso para implantar los requerimientos de gobierno TI, los cuales se muestran en la Figura 1.1.

Figura 1.1. Fases del proceso de implantación de gobierno TI[1]



1.3.1 Identificar necesidades

Los siguientes cuatro pasos son necesarios en la fase inicial de un proyecto de implantación de Gobierno TI:

a) Entender el entorno en que se va a desarrollar el proceso de implantación de gobierno de TI y establecer un proyecto adecuado.
b) Entender los objetivos de negocio y cómo trasladarlos a objetivos de TI

[1] Fuente: Elaboración propia

c) Entender los riesgos potenciales y la forma en la que estos puedan afectar a los objetivos de TI
d) Definir el alcance del proyecto y qué procesos deben ser implantados o mejorados.

1.3.2 Autoevaluación

Esta fase revisa el estado de madurez actual de los procesos de TI seleccionados y el estado de madurez objetivo en el que se desea que estén tras implantar la solución. En análisis de brecha entre la situación actual y la situación deseada, se convierte en oportunidades de mejora.

1.3.3 Diseño del Plan

En esta fase se identifican iniciativas de mejora factibles y las traslada a proyectos justificados. Tras su aprobación, dichos proyectos deben ser integrados en la estrategia de mejora con un plan detallado para alcanzar la solución.

1.3.4 Ejecución de las acciones

Conforme los proyectos van avanzando, el resultado del mismo debe ser monitorizado y dichos resultados deben servir para tomar decisiones acerca de las siguientes iteraciones sobre cada uno de los procesos que se han implantado.

1.4 Norma ISO/IEC 27001[2]

1.4.1 Historia

ISO (International Organization for Standardization) es una federación internacional con sede en Ginebra (Suiza), la cual desarrolla estándares requeridos por el mercado que representen un consenso de sus miembros acerca de productos, tecnologías, métodos de gestión, entre otros. Estos estándares por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de la ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

A continuación se menciona en orden cronológico el origen:

- 1990 – El Departamento de comercio e industria del Reino Unido apoyó su desarrollo
- 1995 – Por primera vez se adopta como norma inglesa (BSI)
- 1998 – Se lanzan los requisitos para su certificación
- 1999 – Se emite una segunda edición de la norma
- 2000 – Fue aprobada como la parte 1 de ISO17799
- 2002 – BS7799-2 se publicó el 5 de septiembre: en esta revisión se adoptó el "modelo de proceso" con el fin de alinearla con ISO9001 e ISO14001
- 2004 – A finales del 2004, cerca de 950 compañías se habían certificado en BS 7799-2

[2] Norma Técnica Peruana NTP-ISO/IEC 27001:2008, accesible en http://www.ongei.gob.pe/banco/ongei_normas_detalle.asp?pk_id_normas=220

- 2005 – Se publica ISO/IEC17799:2005 en Junio y la ISO27001:2005 en Octubre.
- 2007 – Se publica ISO27002:2005 (se renombra ISO/IEC17799:2005)
- 2007 – Se publica ISO27006:2007, requisitos para organismos certificadores

1.4.2 La Serie ISO 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. A continuación se presenta algunas de ellas[3]

- ISO27000 – Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del ciclo Plan-Do-Check-Act y **términos y definiciones** que se emplean en toda la serie 27000.
- ISO27001 – Es la norma principal de la serie y contiene los **requisitos** del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada), **es certificable**. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados
- ISO27002 – Es una **guía de buenas prácticas** que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005
- ISO27003 – No certificable. Es una **guía** que se centra en los aspectos críticos necesarios **para el diseño e implementación** con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI
- ISO27004 – No certificable. Es una guía para el desarrollo y utilización de **métricas y técnicas de medida** aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001
- ISO27005 – No certificable. Proporciona **directrices para la gestión del riesgo** en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO27006 – Requisitos para los organismos que certifican y registran un SGSI (ISO27001).
- ISO27007 – No certificable. Guía de Auditoría para un SGSI, como complemento a lo especificado en ISO 19011
- ISO27008 – No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI

[3] Una lista más completa se puede obtener accediendo a http://www.iso27001security.com/index.html

1.4.3 Estructura

La Norma ISO/IEC 27001:2005 se compone de la siguiente estructura:

0. Introducción
1. Alcance
2. Normas de referencia
3. Términos y definiciones
4. Sistema de Gestión de Seguridad de la Información
5. Responsabilidad de la Dirección
6. Auditorías Internas del SGSI
7. Revisión Gerencial del SGSI
8. Mejora del SGSI

Anexo A. Objetivos de Control y Controles

11 Cláusulas, 39 objetivos de control y 133 controles

Anexo B. Principios de la OCDE y este estándar internacional

Anexo C. Correspondencia entre ISO9001:2000, ISO14001:2004 y este estándar internacional

Por otra parte en nuestro país, por Resolución Ministerial Nº 129-2012-PCM publicada el día 25 de Mayo del 2012[4], en el Diario Oficial el Peruano, se aprobó el uso obligatorio de la Norma Técnica "NTP-ISO/IEC 27001: 2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática. Siendo opcional la certificación en ISO/IEC 27001:2005.

La NTP 27001 se encuentra publicada en internet[5], Esta norma técnica peruana de seguridad de la información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de la Seguridad de la Información (SGSI).

1.5 Norma ISO 27002

Es un conjunto de recomendaciones sobre qué medidas tomar en la organización para asegurar los sistemas de información.

Los objetivos de seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva se aplican para la gestión del riesgo analizado.

Es una herramienta esencial para organizaciones de cualquier tipo o tamaño, es una norma flexible y genérica.

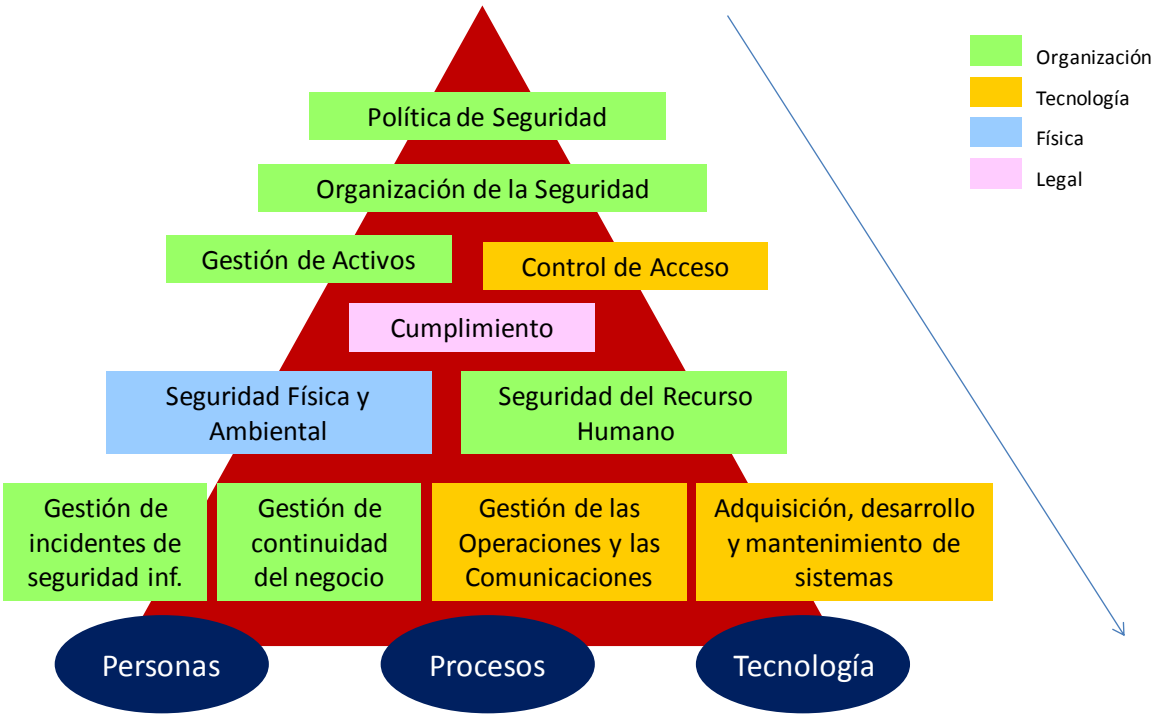
---

[4] Se accede desde http://www.ongei.gob.pe/banco/ongei_normas_detalle.asp?pk_id_normas=220

[5] Se accede desde el portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI): http://bvirtual.indecopi.gob.pe/normas/isoiec27001.pdf

Posee 11 **dominios**, los cuales se derivan en 39 **objetivos de control** (resultados que se esperan alcanzar mediante la implementación de controles) y 133 **controles** (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). Véase figura 1.2.

Figura 1.2. Dominios de Control de la Norma ISO/IEC 27002



La Norma contiene explicaciones exhaustivas de cómo se puede implantar cada uno de los controles, pero hay que tener en cuenta que no es una norma preceptiva sino informativa, por lo que la información que da puede y debe ser adaptada a las necesidades y situación específica de la organización. Debe evitarse caer en el error de tratar de seguir al pie de la letra las indicaciones que se dan, ya que pueden ser excesivamente complejas e innecesarias para muchas organizaciones.

A continuación se comentan los detalles de cada dominio de control:

1.5.1 Política de Seguridad

Su objetivo es dirigir y dar soporte a la gestión de la seguridad de la información. La Alta Dirección debe definir una **política** que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicarla de forma adecuada a todo el personal. Está compuesto por los siguientes controles (2):

- Documento de Política de Seguridad de la Información.
- Revisión de la Política de Seguridad de la Información.

1.5.2 Organización de la Seguridad

Gestionan la seguridad de la información dentro de la organización. Mantienen la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros. Mantienen la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización. Está compuesto por los siguientes objetivos de control (2) y controles (11):

- Organización Interna
  - Comisión de gestión para la Seguridad de la Información.
  - Coordinación de la Seguridad de la Información.
  - Asignación de responsabilidades sobre Seguridad de la Información.
  - Proceso de autorización de recursos para el tratamiento de la información.
  - Acuerdos de confidencialidad.
  - Contactos con autoridades.
  - Contactos con grupos de interés.
  - Revisión Independiente de la Seguridad de la Información.

- Partes externas
  - Identificación de riesgos relacionados con terceros.
  - Seguridad en las relaciones con clientes.
  - Seguridad en contratos con terceras partes.

1.5.3 Gestión de Activos

Mantener una protección adecuada sobre los activos de la organización. Asegurar un nivel de protección adecuado a los activos de información. Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización. Está compuesto por los siguientes objetivos de control (2) y controles (5):

- Responsabilidad de los activos
  - Inventario de activos.
  - Propiedad de los activos.
  - Uso aceptable de activos de información

- Clasificación de la información
  - Guías de clasificación.
  - Marcado y tratamiento de la información.

1.5.4 Recursos Humanos

Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurar que los usuarios sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Las implicaciones del factor humano en la seguridad de la información son muy elevadas. Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad como las implicaciones de su trabajo en el

mantenimiento de la seguridad global. Está compuesto por los siguientes objetivos de control (3) y controles (9):

- Antes de la Contratación
  - Perfiles y responsabilidad
  - Revisión y verificación
  - Términos y condiciones de la relación laboral

- Durante la Contratación
  - Gestión de responsabilidades
  - Educación y capacitación en seguridad de la información
  - Procesos disciplinarios

- A la finalización del Contrato
  - Responsabilidades en la finalización
  - Devolución de activos
  - Retirada de los derechos de acceso

1.5.5 Seguridad Física

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización. Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.
Las áreas de trabajo de la organización y sus activos deben ser clasificados y protegidos en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...). Está compuesto por los siguientes objetivos de control (2) y controles (13):

- Áreas Seguras
  - Perímetro de seguridad física
  - Controles físicos de accesos
  - Seguridad de oficinas, despachos y recursos
  - Protección ante amenazas externas y de entorno
  - El trabajo en las áreas de seguridad
  - Acceso y salida pública y zonas de carga y descarga

- Seguridad de los equipos
  - Localización y protección del Equipamiento
  - Suministros
  - Seguridad del cableado
  - Mantenimiento de equipos
  - Seguridad de equipos fuera de los locales de la Organización
  - Seguridad en la reutilización o eliminación de equipos
  - Salida de propiedades

1.5.6 Gestión de Comunicaciones y Operaciones

Asegurar la operación correcta y segura de los recursos de tratamiento de información.
Minimizar el riesgo de fallos en los sistemas. Proteger la integridad del software y de la información. Mantener la integridad y la disponibilidad de los servicios de tratamiento de

información y comunicación. Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo. Evitar daños a los activos e interrupciones de actividades de la organización. Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones. Está compuesto por los siguientes objetivos de control (10) y controles (32):

- Procedimientos y responsabilidades
  - Documentación de procedimientos operativos
  - Gestión de cambios
  - Segregación de tareas
  - Separación de entornos de desarrollo, pruebas y operación

- Gestión de la externalización
  - Prestación de servicios
  - Monitorización y revisión de servicios de terceras partes
  - Gestión de cambios

- Planificación y aceptación
  - Planificación de capacidades
  - Aceptación de Sistemas

- Control contra código malicioso y código móvil
  - Control contra código malicioso
  - Control contra código móvil

- Copias de seguridad
  - Copia de la información

- Gestión de la seguridad de red
  - Controles de redes
  - Seguridad en servicios de red

- Gestión de soportes
  - Gestión de soportes removibles
  - Eliminación de soportes
  - Procedimientos de utilización de la información
  - Seguridad de la documentación de sistemas

- Intercambio de información
  - Políticas y procedimientos para intercambio de información
  - Acuerdos para intercambio
  - Seguridad de soportes en tránsito
  - Seguridad de la mensajería electrónica
  - Sistemas de información de negocio

- Servicios de comercio electrónico
  - Comercio electrónico
  - Transacciones online

- Información de difusión pública

➢ Monitorización
- Registros de auditoría
- Revisión de uso de sistemas
- Protección de logs
- Logs de administradores y operadores
- Logs de fallo del sistema
- Sincronización de relojes

1.5.7 Control de Acceso

Controlar los accesos a la información, evitar accesos no autorizados a los sistemas de información, evitar el acceso de usuarios no autorizados, proteger los servicios en red. Evitar accesos no autorizados a ordenadores, el acceso no autorizado a la información contenida en los sistemas. Detectar actividades no autorizadas. Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y tele-trabajo. Está compuesto por los siguientes objetivos de control (7) y controles (25):

➢ Requerimientos del negocio para el control de accesos
- Política de control de accesos

➢ Gestión de accesos de usuario
- Registro de usuarios
- Gestión de privilegios
- Gestión de contraseñas de usuario
- Revisión de los derechos de acceso de los usuarios

➢ Responsabilidades de los usuarios
- Uso de contraseñas
- Equipamiento informático de usuario desatendido
- Política de pantallas y mesas limpias

➢ Control de accesos en red
- Política de uso de los servicios de red
- Autenticación para conexiones externas
- Identificación de equipos en la red
- Protección a puertos de diagnóstico remoto y configuración
- Segregación en las redes
- Control de conexión a las redes
- Control de enrutamiento en red

➢ Control de accesos al sistema operativo
- Procedimientos de log-on seguro
- Identificación y autenticación de los usuarios
- Sistema de gestión de contraseñas
- Utilización de utilidades del sistema
- Desconexión automática de sesiones
- Limitación del tiempo de conexión

- Control de acceso a la información y aplicaciones
  - Restricción de acceso a la información
  - Aislamiento de sistemas sensibles

- Portátiles y teletrabajo
  - Informática móvil y comunicaciones
  - Teletrabajo

1.5.8 Compras, Desarrollo y Mantenimiento de Sistemas

Asegurar que la seguridad está incluida dentro de los sistemas de información.
Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
Proteger la confidencialidad, autenticidad e integridad de la información. Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevados a cabo de una forma segura. Mantener la seguridad del software y la información de la aplicación del sistema. Está compuesto por los siguientes objetivos de control (6) y controles (16):

- Requerimientos de seguridad de los sistemas
  - Análisis y especificación de los requerimientos de seguridad

- Procesamiento correcto de aplicaciones
  - Validación de los datos de entrada
  - Control de proceso interno
  - Integridad de mensajes
  - Validación de los datos de salida

- Controles criptográficos
  - Política de uso de los controles criptográficos
  - Gestión de claves

- Seguridad de los ficheros del sistema
  - Control del software en explotación
  - Protección de los datos de prueba del sistema
  - Control de acceso al código fuente

- Seguridad en los procesos de desarrollo y soporte
  - Procedimientos de cambios operacionales
  - Revisión técnica de aplicaciones tras cambios del sistema operativo
  - Restricción de cambios a paquetes de software
  - Fugas de información
  - Desarrollo externalizado

- Gestión de vulnerabilidades
  - Control de vulnerabilidades técnicas

1.5.9 Gestión de Incidentes de Seguridad

Que los incidentes y/o eventos de seguridad de la información, sean comunicados oportunamente y que asimismo se tomen las acciones necesarias para que los mismos no vuelvan a ocurrir. Está compuesto por los siguientes objetivos de control (2) y controles (5):

- Comunicación de eventos y debilidades de seguridad
  - Notificación de eventos de seguridad
  - Notificación de debilidades

- Gestión de incidentes y mejora de seguridad
  - Responsabilidad y procedimientos
  - Aprendiendo de los incidentes
  - Recolección de evidencias

1.5.10 Gestión de la Continuidad de Negocio

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres. Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.

Los planes de contingencia deben ser probados y revisados periódicamente.

Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre. Está compuesto por los siguientes objetivos de control (1) y controles (5):

- Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
  - Inclusión de seguridad en el proceso de gestión de continuidad de negocio
  - Continuidad del negocio y análisis de riesgos
  - Redacción e implantación de planes de continuidad incluida la seguridad de la información
  - Marco de planificación de la continuidad del negocio
  - Prueba, mantenimiento y reevaluación de los planes de continuidad

1.5.11 Conformidad Legal

Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma. Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas. Está compuesto por los siguientes objetivos de control (3) y controles (10):

- Cumplimiento de los requerimientos de seguridad
  - Identificación de la legislación aplicable
  - Derechos de propiedad intelectual
  - Salvaguarda de los registros de la organización
  - Protección de datos de carácter personal y de la intimidad de las personas
  - Evitar el mal uso de los recursos de tratamiento de información
  - Reglamentación de los controles de cifrado

- Conformidad con políticas, estándares y cumplimiento técnico
  - Conformidad con políticas y normas de seguridad
  - Comprobación de la conformidad técnica

- Consideraciones sobre la auditoria de sistemas de información
  - Controles de auditoría de sistemas de información
  - Protección de las herramientas de auditoría de sistemas de información

1.6 Estándar ITIL

Las prácticas comerciales prudentes exigen que los procesos de TI y las iniciativas se alineen con los procesos de negocio y objetivos. Esto es crítico cuando se trata de seguridad de la información, que debe estar estrechamente alineado con la seguridad del negocio y sus necesidades. Todas las organizaciones TI de proveedor de servicios deben asegurarse de que tienen una política de seguridad y los controles de seguridad necesarios para vigilar y hacer cumplir las políticas.
La política de seguridad debe analizar cada aspecto de la estrategia, con su correspondiente gestión de control y riesgos. Además, la parte de gestión debe incluir las normas, procedimientos y directrices como apoyo a las políticas de seguridad de la información. A nivel global, debe adoptar una seguridad eficaz basada en la estructura de la organización y vinculada a los objetivos, estrategias y planes de negocio. Y por último, es necesaria una formación basada en la estrategia y el plan de seguridad.
La política debe cubrir todas las áreas de seguridad y debe incluir:

- El uso de los activos de la política de TI
- Una política de control de acceso
- Una política de control de contraseña
- Una política de e-mail
- Una política de Internet
- Una política de lucha contra virus
- Una política de clasificación de la información
- Una política de clasificación de documentos
- Una política de acceso remoto
- Una política en materia de acceso proveedor de servicios de TI, la información y los componentes.

El cumplimiento de esta política debe ser contemplado en todos los acuerdos SLR, SLAs y contratos.

Las siglas de ITIL se corresponden a “Information Technology Infrastructure Library”, que se traduce como la Biblioteca de la Infraestructura de las Tecnologías de la Información.
A pesar de no poder considerar a ITIL como el modelo de referencia perfecto para la Gestión de Servicios TI, sí podemos decir que es el modelo de facto en estos momentos a nivel mundial y que ha sido adoptado como base de gestión por grandes compañías.
Fue desarrollado en los años 80 por el Reino Unido dentro del ministerio llamado OGC (Office of Government Commerce)

Figura 1.3. Modelo ITIL v3[6]

1.6.1 Estructura de ITIL

Inicialmente ITIL v1 era un conjunto de 40 libros, que en la versión v2 publicada en el año 2000 se agruparon en 9 publicaciones. Cada una de estas publicaciones describe un conjunto principal de procesos de Gestión de Servicios TI. Las dos publicaciones centrales son la de Soporte del Servicio y la de Entrega del Servicio.

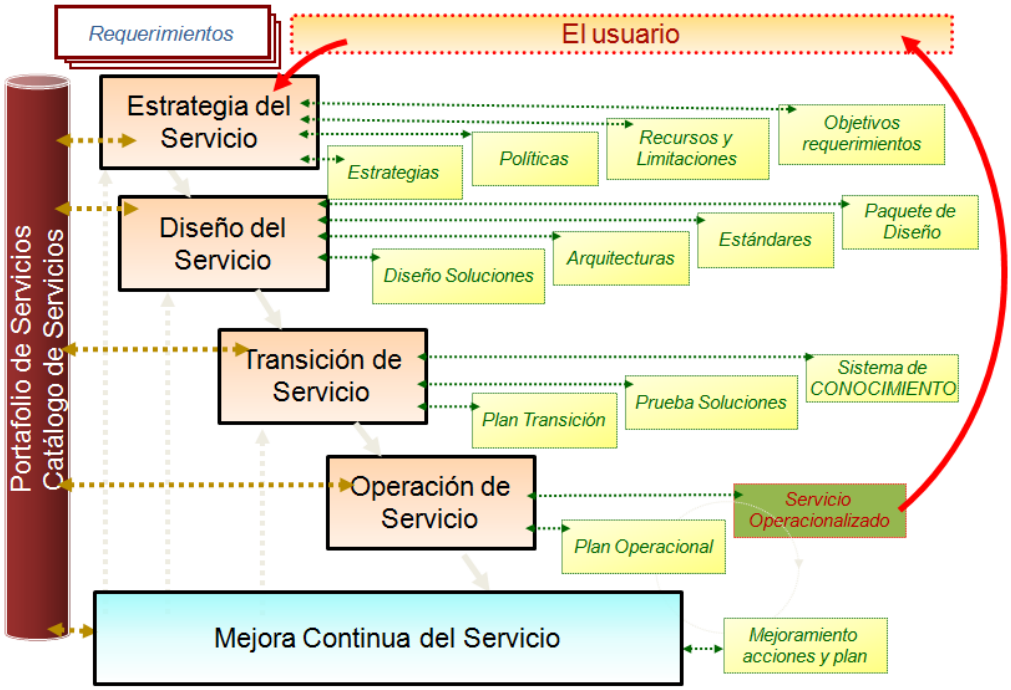
La última versión de ITIL ® (v3) consiste en un sistema sobre la base de 5 publicaciones que substituyen la versión previa del de ITIL v2 (publicado en 2000). Las publicaciones básicas proporcionan la dirección necesaria para un acercamiento integrado según los requisitos de la especificación estándar de ISO/IEC 20000.

ITIL V3 enfoca la Gestión de Servicios desde el Ciclo de Vida de un Servicio. El Ciclo de Vida de un Servicio es un modelo de organización con una visión en:

- Todas las fases del Ciclo de Vida están relacionadas con el valor de los servicios de TI.
- La forma en que la gestión de servicios es estructurada.
- La forma en que varios componentes están enlazados unos con otros.
- El impacto que un cambio puede tener en un componente, en otro componente del sistema o en el sistema entero.

[6] Wellington Redwood, Quint. (2009). Fundamentos ITIL v3 Foundation

Figura 1.4. Ciclo de Vida del Servicio ITIL v3, desde la solicitud de un servicio hasta su entrega[7]



Consiste en 5 fases que se detallan a continuación:

A. *Estrategia del Servicio:*
Se enfoca en el estudio de mercado y posibilidades mediante la búsqueda de servicios innovadores que satisfagan al cliente tomando en cuenta la real factibilidad de su puesta en marcha. Así mismo, se analizan posibles mejoras para servicios ya existentes. Se verifican los contratos en base a las nuevas ofertas de proveedores antiguos y posibles nuevos proveedores, lo que incluye la renovación o revocación de los contratos vigentes.

- Gestión del Portafolio de Servicios
- Gestión Financiera
- Gestión de la Demanda, modelos de la actividad del negocio

B. *Diseño del Servicio:*
Una vez identificado un posible servicio el siguiente paso consiste en analizar su viabilidad. Para ello, se toman factores tales como infraestructura disponible, capacitación del personal y se planifican aspectos como seguridad y prevención ante desastres. Para la puesta en marcha se toman en consideración la reasignación de cargos (contratación, despidos, ascensos, jubilaciones, etc.), la infraestructura y software a implementar.

- Gestión Catálogo de Servicio
- Gestión de Niveles de Servicio
- Gestión de la Capacidad

[7] Fuente: Elaboración propia

- Gestión de la Disponibilidad
- Gestión de la Continuidad de Servicio
- Gestión de la Seguridad de la Información
- Gestión de Proveedores

C. *Transición del Servicio:*

Antes de poner en marcha el servicio se deben realizar pruebas. Para ello se analiza la información disponible acerca del nivel real de capacitación de los usuarios, estado de la infraestructura, recursos IT disponibles, entre otros. Luego se prepara un escenario para realizar pruebas, se replican las bases de datos, se preparan planes de reversión (rollback) y se realizan las pruebas. Luego, de ello se limpia el escenario hasta el punto de partida y se analizan los resultados, de los cuales dependerá la implementación del servicio. En la evaluación se comparan las expectativas con los resultados reales.

- Planeación de Soporte de Transición
- Gestión de Cambios
- Gestión de Activos y Configuración
- Gestión de Liberación y Despliegue
- Validación y Pruebas de Servicio
- Evaluación
- Gestión del Conocimiento

D. *Operación del Servicio:*

En este punto se monitoriza activa y pasivamente el funcionamiento del servicio, se registran eventos, incidencias, problemas, peticiones y accesos al servicio.

- Gestión de Incidentes
- Gestión de Eventos
- Gestión de Cumplimiento de Requerimientos
- Gestión de Problemas
- Gestión de Accesos

E. *Mejora Continua del Servicio:*

Se utilizan herramientas de medición y retroalimentación para documentar la información referente al funcionamiento del servicio, los resultados obtenidos, problemas ocasionados, soluciones implementadas, etc. Para ello, se debe verificar el nivel de conocimiento de los usuarios respecto al nuevo servicio, fomentar el registro e investigación referentes al servicio y disponer de la información al resto de los usuarios.

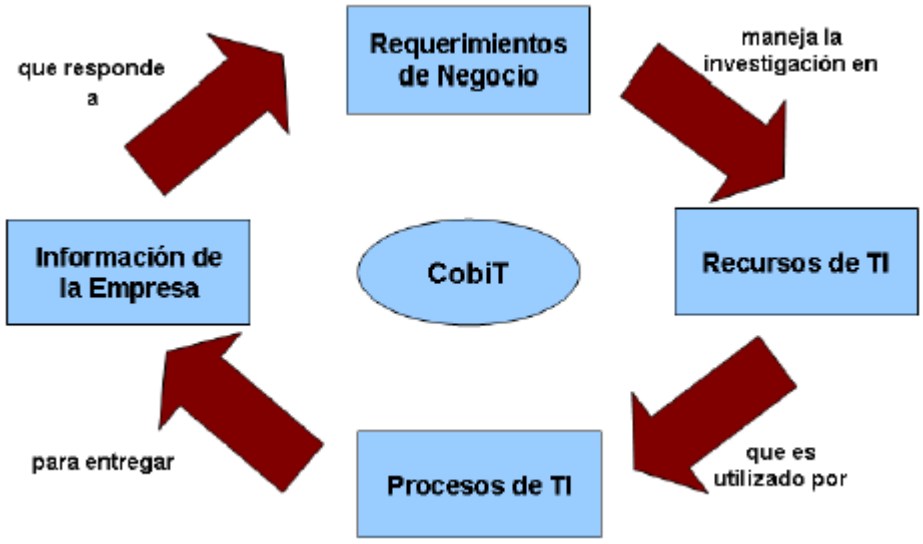
- Definir qué se debe mejorar.
- Definir qué se puede mejorar
- Procesar los datos e información
- Analizar los datos
- Definir acciones
- Implementar acciones

1.7 Otros estándares relacionados a la Gestión de Seguridad

1.7.1 COBIT

Es una herramienta para la administración de las tecnologías de información. Fue desarrollada por ISACA (Information Systems Audit and Control Association) como un estándar para la seguridad de la tecnología de información y buenas prácticas de control.
Se trata de un marco compatible con ISO 27002 (anterior ISO 17799:2005) y COSO, que incorpora aspectos fundamentales de otros estándares relacionados; por tanto, aquellas empresas y organizaciones que hayan evolucionado según las prácticas señaladas por CobiT están más cerca de adaptarse y lograr la certificación en ISO 27001.
CobiT se estructura en cuatro partes; la principal de ellas se divide de acuerdo con 34 procesos de TI. Cada proceso se cubre en cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso. Utiliza un ciclo de vida de tipo PDCA (Plan-Do-Check-Act) que lo integra en 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. El marco de trabajo de COBIT se basa en el siguiente principio (Figura 1.5)[8]

Figura 1.5. Principio Básico de COBIT



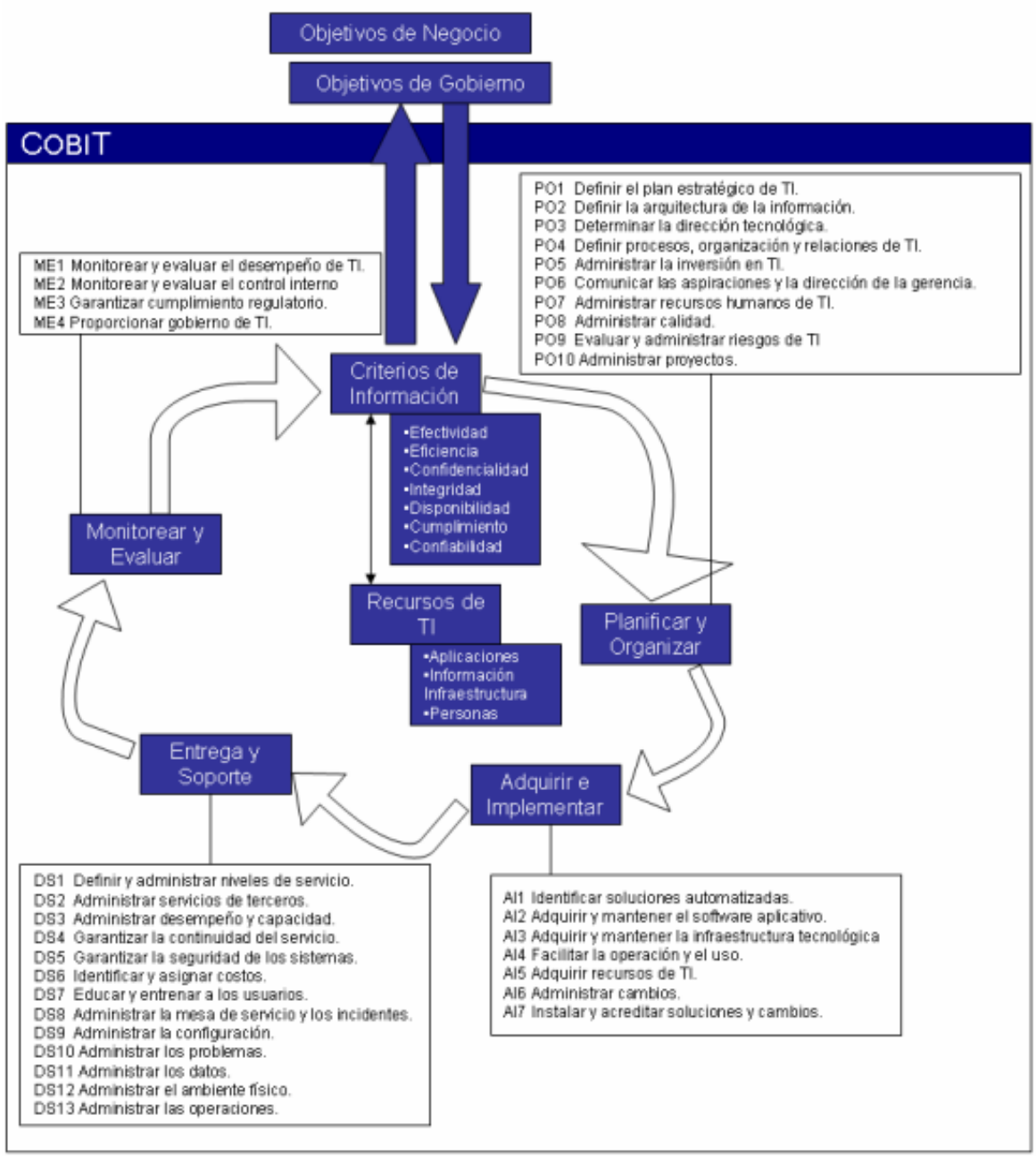
[8] De acuerdo a IT Governance Institute, Cobit 4.1, para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesitará invertir en, administrar y controlar los recursos de TI usando un conjunto estructurado de procesos.

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (*Stakeholders*). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma de políticas claras y buenas prácticas para la seguridad y control de la tecnología de información para organizaciones comerciales, gubernamentales, y financieras entre otras.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI

Figura 1.6. Marco de Trabajo de COBIT [9]



[9] La figura 1.6 resume cómo los distintos elementos del marco de trabajo de COBIT se relacionan con las áreas de enfoque del gobierno de TI

1.7.2 Magerit

El análisis de riesgos propuesto por MAGERIT es una aproximación metódica que permite determinar el riesgo siguiendo unos pasos:

- Determinar los activos relevantes para la Organización
- Determinar a qué amenazas están expuestos aquellos activos
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Valorar dichos activos en función del coste que supondría para la Organización recuperarse ante un problema de disponibilidad, integridad, confidencialidad o autenticidad
- Valorar las amenazas potenciales.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

El método propuesto por MAGERIT da cumplimiento en lo establecido en la ISO 13335, en el epígrafe 4.2.1.d Identificar Riesgos, 4.2.1.e Analizar y evaluar riesgos de la ISO /IEC 27001:2005.

1.7.3 Estándar RFC2196

RCF2196 (*Site Security Handbook*) es una guía para el desarrollo de políticas y procedimientos de seguridad informática para los sitios que disponen de sistemas en internet. [10]

Entre las características de la seguridad informática, según el RFC2196, se tienen las siguientes: se debe poder poner en práctica mediante procedimientos descritos de administración de sistemas, publicación de guías sobre el uso aceptable de los recursos informáticos o por medio de otros métodos prácticos apropiados; debe poder implantarse; debe obligar al cumplimiento de las acciones relacionadas mediante herramientas de seguridad; tiene que detectar fugas o errores; debe definir claramente las áreas de responsabilidad de los usuarios, administradores y dirección, y tener un responsable para toda situación posible.

Por otro lado, el RFC-2196 establece una serie de componentes incluidos en las políticas de seguridad. Éstos son:

- Guías de compras de tecnología de la información. Especifica funciones de seguridad requeridas o preferidas. Estas políticas deben complementar cualquier otra política de compra de la organización.
- Política de privacidad. Determina las expectativas razonables de privacidad sobre temas relacionados con monitoreo de correos electrónicos, acceso a archivos y registro de teclados. Podría incluir también políticas acerca de registro, escucha y control de llamadas telefónicas, control de accesos a sitios web, uso de herramientas de mensajería instantánea, etc.
- Política de acceso. Define derechos o privilegios de acceso a activos o recursos de información protegidos. Especifica comportamientos aceptables para usuarios, empleados soporte y directivos. Debe incluir reglas respecto a las conexiones y accesos externos, así como reglas acerca de la comunicación de datos, conexiones de

[10] http://en.wikipedia.org/wiki/Site_Security_Handbook

dispositivos a las redes e inclusión de nuevas aplicaciones informáticas en los sistemas existentes.

- Política de responsabilidad. Define las responsabilidades de usuarios, personal de mantenimiento y directivos. Debe especificar la capacidad de realizar auditorías y sus características, y proveer las guías para el registro y manejo de incidentes de seguridad.
- Política de autenticación. Debe establecer los mecanismos de "confianza" mediante el uso de una política de contraseñas apropiadas. Debe considerar, si aplica, políticas de autenticación local y de acceso remoto.
- Declaración de disponibilidad. Determina las expectativas de disponibilidad de los recursos de los sistemas e información. Con base en la disponibilidad necesaria, podrán establecerse mecanismos de redundancia y procedimientos de recuperación.
- Política de mantenimiento de los sistemas relacionados con la tecnología de la información. Describe cómo deberá hacerse el mantenimiento realizado tanto por personal interno como externo a la organización. Debe establecerse si se admite o no algún tipo de mantenimiento remoto (por ejemplo, por internet o por módem), y las reglas que aplican, así como los mecanismos internos de control.
- Política de informes de incidentes o violaciones de seguridad. Establece qué tipo de incidentes o violaciones de seguridad deben reportarse y a quién reportar. Para no generar un ambiente "amenazante", puede considerarse la inclusión de reportes anónimos, lo que seguramente redundará en una mayor probabilidad de que los incidentes sean efectivamente reportados.
- Información de apoyo. Proveer a los usuarios, empleados y directivos con información de contacto y de referencia para usarla ante incidentes de seguridad. En todos los casos, los aspectos legales deben tomarse en cuenta.

Conclusiones:

En este capítulo iniciamos con una breve explicación de los conceptos generales que sirven de base para un mejor entendimiento del presente trabajo.

Asimismo se realiza una presentación de los diferentes estándares internacionales y buenas prácticas que emplean actualmente muchas organizaciones a nivel internacional del tipo públicas o privadas referidas a la seguridad de la información en su aplicación de salvaguardas para proteger su información.

El uso de uno o la combinación de estándares dependerá mucho de la misión y visión de la organización respecto al grado de madurez que requiera alcanzar en seguridad de la información y gestión de las tecnologías de la información (TIC's).

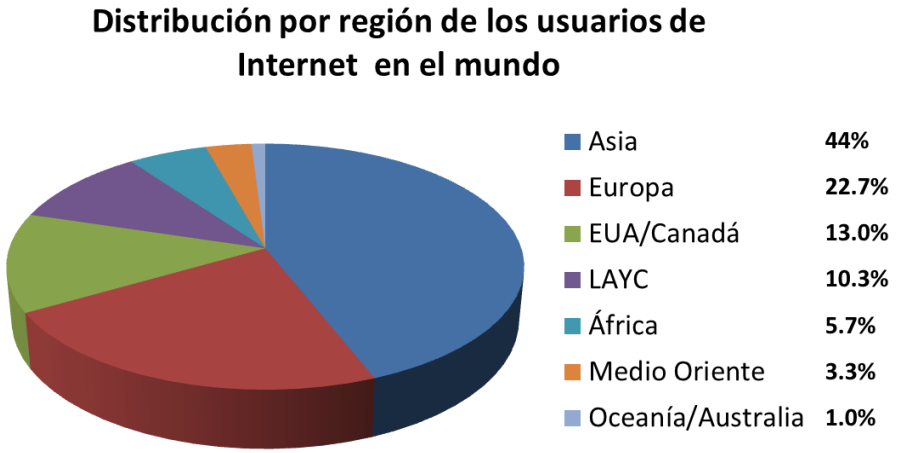
Capítulo 2:
Análisis de Amenazas y Vulnerabilidades

2.1 Brecha Digital

La brecha digital es un fenómeno que puede definirse como "la separación que existe entre las personas (comunidades, estados y países) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas".

La Brecha Digital no sólo se aplica a las condiciones de un país, sino también se aplica a comunidades, inclusive a nivel individual. El término separación o brecha se refiere al nivel de acceso que se tiene a las TIC. Las TIC pueden entenderse como todas aquellas tecnologías de redes, telecomunicaciones e informática (teléfono, televisión, radio, Internet, computadoras, etc.) que de manera directa o indirecta, influyen en nuestro de nivel de vida y educación.

Figura 2.1. La brecha digital en Latinoamérica [11]



[11] Estadística obtenida de http://www.labrechadigital.org/labrecha/, publicado el 10 de febrero del 2012.

En los años noventa nació la expresión “brecha digital” para describir a los ricos y pobres de la tecnología, e inspiró algunas iniciativas para poner en manos de todos los estadounidenses, en especial las familias con ingresos bajos, las últimas herramientas informáticas. Esos esfuerzos han acortado la brecha, pero han generado un efecto secundario tales como amenazas o riesgos en el uso de las TIC’S, que preocupa a investigadores y políticos y que los Gobiernos ahora pretenden resolver.

La brecha digital tiene múltiples aristas y miradas. Como bien señala el programador Hernán Beati en el artículo que escribió[12] , “coexisten varias brechas en paralelo que, en conjunto, indican cercanía o alejamiento a las tecnologías de la información y comunicación”.

Si uno circunscribe el tema a América Latina, las múltiples aristas se tiñen del color de cada país. Si bien en cada lugar la brecha digital es diferente y tiene características propias, notaremos algunos puntos en común, entre ellos, las oportunidades que brinda el acceso a Internet desde teléfonos móviles.

Con la propagación del acceso a dispositivos, los niños de las familias pobres pasan bastante más tiempo que los pertenecientes a familias acomodadas utilizando televisores y artilugios para ver series y vídeos, y para jugar y conectarse a las redes sociales, según demuestran varios estudios, los cuales generan un potencial acortamiento de la brecha.

Este aumento en la diferencia del uso del tiempo, según políticos e investigadores, es más un reflejo de la capacidad de los padres para controlar el empleo que hacen los niños de la tecnología que del acceso a la misma.

La alfabetización digital es muy importante, y esto significa proporcionar a los padres y los estudiantes las herramientas y los conocimientos necesarios para utilizar la tecnología con fines educativos y profesionales.

Pese al potencial educativo de los ordenadores, lo cierto es que su uso para la creación de contenidos educativos o relevantes es minúsculo en comparación con su aplicación al puro entretenimiento, lo cual en lugar de cerrar la brecha de los logros, están ampliando las diferencias en la pérdida de tiempo.

Según el Foro Económico Mundial (FEM) en su informe sobre las tecnologías de la información y la comunicación (TIC), incluye cada año un ranking sobre la utilización de las TIC para potenciar el crecimiento económico y la competitividad en un total de 142 países desarrollados y en vías de desarrollo, que en 2012 lideran principalmente los países nórdicos.

En concreto, Suecia se hace con el primer puesto de esa lista gracias a que su rendimiento es “excepcional en todos los aspectos”, tanto en términos de utilización a nivel personal y empresarial de las TIC como de contenidos digitales o infraestructura.
En el segundo puesto se sitúa Singapur, que capitanea el grupo de los “tigres asiáticos” gracias al favorable entorno político y regulatorio en esa ciudad-Estado, mientras que los

[12] Obtenido del artículo “Brecha Digital: La herida que sigue abierta” en http://www.labrechadigital.org/labrecha/ , publicado el 29 de diciembre del 2011

diez primeros puestos de la lista los completan Finlandia, Dinamarca, Suiza, Países Bajos, Noruega, Estados Unidos, Canadá y Reino Unido. Ninguno de los países de América Latina y el Caribe que se incluyen en la lista logran situarse en los 30 primeros puestos [13], lo que se debe principalmente a la falta de infraestructuras y acceso a banda ancha o la escasez de capacitación de una buena parte de la población para hacer uso de las TIC.

2.2 Amenazas Cibernéticas

Cada día que pasa cada uno de nosotros y los gobiernos dependen aún más de las redes, sistemas de información y tecnologías relacionadas e integradas en el ciberespacio. Individuos, familias, empresas y gobiernos utilizan la red global de internet, computadoras, programas, teléfonos celulares, correos electrónicos; una infraestructura física y virtual para la información y las comunicaciones, critica tanto para la seguridad nacional, regional e individual, como para la seguridad económica, calidad de vida y prosperidad de nuestra gente.

Es que la libre circulación de la información y comunicación y su correspondiente privacidad son esenciales para el funcionamiento y objetivos de dichas redes y la innovación necesaria para el crecimiento económico y el desarrollo social en una economía globalizada.

Los incidentes cibernéticos pueden tener infinidad de formas y acarrear las más serias consecuencias. Gobiernos y estados pueden ser virtualmente paralizados. Compañías y negocios; en suma los niveles de empleo y la prosperidad económica de un país pueden verse afectados por el robo de información confidencial y propiedad intelectual. Individuos pueden sufrir estafas, el robo de su información personal, médica u otra, o convertirse en victimas de infinidad de delitos contra la persona y su propiedad.

Terroristas, delincuentes y organizaciones criminales explotan tanto las vulnerabilidades como las ventajas de las tecnologías de la información y las comunicaciones para llevar a cabo actividades ilegales que varían significativamente de país a país, e incluso entre regiones dentro de un mismo Estado: el tráfico de drogas y armas ilícitas; la trata de personas; el contrabando; el secuestro; el uso de la red de internet con fines terroristas, la incitación al terrorismo; la extorsión; los delitos contra la propiedad; la corrupción y el lavado de activos relacionado con estas y otras formas de crimen organizado nacional e internacional.

Nuestra capacidad de respuesta ante estas amenazas todavía presenta debilidades, para ello, necesitamos incrementar la concientización sobre la importancia de la ciber seguridad en todos los niveles, pero particularmente en el nivel de la toma de decisiones políticas, a fin de promover la adopción de prácticas y estrategias nacionales de seguridad cibernética, que

[13] Según artículo “Alertan por la persistente brecha digital” publicado el 05/04/2012 en http://noticias.universia.net.mx/ciencia-nn-tt/noticia/2012/04/05/921925/alertan-persistente-brecha-digital.pdf

permitan promover de manera efectiva y acertada la implementación de las medidas necesarias para el mejor y honesto uso y aprovechamiento de las tecnologías de la información y la comunicación.

Asimismo necesitamos profundizar la capacitación de personal altamente calificado, requerido para responder adecuadamente a esas amenazas -de naturaleza multidimensional- a las redes y sistema críticos de información, para poder prevenir y responder a incidentes de seguridad cibernética, así como para poder detectar, investigar y someter a la justicia a los responsables de esos delitos.

Para combatir a una red se necesita una red. Por lo tanto, para combatir tanto a las amenazas de la ciberseguridad, terrorismo, así como a las redes del crimen organizado transnacional, se necesitarán redes transnacionales de actores públicos y privados dispuestos y preparados para cooperar a fin de prevenir la acción criminal y hacer respetar las leyes.

La OEA, a través de la Secretaria del Comité Interamericano contra el Terrorismo (CICTE), ha venido trabajando en este tema y tiene entre sus objetivos, apoyar a los Estados Miembros que todavía no han instalado sus Centros Nacionales de Respuesta a Incidentes de Informática (CSIRTs); para mejorar las capacidades técnicas del personal en CSIRTs nacionales ya establecidos; promover el desarrollo de marcos o estrategias nacionales de ciberseguridad; aumentar y consolidar la cooperación regional e internacional existentes, así como con el sector privado, en temas relacionados con la seguridad cibernética y especialmente con la protección de la infraestructura de información crítica.

2.3 Amenazas Humanas

Suele decirse que todos tenemos un precio (dinero, chantaje, factores psicológicos, etc.), por lo que nos pueden arrastrar a robar y vender información o simplemente proporcionar acceso a terceros.los ataques pueden ser del tipo pasivos o activos, y el personal realiza ambos indistintamente dependiendo de la situación concreta.
Menciono aquellos potenciales atacantes a un sistema dentro de una organización:

a) Personal Interno:
   Personal que trabaja en una organización y que hace uso de sus privilegios para actuar en forma mal intencionada o no.

b) Ex-Empleado:
   Este grupo puede estar especialmente interesado en violar la seguridad de la empresa, sobre todo aquellos que fueron despedidos y quedaron inconformes.

c) Curiosos:
   Suelen ser los atacantes más actuales de un sistema. Son aquellos que no tienen conocimiento ni experiencia.

d) Terroristas:
   Es cualquier persona que ataca el sistema para causar daño.

e) Intrusos Remunerados
   Este es sin duda, el grupo de atacantes más peligroso. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" (códigos fuente de programas, bases de datos de clientes, diseño de un nuevo producto, etc.), o simplemente para dañar de alguna manera la imagen de una organización.

Algunas medidas recomendadas[14] que se mencionan son:

- Una norma básica: cuando una persona postule a un trabajo, se deben revisar las referencias, identidad y diplomas.
- Acuerdos de no divulgación: todo empleado con una posición que involucre confidencialidad debe firmar un acuerdo de no divulgación.
- Acceso: cada usuario debe tener el mínimo de privilegio para realizar su trabajo.
- Concientización de seguridad: el empleado debe asistir a un curso de sensibilización cuando ingresa a trabajar. Este curso puede ser parte de la introducción y formación interna. Otros medios son: volantes, folletos, mensajes en la pantalla, boletines, videos, entre otros.
- Separación de funciones: es necesario que definan y separen correctamente las funciones de cada persona
- Cancelación inmediata de cuenta: cuando un empleado abandona la organización se debe cancelarse inmediatamente el acceso a sus antiguos recursos.

Existen otras amenazas comunes que desde mi punto de vista están relacionados a la persona como son: errores y omisiones, fraude y robo, hackers maliciosos (hackers, crackers y phreakers), código malicioso (virus, gusanos, troyanos, bomba lógica), ataques de denegación de servicio e ingeniería social.

2.4 Amenazas de interoperabilidad

Aplicado para Gobierno Electrónico en línea o llamado también Gobierno-e con el propósito de satisfacer de mejor manera las necesidades y expectativas del ciudadano, donde los sistemas de información deben inter-operar con otros sistemas de información, utilizando estándares técnicos comunes, para alcanzar los objetivos de Gobierno en línea, en lugar de enfocarse en las opciones técnicas que tienen poco impacto en la entrega del servicio.

Las amenazas están asociadas a la información intercambiada lo cual debe estar protegido, evitando el uso no autorizado de la misma y garantizando su integridad, confidencialidad, disponibilidad y resguardo.

Los trámites y servicios que se presten a través de los sistemas de información deberán proteger la seguridad del aislamiento y de la información de los ciudadanos, los negocios, la comunidad y otras organizaciones. Los consumidores deben poder proporcionar la

[14] Según sección 9 llamado "organizational measures" del libro The Basics of Information Security – A Practical Handbook

información a los servicios de la entidad con la certeza que la información será utilizada de acuerdo con la legislación existente.

Una de las medidas de seguridad es que la información que transita en redes IPv4 inseguras, incluyendo aquellas sin claves deben adoptar los controles de seguridad disponibles en el protocolo IP v4. Los sistemas de información del gobierno deben ser protegidos contra riesgos de seguridad en la conexión con esas redes.

La información que transita en redes de LAN sin cable se recomienda usar los protocolos de seguridad específicos de esta tecnología, cuando sea necesario. Los sistemas de información del gobierno deben ser protegidos contra riesgos de seguridad en la conexión con esas redes.

Los sistemas deben poseer registros históricos (*logs*) para permitir auditorias y exámenes forenses, siendo imprescindible la adopción de un sistema de sincronismo de tiempo centralizado. Asimismo, se requiere utilizar mecanismos que garanticen la autenticidad de los registros almacenados, de ser posible con firma digital.

La documentación de los sistemas, de los controles de seguridad y de las topologías de los ambientes debe estar actualizada y protegida.

2.5 Infraestructura crítica

Las Infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas. Por tanto cada vez más su adecuada protección no sólo se hace necesaria, sino obligatoria a raíz de la publicación de numerosos marcos regulatorios y directivas internacionales a lo largo de todo el planeta.

Analizar y comprender el riesgo asociado a estas infraestructuras y su relación básica con los Sistemas de Control Industrial es necesario para cualquier profesional de la seguridad involucrado o relacionado con áreas como las TIC, energía, industria química y nuclear, sistemas financieros y tributarios, alimentación o transporte, entre otros.

La protección de las infraestructuras críticas es una preocupación para los gobiernos de todo el mundo. El alto nivel de desarrollo de las sociedades descansa en su mayor parte en una serie de servicios básicos y esenciales cuya prestación radica mayoritariamente en el sector privado. Garantizar la seguridad de los suministros de estos servicios básicos ante nuevas amenazas es una responsabilidad no sólo de las administraciones públicas sino que es necesaria la concienciación y colaboración de los organismos privados.

Los estados modernos se enfrentan actualmente a multitud de desafíos que afectan a su seguridad nacional. Estos nuevos riesgos, que provienen muchos de ellos de la globalización, como el terrorismo internacional, la proliferación de armas de destrucción

masiva, el cambio climático o el crimen organizado, se suman a los ya existentes, como el terrorismo tradicional.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, expuestas a una serie de amenazas, para cuya protección se hace imprescindible, por un lado, catalogarlas y, por otro, diseñar un plan con medidas eficaces de prevención y protección contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y de las comunicaciones.

Para ello, la protección de las infraestructuras críticas (PIC) necesita un enfoque integral y dinámico acorde con el entorno cambiante, que asegure la continuidad y recuperación de los servicios esenciales que prestan a la sociedad. Desde el apoyo, implicación y liderazgo del alto nivel gubernamental, los mecanismos de seguridad y defensa de las infraestructuras críticas deber ser plasmados correctamente en todos los escalafones necesarios para la protección, que deberá reforzar la seguridad del día a día prestando especial atención a los aspectos de seguridad tecnológica.

Por ejemplo en el Catálogo de Infraestructuras Críticas de España, comprende como áreas estratégicas principales a la: energía, suministro de agua, salud, sistema financiero y tributario, alimentación, administración (servicios públicos básicos, redes de información, monumentos nacionales), infraestructura del transporte, entre otros.[15]

Se mencionan a continuación algunas líneas de trabajo para el corto y mediano plazo en PIC:

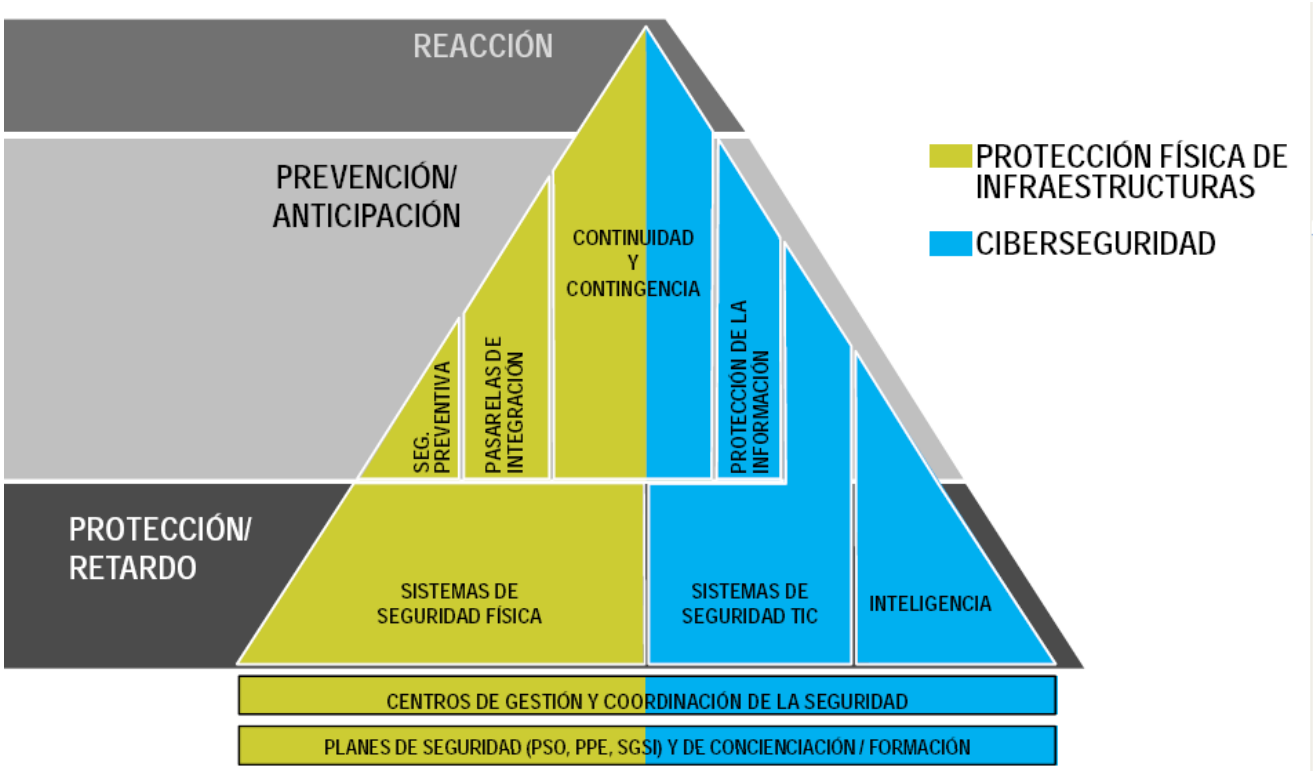
a) Consolidar una Estrategia Nacional con los objetivos principales de: Establecer una línea de defensa contra todas las amenazas actuales con el fin de mejorar el intercambio de información de alertas, vulnerabilidades, amenazas y eventos que se detecten en las redes de la Administración que permitan actuar rápidamente; defenderse contra todo el espectro de amenazas, mejorando las capacidades de contrainteligencia e incrementar la seguridad de las tecnologías y sistemas.
b) Todas y cada una de las Infraestructuras Críticas, requieren el estudio e implantación de medios y medidas con un enfoque holístico de Seguridad integral e integrada que reúna y coordine las diferentes implicaciones y medidas nacionales e internacionales puesto que, en definitiva hemos de pensar en global, aunque actuemos en local puesto que la inseguridad realmente si está globalizada
c) Promover la participación activa del sector público y privado
d) Impulsar los cambios orgánicos necesarios al máximo nivel del Estado para garantizar la gestión correcta de los nuevos paradigmas de la seguridad y la defensa
e) Garantizar la adaptabilidad de la protección a nuevas situaciones que sean radicalmente opuestas a las conocidas, permitiendo la resiliencia de las infraestructuras críticas.
f) Abordar la protección de infraestructuras críticas desde el punto de vista lógico con una gestión integrada

[15] Extraído de la Conferencia expuesta por Manuel Sánchez Gómez-Merelo, celebrado en Madrid el 22/05/2012 en el tema “Protección de Infraestructuras Críticas, un nuevo reto para la Seguridad”. Se encuentra disponible en http://manuelsanchez.com

g) Mejorar la seguridad lógica de las infraestructuras críticas haciendo especial hincapié en la protección adecuada de los sistemas de control.

En este sentido, es ahora el momento de que las empresas de servicios, instalaciones y proveedores de seguridad privada se pongan en disposición especial para la participación en todo el proceso de este Programa de Protección de las Infraestructuras Críticas dados los medios, conocimiento y experiencia que en esta materia irreversiblemente tiene.

Figura 2.2. Tecnologías para la protección de Infraestructuras Críticas [16]



a) Seguridad Preventiva, que incluye:
- Sistemas de detección de intrusión (CCTV, radar y sensores especiales)
- Sensores mallados enterrados
- Video inteligente y representación 3D
- Protección Contra Incendios
- Sistemas de inhibición

b) Pasarelas para intercambio de información y coordinación con:
- Organismos del Estado
- FF y CC de Seguridad
- Otros propietarios de IC

[16] Modelo expuesto por el Director de Protección de Infraestructuras Críticas, Antonio González Gorostiza de la empresa INDRA - España.

c) Sistemas de Seguridad Física, que incluye:
   - Seguridad del perímetro
   - Control de accesos y presencia
   - Identificación y biometría
   - Sistemas avanzados de comunicación para vigilantes y agentes
   - Escáneres directos y retrodispersión
   - Detectores de explosivos y radioactividad

d) Continuidad y Contingencia, que incluye:
   - Análisis de Riesgos
   - Elaboración de BIA (*Business Impact Analysis*)
   - Planes y equipos de respuesta a incidentes

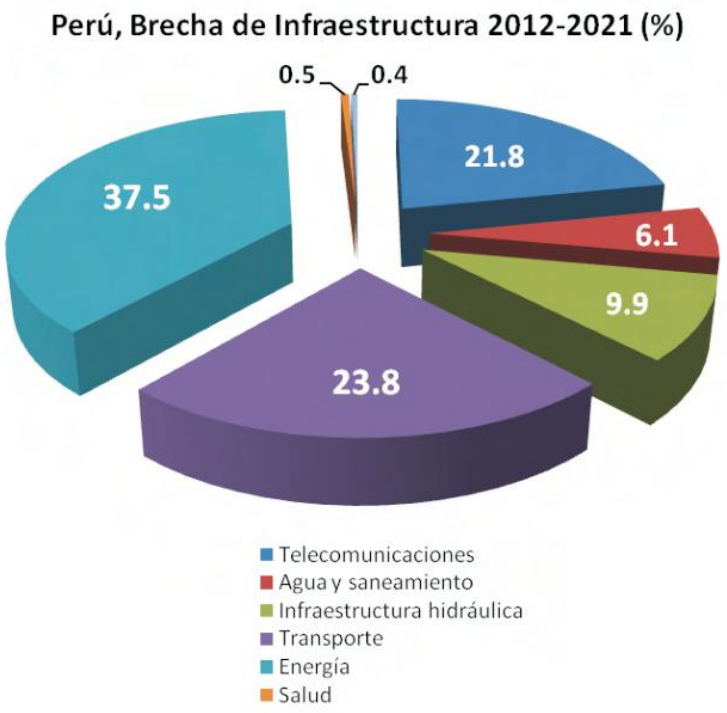
e) Protección de Información, que incluye:
   - Cifrado de datos
   - Cifrado de comunicaciones

f) Sistemas de Seguridad TIC, que incluye:
   - SOC, CERT y oficinas de seguridad
   - PKI y Gestión de Identidades
   - Gestión de logs y eventos

g) Inteligencia, que incluye:
   - Inteligencia competitiva
   - Análisis de fraude y filtraciones
   - Vigilancia tecnológica
   - Soporte a la decisión

En Perú, existe el Plan Nacional de Infraestructura 2012-2021 de la Asociación para el Fomento de la Infraestructura Nacional (AFIN), elaborado por ESAN, las mayores brechas estarían en energía, transporte y comunicaciones. Véase figura 2.3.

Figura 2.3. Brecha de Infraestructura de Servicios Públicos proyectada para el periodo 2012-2021 [17]



Cerrarlas requeriría de un esfuerzo conjunto entre el sector público y el privado, donde el efecto multiplicador del primero dependerá no tanto de la ejecución vía inversión pública, sino de su capacidad de tercerizar al sector privado la ejecución de proyectos. Al Estado también le toca facilitarle la vida al sector privado, reduciendo la burocracia y logrando una mayor celeridad en los trámites para licencias y permisos. Recordemos que la calidad de la infraestructura es un condicionante importante de la competitividad de un país.

2.6 Delitos Informáticos

El fenómeno informático es una realidad incuestionable e irreversible; definitivamente, la informática se ha instalado entre nosotros para no marcharse jamás. Ello es consecuencia del continuo y progresivo desarrollo del campo de la informática aplicada en la actualidad a todos los aspectos de la vida cotidiana; así, por ejemplo, la utilización de computadoras en la industria, el comercio, la administración pública, en instituciones bancarias y financieras.

Esta verdadera invasión de la computadora en todos los ámbitos de las relaciones socioeconómicas ha motivado que muchos hablen ya de una auténtica "era informática". En efecto, pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por la computadora, ya sea de manera directa o indirecta; incluso, en determinados casos, las computadoras no sólo son utilizadas como medios de archivo y procesamiento de

[17] Fuente: AFIN - Plan Nacional de Infraestructura 2012-2021 (Elaborado por Universidad ESAN y Universidad del Pacífico). Disponible en http://www.afin.org.pe

información, sino que, además, se les concede la capacidad de adoptar automáticamente decisiones

No existe un concepto unánimemente aceptado de lo que sea el delito informático debido a que la delincuencia informática comprende una serie de comportamientos difícilmente deducibles o agrupables en una sola definición.
De manera general, se puede definir el delito informático como aquél en el que, para su comisión, se emplea un sistema automático de procesamiento de datos o de transmisión de datos

Dentro de las manipulaciones informáticas se distingue:

a) La fase input o entrada de datos en la cual se introducen datos falsos o se modifican los reales añadiendo otros, o bien se omiten o suprimen datos.
b) Las manipulaciones en el programa que contiene las órdenes precisas para el tratamiento informático.
c) La fase output o salida de datos, donde no se afecta el tratamiento informático, sino la salida de los datos procesados al exterior, cuando van a ser visualizados en la pantalla, se van a imprimir o registrar.
d) Las manipulaciones a distancia, en las cuales se opera desde una computadora fuera de las instalaciones informáticas afectadas, a las que se accede tecleando el código secreto de acceso, con la ayuda de líneas telefónicas.

Existen muchos tipos de delitos informáticos, que viene dado por la conjugación de factores tales como: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas. Algunas de las modalidades conocidas son:

- Ataques con virus informáticos a las propias tecnologías de la información y las comunicaciones, como los servidores y los sitios Web, de alcance mundial que causan considerables perjuicios a las redes comerciales y de consumidores.
- El vandalismo electrónico y la falsificación profesional.
- El robo o fraude, por ejemplo, ataques de piratería contra bancos o sistemas financieros y
- fraude mediante transferencias electrónicas de fondos.
- Las computadoras se utilizan para facilitar una amplia variedad de ventas telefónicas e inversiones fraudulentas mediante prácticas engañosas.
- La “pesca” (phishing) o la inundación de mensajes supuestamente de origen conocido (spam spoofing) es la construcción de mensajes de correo electrónico con páginas Web correspondientes diseñadas para aparecer como sitios de consumidores existentes. Se distribuyen millones de estos mensajes fraudulentos de correo electrónico, que se anuncian como provenientes de bancos, subastas en línea u otros sitios legítimos para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas.
- La difusión de material ilícito y nocivo. Durante los últimos años, la Internet ha sido utilizada para fines comerciales por la “industria del entretenimiento para adultos” legítima. Sin embargo, la Internet se utiliza ahora cada vez más para distribuir material considerado legalmente obsceno en varios países. Otro motivo de preocupación es la pornografía infantil. Desde fines de los años 80, ha venido aumentando su distribución a través de una variedad de redes informáticas, utilizando una variedad de servicios de

Internet, incluidos los sitios Web. Una cierta proporción de la distribución de pornografía infantil se ha vinculado a la delincuencia organizada transnacional.

- Además de la utilización de la Internet para difundir propaganda y materiales que fomentan el odio y la xenofobia, hay indicios de que la Internet se ha utilizado para facilitar la financiación del terrorismo y la distribución de propaganda terrorista.

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.
Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable, tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Los delitos informáticos han sido recientemente regulados en nuestra legislación peruana, mediante la Ley Nº 27309, publicada en el Diario Oficial "El Peruano" el 17/07/2000, con la cual se incorpora al Título V del Libro Segundo del Código punitivo nacional, un nuevo capítulo (Capítulo X) que comprende tres artículos 2O7°-A (Intrusismo informático), 207°-B (Sabotaje informático) y 207º-C (formas agravadas), lo que emerge como un intento de actualizar nuestra legislación interna en relación a los nuevos avances de la tecnología, y sobre todo teniendo en cuenta que estamos dentro de una era informática, la cual no se puede evitar, en sus efectos y consecuencias.

En Perú, La División de Investigación de Delitos de Alta Tecnología (DIVINDAT), es el órgano de ejecución de la Dirección de Investigación Criminal que tiene como misión, investigar, denunciar y combatir el crimen organizado transnacional (Globalizado) y otros hechos trascendentes a nivel nacional en el campo de los Delitos Contra la Libertad, Contra el Patrimonio, Seguridad Pública, Tranquilidad Pública, Contra la Defensa y Seguridad Nacional, Contra la Propiedad Industrial y otros, cometidos mediante el uso de la tecnología de la información y comunicación, aprehendiendo los indicios, evidencias y pruebas, identificando, ubicando y deteniendo a los autores con la finalidad de ponerlos a disposición de la autoridad competente.

A continuación se mencionan los dispositivos legales sobre delitos informáticos:

- LEY 27309 que incorpora al Código Penal del Perú los Delitos Informáticos (Promulgada el 15 de Julio del año 2000)
- Ley N° 27269 Ley de Firmas y Certificados Digitales del Perú
- LEY Nº 27310 - Modifica el artículo 11° de la ley N° 27269
- LEY Nº 28493 - Ley que regula el uso del correo electrónico no solicitado (SPAM)
- LEY Nº 27291 - Modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica
- LEY Nº 27419 - Ley sobre notificación por correo electrónico
- LEY Nº 26612 - Mediante el cual se regula el uso de tecnologías avanzadas en materia de archivo de documentos e información.

Conclusiones:

En este capítulo tratamos una serie de amenazas y vulnerabilidades donde Estados, organizaciones y personas nos podemos ver afectados. Si bien es cierto el auge de las tecnologías de la información es beneficioso para algunos, pero no para otros quienes con mala intención lo utilizan para cometer delitos y hacer daño.

Se realiza un análisis de amenazas sobre la brecha digital, infraestructura crítica, diversas amenazas cibernéticas, delitos informáticos, entre otros.

Para ello, hago una comparación de cómo se encuentra la situación a nivel internacional y cómo nos encontramos en nuestro país, respecto al tratamiento de esta serie de amenazas. Asimismo se presenta pautas para poder combatirlas.

Existen países e instituciones que se encuentran trabajando en ello, cabe mencionar que gran parte de compromiso por mejorar en nuestro país recae en nuestro gobierno y del trabajo en conjunto con instituciones privadas y organismos internacionales; que para ello se requerirá inversión económica y planes de trabajo estratégicos.

Finalmente, este capítulo nos apoyará haber identificado de forma general amenazas y vulnerabilidades a las que está expuesta nuestra organización y de estar forma estar concientizados y decididos en aplicar un sistema de gestión de seguridad.

Capítulo 3:
Metodología para la implementación de un sistema de gestión de seguridad

3.1 Definición de la estrategia metodológica

En este capítulo se plantean interrogantes, aspectos de enfoque, así como lineamientos estratégicos a seguir para implementar un Sistema de Gestión de Seguridad de la Información y TI (SGS).

La Gestión de la Seguridad, como casi cualquier proceso de gestión, tiene tres pilares que deben tenerse en cuenta dado que interactúan mutuamente: Personas, Procesos y Tecnología.
Por lo tanto, un SGS deberá considerar el contexto de la industria, que además debe ser sostenible en el tiempo, con capacidad de incorporar mejoras de forma incremental y continua, con un beneficio comprobable para la organización.
Para ello se requiere de una metodología bien definida, que acompañe el dinamismo necesario de la organización y de la industria, y a su vez respete las estrategias empresariales y su vinculación estructural.

Previo a escoger la metodología a seguir, debemos tener presente el enfoque a aplicar y su dimensión. Por ejemplo no es lo mismo aplicar un SGS en una organización que pertenece a un grupo empresarial en donde es necesario coordinar y armonizar todos sus componentes para lograr efectividad en los objetivos de Seguridad, así como también eficiencia en el uso de los recursos, de tal forma que se adecúe tanto a una estrategia local como a la vez a lineamientos corporativos; y por otro lado, una organización que sea independiente lo cual requiera establecer su propio SGS.

De lo descrito, identificamos dos alternativas:
- Enfoque centralizado: donde exista un único SGS y la Seguridad de la Información y TI sea gestionada en forma central a nivel más alto del grupo empresarial.
- Enfoque distribuido: donde cada empresa tenga su propio SGS y sean independientes.

3.1.1 ¿Qué debemos tener en cuenta?

Al momento de plantearse diseñar, implantar y adoptar un SGS, la organización debe tener claro, qué tan importante es la Seguridad de la Información y TI para su negocio (objetivos, prioridades y estrategia de negocios), considerando aspectos como: la calidad de servicio esperada y exigida por sus clientes, objetivos y recursos financieros, y aspectos legales, regulatorios y/o contractuales.

La Alta Dirección debe mostrar su compromiso y aplicar su experiencia en la consecución de objetivos, gestión de prioridades, toma de decisiones, cumplimiento de cronogramas, etc. Este compromiso supone, liderar las actividades requeridas por la Alta Dirección, aportando los recursos necesarios, y trabajar por la concienciación y capacitación del personal, además de actividades de monitoreo y supervisión.

3.1.2 Estrategia de implementación

La definición de la estrategia de implementación de un sistema de gestión de seguridad (SGS) depende mucho de la estructura empresarial, considerando aspectos políticos, de dirección, constitutivos, así como la alineación de sus estrategias empresariales.
Deberá definirse por ejemplo:

- Cómo se analizarán los riesgos, cómo se establecerán las prioridades cuando estos riesgos involucren activos que son comunes o afectan la seguridad de ambas empresas, eventualmente con percepciones de riesgos diferentes. Cómo pesarán y se salvarán esas diferencias y con qué enfoque se gestionarán dichos riesgos. A qué nivel y sobre quién caerá la responsabilidad de definición de los controles, etc.
- Deben identificarse todas las partes involucradas y asignarse los roles y responsabilidades.
- En una empresa corporativa, saber cómo participa la empresa matriz del grupo en las definiciones y políticas sobre la empresa subordinada. Debe estar claro que si se tiene un rol de contralor de las políticas globales del grupo, si tiene participación directa en las políticas de la empresa subordinada, o si sólo hace recomendaciones o de carácter obligatorio.
- A su vez, la empresa subordinada tendrá su propia percepción y evaluación de riesgos, que muchas veces deberá elevar a la empresa matriz del grupo.
- Debe definirse formalmente el escalamiento para la toma de decisiones sobre Seguridad de la Información.
- Deben especificarse los registros de las decisiones y mediciones necesarias.
- Deben definirse los recursos necesarios.
- Debe contar con aprobación Gerencial y de la Dirección, y debe mantenerse y mejorarse continuamente.

3.1.3 Síntesis de requerimientos para la metodología

La metodología para el propósito que se considera, como objetivo de este documento, recomienda:

- Tener en cuenta los aspectos legales, contractuales y de regulación propios del sector industrial.

- Alinear con la estrategia y aspectos propios del negocio en un ámbito competitivo (plan de negocios, metas, prioridades, etc.).
- Alinear y cumplir las políticas.
- Promover la consistencia corporativa y capacidad de adaptación y adecuación en cada una de las empresas del grupo (para aquellas organizaciones que aplique)
- Involucrar a la Alta Dirección.
- Establecer el alcance del Sistema de Gestión de Seguridad, a efectos que la metodología sea aplicable y efectiva, con una infraestructura importante en cuanto a cantidad de activos de información y tecnología.
- Cumplir con la norma ISO/IEC 27001 para una eventual certificación.
- Buscar la integración con otras metodologías y estándares de gestión y calidad.
- Tener en cuenta la relación costo / beneficio.
- Permitir una adecuada gestión de la propia documentación del SGS, en cuanto a su mantenimiento y actualización para permanecer alineado y al día con los cambios en cualquiera de los componentes de: tecnología, recursos humanos y procedimientos de acuerdo a los requerimientos de los atributos de seguridad de la información para el negocio.

3.1.4 Fases de la Metodología

A efectos de lograr que la metodología sea aplicable y efectiva, y mantenga una relación conveniente costo / beneficio en cuanto a su eficiencia operativa y los niveles de seguridad de la información requeridos, es fundamental concentrarse en los procesos críticos del negocio, los de mayor valor agregado y estratégicos para su continuidad, y dar soporte a los procesos que sustentan el desarrollo competitivo y exitoso de la organización.

La metodología a emplear es producto de la recolección de información y experiencia en el ámbito de la seguridad de la información y gestión de las tecnologías de información. Cabe indicar que la misma puede ser aplicada por cualquier institución y manteniendo un enfoque de mejora continua (planear-hacer-verificar-actuar), según Norma ISO 27001.

Las fases que se consideran y que en el presente capítulo detallaremos son:

1) Planeación
2) Diseño
3) Operación
4) Retroalimentación

y Modelo del sistema de gestión de seguridad (véase en figura 3.10)

Además se incluyen documentos anexos que podrán ser utilizados como referencia.

Figura 3.1. Estrategia metodológica de seguridad de la información y TI [18]

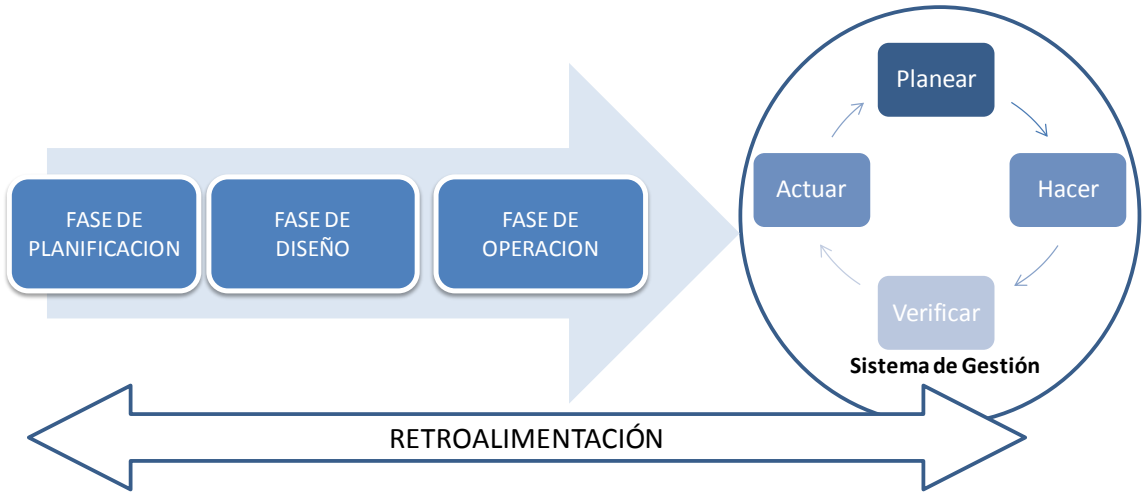
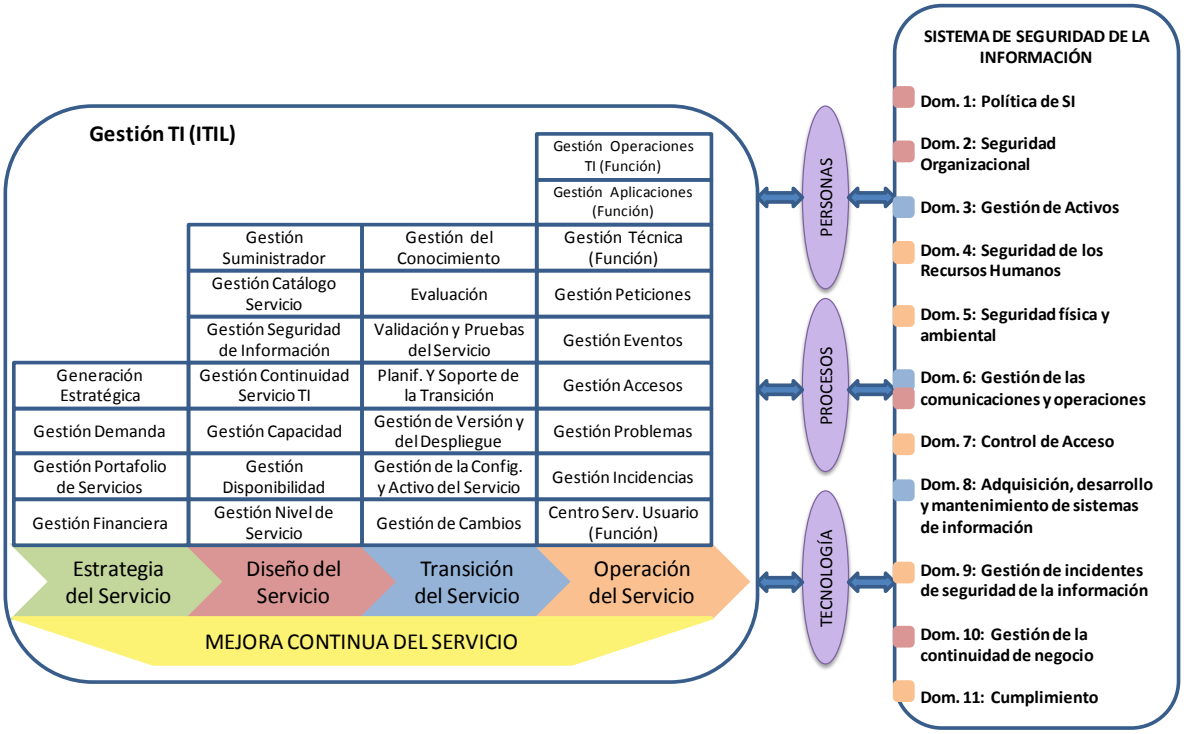


Figura 3.2. Relación ITIL vs 27002 sobre los principios básicos de la gestión de seguridad[19]



[18] Fuente: Elaboración propia

[19] Fuente: Elaboración propia

3.2 Fase de Planificación

Esta fase nos ayudará a tener las bases para el desarrollo del Plan de Seguridad y Modelo del Sistema de Gestión de Seguridad (fase de diseño), es decir nos centraremos en establecer los objetivos, procesos del alcance, la identificación del estado de seguridad inicial en una organización, así como los pasos necesarios a llevar a cabo para una adecuada gestión de riesgos. Notaremos que en esta fase es fundamental la intervención de la Alta Dirección y demás responsables de áreas relevantes de la organización.

3.2.1 Identificación de objetivos de la organización

El alineamiento estratégico de los objetivos de la seguridad de la información con los objetivos del negocio es un elemento crítico para un gobierno efectivo de seguridad.
La estrategia de seguridad de la información es un patrón frente al cual una organización toma sus decisiones de protección de la información con base en sus metas y objetivos. El proceso de toma de decisiones requiere de la definición de una política y de un plan de acción para alcanzar los objetivos de seguridad de la información. La estrategia permite definir los procesos y estructuras requeridos para satisfacer las necesidades de seguridad de la información de los accionistas, empleados, clientes y comunidad.

Para identificar en ¿dónde nos encontramos? (situación actual) y ¿hacia dónde vamos? (situación futura) por ejemplo nos hacemos preguntas como:

1. ¿Mi negocio puede ser más eficaz y productivo?, entonces analicemos en:
   <u>Hábitos y responsabilidad:</u>
   - El personal no está concientizado
   - El personal no está capacitado
   - No se aplican buenas prácticas
   - Malos hábitos laborales
   - Uso inadecuado de las infraestructuras
   - Falta de responsabilidad

   <u>La Dirección:</u>
   - La Alta Dirección no se involucra
   - La seguridad se considera como un gasto sin retorno
   - La seguridad no está integrada en la gestión
   - La seguridad es para los informáticos

   <u>Aplicación de Seguridad:</u>
   - Ausencia de políticas de seguridad
   - No se llevan a cabo copias de seguridad
   - No existen procedimientos
   - Ausencia de control de uso de recursos
   - Ausencia de control de uso de servicios
   - Desconocimiento de los activos de información

2. Si para mi organización es importante la imagen, entonces veamos en debemos mejorar, teniendo en consideración lo siguiente:

- Adecuación a la legislación
- Implantación de SGS
- Auditorías internas y externas
- Aportar garantías para mis proveedores, clientes y socios.

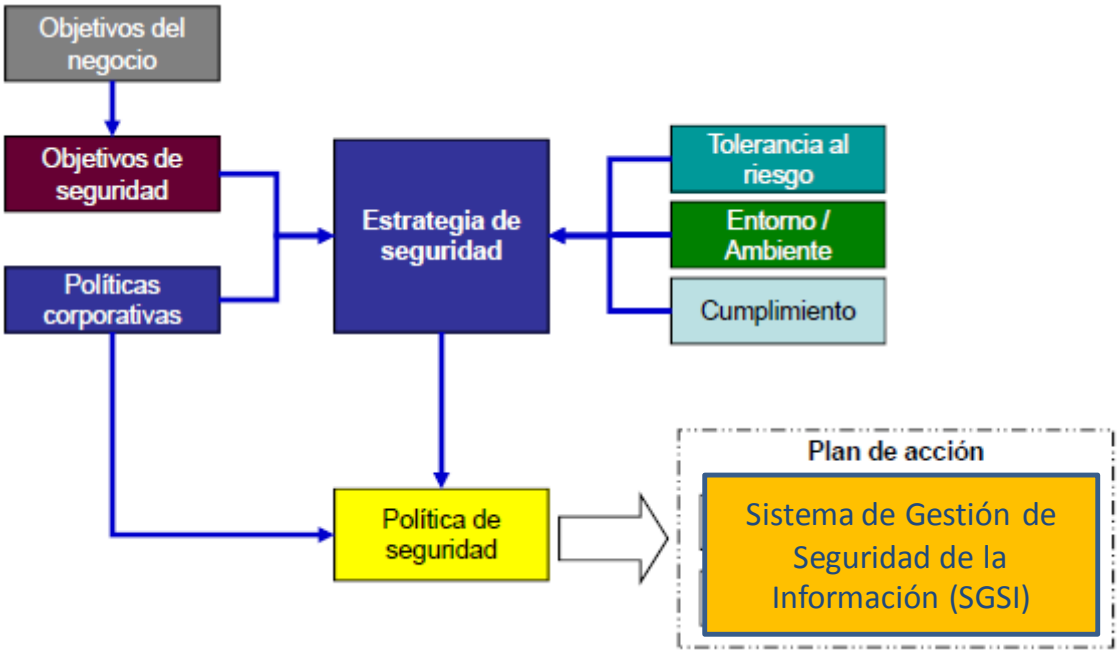
Marca, diferenciación:

- Somos diferentes a los demás
- Nos preocupa la seguridad y las amenazas
- Ofrecemos un valor añadido
- Somos eficientes, organizados y eficaces

Nivel de servicio

- Podemos ofrecer servicios confiables
- Respuesta ante contingencias
- Nuestros clientes pueden confiar
- Podemos ofrecer el nivel de servicio requerido y garantizarlo

Figura 3.3. Estrategia de seguridad[20]



Los objetivos del negocio los cuales son basados en la visión y misión del negocio requerirán la conservación de ciertos atributos de seguridad y por otro lado la generación de nuevas necesidades de seguridad. Por ejemplo: si se define como objetivo de negocio "desarrollar X productos para el mercado"; entonces para identificar el atributo clave del negocio, podemos preguntarnos ¿cuál es el impacto en IMAGEN si la información del nuevo producto es revelada a personas no autorizadas?. Aquí se toma en consideración los atributos de confidencialidad, integridad y disponibilidad que son la base para la clasificación de la información. Cabe precisar que el efecto de los atributos en los procesos nos conllevará a determinar nuevas necesidades de seguridad.

[20] Fuente: Elaboración propia

Para un mejor entendimiento, dejo aquí un modelo de objetivos de seguridad de la información.

Figura 3.4. Modelo de objetivos de seguridad de la información[21]

MODELO DE OBJETIVOS DE SEGURIDAD DE INFORMACIÓN

Objetivo	Indicador	Valor meta	Periodicidad	ALARMA		
Cumplimiento de controles aprobados en el plan de tratamiento de riesgos	% de controles que se han implantado en las fechas previstas	100%	Trimestral	100%	[60-100%>	[0-60%>
Lograr un efectivo grado de concientización de usuarios	% número de personas que aprobaron la evaluación de la charla de concientización	70%	Semestral	[70-100%]	[50-70%>	[0-50%>
Lograr compromiso del Comité						
Cumplimiento de cierre de No identificadas en auditorias						

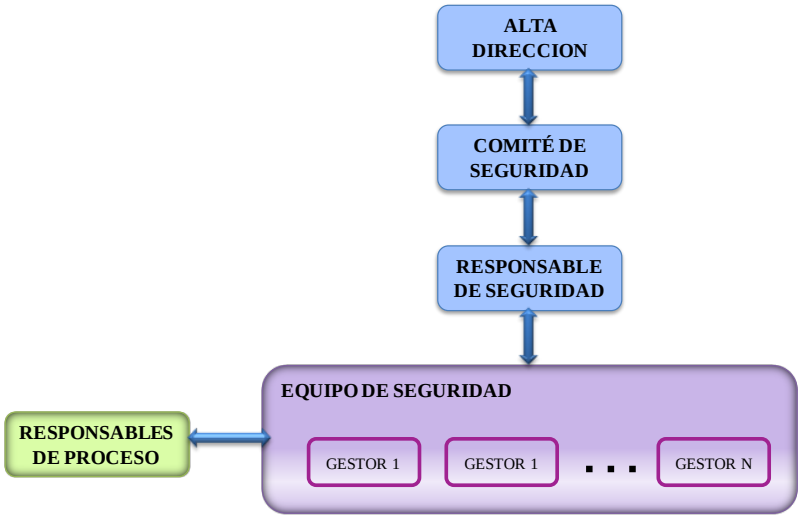
OBJETIVO: Cumplimiento de controles aprobados en el plan de tratamiento de riesgos	Ene	Feb	Mzo	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Gestor X Resultado
Total de Controles implantados en fecha													
Total de Controles planificadas													
Indicador													

OBJETIVO: Lograr un efectivo grado de concientización de usuarios	Ene	Feb	Mzo	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Gestor X Resultado
Número de personas que aprobaron la evaluación de la charla de concientización													
Total de Personas que asistieron a la charla de concientización													
Indicador													

3.2.2 Roles en un Sistema de Gestión de Seguridad

De una manera sencilla que pueda ser adaptada a una organización, se presenta una estructura de roles para un Sistema de Gestión de Seguridad (véase figura 3.3), cuyo detalle se presenta a continuación:

Figura 3.5. Estructura de roles para un sistema de gestión de seguridad[22]



[21] Fuente: Elaboración propia

[22] Fuente: Elaboración propia

3.2.2.1 Alta Dirección y Gerencias Responsables

- Velar por el cumplimiento de los objetivos y planes del SGS.
- Adoptar y difundir la política corporativa de seguridad de la información
- Aprobar la asignación de roles y responsabilidades específicos para la seguridad de la información en la organización
- Proporcionar recursos suficientes para crear, implementar, operar, supervisar, revisar, mantener, y mejorar el SGS.
- Proporcionar una clara dirección y respaldo gerencial visible con respecto a las iniciativas de seguridad.
- Decidir los criterios de aceptación de riesgos y los niveles aceptables de riesgo.
- Velar por el cumplimiento de las auditorias, dirigir las revisiones del sistema.
- Difundir los lineamientos de seguridad con todo el personal directamente involucrado.
- Aprobación de los documentos generales del sistema

3.2.2.2 Comité de Seguridad

- Revisar y aprobar las políticas, procedimientos y estándares de seguridad.
- Evaluar cambios significativos de la exposición de los activos de información a las amenazas de seguridad.
- Seguimiento de incidentes de seguridad reportados por el Responsable de Seguridad.
- Apoyar en la implementación del entrenamiento en seguridad de la información a los usuarios.
- Evaluar los avances en los proyectos o iniciativas de seguridad.

3.2.2.3 Responsables de Procesos

- Asegurar el cumplimiento de las políticas de seguridad y de las acciones de mejoras que la organización ha identificado
- Revisar documentos internos del sistema
- Asegurar el cumplimiento de los procedimientos operativos

3.2.2.4 Responsable de Seguridad

- Desarrollar, implementar y administrar un programa de seguridad de la información.
- Asesorar a la organización como incluir la seguridad de la información en las fases de inicio de todos los proyectos de tecnología de la información.
- Revisar las políticas, procedimientos y estándares según lo estipulado y presentar los cambios para la aprobación del comité de seguridad.
- Participar en la definición de los controles de seguridad para la plataforma tecnológica de la organización.
- Evaluar, realizar el seguimiento y reportar los incidentes de seguridad relevantes al Comité de Seguridad.
- Asegurar que los planes de contingencia sean desarrollados, mantenidos y probados regularmente para su funcionamiento.
- Asegurar que los controles de acceso de cada sistema de información estén de acuerdo con el nivel de riesgo evaluado

3.2.2.5 Equipo de Seguridad

Encargados del cumplimiento de los objetivos de seguridad fijados por la organización dentro de los procesos de su alcance, específicamente en:

- Implementación, cumplimiento y mantenimiento de Políticas de Seguridad.
- Actualización de los análisis de riesgo, identificando nuevas amenazas y vulnerabilidades.
- Velar por la implementación de las acciones definidas en el plan de tratamiento de riesgo.
- Actualización periódica del cuadro de métricas.
- Verificación de los registros definidos en los procedimientos.
- Actualización de los procedimientos internos de cada proceso
- Identificar acciones de mejoras en los procesos del SGS

Asimismo, dependiendo de la estructura que requiera la organización, este equipo se puede subdividir en los siguientes roles como:

A. Gestor de Riesgos:
   - Analizar y evaluar el riesgo de los activos de información
   - Mantener actualizado el inventario de los activos de información, según el criterio de confidencialidad, disponibilidad e integridad
   - Evaluar el impacto por cambios en la organización, regulatorios o contractuales que afecten los activos de información
   - Realizar cálculos de riesgo de seguridad, en función de la probabilidad de las amenazas y vulnerabilidades
   - Establecer evaluaciones de los riesgos a los que está expuesta la información sensible y coordinar con los responsables de los activos para tomar acciones de mitigación.
   - Definir el plan de tratamiento de riesgos (PTR), para los activos de información cuyo valor de riesgo se encuentren por encima del Nivel de Riesgo Aceptable
   - Hacer seguimiento a los responsables del Plan de Tratamiento de Riesgos, para su cumplimiento en fechas acordadas.
   - Evaluar los proyectos de tecnología (nuevos sistemas o evolutivos) que afecten la seguridad de información.

B. Gestor de Incidentes de Seguridad
   - Registrar y clasificar el incidente de seguridad de información, según el nivel de impacto definido
   - Solicitar y recopilar las evidencias necesarias con el apoyo de los Responsables de Procesos y personal que considere
   - Analizar e investigar las causas del incidente de seguridad, para la solución respectiva
   - Generar el Informe del Incidente de Seguridad de Información y presentarlo al Responsable de de Seguridad
   - Control y seguimiento del cuadro de mando de Incidentes de Seguridad de Información
   - Identificar los controles y mejoras necesarias al “Procedimiento de Gestión de Incidentes de Seguridad de Información”

C. Gestor de Accesos
- Controlar y supervisar los requerimientos de accesos a las aplicaciones, servicios de red y recursos de información.
- Reportar al Responsable de Seguridad, cambios en el Procedimiento de Gestión de Accesos y Revisión de Derechos de Acceso.
- Interactuar con el área de RRHH o Proveedor de Servicio para validación de cuentas inactivas y personal cesado.
- Generar Informes de Requerimientos de Accesos

D. Gestor de Continuidad
- Desarrollar y gestionar la gestión de continuidad/recuperación de desastres para garantizar que los procesos de negocio puedan restablecer dentro de los plazos requeridos
- Identificar y acordar responsabilidades asociadas al Plan de Recuperación de Desastres
- Mantener actualizado los procedimientos de los procesos involucrados en el DRP (ejemplo copias de respaldo, procedimiento de contingencia, cronogramas de pruebas, entre otros)
- Probar y actualizar los planes de continuidad/pruebas de recuperación de desastres
- Diseñar actividades de capacitación respecto a los procesos de continuidad para el personal involucrado

E. Gestor de Sensibilización y Capacitación
- Desarrollar y mantener planes de sensibilización y formación.
- Establecer estrategias de concientización, a fin de que el personal comprenda los lineamientos de seguridad establecidos por la organización.
- Llevar el control de los registros de las evaluaciones de sensibilización y formación.
- Monitorear y medir el progreso de la sensibilización y formación del personal.

F. Gestor Documental
- Coordinar con los responsables de procesos, el desarrollo o actualización de la documentación asociada al SGS
- Actualizar los inventarios de documentación
- Gestionar la publicación de los procedimientos (como medio a elegir puede ser: mail, herramienta “e-learning”, repositorio en servidor de archivos, intranet, entre otros)
- Mantener una estructura documentaria para el SGS

G. Gestor de Métricas
- Identificar objetivos de seguridad a ser medidos
- Definir y documentar métricas de seguridad
- Revisar y validar nuevas métricas o modificaciones de las existentes.
- Seguimiento a la publicación de datos respecto a las métricas definidas

H. Coordinador de Auditoria
- Supervisar la ejecución de las auditorías

- Verificar y/o realizar seguimiento al cierre de las acciones correctivas, preventivas y de mejora del SGS
- Acordar las visitas a partes específicas de las instalaciones de la organización para la Auditoria
- Preparar el programa de auditoria
- Presentar los resultados de la auditoria al Responsable de Seguridad

3.2.3 Alcance y Límites

Elegir adecuadamente un alcance es de suma importancia a la hora de implementar un SGS. Si es excesivo puede conllevar a que el proyecto sea inabordable y fracase; caso contrario si es muy reducido puede no contemplar aspectos importantes y den un resultado que no resultado que no se útil para los objetivos de la organización. El alcance puede ser un área de la empresa, proceso o servicio específico.

Entrada:
Deben considerarse objetivos, planes de negocio, la estructura y funciones de la organización, marcos legales, contractuales y regulatorios, expectativas de los clientes, restricciones, políticas, soporte tecnológico, software de gestión, entre otros.

Acción:
Debe analizarse toda la información descrita en la entrada, y considerar aspectos como la cultura organizacional, a los efectos de plantearse un alcance adecuado para los objetivos y prioridades de la empresa y posibles de lograr con los recursos con que se contará.

¿Quienes deberían participar?
Alta Dirección, Comité de Seguridad

Salida:
Una especificación concreta y específica del alcance, que determine en lo posible qué activos de información estarán comprendidos en el SGS y cuáles no.

3.2.4 Política de Seguridad

Una Política de Seguridad, es el plan maestro para proteger adecuadamente los sistemas de información y comunicaciones, el cual está estrictamente alineado con su misión y objetivos, y satisface el marco de requisitos legales, normativos, reglamentarios y contractuales relevantes para el desarrollo de sus actividades.

Figura 3.6. Documentación que se genera con la implementación de un Sistema de Gestión de Seguridad[23]

Las **Políticas** sientan las bases de la seguridad los cuales se encuentran alineados a los objetivos de la organización. Pretenden indicar las líneas generales para conseguir los objetivos marcados sin entrar en detalles técnicos. Deben ser conocidas por todo el personal (propio y terceros) y ser revisadas periódicamente o actualizadas cada vez que ocurran cambios significativos en la organización.

Los **Procedimientos** desarrollan los objetivos marcados en la Políticas. En ellos sí que aparecerían detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las Políticas. No es necesario que los conozcan todas las personas de la organización sino, únicamente, aquellas que lo requieran para el desarrollo de sus funciones.

Las **Instrucciones** constituyen el desarrollo de los Procedimientos. En ellos se llega hasta describir los comandos técnicos que se deben realizar para la ejecución de dichos Procedimientos.

Y por último los **Registros** evidencian la efectiva implantación del Sistema de Gestión de Seguridad y el cumplimiento de los requisitos. En este punto también es importante el contar con una serie de métricas o métricas de seguridad que permitan evaluar la consecución de los objetivos de seguridad establecidos.

Entrada:
- Contexto
- Alcance y Límites

Acción:
Deben definirse al menos:

[23] Se toma como referencia ISO/IEC 27002

Los criterios, principios y lineamientos fundamentales con respecto a la seguridad de la información
Requerimientos del negocio en cuanto a la seguridad de la información
Normativa / Legislación vigente
Es absolutamente imprescindible que la Alta Dirección haga suya dicha política, la firme y establezca la obligatoriedad de su cumplimiento. Esto garantizará una apropiada consideración y compromiso por parte de la organización, factor clave para su éxito.

¿Quienes deberían participar?
Alta Dirección, Comité de Seguridad

Salida
Un documento con la Política de Seguridad

3.2.5 Realización de un diagnóstico (Análisis GAP)

Esta actividad nos permite conocer el nivel de madurez que tiene la organización respecto a la seguridad, para ello se definen objetivos, actividades y duración

Entrada:
- Análisis del Negocio
- Normas, estándares y buenas prácticas
- Marco jurídico y contractual
- Políticas corporativas

Acción
Seleccionar los procesos relevantes del proceso incluidos en el Alcance SGS.
Aplicar una encuesta para obtener el diagnóstico actual de la organización y así definir el nivel de madurez en comparación con los requerimientos de los estándares de referencia (ISO 27002, ITIL)

¿Quienes deberían participar?
- Equipo de Seguridad de la Información de la organización
- Gerentes / Directores
- Responsables de Proceso
- Personal especializado en el área con experiencia en la implementación SGS
- Si hubiera consultor o especialista en seguridad de la información externo

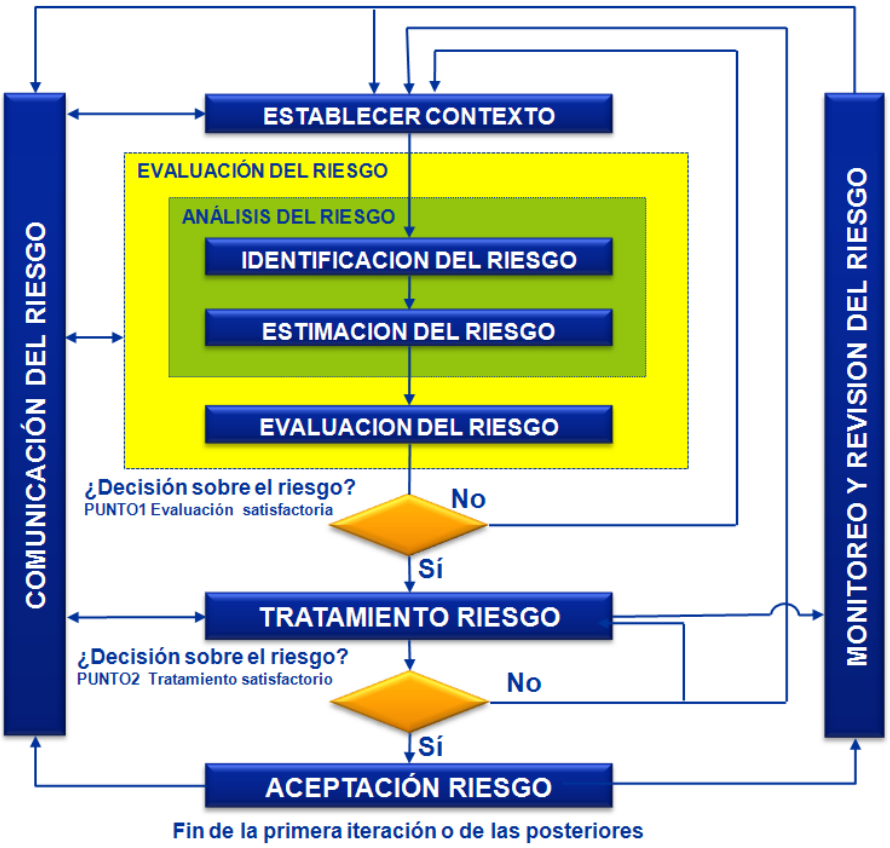
Salida
Un informe de la situación respecto al nivel de madurez de la organización en cuanto a la seguridad de la información y especificando la brecha a fin de alcanzar el nivel deseado.
Una vez que la organización ha sido alineada a los requerimientos de los estándares, entra en un ciclo de PHVA (Planear, Hacer, Verificar, Actuar).

3.2.6 Análisis y Evaluación de Riesgos

Como referencia principal para este trabajo, se consideró especialmente la norma ISO/IEC 27005 Tecnología de la información – Técnicas de seguridad – Gestión del riesgo en la seguridad de la información, justamente por estar estrechamente alineado con la norma ISO/IEC 27001 y ser parte de la serie ISO/IEC 27000. Así el proceso de la gestión de riesgo de seguridad de la información está compuesto de 4 etapas que se detallan a continuación:

1. Establecimiento del contexto.
2. Evaluación del riesgo.
3. Tratamiento del riesgo.
4. Aceptación del riesgo

Figura 3.7. Proceso de gestión de riesgo de seguridad de la información de ISO/IEC 27005:2008



Si comparamos con un SGS[24], el establecimiento del contexto, la evaluación de riesgos, el desarrollo de plan de tratamiento del riesgo y la aceptación de riesgos son parte de la fase "planear". En la fase “Hacer”, se implementa las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo al plan de tratamiento del riesgo. En la fase "Revisar", los administradores determinarán la necesidad de revisiones de la evaluación del riesgo y del tratamiento de los riesgos. En la fase "actuar", se lleva a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo de la seguridad de la información.

[24] De acuerdo al Modelo PDCA de la Norma ISO/IEC 27001:2005

¿Quiénes deberían participar?
La gestión de riesgos debe darse en todos los niveles jerárquicos, pero podemos distinguir un nivel macro. Algunos de ellos son:

- Alta Gerencia / Dirección de la empresa objetivo: en el alto nivel brindando las pautas directivas, políticas y estratégicas de negocios.
- Gerentes de línea o a cargo de unidades de negocios: con una participación directa sobre su área, gestionando los recursos humanos especializados para realizar esta tarea.
- Responsables de procesos de negocios importantes: análisis directo sobre los mismos, brindando la información necesaria para su gerencia responsable de forma proactiva con respecto a la seguridad de los mismos.
- Comité de Seguridad de la Información, en forma de supervisión, dando los lineamientos y coordinando el proceso de análisis de alto nivel con la Dirección. Además apoya al equipo de Seguridad de la Información en cuanto éste lo requiera.
- Equipo de Seguridad de la Información: colaborando en la identificación de los riesgos desde su visión técnica.
- Analista en riesgos

Hago hincapié que las normas no presentan ni especifican un método ni un algoritmo en concreto para realizar un análisis y evaluación de riesgos. Por mi experiencia está metodología se adapta a cualquier tipo de organización por ser sencilla, fácil de comprender y que abarca un enfoque de mejora continua de acuerdo a la Norma ISO/IEC 27001:2005.

3.2.6.1 Establecer el contexto

De acuerdo a la Norma ISO/IEC 27001 no se utiliza el término "contexto". Sin embargo, esto se relaciona con los requisitos de "definir el alcance y los límites" [(véase el numeral 4.2.1 a)]

A. Definición del alcance
   Se define el alcance y los límites de la gestión del riesgo de la seguridad de la información y TI a fin de garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo. Además es necesario identificar limites [(referencia Norma ISO/IEC 27001 numeral 4.2.1 a)].

B. Definición de criterio para el impacto del riesgo
   Se utiliza una escala de 5 niveles para la evaluación del impacto en caso de pérdida de la confidencialidad, integridad y disponibilidad (referencia Norma ISO/IEC 27001 [numeral 4.2.1 d) 4]).

Tabla 3.1. Escalas de Impacto

ESCALA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
MUY ALTO	Implica una alta pérdida o afectación de imagen frente a usuarios/clientes, así como incumplimiento a requerimientos legales aplicables y fuga de información de alto valor para la organización que podría afectar otros procesos.	Se comprometen los resultados de la ejecución de los procesos, provocando pérdidas significativas para la organización de tiempo y dinero.	Implican un paro total o suspensión de las operaciones del negocio por un tiempo prolongado.
ALTO	Implica una alta pérdida de imagen frente a usuarios/clientes, así como incumplimiento a requerimientos legales aplicables y fuga de información.	Implica un retraso o falla en la correcta ejecución de los procesos del negocio con altas pérdidas para la organización en términos de tiempo y dinero.	Implican un paro parcial o suspensión temporal de las operaciones del negocio por un tiempo prolongado.
MEDIO	Implica pérdida de imagen frente a usuarios/clientes, así como incumplimiento a requerimientos legales aplicables y fuga de información de valor medio para la organización.	Implica un retraso o falla en la correcta ejecución de los procesos del negocio con pérdidas moderadas para la organización en términos de tiempo, dinero, entre otros.	Se compromete la operación normal de algunos procesos del negocio, pero que puede ser controlado en forma paralela al desarrollo de las demás actividades del negocio.
BAJO	Se compromete en menor medida la imagen de la organización frente a los usuarios/clientes, y la fuga de información.	No se compromete de forma significativa la correcta operación de los procesos del negocio y los tiempos de remediación involucran baja cantidad de recursos (tiempo, dinero, personas, entre otros).	No se compromete la disponibilidad de las operaciones del negocio, y que por lo tanto no se requiere una acción inmediata.

C. <u>Definición de criterio para la evaluación del riesgo</u>

Nos servirá para determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos, desde el punto de vista de la organización, para así poder priorizarlos según su importancia. A continuación se muestran algunos criterios de

evaluación del riesgo que pueden ser utilizados por la organización para la evaluación de la importancia del riesgo.

Tabla 3.2. Escalas de evaluación del Riesgo

CRITERIOS	DESCRIPCIÓN
Económico	Cuando el impacto económico de la amenaza es mayor a un costo mensual de horas hombre
Continuidad	Cuando se paraliza un proceso de línea o al menos una actividad importante
Imagen/Reputación	Cuando la amenaza puede ocasionar que se vea afectada la imagen de la organización
Legal/Regulatorio	Cuando el impacto ocasiona una demanda de índole civil o penal, lo cual ocasionaría la aplicación de una sanción y/o una indemnización.
Obligaciones Contractuales	Cuando el impacto amenaza el cumplimiento del contrato, debido a causas previsibles o no, siempre que se hallen determinados en el contrato

D. Definición de criterios de la aceptación del riesgo

Para determinar una aceptación del riesgo se deberá evaluar lo siguiente:

- Los activos que se encuentran en un nivel de riesgo insignificante.
- La relación del costo beneficio del riesgo estimado.
- Falta de presupuesto
- Riesgos temporales o de corto plazo
- Aspectos legales y reglamentarios, Operaciones, Tecnología, Factores sociales y humanitarios.
- Los riesgos residuales con criterios menor o insignificante

Los criterios de aceptación del riesgo corresponden a "los criterios para aceptar riesgos e identificar el nivel aceptable del riesgo" que se especifican en la norma ISO/IEC 27001, numeral 4.2.1 c) 2

3.2.6.2 Análisis de Riesgos

A. Identificación de activos

Es necesario identificar o inventariar los activos para luego analizar su valor y sus riesgos.

Además de identificarse los activos debe especificarse y documentarse quién es su propietario o responsable de la seguridad del mismo, tal como se expresa en: A.7.1

y A.7.2 de la Norma ISO 27002. Debe además establecerse una política de uso de dichos activos como se establece en: A.7.1.3.
Sin embargo puede ser muy costoso realizar esta tarea sin categorizar o agrupar los mismos con algún criterio. De acuerdo a la norma ISO/IEC 27001, Activo es "aquello que tenga valor para la organización", lo cual en principio admite una interpretación amplia y eventualmente con cierto grado de subjetividad. Una manera sencilla de dividir los activos según su estado y características propias, sería en:

- ✓ Información (física y lógica)
- ✓ Software (conjunto de programas que puede ejecutar el hardware)
- ✓ Hardware (conjunto de elementos materiales que componen un ordenador u otros equipos)
- ✓ Servicios (tales como la energía eléctrica, agua, telefonía, servicio de correo electrónico)
- ✓ Personal (persona que componen la organización y ejecutan tareas propias del negocio)
- ✓ Entorno (edificios, mobiliario)
- ✓ Intangibles (aquellos que influyen en los aspectos sociales, éticos, técnicos, económicos)

Además de identificar y clasificar los activos según sus requerimientos de seguridad (y su criticidad para el negocio), debe identificarse quién es el propietario (o dueño) de ese activo; el mismo que será el responsable por su seguridad.

Seleccionar los activos es una tarea bajo un enfoque de prioridad. El software por ejemplo, en lo que refiere a un sistema de información, suele ser menos crítico que la información en sí misma, sin embargo puede tener igual importancia si es la única vía de acceso a la información, en ese caso, la indisponibilidad del software provoca que la información tampoco sea accesible o no esté disponible. De esta manera tendremos que ir seleccionando los activos relevantes dentro del proceso de negocio.

En esta metodología se diferencia de forma explícita los procesos, de los "otros" activos, dada su naturaleza y a su carácter de ser: o bien inherentemente crítico atendiendo a la estrategia del negocio, o circunstancialmente crítico en función del flujo de trabajo y procedimientos establecidos.
A continuación, definimos el proceso de identificación de activos, y en particular, de activos críticos:

Entrada:

- Conocimiento del negocio.
- Relevamiento de los procesos del negocio.
- Planes estratégicos.
- Calificación de los activos realizados por la empresa principal que estén comprendidos dentro del alcance del SGS que se analiza.

Acción:

Una vez definidos los "Procesos Críticos" o de mayor valor para el negocio, es posible obtener los activos críticos, que serán todos aquellos que intervengan.

Como una herramienta para determinar activos críticos o prioritarios en cuanto a los sistemas de información y la información en sí misma, menciono algunas preguntas de ejemplo:

- ¿Qué sistemas de información sustentan dichos procesos?
- ¿Qué información es requerida por los mismos?
- ¿Qué información es relevante y particularmente importante en cuanto a su confidencialidad, disponibilidad e integridad?
- ¿Qué factores o incidentes podrían afectar de forma grave o relevante estos procesos?
- ¿Cómo afecta esto a los procesos más relevantes del negocio?

En otras palabras, proceso-activo estarán relacionados si la seguridad de uno está comprometida por la seguridad del otro, es decir, si un incidente de seguridad en uno afecta la seguridad del otro.

Sin embargo, la norma ISO/IEC 27001, en su Anexo A que tiene carácter normativo, requiere que "todos los activos deben ser claramente identificados". Esto es: todos los activos – todo aquello que tenga valor para la organización - comprendidos en el alcance del SGS.
Es decir, que si nos interesa cumplir con la norma, a los efectos de una certificación pero a su vez, concentrarnos en los procesos (y activos) críticos o de mayor valor para el negocio, una estrategia es ser más precisos en la declaración del alcance del SGS.

Salida:
Un relevamiento de los activos de la organización comprendidos en el alcance del SGS, el cual contemple los siguientes atributos: ID o código, nombre del activo, descripción, ubicación, área o proceso al que pertenece y su correspondiente propietario (Inventario de Activos).

B. Identificación de Amenazas

Las amenazas pueden originarse de sucesos o eventos accidentales o deliberados. Una amenaza debe explotar una vulnerabilidad de un sistema, aplicación o servicio utilizado por la organización, para causarle un daño al activo.
Se debe identificar las amenazas a las que está expuesto el activo de información.

Entrada:

- Incidentes reportados dentro de la organización
- Amenazas para el sector
- Estadísticas de amenazas globales

Acción:
Debe tenerse un catálogo de amenazas bien identificado y lo más completo posible, considerando, tanto amenazas internas como externas, factores humanos y acciones deliberadas como accidentales, ambientales, etc.
Es muy importante referirse a catálogos conocidos y estadísticas globales propias del dominio de aplicación, así como aquellas que afectan y se detectaron en otras empresas comparables y por supuesto estadísticas propias,

estadísticas por la empresa principal (cuyo análisis se va a realizar sobre una empresa subordinada), y aquellas estadísticas detectadas a nivel nacional.
Deben clasificarse las amenazas por el tipo de activo que afecte (información, software, servicios, etc.).
Es importante mantener actualizado el catálogo de amenazas dado que en el tiempo pueden variar respecto a las anteriores y surgen otras nuevas.

Salida:
Una lista de amenazas reales y clasificadas según su tipo (Catálogo de Amenazas).

C. Identificación de Controles

Se deberían identificar los controles existentes y los planificados para evitar trabajo o costos innecesarios y su estado de implementación y utilización

Entrada:

a. Documentación de los controles existentes.
b. Documentación de la Implementación del Plan de Tratamiento de Riesgos (anteriores).

Acción:

A efectos de no caer en costos e inversiones de tiempo y trabajo en controles que se superpongan con otros existentes (ineficiencia operativa), es importante conocer el grado de cobertura actual de los mismos. Para esto pueden ser útiles tanto los informes de implementación de controles de planes de tratamiento de riesgos anteriores así como informes de auditoría. Deben considerarse tanto los controles existentes como aquellos incluidos en el Plan de Tratamiento de Riesgos.
Esto permite tener todos los elementos para una mejor evaluación de los riesgos reales y una utilización más racional de las inversiones en seguridad estableciendo prioridades con mayor certeza.
El campo de acción de los controles, es potencialmente el escenario de riesgo constituido por las vulnerabilidades existentes, las amenazas detectadas y el impacto que tendrían sobre los activos en caso de efectivizarse.
Por lo tanto, pueden y deben establecerse controles tendientes a:

- Minimizar las vulnerabilidades
- Eliminar o reducir / inhibir las amenazas
- Eliminar, mitigar o transferir el impacto sobre los activos.

Algunos aspectos no tecnológicos que también deben tomarse en cuenta al momento de identificar y establecer controles:

- Información del lanzamiento de nuevos productos.
- Gestión de permisos y manejo de las claves de acceso a información privilegiada (infraestructura, futuros proyectos, información técnica, información confidencial de interés para la competencia), considerando aún los funcionarios que eventualmente dejan de pertenecer a la empresa.
- Gestión de la información confidencial o privada / reservada.
- Datos privados, de la empresa y de clientes.
- Acceso Físico.

- Relaciones contractuales, comerciales y laborales.

Algunos recursos a tener en cuenta para esta actividad son:

- Informes y recomendaciones del área Legal, respecto a la legislación vigente aplicable.
- Informes de Auditoría de la propia organización.
- Informes o la percepción de los propios usuarios involucrados y el "propietario" de la información. (Grado de uso y efectividad de los controles).

Podemos tomar algunas características durante el análisis de controles existentes, como por ejemplo:

- En cuanto a su oportunidad: preventivo ó correctivo
- En cuanto a su periodicidad: permanente, periódico u ocasional
- En cuanto a su automatización: manual, semi-automático o automático
- En cuanto a su estado: permanente, parcialmente implementado, no implementado
- En cuanto a su efectividad: si ó no

Salida:
Un escenario claro de los controles existentes.

D. Identificación de Vulnerabilidades

Las vulnerabilidades son debilidades asociadas a los activos de una organización. Estas debilidades pueden ser explotadas por una amenaza causando incidentes no deseados que pueden resultar en pérdida o daño de estos activos. Una vulnerabilidad por sí sola no causa un daño; es simplemente una condición o grupo de condiciones que puede permitirle a una amenaza afectar a un activo. Las vulnerabilidades se deben básicamente a fallos naturales de la tecnología, malos diseños de los productos tecnológicos o malas implementaciones o configuraciones de los productos. Estas vulnerabilidades pueden ser explotadas por una amenaza para causar daño a los activos y los negocios que ellos soportan.

Entrada:

- Informes internos de vulnerabilidades.
- Reportes y repositorios de vulnerabilidades de sitios y organizaciones especializadas (Internet).
- Listas de vulnerabilidades conocidas (ejemplo: NIST I-CAT)
- Reportes de incidentes (locales o de otras empresas).
- Informes de auditorías previas.
- Informe de vulnerabilidades de la empresa principal en lo que corresponda (por ejemplo: infraestructura).
- Informes y noticias de seguridad de fabricantes y firmas especializadas.
- Listas de distribución y Foros de seguridad
- Listas de verificación de requerimientos de seguridad
- Evaluaciones previas y pruebas (prediseñados) de seguridad
- Análisis de riesgos realizados previamente

Acción:
Las vulnerabilidades tienen su importancia relativa en función de la existencia de amenazas reales (factibles), que puedan explotarla, y el impacto que eso pueda generar para la organización. Así mismo deben considerarse los controles existentes (y planificados) que pueden mitigar o eliminar dicha vulnerabilidad.
Si se detectan vulnerabilidades que no tienen una amenaza conocida factible, deben igualmente documentarse, porque el escenario (y las amenazas) podrían cambiar.

Deben identificarse las vulnerabilidades no sólo referentes a la tecnología, dispositivos y protocolos de comunicaciones utilizados, sino que la cobertura debe ser de todas las áreas:

- Organización
- Procesos y Procedimientos (organización y métodos, operaciones)
- Recursos Humanos
- Condiciones ambientales y físicas.
- Aspectos técnicos (configuración, infraestructura: hardware, software, comunicaciones, etc.)
- Relaciones y dependencias de terceros.

Algunas herramientas útiles para la detección de vulnerabilidades son:

- Herramientas automáticas de escaneo y detección de vulnerabilidades.
- Test de penetración (Hacking ético)
- Auditorías de Evaluación de Seguridad.
- Revisión de código.
- Encuestas y observaciones en el lugar (inspecciones físicas).
- Reportes de incidentes.
- Grafos o árboles de vulnerabilidades, incluyendo como son afectados los servicios y/o activos de información, aún para las dependencias entre la empresa principal y la subordinada.

Salida:
Una lista de vulnerabilidades de los activos, considerando las amenazas y controles existentes (Catálogo de vulnerabilidades).

3.2.6.3 Evaluación de Riesgos

Se utilizará la estimación cualitativa esta estimación utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala. Estas escalas se pueden adaptar o ajustar para satisfacer las circunstancias y se pueden utilizar descripciones diferentes para riesgos diferentes.

¿Quienes deberían participar?

- Gerencias de línea

- Equipo de Planeamiento de Seguridad de la Información
- Comité de Seguridad de la Información (estimación de alto nivel).
- Analista de Riesgos.
- Alta Dirección General (en caso de ser necesario)

A. Valoración de activos

La valoración de activos, es fundamental para cualquier plan de seguridad de la información.

Como plan que es, requerirá de recursos, y cuanto más fundamentado esté la importancia de los activos que se esté protegiendo, será más fácil justificar las inversiones requeridas en seguridad y también las decisiones tendrán más elementos para basarse en una relación costo / beneficio.

La valoración de activos puede ser muy simple o compleja dependiendo del tipo de activo.

Por ejemplo, para algunos activos puede considerarse simplemente el valor de reposición como valor del mismo. En otros casos deben considerarse otros costos, indirectos como por ejemplo "costo de oportunidad", "lucro cesante", etc. Para otros puede tener que asignarse un valor subjetivo o abstracto difícil de cuantificar como por ejemplo la pérdida de imagen institucional (tipo de activo "intangible").

También pueden intervenir aspectos financieros que hagan más compleja aún la valuación. Por ejemplo el valor de la pérdida de confidencialidad del lanzamiento de un nuevo producto / proyecto o de datos privados de clientes.

Por este motivo, no siempre es viable ni conveniente, intentar una valoración cuantitativa de los activos (ni siquiera los críticos), sino que a veces es más viable y conveniente utilizar una valoración cualitativa.

Una clasificación probable y valoración cualitativa típica, tal como lo establece la norma ISO/IEC 27005 es: Irrelevante, Muy Bajo, Bajo, Medio, Alto, Muy Alto y Crítico.

Sin embargo, atendiendo al tipo de organización, puede ser más adecuada una primera clasificación, de alto nivel, en Bajo, Medio, Alto y Crítico, para eventualmente hacer la escala más fina en etapas posteriores.

Para la valoración de activos se plantea en términos de cuánto pierde la organización por no poder cumplir con los objetivos de control (ISO/IEC 27002). Para ello, deben considerarse en sentido amplio aspectos tangibles y no tangibles; es decir considerar los impactos en los siguientes valores / atributos relativos a la seguridad de la información:

- Confidencialidad de la información (Confidencialidad)
- Precisión y Confiabilidad de la información (Integridad)
- Disponibilidad y Oportunidad de la información (Disponibilidad)

Fórmula de cálculo:

Impacto= Suma del valor de la Confidencialidad, la Disponibilidad e Integridad para cada activo de información, teniendo en cuenta:

Tabla 3.3. Relación valor cualitativa – cuantitativo del impacto

Valor Cuantitativo	Valor Cualitativo
5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo
0	No aplica

Debe tenerse presente, que los valores asignados pueden cambiar con el tiempo dada su naturaleza, por ejemplo información que es reservada hasta que se decide hacerse pública. En ese caso, debe revisarse periódicamente esta valoración ya que no es estática, y de no hacerse se estaría incurriendo en un gasto debido a esta sobrevaloración no justificada.

B. Valoración de amenazas y vulnerabilidades

Después de identificar las amenazas y vulnerabilidades, es necesario tasar la probabilidad de que una combinación de amenazas y vulnerabilidades ocurra (ISO 27001:2005 cláusula 4.2.1 d)

La probabilidad total para que un incidente ocurra depende también de la vulnerabilidad de los activos. Por ejemplo, qué tan fácilmente pueden ser explotados. En consecuencia, las vulnerabilidades y amenazas se clasifican de acuerdo con la siguiente escala:

Tabla 3.4. Escala de Evaluación de Probabilidad (Amenazas y Vulnerabilidades) impacto

Valor	Descripción
0	No aplica
1	**Raro**: Puede ocurrir sólo en circunstancias excepcionales.
2	**Improbable**: Puede ocurrir en algún momento.
3	**Moderado**: Podría ocurrir en algún momento.
4	**Probable**: Probablemente ocurra en la mayoría de las circunstancias.
5	**Casi cierto**: Se espera que ocurra en la mayoría de las circunstancias.

C. Estimación de la probabilidad de ocurrencia y nivel del riesgo

Además del impacto de los riesgos, debe analizarse qué tan frecuente ocurren las amenazas y que tan fácil es explotar las vulnerabilidades.

Entrada:

Algunos datos a tener en cuenta para la estimación de probabilidad de ocurrencia:

- Registros históricos propios.
- Datos estadísticos de Organizaciones similares (Sector de la Industria)
- Datos estadísticos globales.
- Consultoras / sitios especializados. Asesoramiento y recomendaciones de profesionales de Seguridad de la Información.
- Estadísticas relacionadas, y la experiencia de organizaciones especializadas ya sea de CSIRTs locales o CERTs.
- Controles existentes (y los planificados) y cómo pueden y/o logran efectivamente mitigar los riesgos / vulnerabilidades o reducir y eliminar amenazas.
- Informes de especialistas y técnicos del dominio de aplicación o dueños de los activos.
- Factores accidentales o ambientales. Estadísticas y previsiones.

Acción:

Esta medición es función de la relación del peso de las amenazas y del peso de las vulnerabilidades, respecto del total de amenazas y vulnerabilidades identificadas. (ISO 27001:2005 cláusula 4.2.1 e). Entonces se calcula:

- Factor de ocurrencia de vulnerabilidades: Suma del valor total de vulnerabilidades (probabilidad) para cada activo de información.

- Factor de ocurrencia de amenazas: Suma del valor total de amenazas (probabilidad) para cada activo de información.

- Factor de ocurrencia de amenazas y vulnerabilidades: Suma del Factor de Ocurrencia de Amenazas y el Factor de Ocurrencia de Vulnerabilidades.

$$F(oav) = \sum vulnerabilidades + \sum amenazas$$

Cálculo del Nivel del Riesgo:
Para calcular el Nivel de Riesgo de cada activo, se relacionan los valores establecidos para "Impacto" y el valor obtenido en el cálculo del "Factor de Ocurrencia".

Los valores de nivel de riesgo se normalizan a una escala predefinida para que en el momento de establecer un Sistema de Gestión de Seguridad alineado con la norma ISO/IEC 27001:2005 se determine el Nivel de Riesgo Aceptable y todos los activos que se encuentren por encima de este umbral, sus riesgos deberán ser minimizados mediante la aplicación de controles de seguridad.

Valor de Riesgo = Producto del Impacto por el Factor de Ocurrencia de Amenazas y Vulnerabilidades.

$$R = Impacto * F(oav)$$

Salida:
Una tabla de riesgos calificados considerando el impacto y a su probabilidad de ocurrencia, a los efectos que puedan priorizarse los mismos para su tratamiento.

D. Evaluación de Riesgos

El objetivo principal de la evaluación de riesgos es priorizar los mismos y racionalizar los recursos disponibles para la implantación de controles. Incluso establecer el cronograma de acciones en función de estas prioridades, en ese caso, el recurso tiempo es un recurso más a racionalizar, que también es escaso si se consideran las ventanas de oportunidad que se abren para las amenazas latentes, vulnerabilidades presentes y el tiempo disponible para mitigar estos riesgos.
Por otra parte, por un tema de eficiencia operativa y de la relación costo / beneficio, como en cualquier proyecto, es necesario priorizar las actividades relevantes.
Evaluar todos los riesgos posibles, a nivel detallado, sobre todos los activos indiscriminadamente, supondría una inversión en recursos (técnicos y profesionales) y tiempo difícil de justificar. Por otro lado, los riesgos más graves que podrían suponer impactos nefastos para el negocio o pérdidas financieras importantes, se verían postergados debido a una aplicación sistemática de

evaluación de todas las vulnerabilidades, amenazas, controles y activos, cosa que claramente no es deseable.

Entrada:

- La inversión que realiza la organización en cada activo / proceso (inicial, mantenimiento, control, gestión, etc.).
- Especificación de los procesos y activos de mayor valor agregado para el negocio.
- Las consecuencias de incidentes conocidos y comparables, ya sea propios o de otras empresas similares.
- Especificación de los criterios de evaluación de riesgos establecidos.

Acción:

La evaluación del riesgo sirve para darle significancia y para identificar los riesgos que requerirán la aplicación priorizada de controles para su mitigación en la etapa de tratamiento del riesgo, o decidir que ciertos niveles de riesgo pueden ser aceptables, y que por tanto no requieren mayor acción.

El cálculo será:
El valor total resulta de la combinación del valor del riesgo (obtenido de 3.2.5.3 C) por la cantidad de criterios aplicables (referencia 3.2.5.1 B). Luego se procede a ordenar los riesgos dándoles un orden de prioridad.

¿Quiénes deberían participar?

- Gerencias de línea
- Equipo de Planeamiento de Seguridad de la Información
- Comité de Seguridad de la Información, eventualmente con el asesoramiento de un
- Analista de Riesgos.
- Dirección y Gerencia General (en caso de ser necesario)

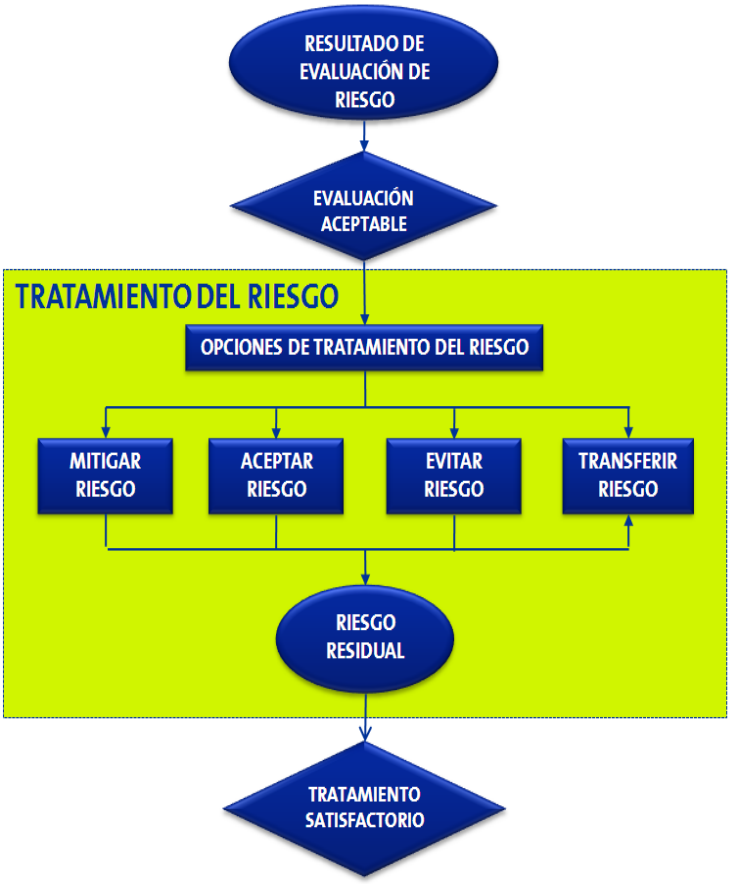
Salida:

Un documento con los lineamientos de gestión de riesgos, y riesgos priorizados de acuerdo al criterio de evaluación previamente establecido.

3.2.6.4 Tratamiento de Riesgos

El tratamiento de riesgos debería ser guiado por algunos principios de gestión básicos, atendiendo a que no se busca una protección absoluta, con todos los controles posibles, sino una seguridad conveniente, atendiendo a: los aspectos legales, estratégicos y a la disponibilidad de los recursos.
Debe perseguirse la eficacia de los controles para lograr los requerimientos de seguridad del negocio, fundamentalmente sobre cada activo y proceso importante.
Por otra parte, debe procurarse la eficiencia operativa, intentando racionalizar los recursos acorde a las prioridades. Debe primar el principio de costo / beneficio, así como también aspectos estratégicos y valores menos tangibles como la imagen, prestigio, etc.

Figura 3.8. Actividad del tratamiento de riesgos



Entrada:

- Una lista de riesgos priorizados, de acuerdo al criterio de evaluación de riesgos y acorde a los escenarios de riesgos identificados.
- Restricciones (de tiempo / oportunidad, financieras, técnicas, ambientales, legales / regulatorias, contractuales, culturales, de interoperabilidad, adecuación etc.).
- Lista de amenazas sobre los activos de información.
- Lista de vulnerabilidades de los activos.

Acción:

Debe decidirse cómo se enfrentará cada uno de los riesgos, los cuales pueden:

- mitigarse: implementando controles y obteniendo así un riesgo residual.
- aceptarse, según los criterios y umbrales de aceptación inicialmente especificados.
- evitarse: una de las formas más simples de evitar un riesgo es eliminar el activo que lo presenta o decidir no procesar cierto tipo de información sino se consigue la protección adecuada.
- transferirse: a terceros, por ejemplo a otra empresa mediante contrato o una compañía aseguradora.

Los controles pueden operar sobre el impacto (mitigando el mismo), sobre las amenazas (disminuyendo su probabilidad de ocurrencia) o sobre las vulnerabilidades (fortaleciendo esos aspectos).

Es posible combinar más de una estrategia para un riesgo, por ejemplo, aplicar controles para mitigar un riesgo y el riesgo residual transferirlo mediante la contratación de un seguro.
En sentido complementario, también se espera, que un mismo control sirva como medida para contener o mitigar más de un riesgo y funcione como salvaguarda para varios activos.

¿Quienes deberían participar?
- Gerencias de línea
- Técnicos / especialistas del área
- Equipo de Planeamiento de Seguridad de la Información.
- Eventualmente con el asesoramiento de un Analista de Riesgos.

La norma ISO/IEC 27002 proporciona información detallada sobre los controles. Existen muchas restricciones que puede afectar la selección de los controles. Las restricciones técnicas tales como los requisitos de desempeño, el manejo (requisitos de soporte operativo) y los aspectos de compatibilidad pueden dificultar el uso de algunos controles o podrían inducir al error humano bien sea anulando el control, dando una falsa sensación de seguridad o incluso aumentando el riesgo aún mas que con la inexistencia del control (por ejemplo exigiendo contraseñas complejas sin entrenamiento adecuado, haciendo que los usuarios escriban las contraseñas). Además, podría darse el caso de que un control pueda afectar el desempeño.
A los efectos de dimensionar el Plan, puede ser necesario consultar a la Dirección y/o Gerencia General para saber la viabilidad de contar con los recursos suficientes y así adecuar el alcance del mismo.

Salida:
Un Plan de Tratamiento de Riesgos con los correspondientes riesgos residuales, sujetos a la aprobación de la Alta Dirección o Comité de Seguridad.

3.2.6.5 Aceptación del Riesgo

Después de la implementación de las decisiones relacionas con el tratamiento de un riesgo, siempre habrá un remanente de ese mismo riesgo. A este riesgo se denomina riesgo residual.

La Alta Dirección toma la decisión de aceptar los riesgos y las responsabilidades de la decisión y se registra de manera formal (esto se relaciona con la norma ISO/IEC 27001, párrafo 4.2.1 h)).

Los planes para el tratamiento del riesgo deberían describir la forma en que los riesgos valorados se deben tratar, con el fin de satisfacer los criterios de aceptación del riesgo *(véase criterios de aceptación del riesgo en 3.2.5.1 C)*. Es importante que los directores responsables revisen y aprueben los planes propuestos para el tratamiento del riesgo y los riesgos residuales resultantes, y que registren todas las condiciones asociadas a tal aprobación.

Luego se obtendrá una lista de los riesgos aceptados con la justificación para aquellos que no satisfacen los criterios normales de aceptación de riesgos de la organización.

Entrada:
Plan de Tratamiento de Riesgos validado por las áreas técnicas, especificando sus riesgos residuales, los recursos necesarios y un cronograma tentativo de alto nivel a los efectos de su evaluación.

Acción:
La Alta Dirección debe dar su aprobación al Plan de Tratamiento de Riesgos, velando que se cumpla con los niveles de aceptación de riesgos especificado y si se optara por aceptar algún riesgo mayor al nivel esperado (especificado) debe dejarse explícitamente documentado en que se fundamenta la decisión.
Para calcular el riesgo residual se debe:

- Determinar si los controles disminuyen la probabilidad o el impacto
- Calcular la probabilidad e impacto residuales utilizando la misma metodología descrita en los pasos anteriores.

¿Quienes deberían participar?

- Comité de Seguridad (que tenga al menos un representante de la empresa principal del grupo empresarial).
- Dirección y Gerencia de la empresa en cuestión (subordinada).
- Dirección y Gerencia del grupo empresarial en el caso que involucre niveles de aceptación que están por encima de los niveles pautados en su propio SGS y políticas corporativas (en caso lo determinen así).

Salida:
La aceptación del Plan de Tratamiento de Riesgos, incluyendo las decisiones excepcionales tomadas (si las hubiera).

3.2.6.6 Comunicación de los riesgos

Entrada:
Todos los resultados de las etapas anteriores del Análisis y Evaluación de Riesgos, en particular, el Plan de Tratamiento de Riesgos incluyendo los riesgos residuales.

Acción:
Es necesario una adecuada comunicación a los efectos de por un lado: entender los lineamientos de seguridad de la información, conocer las políticas específicas y la existencia y potencial impacto de los riesgos. Esta comunicación debe ser bidireccional, tanto entre empresas como al interior de cada empresa.

De acuerdo a la norma ISO/IEC 27005 es necesario un plan de comunicación de riesgos a efectos de:

- Recopilar información sobre los riesgos (percibidos).
- Compartir los resultados de la evaluación de riesgos y presentar el plan de tratamiento de riesgos.
- Evitar o reducir la ocurrencia y el impacto de los incidentes e infracciones de la seguridad de la información debido a la falta de comprensión mutua o mala interpretación entre los encargados de adoptar decisiones y los involucrados.
- Apoyar la toma de decisiones.

- Obtener nuevos conocimientos de seguridad de la información
- Coordinar con otros involucrados y planificar las respuestas para mitigar su impacto.
- Dar a los responsables de la toma de decisiones y a las partes interesadas un sentido de responsabilidad acerca de los riesgos.
- Mejorar el conocimiento

Todo esto, es necesario realizarlo para alinear y armonizar las necesidades de seguridad de la información, y tomar acciones conjuntas.

¿Quienes deberían participar?

- Dirección y Gerencia de la empresa (subordinada).
- Comité de Seguridad (que tenga al menos un representante de la empresa principal del grupo empresarial).
- Equipo de Seguridad.
- Departamento de Capacitación
- Áreas involucradas.

Salida:

La toma de conciencia hacia el interior de la empresa, de la importancia de la seguridad de la información, el impacto potencial y las medidas que se adoptan. Mejorar continuamente el conocimiento sobre la gestión de riesgo y sus resultados.

3.2.7 Documento de Aplicabilidad

Debe elaborarse un documento que especifique los controles adecuados que aplican al SGS.
La norma ISO/IEC 27001 especifica en su Anexo A - el cual tiene carácter normativo – un conjunto de Objetivos de Control y Controles generales. No obstante, aclara la propia norma que esa lista no pretende ser exhaustiva y debe ampliarse de acuerdo a las necesidades y características de la organización y sector de la industria correspondiente.

En particular, resultan de especial interés, controles adicionales que puedan detectarse para el sector o la industria y tengan un carácter más específico. Algunos controles podrían excluirse por no aplicar su objetivo de control y en ese caso debe especificarse su justificación en el documento.

Quienes deberían participar:

- Alta Dirección o Gerencia General.
- Comité de Seguridad
- Equipo de Seguridad.
- Gerentes de línea y de las diferentes unidades de negocio.
- Responsables de los procesos sustantivos (críticos y prioritarios) de la empresa.

Este documento deberá quedar aprobado por la Alta Dirección.

3.3 Fase de Diseño

Esta fase se establece un plan de seguridad y modelo del sistema de gestión de seguridad de la información y TI (SGS), así como consideraciones para el establecimiento de un proyecto.

3.3.1 Plan de Seguridad

El Plan de Seguridad viene a ser el desarrollo de los objetivos estratégicos identificados en la política y normativas de seguridad de la organización, y su finalidad es ubicar a la organización, a nivel global, en un entorno de riesgo aceptable. En la práctica es una herramienta sistemática que permite establecer pautas y directrices para planificar de forma ágil las diferentes iniciativas de la organización. El Plan de Seguridad es el camino, que se refleja en el mapa y que sirve para guiar los pasos de la organización en el cumplimiento de sus objetivos de seguridad.

Recapitulando, los pasos que la organización ha recorrido en la senda hacia la Gestión Estratégica de Seguridad son:

- Diseño, redacción y aprobación de la Política de Seguridad de la organización. Este documento desgrana los objetivos estratégicos de la entidad en materia de seguridad, y plantea el alcance de los mismos.
- Análisis y Evaluación de Riesgos de los procesos incluidos en el alcance de la Política de Seguridad. Gracias a él, se conocen los activos que soportan los procesos (conocimiento del entorno), así como las vulnerabilidades de las que adolecen y las amenazas a las que se enfrentan.

En este punto, el objetivo es identificar y planificar las acciones, correctivas o de mejora que permitirán reducir los riesgos identificados para los activos, y luego plasmarlas y gestionarlas a través del Plan de Seguridad.

Muchos de los riesgos podrán ser reducidos mediante la aplicación de un único control de baja complejidad (como por ejemplo, la implantación de un sencillo antivirus). No obstante, en numerosas situaciones no bastará con una actividad sencilla y habrá que diseñar proyectos específicos para afrontar riesgos complejos (como el diseño e implantación de un Plan de Contingencias).

La base de un Plan de Seguridad es una colección de actividades, muchas de ellas con carácter complejo, que se deberán abordar para alcanzar el objetivo de seguridad establecido a través del umbral de riesgo.

Tras disponer de dicha colección de actividades y proyectos derivados, la siguiente incógnita es el orden en el que se deberán acometer. Sin duda, la mejor opción es priorizar las acciones en base a un único criterio, aunque luego se utilizarán otros que matizarán dicha ponderación. El criterio base a la hora de planificar y priorizar el despliegue de los controles de seguridad será el nivel de riesgo cubierto por el control. Asociada a cada línea de acción se dimensiona también el beneficio cuantitativo obtenido tras su implementación para cada dimensión de seguridad (confidencialidad/integridad/disponibilidad).

Su objetivo es por tanto priorizar las líneas de acción y definir diferentes categorías de proyectos:

- Inmediatos (también denominadas "Quickwins", y que permiten obtener resultados importantes en un tiempo o con unos recursos mínimos).
- Corto plazo.
- Medio plazo (como máximo 2 ó 3 años)

Figura 3.9. Esquema de priorización derivados del Plan de Seguridad

Así un Plan de Seguridad basado en la ISO 27002 e ITIL deberá reflejar las buenas prácticas en la gestión de seguridad que una organización puede tener, permitiéndose verificar el estado actual de la seguridad del sistema e identificar claramente los objetivos a alcanzar de forma inmediata, de corto y mediano plazo, que posteriormente serán verificados con la misma norma.

Entrada:
- Objetivos estratégicos de la organización
- Requisitos de negocio

Acción
Debe asegurarse cubrir a toda la organización, ello incluye personal interno, proveedores
Se deberá:
- Identificar los requisitos de negocio para la seguridad
- Determinar el estado actual de la seguridad en la organización (infraestructura, aplicaciones, organización, procesos)
- Análisis de la gestión de seguridad (sirve para identificar cuáles son los puntos fuertes a mantener y las debilidades a mejorar)
- Definir la estrategia y plan de seguridad. Se recomienda que cumpla con las propiedades "SMART":
  - Específicos (Specific): deben ser concretos para comunicarlos efectivamente
  - Medibles (Measurables): deben poderse medir para poder comprobar en qué grado se están alcanzando.
  - Conseguibles (Achiveable): deben ser posibles de conseguir, en caso contrario producirán confusión y frustración.
  - Relevante (Relevant): deben estar alineados a los objetivos que importan.

  - Acotados en el tiempo (Time-bound): ¿cuáles son los plazos para su cumplimiento esperado?
- Desarrollar el programa de despliegue (se planifica y gestiona de manera similar a cualquier otro proyecto)

¿Quienes deberían participar?
- Alta Dirección
- Personal relevante de las diferentes áreas de la organización

Salida
- Plan de Seguridad

El Plan de Seguridad diseñado para la operación del SGS en la organización debe divulgarse paulatinamente y considerando al personal que tienen responsabilidades definidas en estos documentos; de esta manera es necesario que la divulgación de los documentos del SGS se realice por grupos de personas y por proceso con el fin de garantizar un adecuado entendimiento y aplicación de estos. Las estrategias de divulgación "puesto a puesto" por procesos y actividades, son las más adecuadas, teniendo en cuenta el mapa de procesos, las caracterizaciones, los procedimientos, instructivos y formatos, los mapas de riesgos, los métricas y los requisitos legales aplicables al proceso o actividad.

Es necesario que la organización defina cuál(es) serán las herramientas de las que dispondrá para garantizar la consulta de la documentación; esto con el fin de que en la medida que se realice la divulgación de la documentación, se comuniquen además las herramientas definidas para el acceso a ésta y los controles establecidos; entre otras se relacionan:
- Intranet
- Impresión física
- Página web
- Software especializado

Asimismo debe existir un administrador o encargado de la documentación que asegure la última versión del documento aprobado.

3.3.2 Modelo del Sistema de Gestión de Seguridad

Este modelo se apoya en el análisis de los estándares y normas de la seguridad de la información y tecnologías de información como lo son ISO 27002 e ITIL.
Su principal aporte es ser un facilitador en la implementación y/o aplicación de la seguridad de la información en cualquier tipo de organización.

La estructura que presenta el modelo se basa sobre la implementación práctica y concreta relacionada con las actividades que permitan dar seguridad a la organización, la cual, en base a sus propias necesidades, lineamientos y perspectivas de negocio, busca mantener la información asegurada.

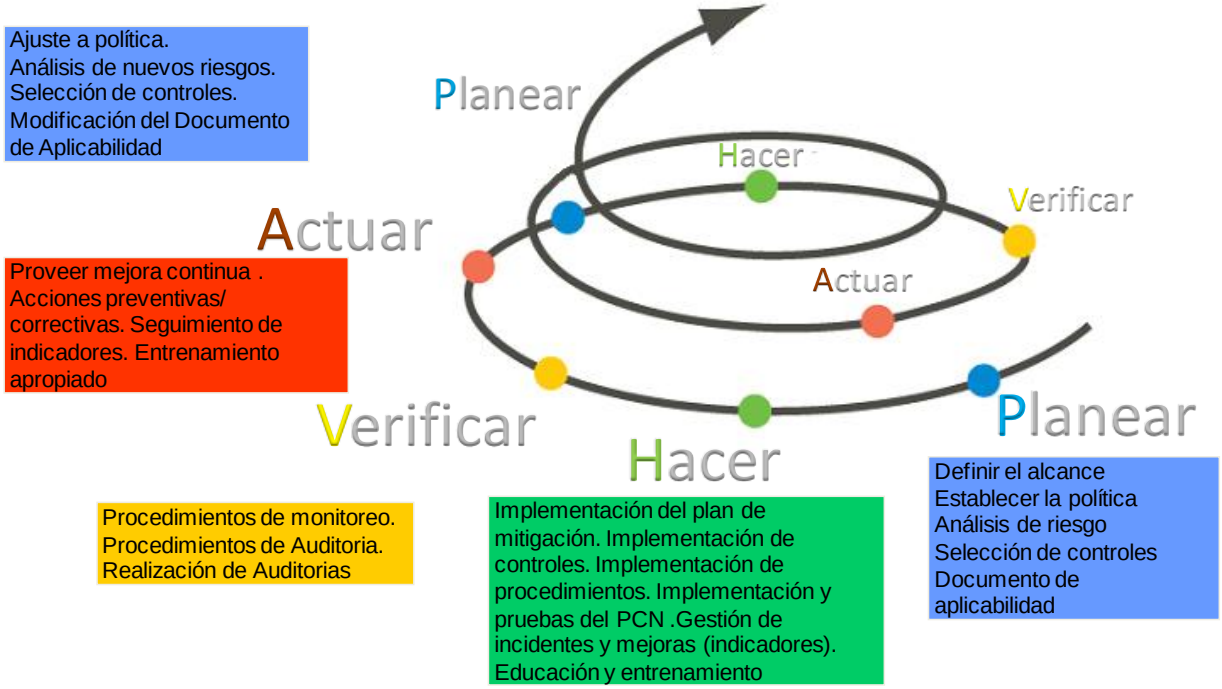
Otro aspecto importante que aporta este modelo, es que puede ser correlacionada sin mayor dificultad con las actividades que realiza cualquier tipo de organización, de manera que se logre asegurar la información en conformidad a la realidad de Tecnologías de Información (TI) que se disponga.

En la implementación del modelo se debe tener conocimiento de las funciones, tareas, actividades y diseño relacionadas con cada una de las etapas, por lo cual, se enfatizan los roles en la gestión de seguridad, ya que con su aporte la organización podrá estructurar de forma adecuada su seguridad. El responsable de Seguridad es relevante en el control, monitoreo y seguimiento de los planes de acción, ya que esto permite el ciclo continúo de perfeccionamiento y de vida del modelo.

El presente modelo, avalado en los estándares presentados en este artículo, pretende ser una solución y aporte en la implementación de la seguridad de la información de cualquier organización.

El modelo además considera los tipos de documentos (procedimientos, registros) necesarios para implementar un adecuado nivel de control. Cabe indicar que el modelo no entrega documentos desarrollados (procedimientos, instructivos), sino que sienta las bases para su desarrollo. Esto se justifica en que cada empresa u organización tiene sus propios entornos y realidades, por lo cual, el desarrollo acabado de este tipo de implementaciones requiere de un detalle superior que escapa al alcance de este estudio.

Figura 3.10. Modelo del sistema de gestión de seguridad [25]



A. *Planear:*

En esta etapa se define el alcance del SGS en términos de negocio, organización, localización, activos y tecnologías. Implica, establecer la política, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización. Asimismo se especifica la forma de llevar a cabo las medidas de seguridad concretada en el Acuerdo de Nivel de Servicio (ANS); lo cual debe estar alineado a la política de seguridad.

- Debe ser aprobada por la Dirección una política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización, alineada con el contexto estratégico de gestión de riesgos y criterios de evaluación de los mismos. Considerando los requerimientos legales o contractuales relativos a seguridad.
- Se establece una metodología de evaluación del riesgo, además de definir los criterios de aceptación del riesgo.
- En esta fase se realiza la identificación de riesgos mediante la identificación de los activos que están dentro del alcance del SGS y sus responsables directos, la identificación de las amenazas en relación a los activos, la identificación de las vulnerabilidades que puedan ser aprovechadas por dichas amenazas, la identificación de los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Los riesgos han de ser analizados y evaluados, en base al impacto que provocaría en el negocio un fallo de seguridad que supongo pérdida de confidencialidad, integridad o disponibilidad de un activo de información, la probabilidad de ocurrencia de un fallo en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados, según los criterios determinar la aceptación del riesgo.

[25] Basado en el ciclo de mejora continua especificado en la Norma ISO/IEC 27001:2005

- Para el tratamiento del riesgo se han de seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- En la declaración de aplicabilidad se incluye los objetivos de control y controles seleccionados y los motivos para su elección, los objetivos de control y controles que actualmente ya están implantados, los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión.

B. Hacer:

Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos. Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos. Desarrollo de las medidas de seguridad planeadas.

- Se define un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información, y se implementa el plan junto con los controles.
- Para obtener los resultados de eficacia de los controles se especifican métricas.
- Se implantan procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

C. Verificar:

Su objetivo es mantener la eficacia de los diferentes controles de seguridad. Analizar y medir donde sea aplicable, los procesos ejecutados con relación a las políticas, evaluar objetivos, experiencias e informar los resultados a la Administración para su revisión. La consecuencia de esta evaluación puede ser la actualización o sustitución de medidas, controles, entre otros.

- La organización deberá ejecutar procedimientos de monitorización y revisión para detectar a tiempo los errores en el procesamiento de la información, identificar brechas e incidentes de seguridad, ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto, detectar y prevenir eventos e incidentes de seguridad mediante el uso de métricas, determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Se revisará regularmente la efectividad del SGS, atendiendo al cumplimiento de la política y objetivos del SGS, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Se verificará la efectividad de los controles para ver si cumple con los requisitos de seguridad.
- Se revisará regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Se realizarán periódicamente auditorías internas en intervalos planificados.
- Se revisará por parte de la Dirección periódicamente el SGS para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras son evidentes.
- Se actualizarán los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Se registrarán acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGS.

D. Actuar:
Las posibles amenazas, así como la propia infraestructura de la organización, evolucionan con el tiempo, por lo tanto, las medidas de seguridad están sujetas a actualizaciones constantes. Ello significa realizar acciones preventivas y correctivas, basados en las auditorías internas y revisiones o cualquier otra información relevante para permitir la continua mejora del SGS. Es importante que las medidas de seguridad y los diferentes controles estén documentados y que los mismos se encuentren actualizados.

- La organización deberá implantar regularmente las mejoras identificadas en el SGS, realizando las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurar que las mejoras introducidas alcanzan los objetivos previstos.

PVHA es un ciclo de vida continuo, lo cual quiere decir que la etapa ACTUAR lleva de nuevo a la etapa de Plan para iniciar un nuevo ciclo de las cuatro fases.

3.3.3 Continuidad del negocio

El Plan de Continuidad del Negocio debería centrarse en los objetivos de negocio prioritarios para continuar operando el mismo en un caso de desastre o de crisis (incidente/s grave/s) y se debería indicar de forma concreta los procedimientos que deben ser realizados y el nivel de servicio que debe ser provisto en estas condiciones. Esto puede incluir seguros, acuerdos con terceros, mecanismos de contingencia, etc.

En particular los procesos críticos podrían depender de servicios provistos por la empresa principal, o viceversa. También puede ocurrir que una de las dos empresas preste servicios en una situación de contingencia mientras la otra restablece sus operaciones, o incluso podría ocurrir que ciertos procesos (de contingencia) y/o controles (prevención) los afronten de forma conjunta para compartir y bajar costos.

Estos planes de continuidad del negocio, tienen su correspondencia con los requerimientos de la seguridad de la información, y en ese contexto establecemos una breve especificación del mismo.

Entrada:
- Objetivos del negocio
- Procesos críticos y prioritarios para el negocio.
- Activos relacionados o de los cuales dependen esos procesos críticos.
- Análisis y tratamiento de riegos. Riesgos residuales y tolerancia admisible.
- Responsabilidades sobre los procesos y activos críticos identificados.

Acción:
Es necesario que para el plan de contingencia estén claramente determinadas las responsabilidades sobre los procesos y activos necesarios para la continuidad del negocio.
A su vez deben determinarse y aprobarse de forma explícita y documentada la tolerancia a fallos o pérdidas admisibles, por ejemplo en la disponibilidad y pérdida de calidad de los servicios o de información. Sobre la base que los riesgos tratados de forma que son eliminados o mitigados hasta que su impacto potencial se encuentre dentro de un margen tolerable, deben definirse acciones para reponerse ante fallos y determinar acciones de contingencia para continuar con la operativa de los procesos y servicios críticos.

Además de la asignación de responsabilidades y la determinación de la tolerancia a fallas sobre los procesos críticos del negocio, deben realizarse las siguientes acciones:
a) Establecer los procedimientos que permitan recuperarse y mantener operativos los servicios y procesos críticos.
b) Establecer prioridades de recuperación y tiempos máximos de tolerancia para el restablecimiento del servicio con niveles aceptables, indicando cuales son estos niveles según corresponda.
c) Especificar otros procedimientos complementarios que deban ser realizados luego de los planes de contingencias ejecutados y los procedimientos necesarios para restablecer el servicio.
d) Documentar los procedimientos acordados y autorizados.
e) Capacitar al personal para actuar en estos casos (desastres, crisis, etc.).
f) Probar y actualizar los planes regularmente.

¿Quienes deberían participar?
En lo que refiere a los planes y acciones respecto de la seguridad de la información, deberían participar al menos:
- Alta Dirección,
- Equipo de Seguridad
- Comité de Seguridad de la Información
- Dueños de los sistemas de información
- Dueños de los procesos estratégicos u operacionales importantes.

Salida:
- Plan de continuidad del negocio

3.3.4 Compromiso de la administración gerencial

Establecer, implantar y mantener un SGS requiere de recursos económicos, humanos y tecnológicos. Debe analizarse como un proyecto, con diferentes objetivos e hitos a cumplir en el corto, mediano y largo plazo.

Vimos que es necesario que el SGSI esté alineado con los intereses y prioridades del negocio, pero no deben subestimarse ni sobrestimarse las necesidades y requerimientos de seguridad, ni las actividades y recursos necesarios para alcanzarlos.

Para ello, puede ser útil un buen análisis costo / beneficio de las diferentes alternativas y escenarios planteados, y dejarlo por escrito para que en el futuro no hayan malos entendidos.

Entrada:
- Alcance y límites del SGS.
- Política de Seguridad
- Resultados de la Evaluación de Riesgos
- Declaración de aplicabilidad (con los objetivos de control y controles)
- Plan de Tratamiento de Riesgos.
- Estándares y procedimientos.
- Restricciones conocidas o detectadas (financieras, técnicas, culturales, legales, de tiempo cronograma, de capacitación y recursos humanos, de integración con otros sistemas de gestión, etc.).
- Análisis de Brecha (con el escenario deseado y los requerimientos de seguridad de la información).

Acción:
Es necesario establecer un plan de asignación de recursos (técnicos y humanos) que esté ajustado al presupuesto y si es necesario, realizar posteriormente las gestiones para su ampliación con un plan que sustente el SGS.

Como todo plan, debe adecuarse, la inversión al retorno esperado, según un criterio costo / beneficio y alineado a las prioridades estratégicas de la Organización. Si es necesario realizar gestiones con la Dirección a los efectos de lograr mayores recursos los ya asignados, serán realizadas por parte del Comité de Seguridad.

Igualmente, si hubiera riesgos compartidos que ameriten su tratamiento por parte de la empresa principal y la subordinada, o coordinar acciones para el mismo, serán analizados y gestionados por parte del Comité de Seguridad.

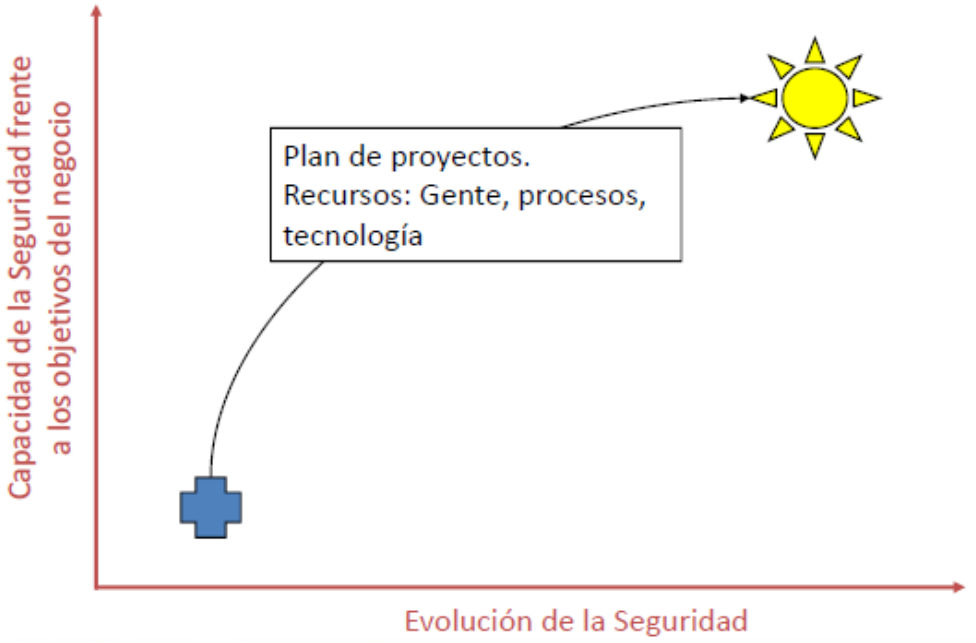
¿Quiénes deberían participar?
- Alta Dirección
- Equipo de Seguridad
- Comité de Seguridad
- Dueños de los sistemas de información
- Dueños de los procesos estratégicos u operacionales importantes.
- Finanzas

Salida:
- Asignación de Recursos Humanos
- Plan de recursos de IT necesarios

3.3.5 El Proyecto

Una vez que la organización tenga definido su plan de Seguridad y conociendo el modelo de gestión de seguridad, la principal dificultad por parte de diversas organizaciones está en gestionar dicho plan. Es recomendable, agrupar los proyectos de seguridad por su priorización de acuerdo a la estrategia de negocio. Existen otras formas como agruparlas según las áreas de conocimiento (procesos y servicios, tecnología, seguridad física, legislación o iniciativas mixtas).

Figura 3.11. Esquema de evolución de la seguridad en una organización[26]



Es importante hacer notar que un Plan de Seguridad se ubica en el plano de la estrategia, por lo cual se deben definir ciertos atributos indispensables para cualquier iniciativa que se vaya a planificar como:

a) Fecha de comienzo y duración:
   Cada proyecto derivado del Plan de Seguridad, independientemente de su prioridad, debe planificarse en un marco temporal concreto, indicándose así mismo su duración. Es especialmente recomendable mantener de forma paralela a la representación tradicional del Plan de Seguridad (apoyada normalmente en hojas de cálculo o herramientas avanzadas) un diagrama de Gantt del proyecto. Gracias a esta representación, será posible entender de forma más clara las dependencias y ejecuciones paralelas de tareas, lo que permitirá a su vez optimizar la planificación.

[26] Fuente: Elaboración propia

b) Recursos y presupuesto:
   Este punto es donde se produce el nexo más importante con el negocio de la organización en el plano financiero. Dado que a través del Plan de Seguridad se planifica la seguridad de forma proactiva y proporcional, a partir de su creación será posible presupuestar y aprovisionar apropiadamente. Así mismo, y dada su naturaleza, en muchos casos podrán ser gestionados como inversiones. De forma adicional, en este punto debe separarse el coste económico de cada proyecto o línea de acción en, al menos, materiales, contrataciones externas y personal (se debe contemplar el coste tanto para personal externo como la ocupación interna de recursos).

c) Responsable de proyecto/acción:
   Toda acción deberá tener un único responsable cuya función principal en el marco del Plan de Seguridad será controlar que dicha tarea se inicia en el momento que debe y cumple la planificación propuesta.
   Ante desvíos sobre lo esperado, ya sea en el plano temporal, de recursos o presupuestario, éste deberá informar inmediatamente para emprender las acciones correctivas pertinentes. Además, una de sus principales funciones será presentar el estado y logros de cada iniciativa al resto de personal involucrado y crear informes ejecutivos para la alta dirección.

d) Nivel de riesgo que cubre:
   Éste es el verdadero indicador de prioridad de cada acción referido del Plan de Seguridad. Este punto es uno de los principales nexos de unión con la Gestión de Riesgos realizada.

e) Otros:
   Adicionalmente, se pueden reunir, según el nivel de madurez en la Gestión de Seguridad de la organización, diversas métricas. Entre ellos, siempre resulta interesante el ratio coste/beneficio.

Por otra parte, existe una alternativa a esta metodología de gestión del Plan de Seguridad: la *Oficina de Gestión de Seguridad*. Se trata de una estructura de gestión que se responsabiliza de organizar y supervisar la colección de proyectos y líneas de acción definidas en el Plan de Seguridad. Se puede abordar su creación de forma interna a la organización o externalizarla, pero en todos los casos y dado su foco, deberá tener una componente importante en gestión de proyectos (un punto útil de partida puede ser el modelo de Oficina de Gestión de Proyectos (PMO) propuesto por el PMI, "Project Management Institute".

3.4 Fase de Operación

En esta fase se implementa el programa de trabajo definido en la fase anterior, de acuerdo a lo establecido en el plan de seguridad comprometido, el cual toma como referencia a la ISO 27002 e ITIL.

Asimismo en esta etapa se registran y controlan los resultados de la implementación del programa de trabajo considerando actividades, dificultades, grado de avance en el cierre de

las brechas, implementación del plan de mitigación de riesgos asociados a cada proyecto o iniciativa y acciones de difusión.

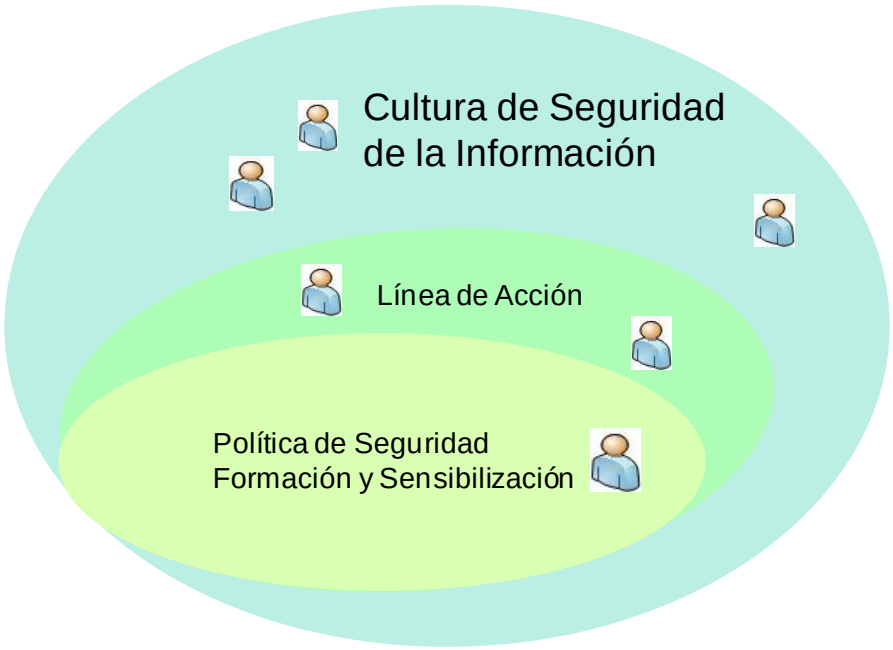
3.4.1 Cultura y educación

Una vez que la política de seguridad está aprobada por la Dirección quienes deben cumplirla son todas las personas de la organización. En este momento es cuando hay que saber explicar y hacer comprender el por qué se ha marcado esa política concreta y no otra.

Uno de los objetivos principales es saber transmitir la información y explicaciones pertinentes; así una persona informada, formada y culturizada sabrá comprender por qué se dictan ciertas normas y por qué es necesario cumplirlas. La formación es muy importante lo cual debe llevar a adquirir los conocimientos necesarios para tener cultura de la seguridad. Esta cultura de seguridad nos llevará a incrementar bidireccionalmente la transmisión de información entre usuarios y responsables de seguridad sobre todo ayudar a detectar posibles incidencias en el uso de la información y las tecnologías.

El trabajo profesional de los responsables de seguridad es tener la *fuerza* para poder implantar las medidas de seguridad necesarias, el *valor* para que todas la cumplan, el *equilibrio* para que estas medidas armonicen la seguridad con la agilidad del trabajo y la *sensatez* para que sean sólo las necesarias para conseguir los objetivos definidos en la política de seguridad.

Figura 3.12. Cultura de Seguridad de la Información[27]



[27] Fuente: Elaboración propia

Entrada:
- Política de Seguridad.
- Resultado de la Evaluación de Riesgos.
- Plan de Tratamiento de Riesgos.

Acción:
Se desarrollará un plan en el cual se establecerán el temario de la difusión, a quienes va dirigido, las fechas de programación, las necesidades de formación del personal, los medios de comunicación que se utilizarán (afiches, mensajes vía correo, boletines, charlas, etc), los recursos que se requerirán, así como los mecanismos de evaluación.
Al final este plan tendrá que ser aprobado en Comité.

¿Quienes deberían participar?
Debe formarse un grupo de personas de los diferentes sectores dentro del alcance del SGS, entre ellos:
- Comité de Seguridad: gestionará los recursos necesarios con la Alta Dirección.
- Equipo de Seguridad: Estimará recursos, tiempos y propondrá estrategias para la difusión de la política, normas y procedimientos.
- Representantes de las Gerencias directamente afectadas.
- Representantes de RR.HH.

Salida:
- Plan de Formación y Sensibilización

3.4.2 Implementación de controles

Entrada:
- Alcance del SGS.
- Política de Seguridad.
- Resultado de la Evaluación de Riesgos (Alto nivel y detallado).
- Documento de Aplicabilidad.
- Plan de Tratamiento de Riesgos.
- Estándares y procedimientos.

Acción:
La implementación de cada control, correspondiente a un objetivo de control, debería de analizarse como un 'mini-proyecto' en el sentido de su estrategia de implementación. Dependiendo de la dimensión del Control, tendrá documentación específica de su fase conceptual y de diseño y por otro lado un nivel más detallado respecto a su implementación concreta con las actividades y aspectos técnicos, instrumentación, planes de capacitación, asesorías, etc.

Es necesario que los controles estén alineados al alcance.

Por lo descrito, resulta conveniente formular un plan de implementación de controles, a los efectos de estimar recursos y tiempo que deberá ser aprobado por la Alta Dirección y/o Comité de Seguridad.

¿Quiénes deberían participar?
Debe formarse un grupo de personas de los diferentes sectores dentro del alcance del SGS, entre ellos:

- Comité de Seguridad: gestionará los recursos necesarios con la Alta Dirección y guiará prioridades en función de las políticas y lineamientos establecidos en su momento por la Alta Dirección.
- Equipo de Seguridad: Estimará recursos, propondrá alternativas técnicas y planes de implementación en un alto nivel, en particular para aquellos controles y objetivos de control relacionados.
- Representantes de las Gerencias directamente afectadas.
- Representantes de RR.HH.
- Representantes de la Seguridad Física.
- Gerencias transversales (de soporte corporativo): RR.HH, Legal, Sistemas etc.
- Dueños de los procesos y activos afectados (estratégicos y operacionales).

Salida:
a. Plan de Implementación de Controles (cronograma, responsable / equipo, etc.)
b. Registro y Documentación de las actividades y controles implementados

3.4.3 Gestión de incidentes

Entrada:

- Alcance del SGS.
- Política de Seguridad.
- Resultado de la Evaluación de Riesgos.
- Declaración de Aplicabilidad.
- Plan de Tratamiento de Riesgos.
- Estándares y procedimientos.

Acción:
Deben tomarse medidas para, por un lado, minimizar los incidentes de seguridad que ocurran, y por otro lado, si ocurren, que causen el menor daño posible.
En ese sentido deben realizarse actividades tendientes a la protección y establecimiento de controles en forma preventiva, y por otro lado, si ocurre un incidente debe detectarse y reaccionarse adecuadamente (acciones correctivas).

Para ello, además de los sistemas de monitoreo y detección de incidentes, alarmas o alertas, análisis de vulnerabilidades y tratamiento de riesgos, etc., debe existir un procedimiento sobre cómo actuar cuando ocurre un incidente: cómo reportarlo, forma de escalamiento, contingencia, acciones de recuperación, etc., de forma de actuar de manera planificada y previamente analizada, y no de forma arbitraria y bajo presión; cabe precisar que el procedimiento debe estar adecuadamente documentado, revisado y actualizado.

A continuación un ejemplo de los estados por el cual pasa un incidente desde su registro hasta su cierre:

Tabla 3.5. Posibles estados de incidentes de seguridad

ESTADO	DESCRIPCIÓN
REGISTRADO	Cuando el incidente de seguridad de información ha sido registrado.
ASIGNADO	Cuando el incidente de seguridad de información ha sido asignado a un Responsable de proceso y éste ha definido las acciones de solución.
EN PROCESO	Cuando el Responsable de proceso tiene un avance de la implementación de las acciones de solución.
EN CONFORMIDAD	Cuando las acciones de solución del incidente de seguridad de información han sido implementadas al 100%, y por tanto deben ser informados a la Gerencia para la obtención de su conformidad de cierre.
CERRADO	Cuando el incidente de seguridad de información tiene la conformidad de la Gerencia.

El procedimiento debe permitir:

- Asegurar la continuidad del negocio, y gestionar incidentes de diferente naturaleza: malware, denegación de servicios, integridad de la información, accesos no autorizados, divulgación de información confidencial, etc.
- Clasificar y priorizar el incidente
- Analizar e identificar las causas del incidente.
- Preservar y recolectar evidencias.
- Planificar e implementar las medidas correctivas que correspondan, a los efectos de evitar que el incidente vuelva a ocurrir o en su defecto mitigar su impacto en un futuro.
- Acotar y minimizar el daño provocado en esta oportunidad. Aislar el problema si es posible, por ejemplo, sustituir un equipo o aislar una subred.
- Comunicar a todos aquellos afectados o involucrados en las acciones de recuperación así como escalar el incidente para su tratamiento cuando corresponda.
- Habilitar las acciones de recuperación por el daño provocado cuando corresponda (por ejemplo porque no se cumplió la calidad de servicio comprometida o sencillamente se incumplió un contrato).
- Informar sobre las acciones correctivas a la/s gerencia/s que corresponda/n.

Se adjunta como ejemplo algunos criterios de impacto:

Tabla 3.6. Ejemplo de criterios de impacto

Nivel de Impacto	Descripción
BAJO	Si el INCIDENTE presenta las siguientes características: • Genera interrupciones en las actividades de una persona. • Posiblemente aplique una solución alternativa. • Las actividades que realizan esta persona no genera una interrupción en el servicio ó línea de producción. • Posiblemente genera un impacto económico. No genera impacto legal ni de imagen.
MEDIO	Si el INCIDENTE presenta las siguientes características: • Genera interrupciones en algún proceso. • Posiblemente aplique una solución alternativa. • Las interrupciones del proceso posiblemente generen una interrupción en una parte de la operativa del servicio ó parte de una línea de producción. • Posiblemente genera un impacto económico y/o legal. No genera impacto de imagen.
ALTO	Si el INCIDENTE presenta las siguientes características: • Genera interrupciones en los procesos esenciales. • Posiblemente aplique soluciones alternativas. • La interrupción del proceso esencial genera la interrupción total de la operativa del Servicio ó línea de producción. • Genera un impacto económico, legal y de imagen

También es necesario llevar una estadística de los incidentes ocurridos y que tratamiento se les dio, a efectos de establecer métricas (frecuencia, costo: horas y recursos invertidos, etc.) y analizar la efectividad de los controles.

¿Quiénes deberían participar?

- Equipo de Seguridad
- Operaciones
- Seguridad Física
- Dueños de los Sistemas de Información
- Dueños de los Procesos Estratégicos y Operacionales.

Salida:

- Procedimiento y formatos de gestión de incidentes.
- Eventualmente podría ameritar la conformación de un CSIRT “Computer Response Information Security Team”, en cuyo caso hay que especificar su alcance y responsabilidades.
- Métricas y seguimiento de la gestión de incidentes

3.4.4 Uso de métricas

Es necesario contar con un conjunto de métricas que permitan levantar un llamado de atención, una alerta en el caso que en la elección de controles o bien en su implementación requieran reajustes o reconsideración.

Para cada control debe establecerse uno o más métricas a los efectos de conocer el grado de satisfacción del objetivo. Una vez conocido este grado, debe ser posible saber de forma concreta si el objetivo fue alcanzado o dicho de otra manera, si ese grado de seguridad es suficiente o se requieren reajustes.

Debe estar claro el procedimiento para llevar a cabo la medición, qué es lo que se va a medir, los criterios de satisfacción de forma objetiva y cuantificable

Entrada

- Normas y/o Estándares
- Procedimientos y/o controles SGS

Acción

- Identificar el objeto a ser medido
- Método y función de la medida
- Definir la frecuencia

¿Quiénes deberían participar?

- Gerencias involucradas
- Responsables de proceso
- Equipo de Seguridad

Salida

- Objetivo de control
- Descripción de métrica
- Unidad de medida
- Frecuencia
- Valoración de la métrica
- Fuente de información
- Valor meta

La norma ISO/IEC 27004 especifica los lineamientos para implementar un programa de definición, implantación y ajuste de métricas además de una serie de ejemplos ilustrativos que están alineados con los requerimientos de la norma ISO/IEC 27001. En el Anexo 2 se incluyen algunos ejemplos de métricas.

3.5 Retroalimentación

Esta fase nos sirve para evaluar los resultados de la implementación del Plan de Seguridad y formular recomendaciones de mejora, difundir a los involucrados los resultados de la evaluación, así como diseñar un programa de seguimiento basado en las recomendaciones

considerando plazos y responsables para superar las brechas aún existentes y debilidades detectadas.

3.5.1 Acciones para el cumplimiento de las políticas

Se deben identificar, analizar y aplicar en los procesos de negocio las políticas y normas relativas a la seguridad de la información incluidas en leyes, decretos y reglamentaciones de organismos nacionales e internacionales que sean de aplicación en la organización.

Para lograr el cumplimiento de políticas y normas, es necesario implementar un conjunto de medidas de seguridad, tanto técnicas como organizativas que garanticen la efectividad de los esfuerzos realizados. Todas las medidas adoptadas se establecen a través de un Manual de Seguridad de la Información, los procedimientos y las instrucciones de trabajo definidas.

Todos los miembros de la organización deberán cumplir y velar por el cumplimiento de lo establecido en el SGSI. Para garantizar el cumplimiento de lo establecido por el SGSI, la dirección delega la responsabilidad de supervisión, verificación y monitorización del sistema sobre el Responsable de Seguridad de Información, el cual posea la autoridad e independencia necesarias y dispondrá de los recursos oportunos, para garantizar la correcta operación de todo lo definido en el SGSI. Todos los miembros de la organización deberán cumplir y velar por el cumplimiento de lo establecido en el SGSI.

Por último, la dirección se compromete a facilitar los medios necesarios y a adoptar las mejoras oportunas en toda la organización, para fomentar la prevención de los riesgos y daños sobre los activos, mejorando así la eficiencia y eficacia del SGSI.

Entrada
Políticas y normas

Acción
Definición de estrategias de divulgación de políticas

¿Quiénes deberían participar?
Gerencias involucradas
Equipo de Seguridad

Salida
Evidencias que el personal haya comprendido las políticas (registros)

3.5.2 Auditorias

Según la ISO/IEC 27001, deben realizarse auditorías internas a intervalos planificados para determinar si los objetivos de control, controles, procesos y procedimientos cumplen:
a. Los requisitos de la norma, la legislación y reglamentaciones
b. Los requisitos identificados de la seguridad de la información.
c. Los controles están implementados y se mantienen de forma eficaz
d. Se desempeñan de acuerdo a lo esperado (eficiencia).

Asimismo Debe documentarse, los criterios, el alcance, la frecuencia y los métodos que se llevarán a cabo.

Sea una auditoría de tipo interna o externa nos llevará a estables medidas correctivas, preventivas y/o de mejora para el sistema de gestión de seguridad (SGS)

Figura 3.13. Elementos para la mejora continua de las organizaciones[28]

Entrada

- Normas y/o estándares
- Calendario de la auditoria
- Plan de auditoría basado en un alcance y objetivo
- Competencia de auditores y/o equipo auditor

Acción

- Seleccionar los auditores
- Desarrollo del programa de auditoria
- Desarrollo de lista de verificación
- Ejecución de la auditoria y recopilación de datos

En la selección de los auditores, además de las capacidades específicas en el área de seguridad, deben considerarse:

- Atributos personales: ética, diplomacia, observador, perceptivo, versatilidad, tenacidad, decisión y seguridad.
- Conocimientos y habilidades: estos deberán estar relacionados con: principios, procedimientos, técnicas de auditoría, normas legales y reglamentos.
- Entrenamiento y experiencia en la realización de auditorias
- Procedimientos, técnicas de auditoría y técnicas para recopilar información

¿Quiénes deberían participar?

- Gerente involucrado

[28] Fuente: Elaboración propia

- Responsables de proceso
- Equipo auditor

Salida

- Actas asistencias (apertura y cierre de auditoría)
- Informe de auditoría (véase Anexo 3, un modelo de informe de auditoría)
- Realización de las actividades de seguimiento de la auditoria

Conclusiones:

En este capítulo se ha desarrollado una propuesta de la metodología de gestión de seguridad de la información y tecnologías de la información (TI), la cual consta de cuatro (04) fases que son: Planificación, Diseño, Operación y Retroalimentación, todo esto se encuentra bajo el enfoque de mejora continua especificado en la Norma ISO/IEC 27001:2005.

En cada una de las fases se plantea a nivel de proceso la entrada, acción, quienes se encuentran involucrados y la salida.

Se plantean asimismo algunos ejemplos ilustrativos para tener una idea a la hora de implementarlo

Capítulo 4:
Factores Críticos de Éxito

Podríamos mencionar muchas maneras y pautas de cómo establecer un Sistema de Gestión de Seguridad de la Información y TI (SGS), sin embargo como parte de la experiencia que he obtenido en las empresas les expongo los siguientes resultados:

a. Obtener un soporte visible por parte de los Gerentes y coordinadores (amplia comunicación sobre su apoyo activo al sistema gestión, mostrando su importancia para toda la organización).

b. La organización deberá contar con una política de seguridad, la cual debe estar alineada con su misión y objetivos, se debe ajustar a la cultura organizacional, se debe articular con todas las áreas de la organización para concertar la definición del alcance, la creación y aplicación de normas, procedimientos y aseguramiento de los procesos y servicios ofrecidos.

c. Los requerimientos de seguridad deben estar claramente articulados con las necesidades de la organización. Los cuales deben surgir después de la identificación y clasificación de los activos de información.

d. Realizar un análisis de riesgo que enlace los activos, su criticidad en términos de confidencialidad, integridad y disponibilidad, las amenazas, las vulnerabilidades, los requisitos normativos, legislativos y regulatorios, los controles implementados, los controles propuestos y el riesgo residual.

e. Obtener la aprobación de la Alta Dirección del proceso de implementación.

f. Definir responsabilidades para cada rol del Sistema de Gestión de Seguridad (SGS).

g. Definir el grupo de trabajo transversal para la seguridad (Comité de Seguridad).

h. Realizar permanentemente la concientización, entrenamiento y educación.

i. Establecer métricas para la evaluación del desempeño del Sistema de Gestión de Seguridad, a fin de visualizar nuestro desempeño y si éstas no llegan al nivel esperado poder aplicar mejoras.

j. Elegir criterios y herramientas adecuadas para la evaluación y tratamiento efectivo de riesgos. Será importante involucrar al personal en el uso de la metodología explicándoles y que participen de forma interactiva durante el desarrollo de riesgos.

k. No hacer de la Seguridad de la Información un fin en sí mismo, buscando un ideal de seguridad que se aparte de los requerimientos del negocio o se concentre únicamente en posibilidades tecnológicas.

l. La estrategia de seguridad, está relacionada con los planes estratégicos de negocios y planes operativos, y por supuesto con la misión y visión de la empresa. Los estándares y prácticas de seguridad deben contribuir en esa dirección y estar alineados tanto con los objetivos concretos de corto y mediano plazo como con el largo plazo.

m. El éxito pasa también por hacer el compromiso sustentable y no sólo en la fase de implantación, sino continuar con la fase de gestión, operación y monitoreo, a los efectos del mantenimiento y mejora del SGS.

4.1 Aplicaciones de la guía

Asimismo en lo que respecta a la aplicación de la Guía en este acápite comentaremos las experiencias más relevantes. Cabe señalar que en los más de 13 años que vengo trabajando en los temas de seguridad, 4 de ellos dedicados a desarrollar e implementar sistemas de gestión de seguridad y que por motivos de confidencialidad debo reservar los nombres de las organizaciones:

<u>Empresa 1 (Privado-Telecomunicaciones)</u>

- El alcance del trabajo abarcaba un proceso de gestión de accesos e incidentes de seguridad donde intervenía muchos activos de tecnología de información (TI).
- Si bien existía ya una política corporativa, se desarrollaron políticas específicas para poder establecer directrices de los elementos que no contemplaba para los activos del alcance.
- Se formó un Comité de Seguridad donde los roles mencionados en 3.2.2 fueron asumidos por personal que formaba parte del alcance, se desarrollaron los planes de concientización trabajando en conjunto con el área de RRHH. La metodología de riesgos se aplicó tal cual se indica en la presente metodología (basado en ISO 27005).
- Como se trataba de un proceso dentro de una jefatura aplicamos un Plan de Recuperación de Desastres con escenarios de prueba acotados al alcance del SGS a fin de validar su funcionamiento.
- Para medir el desempeño del sistema de gestión de seguridad inicialmente se establecieron algunas métricas considerándolas relevantes como por ejemplo: cantidad de incidentes cerrados respecto a los incidentes reportados, porcentaje de personas que aprobaron las charlas, porcentaje de controles que se implementaron en las fechas previstas, entre otros. Posteriormente en cada procedimiento se trataba de definirle su

métrica. Se aplicó tal cual los elementos de salida se indican en 3.4.4 en un cuadro de mando.

- Es importante tener en cuenta capacitar auditores internos que estén fuera del proceso del SGS y que las auditorías internas se programen con debida anticipación y traten de cubrir casi todos los dominios en el lapso de un (1) año a fin de evidenciar de que se lleva una seguridad bien gestionada en la organización.
- Se debe tener identificado el personal que participa en el SGS y cuyas competencias, estudios en seguridad deben estar debidamente actualizados en el file de documentos que gestiona Recursos Humanos. No debe olvidarse que si hay personal externo involucrado se debe tener la confirmación de los mismos documentos por parte de la empresa contratada.
- En la gestión de incidentes se emplearon los mismos criterios utilizados en ésta guía metodológica, lo utilizamos en un cuadro de mando llegando incluso a especificar lecciones aprendidas. En este punto es ideal que se lleguen a valorar el coste de los incidentes como por ejemplo: coste de horas-hombre empleadas en tratar los incidentes, coste por no operatividad de un servicio, coste de reconstrucción de un documento altamente sensible, entre otros. Esto sucede cuando nuestros sistemas de gestión alcancen un mayor grado de madurez.
- La implementación del sistema de gestión en esta empresa se logró en 11 meses, donde finalmente obtuvo la certificación ISO 27001. Aquí intervinieron 6 personas, una (1) de ellas a tiempo completo.

<u>Empresa 2 (Estatal-Administración Pública)</u>

- El alcance del trabajo trató dos (02) procesos que brindan servicio de pensiones. Aquí ya existía una política de seguridad, por lo cual se inició identificando el alcance y límites del sistema de gestión. Asimismo ya contaban con una metodología de riesgos para lo cual sirvieron de mucha ayuda los criterios definidos en las tablas 3.1 y 3.2.
- En los talleres de riesgos se convocaba personal de los procesos tomando el criterio sobre su experiencia a fin de que sus aportes en amenazas y vulnerabilidades sea más enriquecido en el análisis y evaluación de riesgos.
- Los acciones derivados del análisis GAP y plan de tratamiento de riesgos conllevaron a un plan de seguridad que siguieron similar esquema de priorización a la figura 3.9.
- Es importante mencionar que para este tipo de organización la aprobación formal de documentos (firma y sello) era importante a fin de evitar la adulteración de algunas de sus páginas.
- Las charlas de concientización se plasmaron con diferentes enfoques de acuerdo al tipo de trabajo que realiza el persona (sea interno o externo). Ejemplo: vigilancia, limpieza, proveedores, personal operativo, etc.
- Una de las estrategias de concientización aplicadas fue dar mini-charlas con una duración no máxima de 5minutos en las ubicaciones del personal a fin de reforzar los temas de seguridad y que también era evaluado con dos (02) preguntas. Esto ayudó mucho a fortalecer conceptos de seguridad.
- Producto del análisis y evaluación de riesgos algunos temas de seguridad eran necesarios ser reforzados lo cual conllevó actualizar el Plan de Concientización y su correspondiente aprobación.

- Se crearon carpetas protegidas donde se almacenó cada evidencia que sustentaba la implementación de controles derivados del plan de tratamiento de riesgos y que los mismos también eran necesarias para futuras auditorias.
- Cada reunión de seguimiento de avance con los responsables de implementación de controles, se plasmaba en un acta de reunión a fin de mantener el compromiso sostenido.
- Mensualmente se realizaba una reunión de Comité de Seguridad a fin de que la Alta Dirección se encuentre permanente comunicado y buscar algún compromiso para reforzar algún punto pendiente del sistema de gestión de seguridad.
- Las pruebas del plan de recuperación de desastres se evidenciaban con fotografías, adicionalmente de contar con un registro indicándose paso a paso la prueba donde al final era firmado por los participantes.
- El establecimiento del sistema de gestión en ambos procesos permitió que la organización alineara sus necesidades de protección de la información como parte de uno de los objetivos de la organización, así como mejorar la conciencia en seguridad de la información en el personal.

Empresa 3 (Privado-Telecomunicaciones)

- Esta empresa es donde actualmente estoy aplicando todo desde cero, para un servicio en un Datacenter.
- Inicié desarrollando y luego difundiendo las políticas de seguridad a la Alta Dirección (Gerentes, Directores y SubGerentes) quienes apoyaron a desplegar la importancia de la seguridad al personal a su cargo.
- Se estableció una metodología de riesgos utilizando los criterios definidos en la presente tesis en combinación con la estructura general de ISO 31000[29], para que luego de la aprobación de la Alta Dirección se llevaran a cabo los talleres de riesgos.
- Se desarrolló un plan de concientización aplicado a toda la organización y cuyas estrategias fueron coordinadas con el área de Recursos Humanos.
- Lo desarrollado a la fecha ha permitido obtener un soporte visible de la Alta Dirección dado que por sus necesidades de negocio y que brindan servicios externos requieren fortalecer sus controles de seguridad de la información. De la misma manera mantener el cumplimiento legal que afecta al sector de telecomunicaciones (secreto de las comunicaciones y protección de datos personales) y además del cumplimiento de contratos con los clientes.

Tener en cuenta que esta Guía es una base y que algunos valores de los criterios planteados puedan variar por cada organización dependiendo de los objetivos de negocio que manejen (ejemplo, alta disponibilidad, alta sensibilidad de su información, eficiencia de procesos, entre otros) que obligue a cambiar los tiempos, porcentajes, cantidades. Hay que evitar perder el foco principal de los objetivos de negocio que sin ello un SGS quedaría a la deriva y perdería el interés de la Alta Dirección.

[29] International Standard ISO 31000:2009 – Risk management – Principles and guidelines

CONCLUSIONES

- ✓ La implementación de estándares como lo desarrollado en el presente trabajo ISO 27002 e ITIL proporcionan diferentes ventajas a cualquier organización como:
  - Aumento de la seguridad efectiva de los sistemas de información
  - Correcta planificación y gestión de la seguridad
  - Garantías de continuidad de negocio
  - Alianzas comerciales y comercio electrónico más seguros
  - Mejora continua a través del proceso de auditoría interna
  - Incremento de los niveles de confianza de nuestros clientes y socios
  - Aumento del valor comercial y mejora de la imagen de la organización
  - Auditorias de seguridad más precisas y fiables
  - Menor responsabilidad civil

- ✓ El Sistema de Gestión de Seguridad es parte de la estrategia del negocio, como tal responsabilidad de la Alta Dirección.

- ✓ La implementación de controles es un proceso selectivo.

- ✓ La seguridad de la información se enmarca dentro de un proceso continuo.

- ✓ Es posible implementar un modelo ISO 27002 apoyado en ITIL.

- ✓ Es visto que cualquier aplicación de una metodología de buenas prácticas es una organización trae ventajas en la aplicación de una política de seguridad de la información. Los beneficios que las organizaciones pueden obtener son grandes como:
  - La seguridad de la información está alineada con los procesos de negocio, debido a la integración que ITIL-ISO 27002 lo permite.
  - La seguridad está bien definida y estructurada, por la definición de roles y responsabilidades permite controlar la eficiencia de los controles seleccionados.
  - Nada es más importante en la seguridad que permanente auditoría y control. ITIL e ISO 27002 lo permiten debido al enfoque PHVA en la optimización de procesos y servicios.

- ✓ En este trabajo se han descrito los principales elementos considerados en la definición de un Modelo de Gestión de Seguridad de la Información y TI (SGS). Se expuso un breve análisis de la relevancia y urgencia del tema, y se presentaron las principales normas y estándares relacionados con la gestión de seguridad de información, y que fueron consideradas como base para este modelo. Además, se discutió brevemente los diversos aspectos involucrados en la definición de un modelo de gestión de seguridad de información y TI, y se presentó un esquema del modelo propuesto. Si bien este modelo puede parecer muy simple, esto se debe a que todas sus actividades engloban de una u otra forma lo detallado en las normas y estándares presentados, pero bajo un esquema generalizado y adaptable a cada organización. Se debe tener presente que este modelo es totalmente ajustable y que puede ser dimensionado conforme a las particularidades y tamaño de la organización en la cual pueda ser implementado.

- ✓ La seguridad de la información no es un simple cumplimiento, tampoco ninguna solución tecnológica que por sí sola pueda protegernos ante un ataque y proteger nuestra información. Es necesario implementar en una organización la seguridad con un enfoque integral, es decir con el establecimiento de objetivos estratégicos de seguridad, para luego identificar nuestros riesgos, proteger lo más importante, sustentar mediante un plan de seguridad y optimizar para el desempeño del negocio.

- ✓ El establecimiento de un Sistema de Gestión de Seguridad de la Información y TI (SGS) en una organización es de gran utilidad al proporcionar la metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos del negocio que tengan que ver con la información.

- ✓ Para llevar a cabo un SGS es fundamental realizar un plan de seguridad del mismo adaptado a las necesidades y el perfil de la organización (visión, misión y objetivos estratégicos), que sea claro, concreto y ajustado a la realidad de la organización lo cual es clave para evitar problemas y errores de interpretación a la hora de insertar el modelo en la rutina normal de trabajo.

- ✓ El SGS ha de ser dinámico y fácilmente adaptable a los cambios y las mejoras a introducir en la organización, la aplicación del modelo PVHA (Planear Hacer Verificar y Actuar) es fundamental, basado en el concepto de mejora continua, la competencia en su manejo puede ser de gran utilidad en el manejador de procesos de cualquier empresa en cualquier sector, no solo en el contexto de un SGS.

- ✓ Una “inteligente” definición del alcance puede hacer que el proyecto de definición e implantación de un SGS sea un proyecto alcanzable y asumible por la organización o, en caso contrario, un proyecto elefante que conduzca al desaliento de los que participan y al fracaso del mismo.

- ✓ Hay que destacar que hay responsabilidades claves, fundamentales para que el SGS alcance el nivel de madurez adecuado, de ellos el Responsable de Seguridad. Así esta metodología plantea diversas responsabilidades que pueden ser aplicados por la organización dentro de un equipo de seguridad.

- ✓ Es relevante que las organizaciones conozcan el nivel de madurez requerido para alcanzar una cultura sólida de seguridad. Así cada persona con el papel que desempeña dentro de una organización es un actor importante en la garantía de la seguridad, quien debe estar consciente de los riesgos de seguridad y de las medidas preventivas a tomar.

- ✓ Los estándares tales como ISO 27002 e ITIL deja en manos de cada organización el grado de inversión en la gestión del riesgo.

- ✓ Para garantizar la seguridad de los activos de la información se tiene que desarrollar una gestión orientada a mitigar el impacto de los riesgos para lo cual se ha de diseñar un método de evaluación de riesgos completo que ha de permitir conocerlos y afrontarlos de forma coordinada, como lo hace el método de evaluación incluido en el trabajo.

- ✓ Mitigar el riesgo suele ser una buena opción, pero también la más cara. Priorizar siempre en función del análisis del riesgo.

- ✓ Para escoger los controles a implementar, éstos se deben justificar en base a las conclusiones obtenidas del análisis, evaluación y tratamiento del riesgo a los cuales son sometidos los activos de información, teniendo como base la confidencialidad, integridad y disponibilidad.

- ✓ Una vez que los controles se encuentren implementados, éstos deberán ser revisados con regularidad para verificar que su funcionamiento sea el esperado (de acuerdo a la métrica definida).

- ✓ Es contraproducente desarrollar procedimientos de seguridad excesivamente complejos, porque limitan la operatividad y dificultan la toma de decisiones rápidas.

- ✓ No es necesario el desarrollo de un procedimiento o documento por cada uno de los controles escogidos, sino que es más aconsejable agrupar diferentes controles para hacer más utilizable el sistema. Recordemos que la solución más sencilla suele ser la más eficaz ya que es más fácil de implantar y de mantener.

- ✓ Es requerido que los responsables dediquen un tiempo fundamental al diseño del plan sobre todo la descripción general y la primera evaluación de riesgos.

- ✓ Para alcanzar el nivel de madurez en seguridad adecuado es fundamental la formación y sensibilización sobre la importancia de la seguridad a todos los miembros de la organización. Asimismo cuando se sensibilice al personal respecto a las amenazas, se deben poner a disposición una amplia gama de documentación disponible para todo el personal. En ello deben incluir detalles sobre las consecuencias de los ataques exitosos, no hablar de estos ataques en términos de cómo la seguridad se evitó sino en el impacto en el negocio o de los objetivos de seguridad de la organización.

- ✓ Debe realizarse una revisión completa del sistema al menos una vez al año. Para ello se pueden planificar varias auditorías internas durante el año e ir revisando el sistema por partes. De este modo, sólo una parte de la organización estará pendiente de la auditoría, mientras que el resto puede continuar con su trabajo diario sin ninguna alteración.

- ✓ Al finalizar la auditoría interna es necesario llevar a cabo dos tipos de acciones, unas para subsanar las incidencias encontradas y otras para mejorar el sistema. Estas acciones se realizan dentro de la última fase del modelo PVHA, vista con anterioridad, la Fase de Mejora.

- ✓ Hago hincapié que la aplicación de una política de seguridad de la información no es una tarea fácil, ni siquiera con la metodología propuesta. Ello necesitará el apoyo de la Alta Dirección y de la toma de conciencia en la importancia de la seguridad tanto interna como externa.

- ✓ En resumen se ha diseñado un SGS ajustado a las necesidades de una organización cuyo principal activo es la información y que utilizan las tecnologías de información, de acuerdo con las buenas prácticas de ITIL e ISO 27002.

BIBLIOGRAFÍA

Baars, Hans.; Hintzbergen, Kees.; Hintzbergen, Jule.; Smulders, André. (2009). *The Basics of Information Security – A Practical Handbook.* 18g. Netherlands: Creative Commons Attribution

Bramont-Arias Torres, Luis Alberto. "Delitos Informáticos". *Revista Peruana de Derecho de la Empresa Derecho Informático y Teleinformática Jurídica*. Lima N° 51: 1-10

Caro Bejarano, María José. (2011). "La Protección de las Infraestructuras Críticas". *IEEE.ES.* España 27 de Julio del 2011, 021:1-7

Clinch, Jim. (2009). "Itil v3 and Information Security". *Clinch Consulting OGC*. Reino Unido. Mayo 2009.

Díaz Piraquive, Flor Nancy. (2008). "Principales estándares para la seguridad de la información IT". *Revista EOS* Madrid enero-abril 2008. No 2: 77-106

Gobierno de Chile (2012). "Guía metodológica 2012: Programa de mejoramiento de la gestión sistema de seguridad de la información". En línea internet. 30 de noviembre 2012. Accesible en http://www.mop.cl/acercadelmop/PMGSSI/Guia_Metodologica2012.pdf

González Gorostiza, Antonio. (2011). INTECO Protección de Infraestructuras Críticas ¿un nuevo reto para la tecnología?. En línea Internet. 30 de Julio del 2012. Accesible en http://enise.inteco.es

IT Governance Institute (2008). Aligning Cob iT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit ® A Management Briefing From ITGI and OGC. En línea internet. 30 de noviembre del 2012. Accesible en http://www.best-management-practice.com/gempdf/Aligning_COBITITILV3ISO27002_Bus_Benefit_9Nov08_Research.pdf

ISO 27001 Security (2012). Information Security Standards. En línea internet. 30 de agosto 2012. Accesible en http://www.iso27001security.com/index.html

ISO 31000 (2009). Risk Management – Principles and Guidelines. En línea internet. 20 de mayo 2013. Accesible en http://www.aryanapm.com/Files/ISO-31000.pdf

Mancera, S.C. (2011). "Seguridad de la Información en un mundo sin fronteras". Ernest & Young Global 1-20.

Martínez Martínez, Evelio; Serrano Santoyo, Arturo (2012). La Brecha Digital. En línea Internet. 18 de julio del 2012. Accesible en http://www.labrechadigital.org/labrecha/

Ministerio de Comunicaciones de Colombia (2008). Programa Gobierno en Línea-Documento de Políticas de Interoperabilidad. En línea Internet. 30 de julio del 2012. Accesible en http://programa.gobiernoenlinea.gov.co

Norma Técnica Peruana NTP-ISO/IEC 27001:2008. Indecopi. En línea internet. 30 de Agosto del 2012. Accesible en http://www.ongei.gob.pe/banco/ongei_normas_detalle.asp?pk_id_normas=220

Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). Resolución Ministerial N° 129-2012-PCM. En Línea Internet. 30 de Agosto del 2012. Accesible en http://www.ongei.gob.pe/banco/ongei_normas_detalle.asp?pk_id_normas=220

Ontoria Gonzalo, Sandra. (2011*). Gobierno y Modelado de Seguridad de la Información en las Organizaciones*. Tesis de título. España: Escuela Politécnica de Madrid.

Pallas Mega, Gustavo. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*. Tesis de máster. Uruguay: Instituto de Computación – Facultad de Ingeniería - Universidad de la República.´

Peltier, Thomas,; Peltier, Justin,; Blackley, John. (2005). *Information Security Fundamentals*. USA: CRC Press.

Riesgos Globales 2012 (2012). Resumen ejecutivo. En línea Internet. 30 de Julio del 2012. Accesible en http://www3.weforum.org/docs/WEF_RRN_GlobalRisksReport_ExecutiveSummary_2012_ES.pdf

Rodríguez de Roa Gómez, Álvaro. (2012) Seguridad de Servicios de Tercerización de TI y su evolución: ¿necesidad o realidad?. 15 de Noviembre del 2012. Accesible en http://www.isaca.org/Education/Conferences/Documents/LatinCACS-ISRM-Presentations/233.pdf

Sánchez Gómez-Merelo, Manuel. (2012). "Protección de Infraestructuras Críticas, un nuevo reto para la Seguridad". En Línea Internet. 30 de julio del 2012. Accesible en http://manuelsanchez.com

Universia México. (2012). TIC Alertan por la persistente brecha digital. En línea Internet. 15 de julio del 2012. Accesible en http://noticias.universia.net.mx/ciencia-nn-tt/noticia/2012/04/05/921925/alertan-persistente-brecha-digital.pdf

Villena Aguilar, Moisés Antonio. (2006). *Sistema de Gestión de Seguridad de la Información para una institución financiera*. Tesis de título. Lima: Pontificia Universidad Católica del Perú.

Wellington Redwood, Quint. (2009). *Fundamentos ITIL v3 Foundation*. Versión ES-08JUN3. Madrid.

ANEXO A : Glosario de Términos

En la elaboración de este glosario se ha tenido en cuenta las definiciones recogidas de los principales estándares y normas referidas a la gestión de seguridad y tecnologías de la información. Para cada término se ha seleccionado el más adecuado en el contexto del presente trabajo.

Auditoria de seguridad: Procedimiento usado para verificar que se están llevando a cabo controles en un sistema de información y que éstos son adecuados para los objetivos que se persiguen. Incluye el análisis de las actividades para detectar intrusiones o abusos dentro del sistema informático.

Bomba Lógica: Es una parte de código construido dentro de un software, el cual se activará cuando se cumplan ciertas condiciones específicas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

Crackers: Es una persona que tiene fines maliciosos o de venganza mostrando sus habilidades equivocadamente haciendo daño por diversión.

CSIRT: Siglas en ingles "Computer Security Incident Response Team", que significa Equipo de Respuesta a Incidentes de Seguridad Informática.

Disponibilidad: Asegurar el acceso a la información por parte de los usuarios autorizados en el momento que ellos lo requieran.

Divulgación: Conjunto de acciones de tipo comunicacional y de transferencia de conocimientos, ejecutada por diversos medios, con el fin de mejorar su nivel de conocimiento y por lo tanto de competencia.

Firma Digital: Es un método para confirmar si la información fue producida o enviada por quien dice ser. Permite que aquellos trámites y servicios se puedan firmar digitalmente con un certificado de firma digital, emitido por una Entidad de Certificación Digital Abierta.

Implementación: Conjunto de acciones encaminadas a poner en práctica y aplicación las disposiciones planificadas y diseñadas por la Organización

Información: Se refiere a toda comunicación o representación de conocimiento, como datos, en cualquier forma con inclusión de formas textuales, numéricas, gráficas narrativas o audiovisuales, y en cualquier medio, ya sea en digital, en papel, en pantallas de computadora, audiovisual u otro

Ingeniería social: Consiste en engañar a alguien para que proporcione información valiosa o acceder a la información o recurso de una organización.

Integridad: Característica que asegura que la información no haya sido alterada ni modificada de forma no autorizada durante su procesamiento, transporte o almacenamiento.

Propietario del Activo: Es el responsable de coordinar con el Responsable de Seguridad las medidas de seguridad aplicables para proteger los activos de información. Asimismo, es el responsable de clasificar la información y de definir qué usuarios (custodios de la información) deberán tener permisos de acceso a la información, de acuerdo a sus funciones y competencias

Vulnerabilidad: Es cualquier debilidad en los sistemas que puede permitir a las amenazas causar daño y producir pérdidas.

ANEXO B : Métricas Relacionados con la Gestión de Seguridad

Fase ITIL	Proceso	Métrica	Descripción
DISEÑO DEL SERVICIO	Gestión de la Disponibilidad	Índice de resistencia a la disponibilidad	Resistencia de nuestra infraestructura hacia la protección de servicios
		Índice de mejora continúa de la disponibilidad	Mide la proactividad con la que se busca mejorar el servicio de disponibilidad
	Gestión Seguridad de la Información	Cantidad de medidas preventivas implementadas	Mide la Cantidad de medidas de seguridad preventivas implementadas como respuesta a amenazas de seguridad identificadas
		Cantidad de incidentes graves de la seguridad	Cantidad de incidentes de seguridad identificados, clasificados por categoría de gravedad
		Cantidad de pruebas de seguridad	Cantidad de pruebas de seguridad llevados a cabo
		Cantidad de defectos identificados durante las pruebas de seguridad	Cantidad de defectos identificados en los mecanismos de seguridad durante las pruebas
TRANSICIÓN DEL SERVICIO	Gestión de Cambios	Tasa de eficiencia de los cambios	Mide la eficiencia a la hora de gestionar los cambios
		Tasa de cambios replanificados	Mide la eficiencia de implementar cambios en el tiempo estipulado
		Tasa de cambios no autorizados	Porcentaje de cambios que se saltaron el proceso de gestión de cambios
		Tasa de incidencias provocadas por el cambio	Porcentaje de cambios que provocaron incidencias
	Gestión de la Configuración y Activo del Servicio	Tasa de acierto de la CMDB	Mide la precisión de la información contenida en la CMDB
		Número de incidencias relacionadas con información incorrecta de un CI	Mide el número de incidencias causadas debido a una información imprecisa de la CMDB
		Tasa de CMDB	Mide qué porcentaje de la infraestructura está comprendida en la CMDB
		Tasa de propiedad de los Cis	Mide qué parte de la infraestructura no tiene asignado un propietario
	Gestión de Versión y del Despliegue	Tasa de eficiencia de las entregas	Mide la eficiencia a la hora de manejar las entregas
		Tasa de entregas replanificadas	Mide la eficiencia de implementar entregas en el tiempo estipulado
		Tasa de entregas defectuosas	Mide el porcentaje de entregas que causaron incidencias
OPERACIÓN DEL SERVICIO	Gestión de Incidencias	Número total de incidencias	Número de incidencias que ocurren dentro de la infraestructura
		Número de incidencias con prioridad alta	Número de incidencias de prioridad alta que han ocurrido
		Tasa de resolución de incidencias	Mide el porcentaje de resolución de incidencias de negocio
	Gestión de Problemas	Tasa de repeticiones de Incidencias	Mide la efectividad previniendo la repetición de incidencias
		Número de problemas graves	Mide cuantos problemas graves se han producido en la infraestructura
		Tasa de resolución de problemas	Porcentaje de problemas solucionados
		Tiempo medio de resolución de problemas con prioridad alta (días)	Mide la rapidez resolviendo problema
	Gestión de Accesos	Número total de solicitudes de acceso	Número de solicitudes de acceso, solicitud de servicio, RFC, etc. que se dan dentro de la infraestructura

ANEXO C : Modelo de Informe de Auditoría

Informe de Auditoria Interna			
Proceso(s) Auditado(s):			
Alcance de la auditoria:			
Norma(s) de referencia para la realización de la auditoria:			
Auditor Principal:		**Equipo Auditor:**	
Fecha de realización de la auditoria:		**Fecha de presentación del informe:**	
Auditado(s):			
Herramientas de trabajo utilizados en la auditoria:			
Documento(s) Revisados			**Ref. Cláusula/ Control**
Estado del Sistema de Gestión (Cantidad y Detalle):			
Fortalezas:			
Oportunidades de Mejora:			
No conformidades:			
Conclusiones:			
Firma del auditor principal:		**Fecha:**	