MAESTRÍA EN GERENCIA DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

ELABORACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA RADICAL CIA. LTDA. EN LA CIUDAD DE QUITO PARA EL AÑO 2014

Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de la Información

Profesor/a Guía:
Hugo Arcesio Banda Gamboa, MSc, PhD.

Autor:
Carlos Castro Quinde

Año
2014

DECLARACIÓN DEL PROFESOR GUÍA

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

Hugo Banda Gamboa

Philosophy Doctor (PhD)

C.I.: 1702779503

DECLARACIÓN DE AUTORÍA

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

Carlos Oswaldo Castro Quinde
CI: 0602991333

AGRADECIMIENTOS

El presente trabajo no podría haber sido realizado sin el constante apoyo recibido por parte del doctor Hugo Banda Gamboa, quien como tutor, me ha apoyado y dirigido para la consecución del mismo. Me es muy grato el haber sido estudiante de la Universidad de las Américas y formar parte de los excelentes grupos de profesionales, entre personal docente y administrativo, que compartieron conmigo durante este tiempo.

Agradezco a la empresa RADICAL CIA. LTDA y en especial a sus directivos por haberme facilitado y permitido realizar la presente investigación en sus instalaciones y exponer los resultados de la misma.

Un agradecimiento especial a mi amada esposa, quien ha influenciado con sus consejos y sabiduría, propios de alguien que ama a su compañero de vida. Mi amada familia se merece un reconocimiento especial por sus constantes impulsos hacia mí.

DEDICATORIA

A mi amada esposa Patricia Portero, mi excelente, sabia y divina madre Lucía Quinde y a mi querida familia, con todo mi amor.

RESUMEN

El presente trabajo representa los riesgos en Seguridad de la Información que la empresa RADICAL CIA. LTDA. enfrenta y los cuales están asociados a los problemas que se han identificado a través de sus directivos y en base a entrevistas con ellos.

Para identificar a mayor detalle los problemas y la solución a los mismos, se utiliza el método de Marco Lógico. Una vez identificada la solución se procedió con la implementación de la misma, de acuerdo al método establecido y para lo cual se realizó un Análisis de brecha, Análisis de Riesgos e Identificación de los activos de información que son parte esencial de la organización; Análisis de vulnerabilidades relacionadas con estos activos, identificación de los atributos de la información y nivel de impacto en cada uno de ellos, entre otros análisis.

Adicional a este análisis y de acuerdo al método empleado, se proponen tres proyectos a manera de ejemplo, los que permitirán a la organización una reducción del riesgo a un nivel establecido por los directivos y acorde con el nivel de madurez que la organización requiere. Una vez que se hayan implementado estos proyectos, se procederá con un análisis de brecha a fin de determinar que la organización ha alcanzado el nivel de madurez propuesto o que deberá realizar nuevos proyectos, modificaciones u otras acciones acorde al ciclo de mejora continua.

Este método propuesto fue evaluado por los directivos de la organización, luego de lo cual acordaron la implementación del mismo, partiendo de una especialización de su personal en materia de Seguridad de la Información y en la familia de normas ISO 27000 e ISO 31000.

ABSTRACT

This work represents the risks of information security that the company RADICAL CIA. LTDA. faces and which are associated with the problems that have been identified by their managers, based on interviews with them.

To identify in more detail the problems and the solution, the method used the Logical Framework. Once the solution was identified we proceeded with the implementation, according to the established method for which a Gap Analysis, a Risk Analysis and the identification of Information Assets were carried on; this analysis are an essential part of this work, and they allowed to identify vulnerabilities related to these assets, Identification of the attributes of the information and impact level in each of them.

In addition to these analysis and in accordance with the used method, three projects are proposed as an example, which would enable the organization to reduce the risk to a level established by the management, in accordance with the maturity level that the organization requires. Once these projects have been implemented, the gap analysis will proceed to determine that the organization has reached the proposed level of maturity or to carry out new projects, modifications or other actions according to the continuous improvement cycle.

This proposed method was evaluated by the managers of the organization in which they agreed on its implementation, starting from a training of its staff in the field of Information Security and the family of ISO 27000 and ISO 31000 standards.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad con la aparición de la tecnología informática y el apoyo constante que ésta brinda a los procesos del negocio, las empresas u organizaciones se han visto en la necesidad de ofrecer sus servicios a través de los sistemas informáticos. Estos sistemas informáticos tienen la capacidad de almacenar información muy valiosa para la empresa y por ende es el principal activo a salvaguardar. La información es dependiente de la naturaleza del negocio y deberá ser gestionada y tratada con una estrategia diferente en cada caso, sea por los datos que se almacenan o por la criticidad que éstos representan.

Las implicaciones sobre actividades cibernéticas maliciosas tales como: la ciberdelicuencia y el espionaje cibernético que existe en la actualidad, tienen como principales objetivos el ataque a las empresas, gobiernos o negocios para dañar su imagen, obtener información, realizar fraudes o simplemente protestas ideológicas.

Un ejemplo de ejecutores de ataques son los hackers quienes son individuos que utilizan sus habilidades, destrezas y recursos informáticos para invadir sistemas informáticos ajenos con el fin de obtener información y creen que ponerla para consumo general es un extraordinario bien. (Hiamnen, 2001). Actualmente los hackers han dejado de ser personas que intenten ganar reconocimiento o fama dentro de su ambiente informático a través del ataque temporal de algún servicio o computador. Existen grandes organizaciones criminales que están en plena capacidad de provocar desastres de índole económico, social, gubernamental, motivados por creencias, tendencias políticas o sociales (Economía, 2013). Los hackers son responsables del mayor número de violaciones de seguridad y constituyen un 40% de todas las infracciones a nivel mundial. (Symantec, 2013)

Debido a este tipo de ataques, fugas de información, daño a mecanismos tecnológicos de servicios existe la Seguridad de la Información, que tiene como propósito precautelar los atributos de la información y la continuidad del negocio, previniendo los riesgos y minimizando el impacto que la explotación de una vulnerabilidad podría generar, afectando a los procesos del negocio, reduciendo sus ingresos, dañando su imagen, credibilidad y disponibilidad. La protección de la información hace referencia a tres principales propiedades que la misma debe tener: disponibilidad, confidencialidad, integridad. (NTE INEN- ISO/IEC 27000, 2013)

Esta necesidad de precautelar los activos de información ha permitido que la seguridad de la información y gestión del riesgo se conviertan en mecanismos importantes dentro de las organizaciones, al punto que han dejado de ser actividades específicas y pasaron a ser entes que evolucionan al ritmo organizacional, alineados con los objetivos estratégicos y con influencia en la toma de decisiones.

Por lo expuesto anteriormente, y con el fin de resolver estas necesidades dentro de las organizaciones, surgieron estándares internacionalmente aceptados para la gestión del riesgo y la seguridad de la información, tales como la familia de normas ISO/IEC 27000, métodos de Gestión y Análisis de Riesgo como MAGERIT, ISO 31000, ISO 27005, los cuales serán tratados en este trabajo.

Adicionalmente, en el presente proyecto se aplica un método práctico para el Análisis y Solución de un Problema, denominado “Método del Marco Lógico”, el cual proporciona las directrices necesarias para entender el problema, sus causas en forma detallada, y los efectos que ocasionan; de la misma forma, nos permite determinar los objetivos que se desea conseguir basados en la resolución de las causas del problema identificado inicialmente.

CAPÍTULO I

1 GENERALIDADES

1.1 TEMA

Elaboración de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa RADICAL CIA. LTDA. en la ciudad de Quito para el año 2014.

1.2 ANTECEDENTES

Actualmente las organizaciones cuentan con sistemas de información para brindar servicios, los cuales están expuestos a un gran número de amenazas que aprovechan las vulnerabilidades existentes para causar daño o tomar control sobre ellos. Estas amenazas pueden someter a los activos de información críticos a diversas formas de fraude, sabotaje, espionaje o vandalismo sin que los administradores o dueños de los activos los conozcan.

Los virus informáticos, los ataques informáticos, el hacking, hacktivismo, son algunos de los ejemplos comunes a los cuales las organizaciones están expuestas. Estos tipos de amenazas son comunes pero también es importante que se conozcan otros tipos de amenazas, a los cuales la empresa está expuesta y no necesariamente son algunas de las mencionadas anteriormente, ya que existen algunas que son causadas por desconocimiento en el uso de la información.

La seguridad de la información tiene como fin la protección del principal activo de una organización, la información, de una amplia gama de amenazas existentes dentro del ámbito tecnológico, natural y humano. La correcta protección de la información, a través de controles, permiten y

garantizan la continuidad del negocio, minimizando los riesgos y precautelando la Confidencialidad, Integridad y Disponibilidad de la información.

La información, junto a los procesos y todos los sistemas que utilizan esta información son activos primordiales de una organización. Los atributos de la información, mencionados anteriormente, pueden llegar a ser esenciales para mantener una competitividad, conformidad legal, imagen empresarial y rentabilidad económica, de manera que permita a la organización cumplir con los objetivos estratégicos y asegurar sus beneficios económicos.

La seguridad informática y la seguridad de la información no significan lo mismo pero es primordial que estos dos términos converjan para garantizar los atributos de la información.

La seguridad informática puede ser dividida en tres importantes disciplinas que son: Seguridad lógica, seguridad física y seguridad ambiental, las cuales deben interactuar constantemente para mitigar los riesgos y minimizar el impacto ante cualquier incidente de seguridad de la información (Ramos, 2009).

Dentro de la Gestión de la seguridad de la información existen algunos métodos que nos permiten asegurar y garantizar los atributos de la información, por tal motivo, se introduce las siglas SGSI que hacen referencia a un Sistema de Gestión de Seguridad de la Información, el cual es un método de gran utilidad para las organizaciones ya que proporciona los lineamientos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.

Un Sistema de Gestión de Seguridad de la Información es indiferente al tamaño de la organización y sus requisitos se derivan de tres fuentes principales:

- Una fuente se deriva de la correcta evaluación de los riesgos que afronta una determinada organización,
- Otra fuente son los requerimientos legales, normativos y contractuales que deben satisfacer a una organización, accionistas, socios, proveedores y al ambiente socio-cultural.
- Otra fuente es el conjunto de principios, requisitos, objetivos de negocio y requerimientos comerciales para el procesamiento de información. (Murillo, 2012)

El Sistema de Gestión de Seguridad de la Información no es un sistema estático, sino que para que sea de completa utilidad para la organización, deberá ser revisado y mejorado continuamente. Basado en esta continua revisión y mejora a la que está expuesto un SGSI, se determina que la Gestión de Seguridad de la Información es un proceso de mejora continua.

Adicionalmente, para que un SGSI brinde los resultados esperados es importante que esté sometido a auditorías, acciones correctoras, análisis de los datos y revisiones por parte de las direcciones. También es primordial que la organización esté completamente alineada y adopte como política empresarial este método, partiendo desde la alta gerencia e incluya a clientes y proveedores a través de la provisión de sus bienes o servicios. (NTE INEN- ISO/IEC 27000, 2013)

1.3 OBJETIVOS

1.3.1 Objetivo General

Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa de Seguridad Informática RADICAL CIA. LTDA.

1.3.2 Objetivos específicos

- Analizar la situación actual de la empresa RADICAL CIA. LTDA.
- Identificar los procesos, actores, activos de información para el determinar y analizar las causas del problema de la empresa RADICAL CIA. LTDA.
- Realizar un análisis de riesgo en base a la selección de una metodología para Gestión y Análisis de Riesgo.
- Proponer mecanismos de mejora que permitan incrementar el nivel de Seguridad de la Información para la empresa RADICAL CIA. LTDA.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

En la actualidad no existen estadísticas exactas que indiquen las pérdidas de información por ataques cibernéticos, fugas de información u otros delitos informáticos que las empresas enfrentan y el daño que estas realizan sobre una organización, además es muy difícil estimar el valor económico que una empresa puede dar a sus activos de información, pero sí se lo podrá cuantificar en niveles de importancia o el impacto que ésta tiene para un negocio determinado, dependiendo de las amenazas

existentes y los riesgos, los cuales pueden ser internos como externos. (Andes, 2012).

Dentro de las amenazas internas se encuentran los empleados, quienes se han convertido en un foco principal de incidentes de seguridad. El descontento, la venganza, el daño y el acceso a la información sensible son la mezcla primordial que un empleado podría utilizar para su beneficio económico, pero, no todos los incidentes informáticos involucrados con la información tienen una motivación de este tipo. En ocasiones puede existir una falta de sensibilización por parte de la organización, desconocimiento o errores involuntarios.

La empresa RADICAL CIA. LTDA, sobre la cual se desarrolla el presente proyecto, no está libre de esta problemática ya que carece de mecanismos y políticas de control de la Seguridad de la Información que han dado origen a fugas de información, pérdidas económicas, imagen empresarial desmejorada y no se cuenta con una identificación de los riesgos de la información que la empresa afronta. Esta problemática empresarial es analizada a detalle dentro del Capítulo III - Análisis en el dominio del problema.

Para mitigar de alguna manera los riesgos a los cuales se encuentra expuesta la información, se desarrolla un Sistema de Gestión de Seguridad de la Información, sobre el cual se construye la norma ISO 27000, el cual se basa en el análisis de riegos, control de activos de información estableciendo políticas y controles, así como también, impulsando la divulgación y concientización de estas políticas, incorporando la mejora continua, con la finalidad de reducir, mitigar o aceptar los riesgos.

El desarrollar un Sistema de Gestión de Seguridad de la Información permitirá a la organización garantizar que los riesgos de la información sean minimizados o asumidos, dependiendo del caso, pero partiendo del conocimiento y la gestión de los mismos, todo esto en forma documentada, estructurada, eficiente y adaptada para los cambios o evoluciones que uno o varios riesgos puedan generar en cada activo de la información identificado.

1.5 ASPECTOS METODOLÓGICOS

El presente estudio es del tipo no experimental descriptivo; no experimental ya que no interviene el investigador en ninguna variable y descriptivo porque permite la identificación de hechos relacionados con el estudio a fin de diseñar modelos para su resolución. (Bernal, 2006, pp. 112). Adicionalmente se utilizan métodos inductivos y deductivos que nos permiten encontrar conclusiones generales partiendo de hechos particulares. Estos métodos de estudio permiten la verificación de los resultados con base en la fundamentación teórica.

El presente proyecto y su análisis fue fundamentado en: Entrevistas con Directivos de la Organización y empleados de alta jerarquía quienes fueron identificados por los directivos como personal calificado para brindar información, estudio teórico para el desarrollo del análisis del problema y solución, y observación directa para determinar los activos de la información que son parte del presenta análisis.

La población determinada para el proyecto está compuesta por 15 empleados quienes mantienen relación de dependencia con la empresa y cuyas oficinas están en la ciudad de Quito.

CAPÍTULO II

2. FUNDAMENTACIÓN TEÓRICA

2.1 MÉTODO DEL MARCO LÓGICO

La metodología del marco lógico es una herramienta útil que puede ser utilizada en todas las etapas de un proyecto y que nos facilita el proceso de conceptualización, diseño, elaboración y evaluación. Esta metodología se centra en la orientación de los objetivos a cumplir, los grupos a los cuales se está beneficiando y el facilitar la comunicación entre las partes interesadas.

El método fue elaborado, originalmente, para cubrir tres problemas comúnmente identificados en la elaboración de un proyecto:

- Planificación de los proyectos imprecisos, con múltiples objetivos y que no se encontraban completamente alineados con las actividades de un proyecto.
- Proyectos sin ejecución exitosa, en el que el alcance y responsabilidad del gerente del proyecto no estaba definida en forma clara.
- La carencia de una imagen precisa de cómo luciría un proyecto con éxito, de forma que los evaluadores no contaban con una base para determinar lo que ha sido planificado con la realidad del proyecto.

La metodología se enfoca en determinar claramente el análisis del problema, análisis del personal involucrado, objetivo de cumplimiento jerárquico y selección de una estrategia óptima de solución. Además

contempla dos etapas que son desarrolladas durante las fases de identificación y planificación de los proyectos:

- La etapa de identificación del problema y alternativas de solución, en la que se analiza la situación actual para crear una visión de la situación que se desea obtener y seleccionar las estrategias para conseguirla. La idea principal es que los proyectos son diseñados para resolver los problemas que los beneficiarios afrontan continuamente y responder a sus necesidades e intereses. Dentro de esta etapa se debe realizar cinco tipos de análisis: Análisis de involucrados, análisis del problema (imagen de la situación actual), análisis de objetivos (imagen de la situación deseada), análisis de las estrategias (comparación entre las soluciones planteadas), selección de la alternativa óptima.
- La etapa de planificación, en la que la idea del proyecto pasa a ser un plan operativo para la ejecución y consecución de los objetivos planteados.(Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES), 2005, pp. 69-79)

2.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI son las siglas que hacen referencia a un Sistema de Gestión de Seguridad de la Información o por sus siglas en inglés ISMS (Information Security Management System), el cual está basado en la norma ISO 27000. El SGSI aporta con herramientas de gran utilidad y es una importante ayuda para la gestión de la seguridad de la información, independientemente de las compañías y de su tamaño físico, operacional, diversidad, complejidad y sector de negocio.

La gestión de la Seguridad de la Información deberá realizarse a través de un proceso plenamente conocido y adoptado por toda la organización, documentado y persistente.

La información es el activo más importante de la organización. Se entiende por activo de la información a cualquier conjunto de datos que posee valor para la organización y es independiente de cualquier medio en el que se pueda presentar, transmitir, guardar o representar esta información. La manera en la que se representan los datos de manera estructurada puede ser en forma escrita, impresa, oral, en imágenes, digital, proyectada, transmitida en conversaciones o vía electrónica, fax etc.

La Seguridad de la Información, según la norma ISO 27000, consiste en mantener, precautelar y preservar la confidencialidad, integridad y disponibilidad de la información. Al ser un activo muy importante para la organización, éste se encuentra sujeto a riesgos y dichos riesgos pueden estar presentes de forma interna como externa.

La forma más adecuada para garantizar la conservación de los atributos de la información es minimizando los riesgos potenciales a los cuales se encuentran expuestos estos activos. (NTE INEN- ISO/IEC 27000, 2013, pp. 3-14). El diseño e implementación de un Sistema de Gestión de Seguridad de la Información dependerá de la empresa u organización en la cual se vaya a realizar ya que ella deberá introducirlo y ajustarlo de acuerdo a sus procesos y recursos.

En definitiva, un Sistema de Gestión de Seguridad de la Información, es un sistema para implementar, establecer, operar y mejorar la preservación de la información en cada uno de sus atributos: confidencialidad,

integridad y disponibilidad, incluyendo un ciclo de mejora continua basado en ISO 27001.

2.3 LA NORMA ISO 27000

El aseguramiento de la información y de los sistemas informáticos que procesan dicha información es el principal activo de una empresa, el cual es vital para el éxito y continuidad del negocio, por tal motivo, el salvaguardar estos activos debe ser considerado como un objetivo estratégico dentro de la organización.

Para una correcta gestión de la seguridad de la información, es primordial implementar un sistema que permita en forma metódica, basado en objetivos claros y específicos, y en forma documentada, la mitigación de amenazas, ya sean naturales, físicas, voluntarias o por desconocimiento. Para esto se deberá partir de una evaluación de riesgos a los que está sometida la información de la empresa u organización.

ISO/IEC 27000 (International Organization for Standarization e IEC International Electrotechnical Commission), es un conjunto de estándares basado en las mejores prácticas y que proporcionan a cualquier organización un marco de gestión de seguridad de la información. La ISO 27000 cuenta con organismos colaboradores y dentro de los cuales se encuentra el BSI.

El BSI (British Standards Institution) fue la primera entidad a nivel mundial de normalización, quién desde 1901 ha sido la responsable de la publicación de normas importantes como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI, aparece en 1995 por primera vez con el objetivo de proporcionar un conjunto de buenas prácticas para el aseguramiento de la información de la empresa, ya sea de carácter público o privado.

La BS 7799-1 es una guía de buenas prácticas y para la cual no se establece un esquema de certificación. La BS 7799-2, establece los requisitos necesarios de un Sistema de Seguridad de la Información la cual aparece en 1998 y es certificable por una entidad independiente.

Estas dos partes de la norma BS 7799 fueron revisadas en 1999, dando como resultado la adopción de esta norma como ISO 17799 en el año 2000. En 2002 se adoptó, con algunos cambios, la norma BS 7799-2 por la ISO.

Con más de 1700 empresas certificadas a nivel mundial en BS 7799-2, esta norma en el 2005 se publicó como estándar ISO 27001 y al mismo tiempo se actualizó la norma ISO 17799 renombrándola como norma ISO 27002:2005 el 1 de julio del 2007.

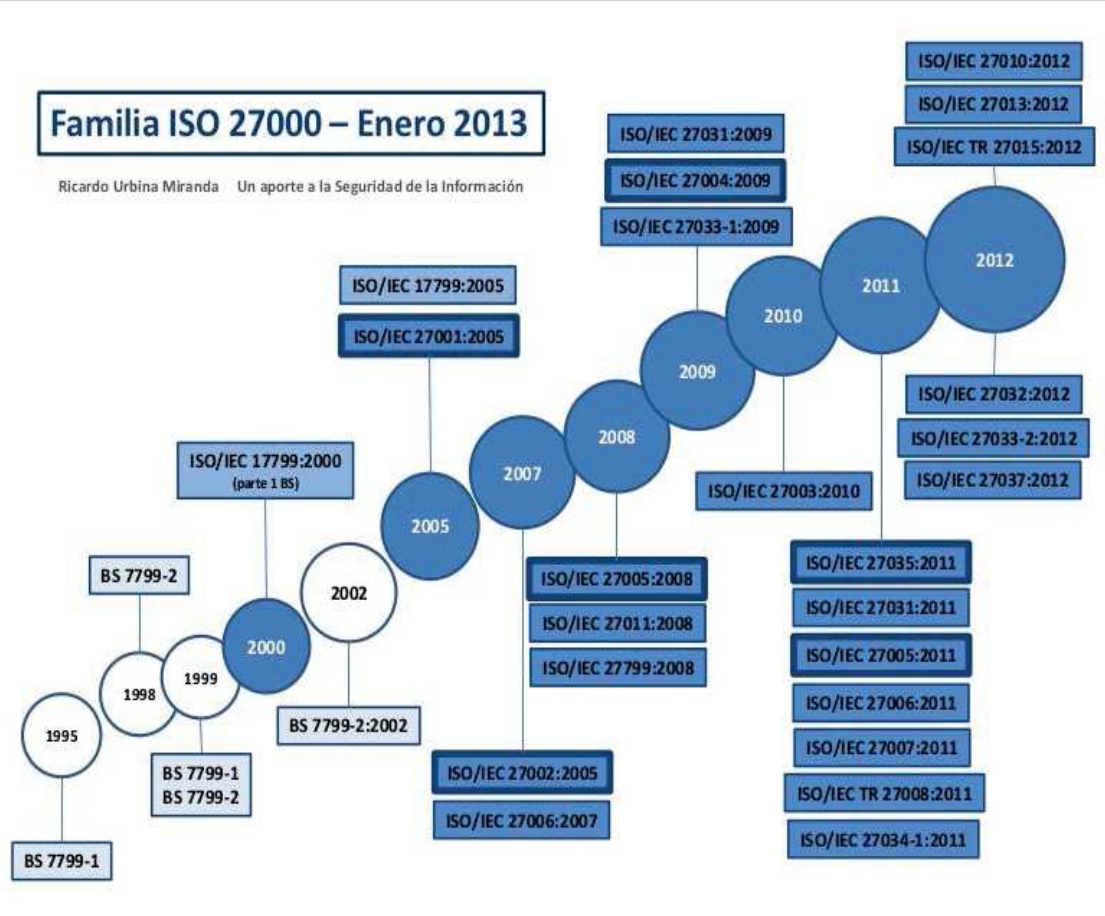

Figura 1. DIAGRAMA DE EVOLUCIÓN DE LAS NORMAS ISO 27000

TOMADO DE: RICARDO URBINA MIRANDA

La norma ISO 27001 define las pautas necesarias para la implementación de un Sistema de Gestión de Seguridad de la Información, manteniendo un mecanismo claro y enfocado a:

1. Limitar en forma clara los objetivos de seguridad de la información, definiendo los objetivos y las políticas relevantes en seguridad.

2. Evaluar los riesgos a través de:
   - Identificación de los riesgos
   - Valoración de los activos de información
   - Identificar las vulnerabilidades y las amenazas

- Identificar las relaciones existentes de las amenazas y vulnerabilidades con los activos de información a nivel cualitativo o cuantitativo.
- Calcular el riesgo existente a través de las relaciones mencionadas.
- Tratamiento del riesgo identificado.
- Selección de los mecanismos de control para mitigar los riesgos identificados y relacionados con los activos.

3. Realizar un seguimiento de los controles que permitan una evaluación de los riesgos. Para esto es necesario:

   - Definir los controles
   - Implementar los controles.
   - Supervisar los controles.

4. Verificar la eficiencia y eficacia de la implementación del SGSI.

5. La adopción de un ciclo de mejora continua.

La norma ISO 27001, incluye el llamado ciclo de “Deming”, que consiste en un ciclo de mejora continua, el cual está basado en el modelo del proceso PDCA (Plan Do CheckAct), que por sus siglas inglés significa: Planificar, Hacer, Chequear y Actuar. (ISO 27000, 2013, pp. 2-16)

2.4 ISO 27005

La norma ISO/IEC 27005 fue publicada el 4 de junio del 2008 sustituyendo a la Gestión de la Seguridad de la Tecnología de la Información y Comunicaciones, la norma ISO/IEC TR 13335-3:1998 y la norma ISO/IEC TR 13335-4:2000, establece las directrices necesarias

para la gestión y análisis de riesgo en la seguridad de la información, sin embargo, esta norma no brinda ninguna metodología específica para la Gestión y Análisis de Riesgos de la Seguridad de la Información, por lo que corresponde a la organización definir un enfoque para la gestión del riesgo dependiendo por ejemplo del alcance del SGSI, del sector industrial o del contexto de la gestión del riesgo.

La estructura de la norma está definida por: Establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, monitoreo y revisión del riesgo.

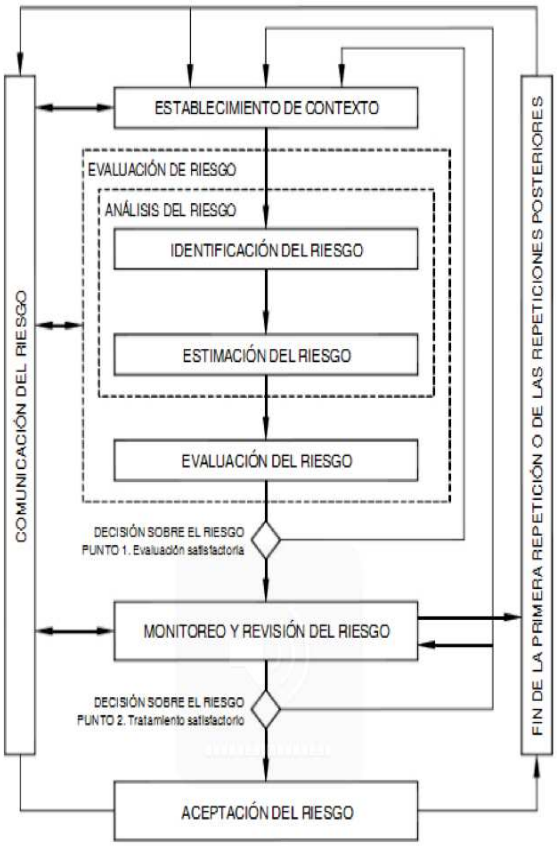

Figura 2. PROCESO DE GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

TOMADO DE: NTE INEN-ISO/IEC 27005

Dentro de esta norma se establece que la gestión del riesgo de la seguridad de la información debería contribuir a:

- Identificación del riesgo.
- Valoración del riesgo, probabilidad de ocurrencia y las consecuencias para el negocio.
- Establecer un orden de prioridades para el tratamiento del riesgo.
- Priorización de las acciones para reducir la materialización de un riesgo.
- Participación e involucramiento de los interesados cuando se toman las decisiones sobre la gestión del riesgo.
- Monitoreo eficaz en el tratamiento de los riesgos.
- Educación sobre el riesgo y las acciones que se toman para mitigarlos.

Esta norma apoya con los conceptos generales establecidos en la ISO/IEC 27001 y está diseñada para ayudar en la aplicación satisfactoria de la Seguridad de la Información desde un enfoque de Gestión y Análisis de Riesgos. (NTE INEN- ISO/IEC 27005, 2011, pp. 1-8)

2.5 CICLO DE MEJORA CONTINUA

El ciclo de mejora continua o ciclo de Deming fue desarrollado, en primera instancia, por Schewart y perfeccionado por Deming de ahí su nombre. Deming nació el 14 de octubre de 1900 en Iowa, Sioux City quién estudió ingeniería en la Universidad de Wyoming y basándose en continuos análisis generó el Ciclo de Mejora Continua.

Demming fue un experto norteamericano en Gestión de la Calidad, quien enseñó la calidad a los japoneses en forma metódica e incluyó el ciclo

PDCA (Plan Do CheckAct) que consiste en cuatro elementos que se llevan a cabo en forma sucesiva, permitiendo que la calidad sea mejorada en cada iteración que se realiza al utilizar esta método. Las siglas de PDCA se describen a continuación:

- P.- PLAN (PLANEAR): Establecer la planificación o los planes a seguir.
- D.- DO (HACER): Llevar a cabo la planificación establecida.
- C.- CHECK (VERIFICAR): Verificar si los resultados concuerdan con lo planificado.
- A.- ACT (ACTUAR): Para corregir los problemas encontrados, prever posibles problemas, mantener y mejorar la calidad.

Planificar: Consiste en programar las actividades que serán llevadas a cabo, por ende, involucra establecer metas, objetivos, métodos para alcanzar lo programado e identificar las áreas de mejora.

Desarrollar o hacer: Consisten en implementar o desarrollar las actividades programadas. En esta etapa es importante aprovechar las sinergias y controlar los efectos de lo que se está desarrollando. Es importante que se comience, en primera instancia, con proyectos pilotos antes de abarcar proyectos de mayor magnitud.

Comprobar: Consiste en verificar si las actividades programadas y desarrolladas cumplen con los resultados programados de acuerdo a los objetivos. Esta etapa consiste en analizar los efectos de lo realizado en la etapa anterior.

Actuar: Consiste en aplicar los resultados obtenidos para identificar mejoras o ajustes de los objetivos, de forma que nos permita una mejora de las acciones a realizar para cumplimiento de los mismos.

Una vez culminado el ciclo de mejora se reinicia el proceso en busca de posibilidades de mejorar lo realizado, llegando al punto de mejora continua y permitiendo que en cada iteración se mejore lo realizado. (Walton, Demming, 1992, pp. 18-23)

Dentro de la ISO 27000 se aplica el modelo de PDCA y las etapas para realizar este ciclo son:

Plan:

- Delimitación del escenario a cubrir.
- Definir la gestión de riesgos, objetivos y estrategias de la política de seguridad.
- Diseño de un método de gestión de riesgos.
- Evaluación del riesgo inicial.
- Delimitación del riesgo residual.
- Estado de aplicabilidad.
- Definición de controles y excepciones.

Hacer:

- Plan de acción para el tratamiento de los riesgos encontrados.
- Implementación de los controles.
- Adiestramiento y formación.

Chequear:

- Seguimiento de los objetivos planteados.
- Adaptación de mejores prácticas.
- Revisión y auditorías programadas.

Actuar:

- Mejoramiento y actualización del Sistema de Gestión de Seguridad de la Información.

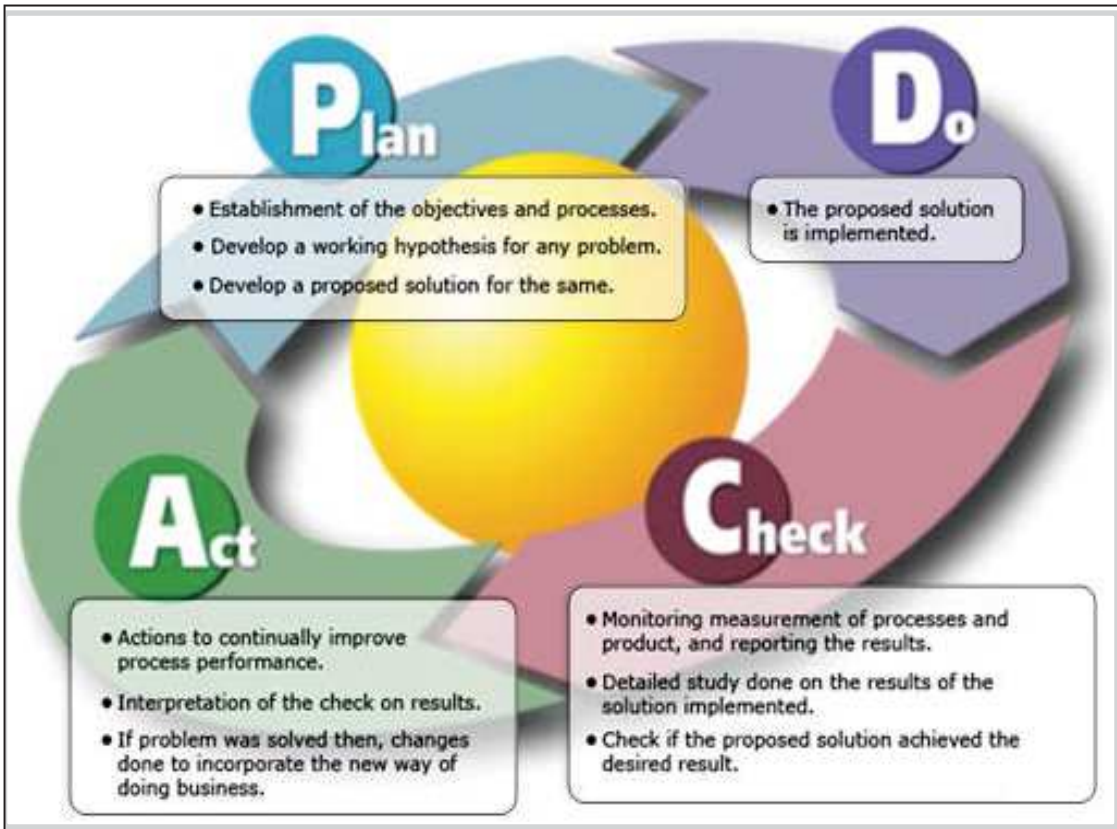

Figura 3. CICLO DE MEJORA CONTINUA

TOMADO DE: ISO 27000

2.6 ITIL

ITIL por sus siglas en inglés (Information Technology Infrastructure Library) es un marco de trabajo de Buenas Prácticas que al ser adoptadas ayudarán a gestionar de forma eficiente y alineada las necesidades del negocio con los servicios de TI de la organización. ITIL V3 contiene cinco fases que van desde:

- Estrategia

- Diseño
- Transición
- Operación
- Mejora Continua con un enfoque de Servicio y generar valor al cliente

La versión de ITIL 3.0 robustece la visión del negocio y se orienta aún más al ciclo de vida del servicio, permitiendo que se asegure la calidad en los servicios ofrecidos, integrando estrechamente las estrategias comerciales del servicio y las de TI, facilitando la administración e implementación de los servicios en un entorno cambiante, mejorando la demostración del valor y medición, identificando mecanismos de alerta automática para mejorar el servicio y corrigiendo las insuficiencias que se encontraban en la versión anterior.

En esta versión 3.0 ITIL integra las personas, herramientas y procesos de TI dentro de la estrategia del negocio a través de los servicios que ofrece. La estructura en la que actualmente se basa describe cómo los procesos se interrelacionan para un rendimiento sustentable como apoyo a los servicios del negocio, dejando de lado el enfoque del ser reactivo a la proactividad y apalancamiento de las estrategias organizacionales.

En términos de seguridad de la información ITIL basa sus políticas y controles más en la Gestión de Continuidad de los Servicios a través de la definición de: Políticas, Alcance, Impacto, Evaluación de riesgos, Estrategias, Organización y Supervisión. (Pardo, García, Pino, Piattini, Baldassarre, 2011).

Aunque este marco de trabajo es fuerte en procesos tiene grandes limitaciones en el desarrollo de sistemas y seguridad, a pesar que en su

última versión ya cuenta con un enfoque hacia la Gestión de Seguridad Informática, pero siempre se ha desarrollado más en el ¿Qué hacer?.

2.7 COBIT

COBIT por sus siglas en inglés (Control Objectives for Information and related Technology), es un Marco de Negocio para el Gobierno y Gestión de las Tecnologías de la Información de las empresas. Es una guía de mejores prácticas presentada como un marco de trabajo o framework, dirigido al Gobierno y Gestión de la Tecnología de la Información TI. Esta guía es mantenida por ISACA, por sus siglas en inglés (Information Systems Audit and Control Association) y el IT Governance Institute ITGI.

COBIT 5 provee de un marco integral de trabajo que permite a las empresas alcanzar sus objetivos para Gobierno y Gestión de TI, manteniendo el equilibrio entre el beneficio y la optimización de los niveles de riesgos y el uso recursos tecnológicos de extremo a extremo y para toda la empresa. Esto significa que:

- Integra el gobierno de TI en el gobierno corporativo. Es decir, el sistema de gobierno para la organización propuesto a través de COBIT 5 por TI, se integra sin problemas con cualquier visión estratégica del negocio.
- Cubre todos los procesos y funciones necesitados para gobernar y gestionar la información organizacional y las tecnologías relacionadas con la información en cualquier lugar que esta pueda ser procesada, es decir, incluye todo y a todos, entes internos y externos, actividades y responsabilidades tanto de las funciones de TI como las de negocio que sean relevantes para el gobierno y gestión de la información.

La misión de COBIT es descubrir, desplegar, propagar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados, actualizados para el uso del día a día de los gestores de negocios incluidos directivos y auditores. Auditores, Gestores y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información. (ISACA, 2012)

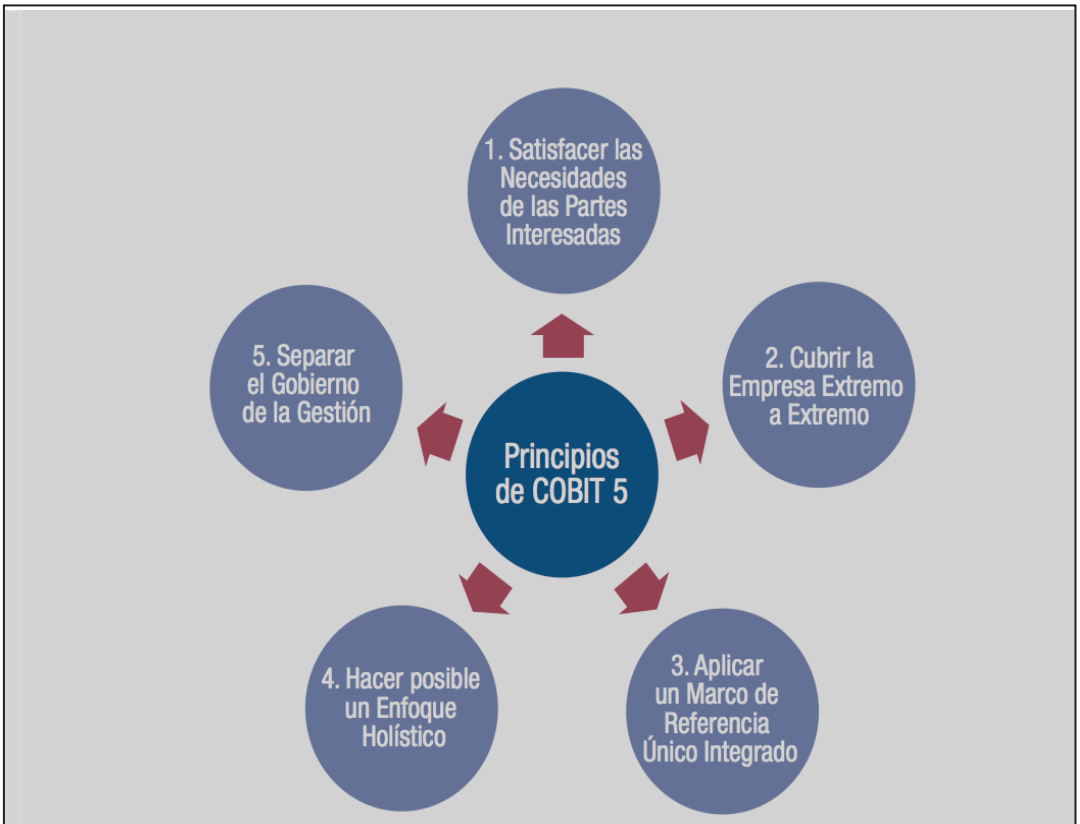

Figura 4. PRINCIPIOS DE COBIT

FUENTE: COBIT 5 ISACA FRAMEWORK

Dentro del campo de la Seguridad de la Información, COBIT 5 ofrece una guía práctica para el personal interesado en la seguridad dentro de todos los niveles de la organización. En esta guía se propone una visión de

gobernanza y gestión de la seguridad de la información en forma detallada para establecer, implementar y mantener, como parte de las políticas, estructuras y procesos de la empresa, la seguridad de la información. La guía se encuentra dividida en tres partes:

- Seguridad de la Información
- Uso de Habilitadores de COBIT 5 para Implementar la Seguridad de la Información en la práctica
- Adaptación de COBIT 5 para la Seguridad de la Información al Entorno Empresarial.

2.8 ISO 31000

La norma ISO 31000:2009 Risk Management – Principles and guidelines, de la International Organization for Standardization (ISO), fue publicada como un estándar el 13 de noviembre del 2009 y tiene como objetivo ayudar a las organizaciones, independiente del tamaño o tipo, a gestionar con efectividad el riesgo.

ISO 31000:2009 establece una serie de principios básicos que deben ser cumplidos para realizar una gestión de cualquier tipo de riesgo, tanto en consecuencias negativas como positivas, y recomienda que las organizaciones desarrollen, ejecuten y mejoren continuamente un marco de trabajo (framework) cuyo objetivo es la integración del proceso de gestión de riesgos en el gobierno corporativo.

Los principios básicos que una organización debe tener en cuenta son:

- Crear valor: Esto contribuye a la consecución de objetivos empresariales y la mejora de aspectos primordiales como la

seguridad, cumplimiento normativo y legal, salud ocupacional, protección ambiental etc.

- Estar integrada a los procesos de la organización: Debe estar siempre alineada con los procesos y actividades principales de la organización y no como una actividad aislada.
- Formar parte de las decisiones: Ayuda a la toma de decisiones evaluando las distintas alternativas existentes.
- Tratar explícitamente la incertidumbre: Tratar aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de su incertidumbre y como podrían remediarse.
- Ser sistemática, estructurada y adecuada: Contribuye con la eficiencia y con la obtención de resultados fiables.
- Se basa en la mejor información disponible: Las entradas de los procesos de gestión de riesgos se basan en información de expertos, previsiones, datos históricos.
- Ser a medida: Se alinea con su perfil de riesgo dentro del contexto interno como externo de la organización.
- Toma en cuenta factores humanos y culturales: Reconoce las percepciones, capacidades e intenciones de la gente externa e interna, que pueden dificultar o facilitar la consecución de los objetivos.
- Es inclusiva y transparente: Oportuna y apropiada participación de los grupos de interés y de los responsables, en todos los niveles, para asegurar que la gestión de riesgos se encuentre actualizada en todo momento.
- Sensible al cambio: La organización debe precautelar que la gestión de riesgos responda y detecte ante cualquier cambio organizacional.
- Facilitar la mejora continua: La organización debe desarrollar mecanismos de mejora continua para la gestión de riesgos y para cualquier otro aspecto organizacional.(ISO 31000, 2009)

La ISO 3100 como cualquier otra norma, cuenta con una estructura que se enfoca en tres elementos:

- Los principios para la gestión del riesgo
- La estructura de soporte o framework
- El proceso de gestión de riesgos

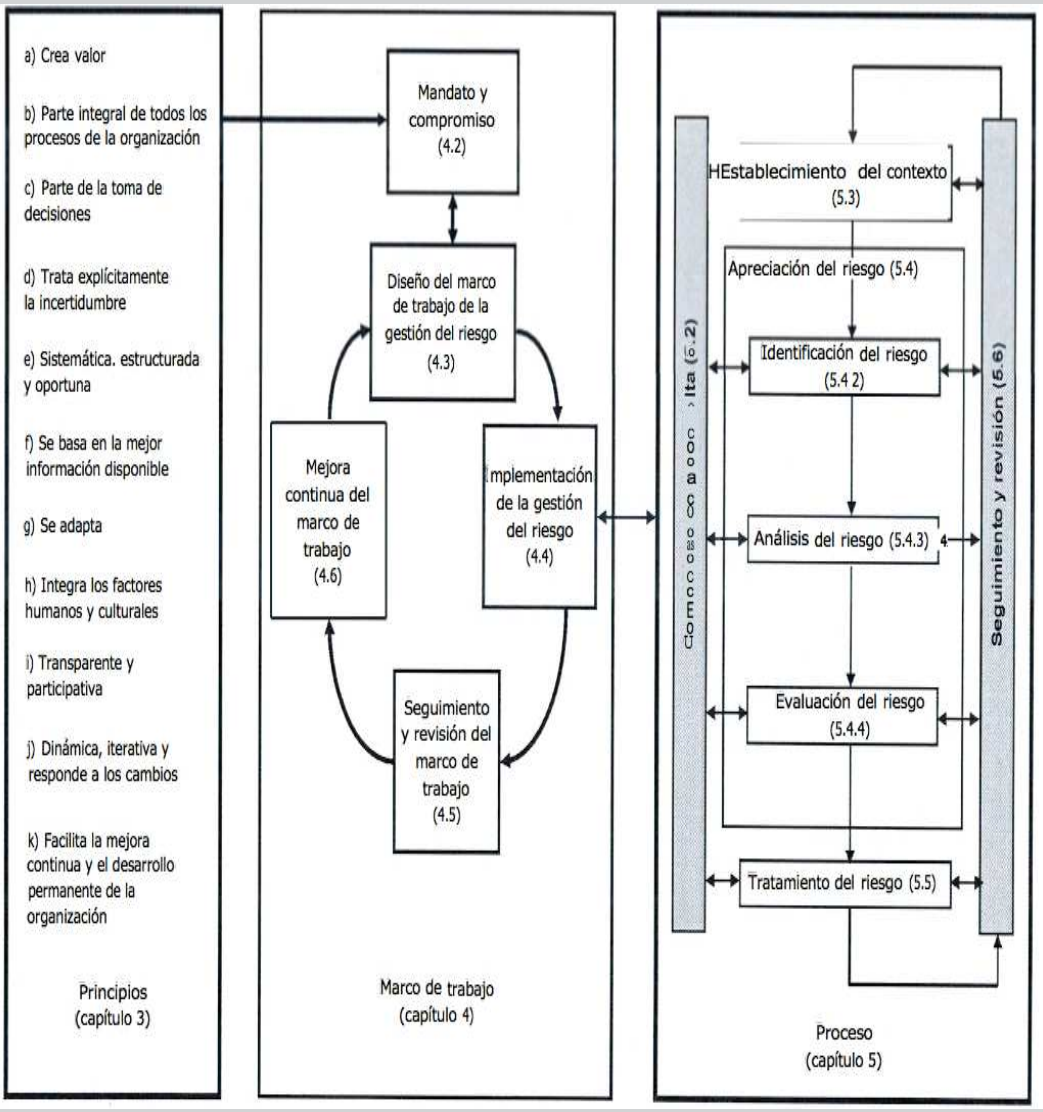

Figura 5. RELACIÓN ENTRE LOS PRINCIPIOS, ESTRUCTURA DE SOPORTE Y PROCESO DE GESTIÓN DE RIESGO

TOMADO DE: ISO 31000:2009

2.9 MÉTODO MAGERIT

Para conocer y determinar el riesgo de una organización es necesario que utilicemos algún método que nos ayude a identificar, analizar y gestionar el riesgo. Dentro de los varios métodos de Análisis y Gestión de Riesgo existentes se encuentra MAGERIT (Método de Análisis de Gestión de Riesgos de los Sistemas de Información), este método ha sido elaborado por el Consejo Superior de Administración Electrónica y reconocido por ENISA (European Network and Information Security Agency), (Díaz, 2009) para tratar y minimizar los riesgos asociados al uso de las Tecnologías de la Información dentro de las Administraciones Públicas en España, e inclusive, la administración pública española ha desarrollado software de Sistemas de Gestión de Riesgo basados en MAGERIT para cuantificar, analizar y tomar acciones sobre los riesgos que afrontan las Instituciones Públicas en España.

El método MAGERIT, responde al denominado “Proceso de Gestión de los Riesgos”, el cual se encuentra dentro de la terminología de la norma ISO 31000 en su sección 4.4 (Implementación de la Gestión de Riesgos) dentro del “Marco de gestión de Riesgos”. MAGERIT implementa un marco de trabajo basado en el Proceso de Gestión de Riesgos para que las organizaciones establezcan sus decisiones, tomando en cuenta los riesgos emanados del uso de las tecnologías de la información.

La primera publicación de MAGERIT fue realizada en 1997 y desde entonces, el análisis de riesgo se ha venido consolidando en las organizaciones como un paso necesario para gestionar la seguridad de la información.

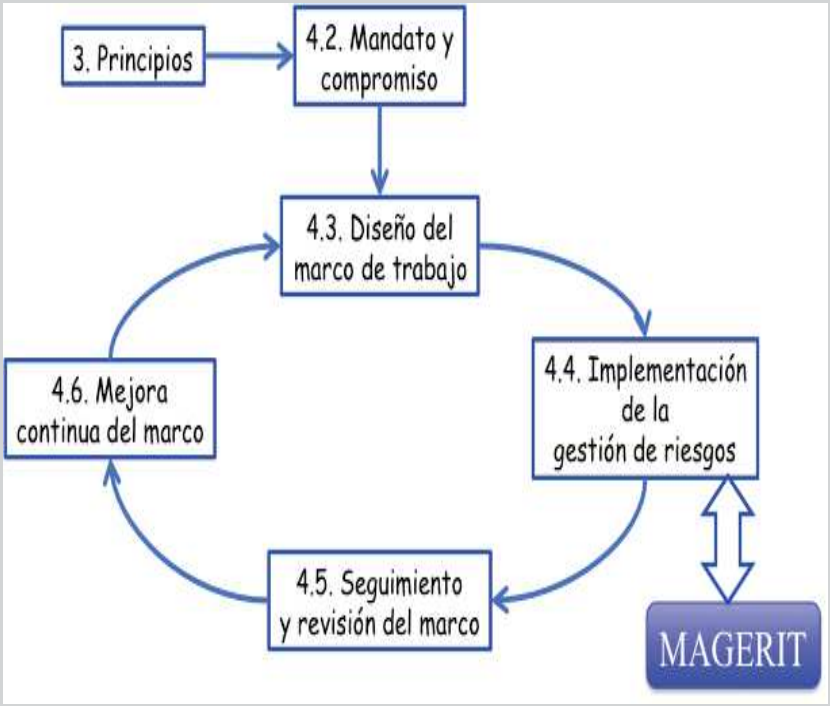

Figura 6. MARCO DE TRABAJO PARA ANÁLISIS DE RIESGO

TOMADO DE: METODOLOGÍA MAGERIT

El método MAGERIT cuenta con los siguientes objetivos:

- Concienciar de la existencia de los riesgos y la necesidad de gestionarlos.
- Ofrecer un método persistente para el análisis de los riesgos emanados del uso de las TIC
- Ayudar a mantener controlado al riesgo a través del tratamiento oportuno, partiendo del descubrimiento y planificación.
- Ayudar a la organización para estar preparada ante una auditoría, certificación o evaluación.

El cumplimiento de estos objetivos permite a las organizaciones entender, conocer y gestionar los riegos organizacionales. (Magerit, 2012, pp 6-10)

2.10 ATRIBUTOS DE LA SEGURIDAD DE LA INFORMACIÓN

La información, según el Diccionario de la Lengua Española, es la "comunicación o adquisición de conocimientos, que permiten ampliar o precisar los que se poseen sobre una materia determinada". También se la puede definir, dentro del ámbito informático, como, un conjunto de datos que se presentan de alguna forma desde un emisor y que es entendible para el receptor.

La información cuenta con varios atributos como lo son: Confiabilidad, Calidad, Accesibilidad, Claridad, Selectividad, Relevancia, entre otros, pero dentro de la norma ISO 27000 se contemplan atributos primordiales para garantizar la Seguridad de la Información. Estos atributos son: Confidencialidad, Integridad y Disponibilidad.

Los atributos de la información son las características que permiten y motivan al usuario para usarla en cualquier forma y bajo su elección.

2.10.1 Confidencialidad

La confidencialidad es la necesidad de que la información sólo sea conocida por personas autorizadas. También se la denomina privacidad e implica que la información no podrá estar disponible para otras personas, procesos, medios, entidades que no cuenten con la autorización necesaria. (NTE INEN- ISO/IEC 27000, 2013)

2.10.2 Integridad

La integridad garantiza que la información sólo puede ser creada, modificada, eliminada por el personal autorizado. Es importante que este

atributo conste con una bitácora de control que incluya los cambios que se hayan efectuado sobre un dato o registro ya que es evidencia para un proceso de auditoría.

La integridad garantiza que la información no haya sido falseada o sujeta a cambios intencionales o accidentales. (NTE INEN- ISO/IEC 27000, 2013)

2.10.3 Disponibilidad

La disponibilidad es la capacidad de que la información se encuentre en lugar, momento y forma precisa en la que un usuario, proceso, o medio externo necesiten acceder sin interrupciones a fin de que pueda ser procesada por un periodo de tiempo aceptable. (NTE INEN- ISO/IEC 27000, 2013)

2.11 ATRIBUTOS DE LA INFORMACIÓN SEGÚN MAGERIT

En base al método de análisis y gestión de riesgos de los Sistemas de Información MAGERIT, los atributos anteriormente mencionados son las dimensiones canónicas de la seguridad de la información, pero, MAGERIT adicionalmente involucra otros atributos o dimensiones canónicas como: Autenticidad y Trazabilidad. Estas dos dimensiones adicionales permiten el acercamiento de los usuarios con los sistemas de información en forma de seguimiento e identidad. (Magerit, 2012, pp. 9)

2.11.1 Autenticidad

Es la propiedad o característica que consistente en que una entidad es quien dice ser o que garantiza la fuente de la que proceden los datos. Está orientado a evitar la suplantación de identidad. (Magerit, 2012, pp. 9)

2.11.2 Trazabilidad

Es el aseguramiento de que en todo momento se podrá determinar el origen y el instante de tiempo de quién hizo qué y en qué momento. Es esencial para analizar los incidentes de seguridad, realizar seguimiento de los atacantes y aprender de lo experimentado. La trazabilidad se basa en la integridad de los registros de actividad. (Magerit, 2012, pp. 9)

2.12 PLAN DE CONTINUIDAD DEL NEGOCIO

El plan de continuidad del negocio o BCP (Business Continuity Planning) consiste en la elaboración de un documento que analiza, en forma detallada, la preparación con la que una empresa cuenta para afrontar desastres o situaciones que averíen la operatividad de sus procesos internos y que a través de acciones, que deben ser ejecutadas de forma continua, permitan y garanticen que la organización no pierda su operatividad.

El concepto de Plan de Continuidad del Negocio, siempre ha estado presente entre los empresarios y ha adoptado un auge en las organizaciones de TI por la importancia de la información y el apoyo que los activos de la información brindan a la operatividad del negocio y la llegada de la Sociedad de la Información.

Un BCP puede definirse como el proceso que las organizaciones han podido y podrán definir para la recuperación ante desastres de cualquier índole lo antes posible bajo condiciones mínimas, pero aceptables para el negocio y sus clientes.

El Plan de Continuidad del Negocio debe ser parte del marco de la Seguridad de la Información de la empresa. (Fort, 2010)

CAPÍTULO III

3. ANÁLISIS DEL DOMINIO DEL PROBLEMA

3.1 SITUACIÓN ACTUAL

Radical CIA. LTDA. es una empresa ecuatoriana reconocida dentro de los principales proveedores de tecnología, consultoría y servicios del país. Cuenta con una base sólida de expertos en cada uno de los servicios y productos que ofrece, lo que le ha permitido desarrollar un amplio espectro de soluciones.

Esta organización brinda servicios y productos de seguridad informática. Dentro de sus servicios se encuentran: Comercialización de equipamiento tecnológico de seguridad informática, ciberdefensa y asesoría en seguridad informática.

La visión de RADICAL CIA. LTDA. es: “Ser la empresa regional referente en la implementación y gestión de servicios de ciberseguridad en las instituciones públicas y privadas, fortalecidos en la innovación, creatividad, capacitación y excelencia”

RADICAL CIA. LTDA. está compuesta por un grupo de 15 personas entre: ingenieros especialistas, personal de comercialización y venta, personal administrativo y personal directivo. Cuenta con equipamiento de infraestructura tecnológica física propia que aloja servicios virtuales como: Directorio Activo o Controlador de Dominio, CRM, ERP, Sistema de Gestión de Proyectos, Aplicativos web entre otros. Adicionalmente, la empresa, cuenta con servicio de Internet y servicio de transferencia de datos a través de redes privadas virtuales, las mismas que son utilizadas

para acceso a la infraestructura o servicios que la empresa ha implementado en varios clientes.

La empresa ha desarrollado importantes y novedosos proyectos dentro del ámbito de la Seguridad de la Información, los cuales han sido implementados dentro de organismos públicos del Ecuador.

3.2 PROCESOS INTERNOS

RADICAL CIA. LTDA. es una organización que tiene como objetivo brindar soluciones de seguridad informática en base a las tendencias y estándares mundiales. Actualmente RADICAL CIA. LTDA. cuenta con procesos que están directamente enfocados en la planeación estratégica de la empresa, a pesar de no estar normados o plenamente establecidos, se pudo obtener los procesos que se encuentran identificados en base a una entrevista realizada al Director de Proyectos.

Para entender mejor los procesos de RADICAL CIA. LTDA. se muestra un diagrama con los procesos que actualmente son parte de la organización:

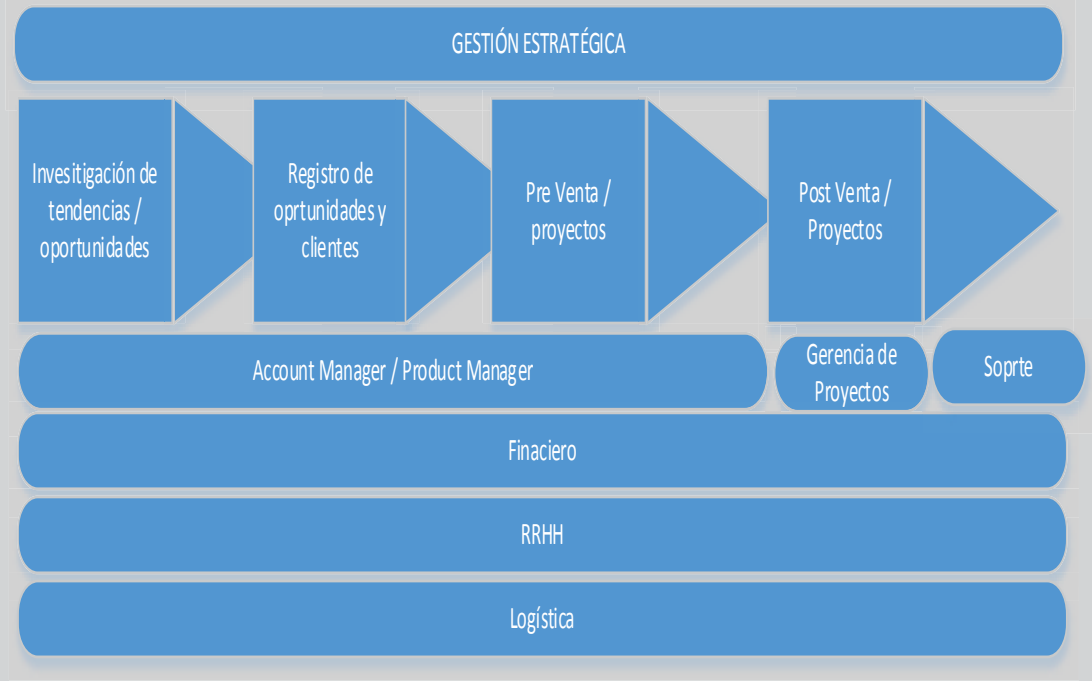

Figura 7. DIAGRAMA DE PROCESOS DE RADICAL CIA. LTDA

TOMADO DE: GERENTE DE PROYECTOS DE RADICAL CIA .LTDA.

Los principales procesos, identificados por el Director de Proyectos y que forman parte de la Cadena de Valor son:

- Investigación de tendencias y oportunidades
- Registro de oportunidades y clientes
- Pre venta de productos y servicios
- Post venta de productos y servicios

3.3 COMPORTAMIENTO E INTERACCIÓN DE LOS COMPONENTES MACRO DEL PROBLEMA

A continuación se muestra en forma ilustrativa el comportamiento e interacción entre los diferentes actores, departamentos y equipos de trabajo que forman parte de la organización.

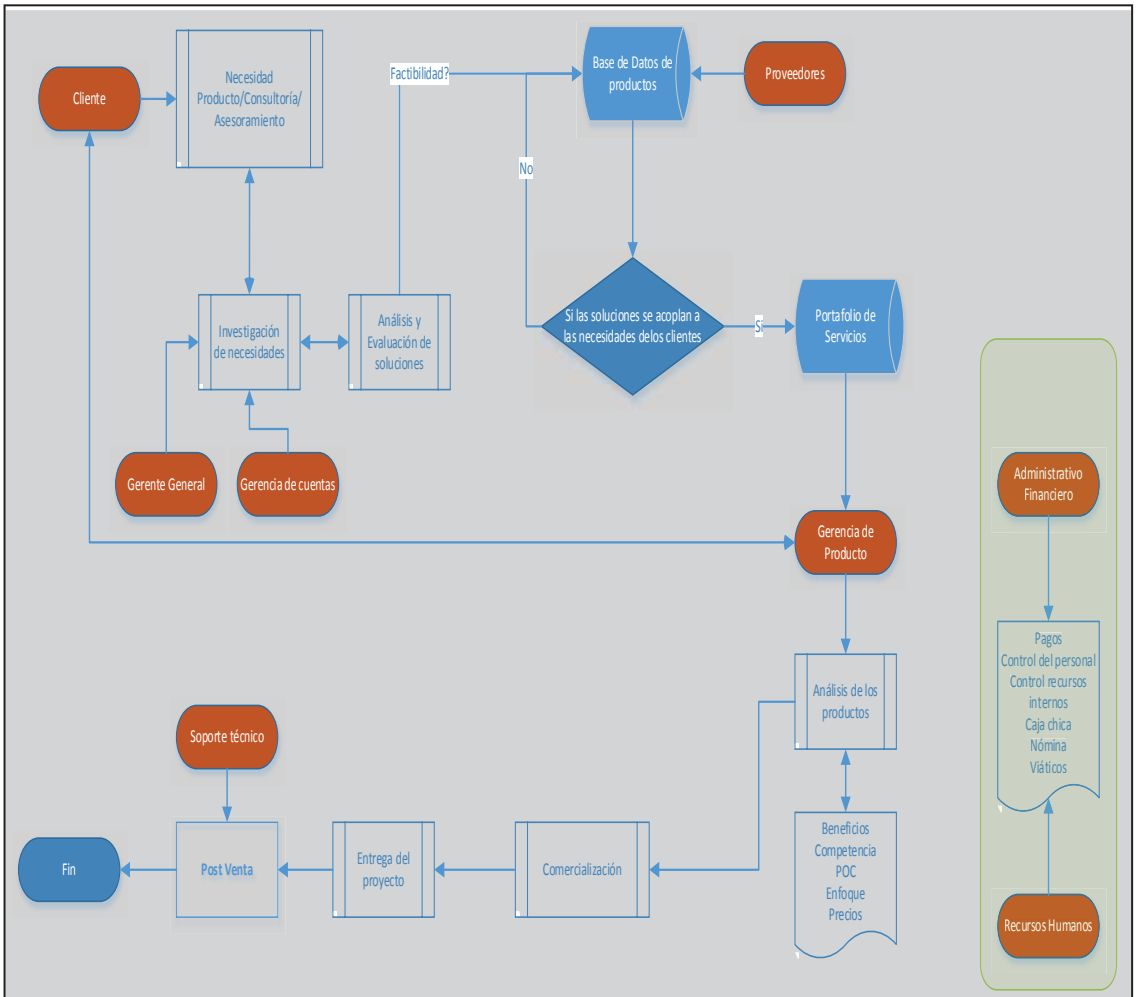

Figura 8. INTERACCIÓN DE LOS COMPONENTES DEL PROBLEMA

TOMADO DE: GERENTE DE PROYECTOS DERADICAL CIA. LTDA.

Se puede evidenciar que las necesidades pueden ser originadas por el cliente o a su vez son identificadas a través de la interacción del departamento de Gerencia de Cuentas o Gerencia General. Una vez identificadas estas necesidades se busca una solución con la ayuda de proveedores, con los cuales se interactúa en forma constante en busca de soluciones innovadoras que puedan satisfacer las necesidades de los clientes o tendencias a nivel mundial, que podrían ser implementadas en el mercado local.

3.4 INFORMANTES CALIFICADOS

Para determinar los problemas que la empresa afronta, en materia de seguridad de la información, es necesario que se identifique al personal que puedan ayudar a determinar la causa raíz de dichos problemas. Para este proyecto, la empresa RADICAL CIA. LTDA determina que los informantes calificados son:

- Gerente General
- Gerente de proyectos
- Gerentes de cuentas
- Gerentes de productos
- Equipo de soporte técnico de proyectos
- Departamento Administrativo Financiero

3.5 IDENTIFICACIÓN DEL PROBLEMA

Para identificar los problemas estratégicos de la empresa, se realizó entrevistas a los principales directivos de la organización que son el Gerente General y el Director de Proyectos de RADICAL CIA. LTDA. Dentro de la entrevista realizada, tanto el Gerente General como el Director de Proyectos, identificaron varias causas, en relación a Seguridad de la Información, que han ocasionado problemas dentro de los proyectos y de la empresa. Ver Anexo 7 - Constancia entrevistas.
Los problemas encontrados en la organización son:

- Las pérdidas, robos, fugas de información, ataques informáticos, programas informáticos malignos y el desconocimiento en el manejo de la información han ocasionado que la empresa pierda importantes proyectos y rentabilidad económica.

- La información imprecisa e incorrecta ha generado que continuamente la empresa enfrente: pérdidas de productividad, desgaste de recursos tecnológicos, sobre esfuerzo del personal técnico y administrativo e inversiones adicionales.
- La carencia de procedimientos y políticas ha generado que los servicios internos y externos no sean garantizados.

3.6 ÁRBOL DE PROBLEMAS

Utilizando el método del marco lógico, se realiza la identificación de los problemas que actualmente RADICAL CIA. LTDA. presenta. Se realiza un análisis de la causa raíz del problema y se determina el efecto que este representa para la organización. Las causas de origen del problema ayudan a determinar que la empresa no garantiza que sus recursos de información cuenten con sus principales atributos de Seguridad de la Información que son:

- Disponibilidad
- Integridad
- Confidencialidad

A continuación se muestra en forma gráfica la utilización del “Árbol de Problemas” para identificar las causas que originan el problema, los efectos inmediatos que estos ocasionan a la organización y los efectos a nivel macro.

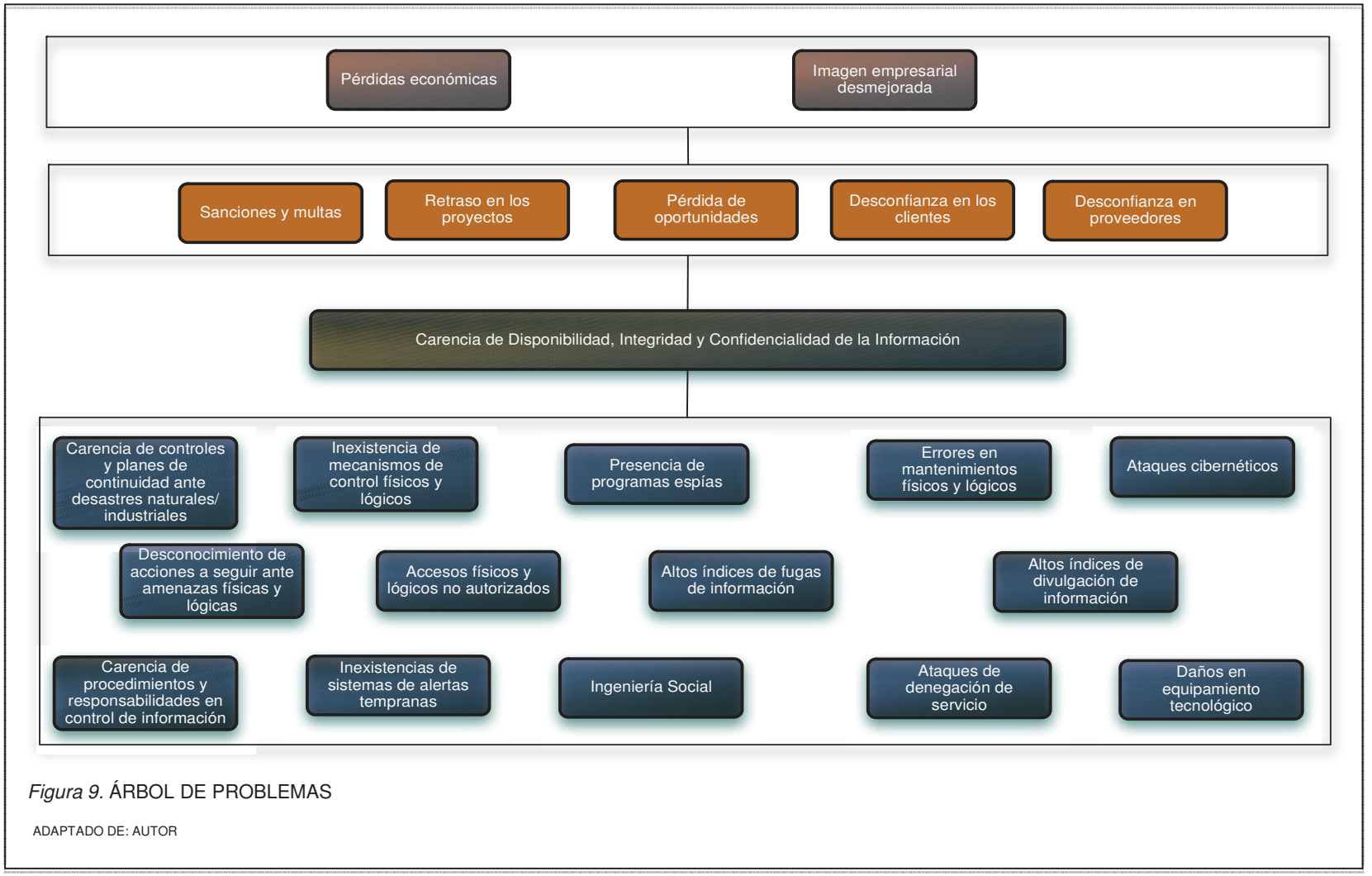

Figura 9. ÁRBOL DE PROBLEMAS

ADAPTADO DE: AUTOR

3.7 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Un activo de la información es un objeto que puede ser tangible o intangible y que representa un valor para la empresa. Estos activos de la información necesitan estar salvaguardados para que se garanticen los servicios empresariales en los cuales tienen relación. Para que un activo de la información sea útil para la organización se deberá minimizar el riesgo ante las amenazas que se encuentra expuesto. (Alexander, 2012).

Estos activos de la información son:

- Activos de almacenamiento: Bases de datos, archivos digitales, registros de auditoría e información archivada en forma digital.
- Documentos impresos: Documentación física importante con datos del negocio, contratos, documentos de la empresa, manuales, documentación física de los sistemas, planes de continuidad, procedimientos de operación, procedimientos de soporte e información de investigaciones y otros archivos físicos.
- Activos de software: Software del sistema, software de aplicación, software utilitario y herramientas de desarrollo.
- Activos físicos: Equipos electrónicos removibles o medios removibles, equipos de comunicación, equipos de cómputo y otros equipos etc..
- Servicios: Servicios de comunicación, servicios de cómputo, servicios generales del tipo: calefacción, energía, acondicionadores de aire etc..
- Personal: Personas, calificaciones del personal, experiencia, capacidades etc..
- Intangibles: Imagen y reputación organizacional.

CAPÍTULO IV

4. INTEGRACIÓN SISTÉMICA PROBLEMA – SOLUCIÓN

4.1 ANÁLISIS DE OBJETIVOS

Basados en el método del Marco Lógico utilizado para el desarrollo del presente proyecto, se desarrolla el análisis de objetivos, que nos permite definir la situación futura que se desea alcanzar dentro del desarrollo de un proyecto y una vez se hayan resuelto los problemas identificados.

Este análisis consiste en convertir los estados negativos del árbol de problemas en soluciones, expresados en forma de estados positivos. Todos estos estados positivos se los representa en un diagrama de objetivos y permite tener una visión global y clara de la situación positiva que se desea obtener. Mantiene una amplia flexibilidad lo que nos permite modificar los enunciados que no sean considerados correctos. (Ortegón, 2005)

Una parte importante de este análisis es que si se determina inconsistencias de la relación existente entre causa y efectos, es necesario que sea revisado para detectar las fallas que se pudo haber producido.

4.2 ÁRBOL DE OBJETIVOS

En la siguiente Figura denominada “Árbol de objetivos” se establecen acciones para la solución del problema identificado. En el recuadro de color azul se muestran las acciones a realizar que derivan en garantizar la disponibilidad, integridad y confidencialidad de la Información, y en los recuadros superiores se muestra el efecto ocasionado por estas acciones:

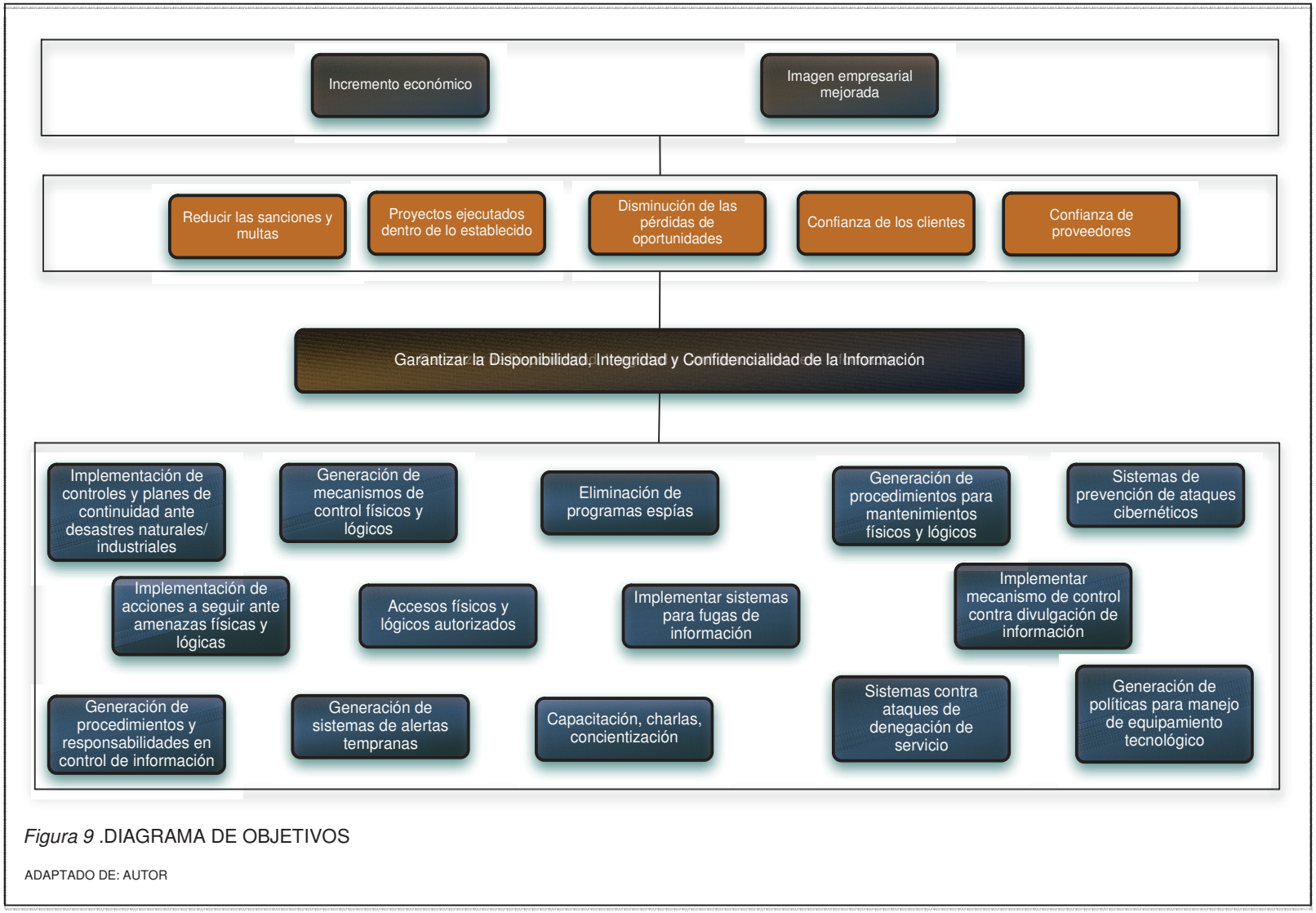

Figura 9 .DIAGRAMA DE OBJETIVOS

ADAPTADO DE: AUTOR

4.3 GENERACIÓN DE IDEAS

En busca de soluciones que permitan satisfacer los objetivos planteados y a través de un taller realizado en conjunto con los directivos de la organización, se proponen tres alternativas de solución: COBIT 5, ITIL V3 e ISO 27000.

Estas tres alternativas propuestas tienen relación con las áreas de Tecnologías de la Información, ya que están fundamentadas en: procesos, métodos y mejores prácticas para apoyo a la Gestión de TI y adicionalmente contemplan, dentro de su ámbito de aplicación, sistemas, marcos de referencia, normas etc.. para la Gestión de Seguridad de la Información.

A continuación se analizará cada una de ellas y su aporte a los objetivos de solución.

4.3.1 ITIL V3

ITIL V3 incorpora principales objetivos de la Seguridad de la Información, los cuales se resumen en:

- Diseñar, en colaboración con proveedores y clientes, una política de seguridad correctamente alineada con las necesidades del negocio.
- Garantizar el cumplimiento de los estándares de seguridad acordados dentro de los Acuerdos de Niveles de Servicio (SLAs).
- Reducir los riesgos de seguridad que amenacen la continuidad del servicio.

Como ITIL está enfocado en la gestión del servicio, este marco de referencia basado en mejores prácticas incluye en sus procesos varias áreas enfocadas a la Seguridad como: Mantenimiento y Seguridad dentro del proceso de Gestión de la Disponibilidad, Evaluación de Riesgos en el proceso de Gestión de la Continuidad de servicios TI y un proceso específico para Gestión de la Seguridad en el que se establece:

- Política y plan de Seguridad
- Aplicación de las Medidas de Seguridad
- Evaluación y mantenimiento
- Control del proceso

ITIL también incluye el ciclo de mejora continua para generar cambios y mejoras dentro de su enfoque orientado al Servicio.

4.3.2 COBIT 5

Uno de los enfoques en la versión 5 de COBIT es la Gestión de la Seguridad y aporta con herramientas para la implementación de mecanismos de seguridad en sus procesos. Algunos de sus procesos utilizan la ISO 27000 y la ISO 31000 para cubrir ciertas áreas o dominios. Las áreas o dominios que están cubiertas por estas normas son:

- Procesos de seguridad y relativos al riesgo en los dominios Evaluación Orientación y Monitoreo (EDM), Alinear Planificar y Organizar (APO), y Entregar Dar Servicio y Soporte (DSS).
- Varias actividades relacionadas con la seguridad dentro de procesos en otros dominios.
- Actividades de Supervisión y Evaluación (MEA).

- Procesos relativos a la Gestión del riesgo en los dominios Evaluación Orientación y Monitoreo (EDM), Alinear Planificar y Organizar (APO).

En base a la generación de ideas planteadas para la solución del problema, en conjunto con los directivos de la organización, se determina qué acción satisface cada una de estas posibles soluciones a los objetivos (acciones) que se determinaron en el Árbol de Objetivos.

4.3.3 ISO 27000

La ISO 27000 se basa en controles enfocados a la seguridad de la información en busca de garantizar la Disponibilidad, Confidencialidad e Integridad de la Información.

Esta norma contiene las mejores prácticas recomendadas para desarrollar, implementar y mantener la Seguridad de la información, adicionalmente cuenta con especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Esta norma es utilizada por COBIT para apalancar ciertos controles dentro de sus áreas o dominios, como se detalló en la anterior sección.

4.4 MAPEO DE IDEAS GENERADAS CON LOS OBJETIVOS DE SOLUCIÓN

Para la identificación de una posible solución, se toman las tres alternativas anteriormente planteadas y en base al campo de aplicación de cada una de ellas se realiza una matriz de cumplimiento, en la que se relaciona si las alternativas permiten obtener los resultados necesarios para resolver los problemas inicialmente identificados.

En la figura de la matriz que se muestra a continuación se coloca un círculo de color rojo o verde, dependiendo si la alternativa satisface o no el cumplimiento del objetivo, para identificar si dicha alternativa de solución satisface o no el objetivo que se busca.

Tabla 1. MATRIZ DE RELACIÓN SOLUCIÓN - OBJETIVO

		Posibles Soluciones		
		ITIL V3	COBIT	ISO 27000
OBJETIVOS	Implementación de controles y planes de continuidad ante desastres naturales/industriales	🔴	🟢	🟢
	Generación de mecanismos de control físicos y lógicos	🟢	🟢	🟢
	Eliminación de programas espías	🔴	🟢	🟢
	Generación de procedimientos para mantenimientos físicos y lógicos	🟢	🟢	🟢
	Sistemas de prevención de ataques cibernéticos	🔴	🟢	🟢
	Implementación de acciones a seguir ante amenazas físicas y lógicas	🟢	🟢	🟢
	Accesos físicos y lógicos autorizados	🟢	🟢	🟢
	Implementar sistemas para fugas de información	🟢	🟢	🟢
	Implementar mecanismo de control contra divulgación de información	🟢	🟢	🟢
	Generación de procedimientos y responsabilidades en control de información	🟢	🟢	🟢
	Generación de sistemas de alertas tempranas	🟢	🟢	🟢
	Capacitación, charlas, concientización	🔴	🟢	🟢
	Sistemas contra ataques de denegación de servicio	🔴	🟢	🟢
	Generación de políticas para manejo de equipamiento tecnológico	🟢	🟢	🟢

Indicadores: 🔴 No Aplica 🟢 Aplica

En base a la figura, se determina que existen dos alternativas de solución que satisfacen el cumplimiento de los objetivos, ya que cumplen con la relación existente entre Posibles Soluciones y Objetivos, sin embargo y en análisis realizado por los directivos de la organización, se opta por la implementación de un Sistema de Gestión de Seguridad de la Información.

Las razones por las cuales se toma esta alternativa de solución son:

- La problemática actualmente identificada es la falta de una correcta Gestión en Seguridad de la Información. Lo que es una prioridad para los directivos organizacionales.
- La norma ISO 270001 permite que la organización opte por la obtención de una certificación. Lo que conlleva a que la organización, que se dedica a comercializar productos y servicios de Seguridad Informática, pueda contar con una ventaja competitiva sobre empresas que brindan servicios similares y además garantizar a sus proveedores y clientes una correcta Gestión del Riesgo de Seguridad de la Información, mejorando su imagen y generando confianza.
- La ISO 27001 cumple un objetivo mucho más específico: la seguridad, por lo tanto es exclusivo para la gestión desde un nivel inferior y detallado del control, lo que es una gran diferencia de COBIT, que se dirige a las necesidades de alto nivel organizacional, buscando mejorar la orientación general del negocio con apoyo de la tecnología a través de controles y métricas.
- La norma ISO 27001 es un complemento para los sistemas de Gestión Medioambiental ISO 14001, Gestión de la Calidad ISO 9001 y construye una cultura de la seguridad dentro de la organización.
- ISO 27000 permite a la reducción de barreras para el comercio electrónico o e-commerce, la cual es una opción que la organización

está evaluando para la comercialización de sus productos, por su aceptación internacional.

- ITIL, aunque incluye mejores prácticas para la Gestión de Seguridad de la Información, estas están más orientadas a la Gestión del servicio.
- ISO 27001 y COBIT no tienen que ser competidores entre ellos ya que son un complemento esencial. COBIT actúa como "paraguas" para conectar a la norma ISO 27001 y es un marco de referencia que está compuesto por normas y mejores prácticas tales como: ISO 27001 e ITIL.

4.5 INTERACCIÓN DE LOS COMPONENTES DEL PROBLEMA CON LOS ACTIVOS DE LA INFORMACIÓN

Una vez identificada la solución a implementar y basados en el método de implementación propuesto por el Sistema de Gestión de Seguridad de la Información se procede a determinar los activos de información que son parte de la problemática.

A continuación se detalla la relación entre las acciones a realizar para la solución del problema, denominado como Objetivos, y la interacción con los activos de la información según la norma ISO 27005 que es parte del método propuesto.

Tabla 2. INTERACCIÓN COMPONENTES CON ACTIVOS DE LA INFORMACIÓN

	Componentes / Activos de la Información							
		Almacenamiento	Documentos impresos y magnéticos	Software	Físicos	Servicios	Personal	Intangible
Objetivos	Implementación de controles y planes de continuidad ante desastres naturales/industriales	X	X	X	X	X	X	X
	Generación de mecanismos de control físicos y lógicos	X	X	X	X	X	X	X
	Eliminación de programas espías	X	X	X				X
	Generación de procedimientos para mantenimientos físicos y lógicos	X			X	X		X
	Sistemas de prevención de ataques cibernéticos	X		X		X		
	Implementación de acciones a seguir ante amenazas físicas y lógicas	X	X	X	X		X	
	Accesos físicos y lógicos autorizados			X	X	X		X
	Implementar sistemas para fugas de información	X	X				X	X
	Implementar mecanismo de control contra divulgación de información						X	X
	Generación de procedimientos y responsabilidades en control de información	X	X	X	X	X		
	Generación de sistemas de alertas tempranas	X		X	X	X		
	Capacitación, charlas, concientización						X	X
	Sistemas contra ataques de denegación de servicio		X			X		
	Generación de políticas para manejo de equipamiento tecnológico	X	X	X	X	X		

CAPÍTULO V

5. DISEÑO LÓGICO

1.1 MÉTODO EMPLEADO

El método seleccionado para la solución de los problemas encontrados en RADICAL CIA. LTDA. es la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información), usando el método de Análisis y Gestión de riesgos MAGERIT.A diferencia de la ISO 27005 de Gestión de Riesgos de Seguridad de la Información, MAGERIT utiliza dos atributos adicionales de la información y está basado en la norma ISO 31000 de Gestión de Riesgos.

Para un mejor entendimiento de la solución propuesta, se elabora la siguiente figura (Ver Figura 11). La figura nos muestra los pasos lógicos a seguir dentro del Sistema de Gestión de Seguridad de la Información para la solución del problema identificado y en la cual se incluye el Ciclo de Mejora Continua o de Demming, que fue detallado en la sección 2.5 del presente proyecto.

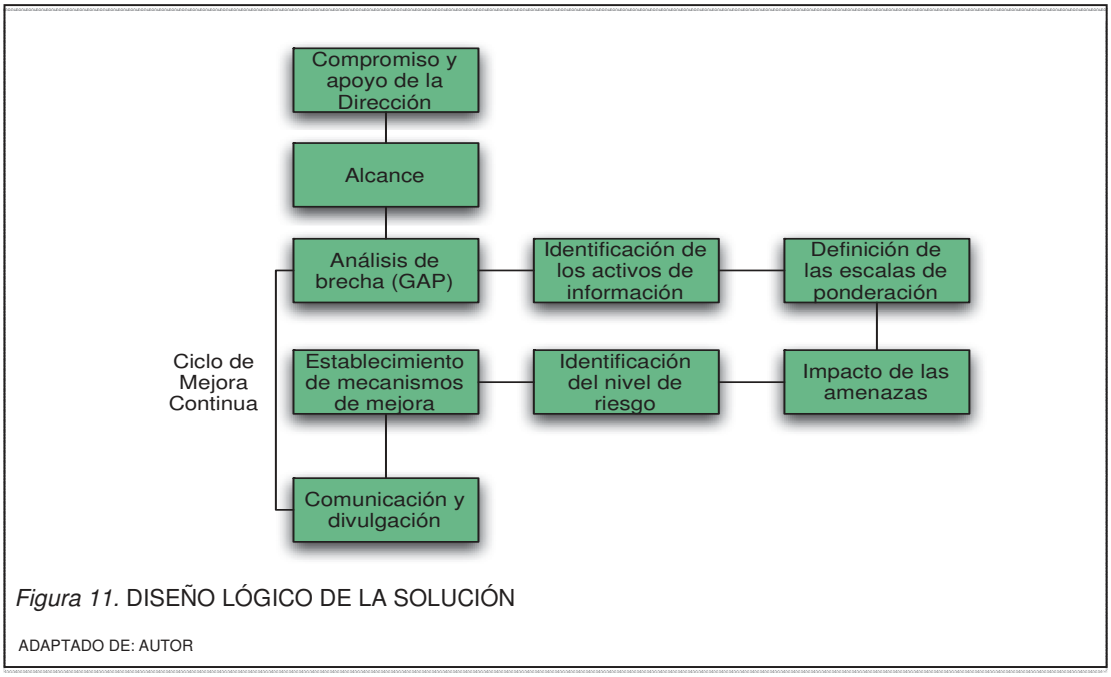

Figura 11. DISEÑO LÓGICO DE LA SOLUCIÓN

ADAPTADO DE: AUTOR

Para entender las fases del método propuesto, es importante que conozcamos la descripción de cada una de ellas.

5.2 COMPROMISO Y APOYO POR PARTE DE LA DIRECCIÓN

Para la implementación de un Sistema de Gestión de Seguridad de la Información, es primordial que se cuente con la concientización de los altos Directivos de la organización de que el activo más importante de la organización es la Información. Partiendo de esta concientización se deberá comprometer y divulgar en la organización que se optará por la implementación de políticas, procedimientos, proyectos y controles que permitan mitigar los riesgos asociados a los activos informáticos. Ver SGSI Anexo 1 – Compromiso de la empresa.

5.3 ALCANCE

Para la implementación de un SGSI es importante delimitar claramente el alcance del mismo. El alcance contendrá una especificación objetiva de lo que se desea conseguir dentro del proyecto, entregables, áreas del negocio, delimitación geográfica, compromisos y las partes que se verán afectadas por el proyecto.

5.4 ANÁLISIS DE BRECHA

El análisis de brechas es una herramienta que nos permite realizar un análisis de la Situación Actual de la organización, en materia de Seguridad de la Información en este caso, y comparar entre este estado actual obtenido respecto a uno o varios puntos de alguna normativa o estándar, ya sea de carácter local, nacional o internacional.

El análisis de brechas está compuesto por 4 acciones primordiales:

- Identificación de la situación actual en la que se encuentra la organización a evaluar.
- Identificación del objetivo que se desea conseguir a futuro.
- Identificación de la brecha existente entre la relación actual y la que se desea obtener.
- Determinación de los planes o acciones a seguir para alcanzar el objetivo planteado.

Para llevar a cabo el análisis es necesario realizar ciertas preguntas que permiten identificar de mejor forma el grado de madurez empresarial. Estas preguntas se encuentran detalladas en la guía “DATA SECURITY MATURITY MODEL”. Ver Anexo 3 - Data Security Maturity Model.

5.5 GRUPOS DE CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

La clasificación de los activos de información consiste en relacionar cada uno de los componentes informáticos que forman parte del alcance establecido dentro del SGSI, de manera que se identifiquen cómo, cuándo y qué tipo de activo forma parte, en un momento determinado, de la operación del negocio en relación con el alcance propuesto.

La siguiente tabla permite entender y clasificar cada activo de la información identificado y su relación, en base a sus características, con un grupo determinado de activos.

Tabla 3.TIPOS DE ACTIVOS DE LA INFORMACIÓN

Inicial	Grupo	Descripción
I	Instalaciones	Instalaciones físicas, ubicaciones de los equipos informáticos y de comunicación.
H	Hardware	Equipamiento físico que alojan datos, información, aplicaciones.
A	Aplicaciones / Software	Equipamiento de software que permite interactuar y gestionar los datos.
D	Datos / Información	El principal activo de la organización.
R	Redes / Comunicaciones	Equipamiento que permite el intercambio de datos e información entre los activos de la información.
S	Servicios	Conjunto de activos de información que permiten a la organización satisfacer las necesidades de sus clientes.
P	Personal / Empleados	Son los que operan, organizan, brindan o gestionan todos los activos

5.6 IDENTIFICACIÓN DE LAS ESCALAS DE PONDERACIÓN

Para determinar el nivel de riesgo que afronta la organización en Seguridad de Información de cada activo de la información identificado, se utilizan escalas de ponderación que ayudan a cuantificar o cualificar, dependiendo del método, este nivel de riesgo. En las siguientes secciones se detallan las escalas que son empleadas dentro del presente proyecto.

5.6.1 Escala de valoración de los activos de información

La escala de valoración de los activos de información se establece en niveles que van desde lo Despreciable con un valor de 0 hasta el nivel Muy Alto con un valor de 5. En el presente proyecto se utiliza la Escala definida por Likert (Malave, 2007), la cual puede estar sujeta a cambios, en los parámetros que la organización desee, si fuese necesario.

Tabla 4.ESCALA DE VALORACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN EN BASE A LA CRITICIDAD

Descripción	Abreviatura	Valor
Muy alto	MA	5
Alto	A	4
Medio	M	3
Bajo	B	2
Muy bajo	MB	1

5.6.2 Escala de posibilidad de ocurrencia de un evento

La presente escala está relacionada con la frecuencia de que un evento pueda suceder o no, en algunas ocasiones, la relación existente entre las amenazas con los activos de información, se basa en análisis y datos históricos que ayudan a determinar si la amenaza se ha materializado en algún determinado momento.

Para el establecimiento de esta escala se utiliza la Escala de Likert (Malave, 2007). La posibilidad de ocurrencia de un evento va en niveles que van desde lo Despreciable con un valor de 0 hasta el nivel Muy Alto con valor de 5 y contendrán un ítem de cuantificación relacionado a cada nivel. La escala está sujeta a cambios en sus niveles si la organización lo desea.

Tabla 5.ESCALA DE POSIBILIDAD DE LA OCURRENCIA DE UN EVENTO

Descripción	Abreviatura	Valor
Muy alta	MA	4
Alta	A	3
Media	M	2
Baja	B	1
Despreciable	D	0

5.6.3 Atributos de la información

Los atributos de la información son las características esenciales que debe cumplir un dato, tanto en elementos individuales como en conjunto. En Seguridad de la Información estas características están definidas de acuerdo al método de Gestión y Análisis de Riesgo que se utiliza, para este proyecto se realiza con MAGERIT y que incluye dos atributos adicionales a los contemplados dentro de la ISO 27000:2005.

Tabla 6. ATRIBUTOS DE LA INFORMACIÓN MAGERIT

Abreviatura	Detalle
A	Autenticidad
C	Confidencialidad
D	Disponibilidad
I	Integridad
T	Trazabilidad

5.6.4 Amenazas

Para realizar la clasificación de las amenazas a las que los activos de la información están expuestos, de acuerdo a su naturaleza, se ha utilizado el método MAGERIT, en el cual sugiere que las amenazas sean agrupadas en cuatro grupos que son: Desastres naturales, De origen Industrial, Errores y fallos no intencionados, Ataques intencionados.

A continuación se muestra un detalle de las amenazas que son identificadas y relacionadas a los grupos de activos:

Tabla 7. AMENAZAS IDENTIFICADAS

Grupo	Ref	Amenaza
Desastres naturales	N1	Fuego
	N2	Daños por agua
	N3	Otros desastres Naturales
De Origen Industrial	I1	Fuego
	I2	Daños por agua
	I3	Contaminacion Mecanica
	I4	Contaminación electromagnética
	I5	Avería de origen físico o lógico
	I6	Corte del suministro eléctrico
	I7	Condiciones inadecuadas de temperatura o humedad
	I8	Fallo de servicios de comunicaciones
	I9	Interrupción de otros servicios y suministros esenciales
	I10	Degradación de los soportes de almacenamiento de la información
	I11	Emanaciones electromagnéticas
Errores y fallos no intencionados	E1	Errores de los usuarios
	E2	Errores del administrador
	E3	Errores de monitorización (log)
	E4	Errores de configuración
	E7	Deficiencias en la organización
	E8	Difusión de software dañino
	E9	Errores de [re-]encaminamiento
	E10	Errores de secuencia
	E14	Escapes de información
	E15	Alteración accidental de la información
	E18	Destrucción de información
	E19	Fugas de información
	E20	Vulnerabilidades de los programas (software)
	E21	Errores de mantenimiento / actualización de programas (software)
	E23	Errores de mantenimiento / actualización de equipos (hardware)
	E24	Caída del sistema por agotamiento de recursos
	E25	Pérdida de equipos
Ataques intencionados	A3	Manipulación de los registros de actividad (log)
	A4	Manipulación de la configuración
	A5	Suplantación de la identidad del usuario
	A6	Abuso de privilegios de acceso
	A7	Uso no previsto
	A8	Difusión de software dañino
	A9	[Re-]encaminamiento de mensajes
	A10	Alteración de secuencia
	A11	Acceso no autorizado
	A12	Análisis de tráfico
	A13	Repudio
	A14	Interceptación de información (escucha)
	A15	Modificación deliberada de la información
	A18	Destrucción de información
	A19	Divulgación de información
	A22	Manipulación de programas
	A23	Manipulación de los equipos
	A24	Denegación de servicio
	A25	Robo
	A26	Ataque destructivo
	A27	Ocupación enemiga
	A28	Indisponibilidad del personal
	A29	Extorsión
	A30	Ingeniería social

5.7 IDENTIFICACIÓN DE LOS ACTIVOS Y RELACIÓN CON EL ALCANCE

Para la identificación de los activos se realiza un análisis de los componentes informáticos que son parte de la organización y del alcance establecido como se menciona en la sección 5.5 anteriormente expuesta. Los activos de información están divididos en: Instalaciones, Hardware, Aplicaciones/Software, Datos/Información, Redes/Comunicaciones, Servicios, Personal/Empleados, con lo cual se elabora un listado.

Tabla 8. IDENTIFICACIÓN DE LOS ACTIVOS Y RELACIÓN CON EL ALCANCE

Grupo	Item	Activo Identificado
Instalaciones	I01	Oficinas
Hardware	H01	Controlador de dominio principal
Hardware	H02	Servidor de Base de Datos
Hardware	H03	Servidor de correo
Hardware	H04	Granja de Servidores Vmware
Hardware	H05	Administración Vmware
Hardware	H06	Servidor Web
Hardware	H07	File Server
Hardware	H08	FTP, VPN, Terminal Server
Hardware	H09	Antivirus
Hardware	H10	SharePoint y Project Server
Aplicaciones/Software	A01	CRM
Datos/Información	D01	ERP Database
Datos/Información	D02	Clientes Database
Redes/Comunicaciones	R01	Firewall
Redes/Comunicaciones	R02	Antispam
Redes/Comunicaciones	R03	Switch core
Redes/Comunicaciones	R04	Router de datos
Servicios	S01	Internet
Servicios	S02	Correo Electrónico
Servicios	S03	FTP
Servicios	S04	VPN
Servicios	S05	Red LAN
Servicios	S06	Red WAN
Personal/Empleados	P01	Staff de soporte N1
Personal/Empleados	P02	Staff de servicios y consultorías
Personal/Empleados	P03	Staff de Ingenierios Especialistas
Personal/Empleados	P04	Staff Infraestructura y telecomunicaciones
Personal/Empleados	P05	Staff de Ejecutivos de cuenta
Personal/Empleados	P06	Personal administrativo
Personal/Empleados	P07	Personal Directivo

5.8 IDENTIFICACIÓN DEL NIVEL DE RIESGO

El valor porcentual encontrado del resultado del producto entre el Impacto x Posibilidad nos da el nivel de Riesgo de un activo de la información. Los niveles de riesgo están sujetos a los deseados por la compañía y en base a los cuales se debe establecer si los mecanismos de control se deben o no aplicar, de la misma forma la organización define si asume, mitiga o acepta el riesgo.

Tabla 9. NIVEL DE RIESGO

Descripción	Abreviatura	Valor (en porcentaje)
Crítico	C	Mayor a 60%
Alto	A	Mayor a 40% y menor a 59%
Medio	M	Mayor a 20% y menor a 39%
Bajo	B	Menor a 20%

5.9 ESTABLECIMIENTO DE MECANISMOS DE MEJORA

Los mecanismos de mejora serán desarrollados por la organización acorde a sus necesidades. Se plantean alternativas como: ejecución de proyectos en forma ejemplar y didáctica, elaboración de procedimientos, controles y políticas. Los controles y políticas serán implementados por la empresa acorde a las capacidades y necesidades determinadas por la organización. (Ver ANEXO 10 – Controles a Implementar).

5.10 COMUNICACIÓN Y DIVULGACIÓN

La comunicación y divulgación de las políticas, controles, proyectos u otras acciones de mejora, deberán ser difundidas e irrigadas a toda la organización a fin de que exista un lineamiento claro de lo que la organización persigue y la concientización por parte de los empleados. Es importante incluir acciones constantes de motivación y comunicación para el cumplimiento de los mecanismos de control.

CAPÍTULO VI

6. DISEÑO FÍSICO DE LA SOLUCIÓN

6.1 IMPLEMENTACIÓN

La implementación de un Sistema de Gestión de Seguridad de la Información es una decisión que debe ser tomada a nivel estratégico e involucrando a toda la organización, con el apoyo de la dirección.

Los lineamientos declarados a continuación para la gestión del riesgo son planteados a través de un enfoque fundamentado en los riesgos, amenazas y vulnerabilidades que se encuentran presentes en los activos de información.

Los activos de información estarán sometidos a cálculos de materialización del riesgo a través de la probabilidad e impacto de cada una de sus amenazas. Es importante que tomemos en cuenta los efectos o consecuencias de la materialización de los riesgos y el impacto a las operaciones normales de los proceso de producción de una organización.

El método planteado contempla varios pasos a seguir para la mitigación del riesgo y que fueron expuestos en el Capítulo anterior. Estos pasos son:

- Compromiso y apoyo por parte de la dirección
- Alcance
- Análisis de brechas
- Grupos de clasificación de los activos de información
- Identificación de las escalas de ponderación
- Identificación de los activos y relación con el alcance

- Identificación del nivel de riesgo
- Establecimiento de mecanismos de mejora
- Comunicación y divulgación

A continuación se desarrolla cada uno de ellos.

6.1.1 Compromiso y apoyo por parte de la dirección

La empresa RADICAL CIA. LTDA a través de sus directivos y en el ACUERDO Nº 006-2014 establece el compromiso y apoyo para la implementación de un Sistema de Seguridad de la Información en sus instalaciones, adicionalmente designa al Ing. Lenin Cortés como Oficial de Seguridad de la empresa y contraparte para la ejecución del análisis e implementación.

6.1.2 Alcance SGSI

Elaboración de un Sistema de Gestión de Seguridad de la Información para la empresa RADICAL CIA. LTDA. en la ciudad Quito para el año 2014.

6.1.3 Análisis de brecha

El Análisis de Brechas o (GAP ANALYSIS) permite la obtención del estado de la organización en comparación con los controles de seguridad establecidos en la norma ISO/IEC 27002. Para este fin se utilizó una herramienta elaborada en Excel de nombre “DATA SECURITY MATURITY MODEL”. Ver Anexo 4 - Data Security Maturity Model Radical.

La escala del nivel de cumplimiento está basada en el nivel de madurez, lo que significa que a través del esfuerzo claramente definido y evolutivo

se alcance la institucionalización de todas sus prácticas en ese nivel y en el de las inferiores.

Existen 6 niveles que son definidos en base a un conjunto de procesos o prácticas clave. Los 6 niveles partiendo desde el nivel 0 son:

Tabla 10. NIVELES DE MADUREZ

Nivel	Porcentaje	Descripción
Inexistente	0%	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
Inicial / Ad-hoc	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
Reproducible, pero intuitivo	50%	Los procesos se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
Proceso definido	90%	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
Gestionado y medible	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, Se tienen herramientas para mejorar la calidad y la eficiencia.
Optimizado	100%	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
No Aplica	N/A	El control no es aplicable a la organización.

RADICAL CIA. LTDA, actualmente y luego del análisis de brechas realizado (Ver Figura 12), se encuentra en un nivel de madurez de seguridad de la información “Inexistente”, ya que no cuenta con una política de seguridad de la información ni se han implementado procedimientos, normas, controles y menos la concientización del personal.

Por tal motivo y de acuerdo al servicio que la empresa brinda, su CEO (Chief Executive Officer o Gerente General) ha comenzado con el análisis de empresas locales que le puedan ayudar a que sus procesos se encuentren normados y certificados con estándares de Calidad, razón por la cual se encuentra en proceso de levantamiento de información, establecimiento y documentación de procesos.

La figura que a continuación se muestra nos describe claramente el estado actual de la empresa en términos de madurez de la Seguridad de la Información.

DATA SECURITY MATURITY MODEL

	Security Maturity Levels >	0: Nonexistent	1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized	
	Maturity Level Description >	*There is no evidence of this standard or practice in the organization.*	*The organization has an ad hoc and inconsistent approach to this privacy standard or practice.*	*The organization has a consistent overall approach, but it is mostly undocumented.*	*The organization has a documented, detailed approach, but no routine measurement or enforcement of it.*	*The organization regularly measures its compliance and makes regular process improvements.*	*The organization has refined its compliance to the level of best practice.*	
	process documentation	none	none	minimal, high-level	detailed	detailed	detailed	average maturity
	business objectives	not met	not met	partially met	mostly met	fully met	value added	0,38
	process measurement	none	none	none	ad hoc	routine	systemic	scaled to 100
	policy enforcement	none	none	none	ad hoc	routine	systemic	7,58
	process improvement	none	ad hoc	ad hoc	ad hoc	routine	systemic	score out of 55
	process benchmarking	none	none	none	ad hoc	ad hoc	routine	4,17
	Corresponding Level of Risk of a Data Breach or Regulatory Noncompliance	*Very high across the organization*	*High across the organization, and very high in key parts of the organization*	*Moderate across the organization, with some pockets of high risk*	*Moderate across the organization.*	*Low across the organization.*	*Remote across the organization.*	
ISO #	Domains							
5	Security Policy							0,0
6	Organization of Information Security							0,0
7	Asset Management							1,0
8	Human Resource Security							0,3
9	Physical and Environmental Security							0,7
10	Communications and Operations Management							0,7
11	Access Control							0,3
12	Information Systems Acquisition, Development and Maintenance							0,7
13	Information Security Incident Management							0,5
14	Business Continuity Management							0,0
15	Compliance							0,0

Figura 12. ANÁLISIS DE BRECHA REALIZADOEN RADICAL CIA. LTDA.

TOMADO DE: ISO 27000 – INFORMATION SECURITY STANDARDS

Tabla 11. RESULTADOS DE MADUREZ POR DOMINIO

		As is	Should Be	Could be
5	Security Policy	0,00	3,00	5,00
6	Organization of Information Security	0,00	3,00	5,00
7	Asset Management	1,00	3,00	5,00
8	Human Resource Security	0,33	3,00	5,00
9	Physical and Environmental Security	0,67	3,00	5,00
10	Communications and Operations Management	0,67	3,00	5,00
11	Access Control	0,33	3,00	5,00
12	Information Systems Acquisition, Development and Maintenance	0,67	3,00	5,00
13	Information Security Incident Management	0,50	3,00	5,00
14	Business Continuity Management	0,00	3,00	5,00
15	Compliance	0,00	3,00	5,00

TOMADO DE: ISO 27000 – INFORMATION SECURITY STANDARDS

En base al análisis realizado en conjunto con los directivos y responsables de áreas de la empresa, se determina que la organización se encuentra en un nivel de madurez “Inexistente” con una calificación de 0,38/5.

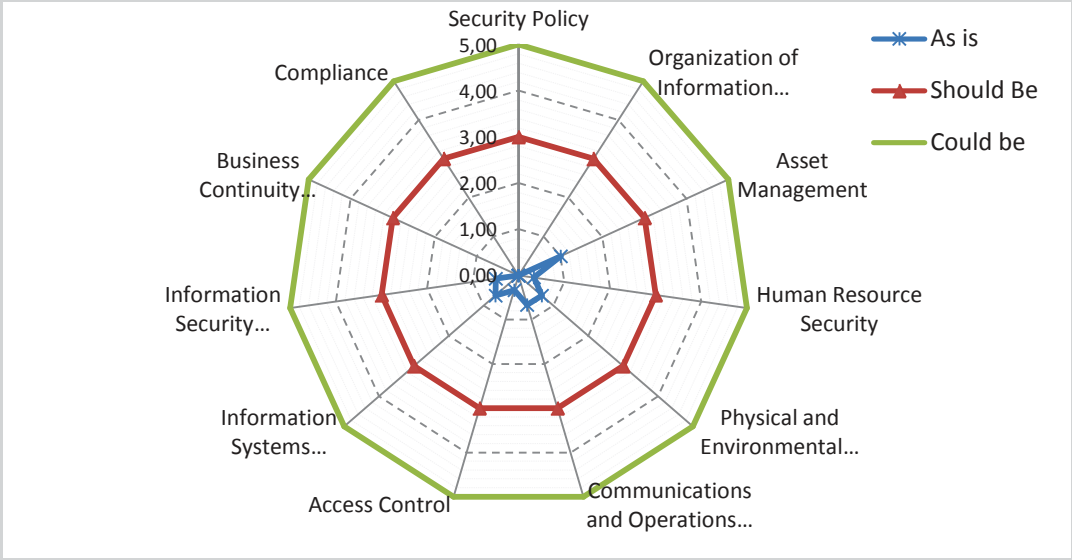

Figura 13. DIAGRAMA RADAR DE RESULTADOS MADUREZ POR DOMINIO

FUENTE: ISO 27000 - INFORMATION SECURITY STANDARDS

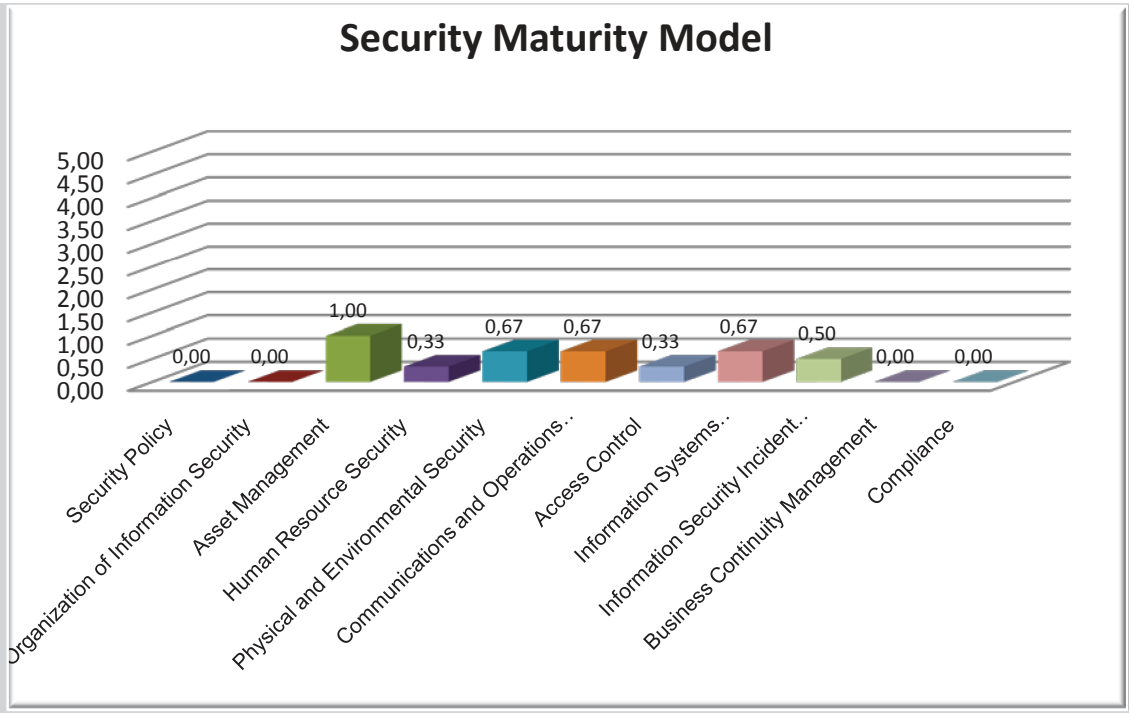

Figura 14. DIAGRAMA DE BARRAS RESULTADO DE MADUREZ POR DOMINIO

TOMADO DE: ISO 27000 - INFORMATION SECURITY STANDARDS

6.1.4 Grupo de clasificación de los activos

Como parte inicial del proyecto es necesario identificar los activos de información que son parte de la organización y del alcance propuesto. Estos activos están clasificados acorde a la TABLA 3:ACTIVOS DE LA INFORMACIÓN, y dentro del Análisis de Riesgo, los activos de la información serán ponderados acorde al nivel de criticidad que la organización determine, basados en la TABLA 4: ESCALA DE VALORACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN EN BASE A LA CRITICIDAD.

6.1.5 Identificación de las escalas de ponderación

La identificación de las escalas de ponderación son las que de determina en la sección 5.6 IDENTIFICACIÓN DE LAS ESCALAS DE PONDERACIÓN. Las escalas que se encuentran definidas son: Escala de valoración de los activos de información, Escala de probabilidad de ocurrencia de un evento, Atributos de la información, Amenazas.

6.1.6 Identificación de los activos en relación con el alcance

La identificación de los activos en relación con el alcance del SGSI propuesto dentro de la empresa RADICAL CIA. LTDA., son los que se encuentran en la TABLA 8: IDENTIFICACIÓN DE LOS ACTIVOS Y RELACIÓN CON EL ALCANCE.

Dentro de esta sección se adiciona la tabla en la cual se obtiene la cuantificación entre los activos de la información, el valor del activo o importancia para la organización y los atributos de información que tienen relación con dicho activo.

Tabla 12. MATRIZ DE RELACIÓN ENTRE ACTIVOS, IMPORTANCIA Y ATRIBUTOS

Grupo	Ref	Activo	Valor	Escala de Criticidad	Aspectos Criticos				
					A	C	I	D	T
Instalaciones	I01	Oficinas	MA	4	2	4	3	5	2
Hardware	H01	Controlador de dominio principal	A	3	5	5	4	4	5
	H02	Servidor de Base de Datos	M	5	3	5	3	5	5
	H03	Servidor de correo	M	4	4	3	3	5	3
	H04	Granja de Servidores Vmware	A	4	4	3	3	5	4
	H05	Administración Vmware	M	3	5	5	5	4	4
	H06	Servidor Web	B	3	4	3	4	4	4
	H07	File Server	M	3	4	3	3	5	5
	H08	FTP, VPN, Terminal Server	B	3	4	4	4	4	5
	H09	Antivirus	M	3	4	3	4	4	3
	H10	SharePoint y Project Server	MA	4	5	5	4	4	3
Aplicaciones	A01	CRM	A	5	5	3	3	3	3
Datos	D01	ERP Database	A	5	4	4	3	3	3
	D02	Clientes Database	M	5	3	3	5	5	3
Red	R01	Firewall	M	4	4	4	4	4	5
	R02	Antispam	M	3	5	3	4	4	5
	R03	Switch core	M	4	5	3	3	4	5
	R04	Router de datos	M	4	5	3	3	4	5
Servicios	S01	Internet	M	3	5	3	3	4	5
	S02	Correo Electrónico	A	4	4	5	5	5	4
	S03	FTP	B	2	4	3	4	4	4
	S04	VPN	B	4	4	3	3	4	4
	S05	Red LAN	M	2	4	4	4	4	4
	S06	Red WAN	M	3	4	4	4	5	4
Personal	P01	Staff de Soporte N1	MA	5	4	5	4	4	4
	P02	Staff Servicios & Consultorías	MA	5	4	4	4	4	4
	P03	Staff de Ingenieros Especialistas	MA	5	3	3	5	4	4
	P04	Staff Infraestructrura y Comunicaciones	MA	5	4	5	4	5	5
	P05	Staff de ejecutivos de cuentas	MA	5	5	4	5	4	5
	P06	Personal Administrativo	MA	5	4	5	3	4	5
	P07	Personal Directivo	MA	5	4	4	4	5	5

6.2 IDENTIFICACIÓN DEL NIVEL DE RIESGO

El riesgo es la valoración de la pérdida o afectación ante la materialización de una amenaza y que resulta del producto entre el

Impacto x Posibilidad. La organización estableció que un nivel de riesgo aceptable estaría contemplado en un valor inferior al 20%, por lo tanto, los valores que se encuentren con nivel superior a este parámetro serán seleccionados para el diseño e implementación de mecanismos de control. La empresa, en base a este nivel de riesgo, define los controles a implementarse que se encuentran detallados en el Anexo 10. Ver ANEXO 10 – Controles a Implementar.

A continuación se muestra el nivel de riesgo en los activos de información y por la cantidad de datos que son generados a través de este análisis, se colocan sólo dos grupos de activos de información y parte de un tercer grupo. El detalle total de este análisis se encuentra en el Anexo 5 - Análisis de Riesgo.

Tabla 13. ESCALA DE RIESGO EN EL GRUPO DE ACTIVO INSTALACIONES

ACTIVO		AMENAZA		RIESGO
I01	Oficinas	N01	Fuego	20%
		N02	Daños por agua	20%
		N03	Otros desastres Naturales	20%
		I01	Fuego	20%
		I02	Daños por agua	20%
		I11	Emanaciones electromagnéticas	20%
		A11	Acceso no autorizado	24%
		A26	Ataque destructivo	16%
		A27	Ocupación enemiga	16%

Tabla 14. ESCALA DE RIESGO EN EL GRUPO DE ACTIVO PERSONAL

P03	Staff Ingenieros especialistas	E07	Deficiencias en la organización	30%
		E19	Fugas de información	40%
		A28	Indisponibilidad del personal	60%
		A29	Extorsión	45%
		A30	Ingeniería social	45%

Tabla 15. ESCALA DE RIESGO EN EL GRUPO DE ACTIVO HARDWARE

H02	Servidor de Base de Datos	N01	Fuego	25%
		N02	Daños por agua	20%
		N03	Otros desastres Naturales	20%
		I01	Fuego	25%
		I02	Daños por agua	20%
		I03	Contaminacion Mecanica	15%
		I04	Contaminación electromagnética	10%
		I05	Avería de origen físico o lógico	30%
		I06	Corte del suministro eléctrico	30%
		I07	Condiciones inadecuadas de temperatura o humedad	15%
		I11	Emanaciones electromagnéticas	10%
		E02	Errores del administrador	45%
		E23	Errores de mantenimiento / actualización de equipos (hardware)	45%
		E24	Caída del sistema por agotamiento de recursos	40%
		E25	Pérdida de equipos	20%
		A06	Abuso de privilegios de acceso	40%
		A07	Uso no previsto	30%
		A11	Acceso no autorizado	30%
		A15	Modificación deliberada de la información	30%
		A23	Manipulación de los equipos	30%
		A24	Denegación de servicio	45%
		A25	Robo	40%
		A26	Ataque destructivo	40%

6.3 ESTABLECIMIENTO DE MECANISMOS DE MEJORA

Como mecanismos de mejora, en base a los riesgos identificados, la empresa opta por la implementación de controles y políticas basados en la norma ISO 27000, que están expuestas en el Anexo 10, y las cuales están acorde a las necesidades que la empresa puede desarrollar inicialmente. Adicional a la implementación de controles, en esta sección, se proponen tres proyectos, en forma ejemplar como parte de los mecanismos de mejora, a fin de que la organización opte por analizar los objetivos que se buscan dentro de ellos y puedan ser, una base o guía, para posterior implementación de alguno de ellos con los cambios que sean considerados.

Como se expone en esta sección, los proyectos son con fines académicos y con su aporte permiten simular la reducción del riesgo dentro del presente trabajo y posterior obtención del riesgo residual, sin embargo, estos proyectos propuestos han sido desarrollados y ajustados de acuerdo a los servicios que algunas empresas ofrecen en el mercado nacional y cuyos objetivos podrían satisfacer las necesidades de la empresa en estudio.

6.3.1 Aspectos Generales

En esta etapa del proyecto, ya se encuentran identificados los riesgos a los que la organización requiere llegar, por tal motivo es importante que se puedan llevar a cabo los proyectos que sean necesarios para permitir a la organización incrementar su nivel de seguridad y alcanzar el objetivo planteado.

Los proyectos que a continuación se detallan, están agrupados en base a las recomendaciones que fueron planteadas luego de la fase del análisis de riesgo anteriormente realizada.

6.3.2 Objetivos de los proyectos

Dentro del presente documento, se establecen los siguientes objetivos a cumplir a través de los proyectos a realizarse:

- Garantizar la disponibilidad, integridad y confidencialidad de la Información.
- Ejecución de proyectos dentro de los cronogramas establecidos, garantizando la disponibilidad de los recursos tecnológicos.
- Generar confianza en los clientes y proveedores, garantizando la correcta ejecución y gestión de la información.
- Reducir o minimizar el impacto, en base a acciones preventivas, a un nivel de aceptación de los riesgos identificados.
- Aportar con la evolución de la organización, en materia de seguridad de la información, basado en las mejores prácticas.
- Establecer una Política de Gestión de Seguridad de la Información y planes de divulgación de la misma.
- Otorgar herramientas que permitan establecer la salud de la organización en materia de seguridad de la información.

El detalle de los proyectos se encuentra dentro del Anexo 6 - Propuesta de proyectos SGSI.

6.3.3 Alcance de los proyectos a ejecutarse

Los proyectos establecidos en el presente documento están basados en la cuantificación del riesgo y del impacto que estos podrían generar a la organización, por ende, están enfocados en satisfacer las debilidades o vulnerabilidades identificadas. Estos proyectos se relacionan directamente con los activos de información identificados y los cuales están expuestos a una materialización significativa de las amenazas (impacto), lo que puede ocasionar la interrupción de los servicios operativos de la empresa; por esta razón, no sólo están considerados elementos tecnológicos, sino que se incluyen elementos importantes como personas, procesos y cultura organizacional.

6.3.4 Acuerdos de confidencialidad

Para los proyectos propuestos es indispensable que se cuente con acuerdos de confidencialidad de la información. Los acuerdos deberán garantizar que la información utilizada y analizada para el desarrollo de los proyectos no será publicada ni divulgada a través de ningún medio de comunicación, ya sea físico, digital, verbal etc.. u otra forma.

Las empresas que realicen la implementación de los proyectos deberán someterse a los lineamientos de los acuerdos de confidencialidad establecidos por la empresa y no podrán ser excluidos por ningún motivo.

6.4 AGRUPACIÓN DE PROYECTOS EN BASE A SU INTERRELACIÓN

Los proyectos a realizarse se han divido en tres grupos que forman parte de la mitigación de los riesgos de acuerdo a la interrelación existente entre ellos. Los proyectos son:

- Relacionados a desastres de origen industrial o natural.
- Relacionados a ataques intencionados.
- Relacionados a errores involuntarios.

A continuación se detallan ciertos aspectos, en forma de resumen, de los proyectos que podrían ser ejecutados por la empresa RADICAL CIA. LTDA. y en los cuales se contemplan los costos, cronogramas, relación con los activos identificados y mecanismos de control o acciones a seguir dentro de los proyectos. Estos proyectos se encuentran detallados, en su totalidad, dentro del Anexo 5 – Propuesta de Proyectos.

6.4.1 Relacionados a desastres de origen industrial o natural

Antecedentes

El presente proyecto a implementar, se basa en la creación o fortalecimiento de los controles que se encuentran relacionados a seguridad física, ambiental y adicionalmente pretende generar un impacto positivo en la cultura organizacional, de forma que se tome conciencia, conocimiento de los riesgos y su mitigación a través de buenas prácticas.

El alcance definido para el proyecto está relacionado, específicamente, con las instalaciones y hardware:

- Edificio
- Granja de servidores VMware

Acciones a implementar

A continuación se muestra un resumen de las acciones que están contempladas en el proyecto:

- Periodicidad y mantenimiento de equipos (existentes y los adquiridos en base al análisis de brecha)
- Acuerdos de niveles de servicio o SLA´s.
- Adquisición de seguros frente a la protección de desastres industriales o naturales.
- Capacitación al personal en mecanismos de operación, auxilio, evacuación etc.
- Gestión de equipos de monitoreo de alerta temprana o evacuación.
- Gestión de la comunicación con entidades de seguridad y auxilio como: bomberos, policía, ECU 911 etc.

Cronograma

El cronograma establecido para el proyecto tiene un tiempo de duración de tres meses. Este cronograma puede ser modificado de acuerdo a los tiempos que la empresa necesite.

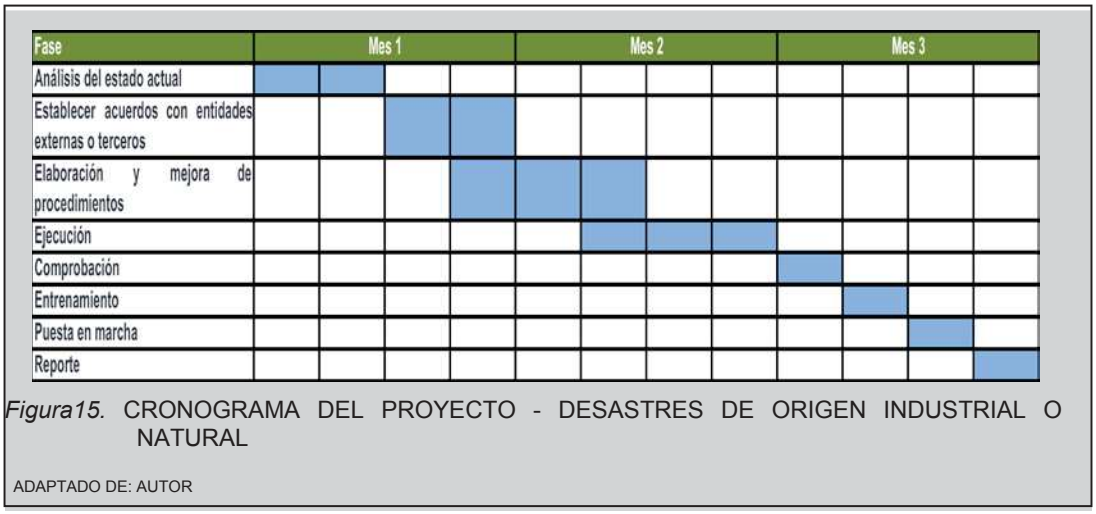

Figura15. CRONOGRAMA DEL PROYECTO - DESASTRES DE ORIGEN INDUSTRIAL O NATURAL

ADAPTADO DE: AUTOR

Costos

A continuación se muestran los costos del proyecto. Los precios están basados en relación a las ofertas recibidas de especialistas en estas

áreas y con quienes la empresa se presenta para proyectos o licitaciones que son trabajadas conjuntamente.

Tabla 16. COSTOS DEL PROYECTO RELACIONADO A DESASTRES DE ORIGEN INDUSTRIAL O NATURAL

Integrante	% Participación	Honorarios
Gerente de proyecto	20	$5.000,00
Coordinador de proyecto	20	$4.000,00
Consultores	60	$5.000,00

Costo real del proyecto: $29.000,00.

6.4.2 Relacionados a ataques intencionados

Antecedentes

El presente proyecto busca crear y endurecer los controles existentes en seguridad lógica y física. Dentro de este ámbito se contemplan los ataques lógicos y físicos que pueden ser ejecutados por personal externo, pero no se descarta, que dichos ataques pueden ser originados por personal interno.

El presente proyecto pretende cubrir los activos de información como: hardware, aplicativos, bases de datos, instalaciones, servicios y equipamiento informático de forma específica en:

- Instalaciones
- Granja de servidores VMware
- Directorio Activo

- Servidor de bases de datos
- Servidor de correo electrónico
- CRM
- Base de datos ERP
- Personal técnico e ingenieros especialistas

Acciones a implementar

Dentro de las acciones a implementar se plantea la ejecución de un análisis de vulnerabilidades a nivel tecnológico, físico y del personal, partiendo de este análisis se propone que la empresa realice las siguientes acciones:

- Análisis de vulnerabilidades y Ethical Hacking
- Acuerdos de niveles de servicio o SLA`s
- Periocidad y mantenimiento de equipos existentes
- Adquisición de seguros o repuestos inmediatos frente a la protección de equipamiento tecnológico importante.
- Capacitación al personal en mecanismos de prevención de amenazas e intrusos.
- Gestión de equipos de monitoreo y alerta temprana ante ataques o amenazas.
- Generación de políticas y procedimientos relacionados a los activos comprometidos y objetivos del proyecto.

Cronograma

El cronograma establecido para el proyecto tiene un tiempo de duración de tres meses. Este cronograma puede ser modificado de acuerdo a los tiempos que la empresa necesite.

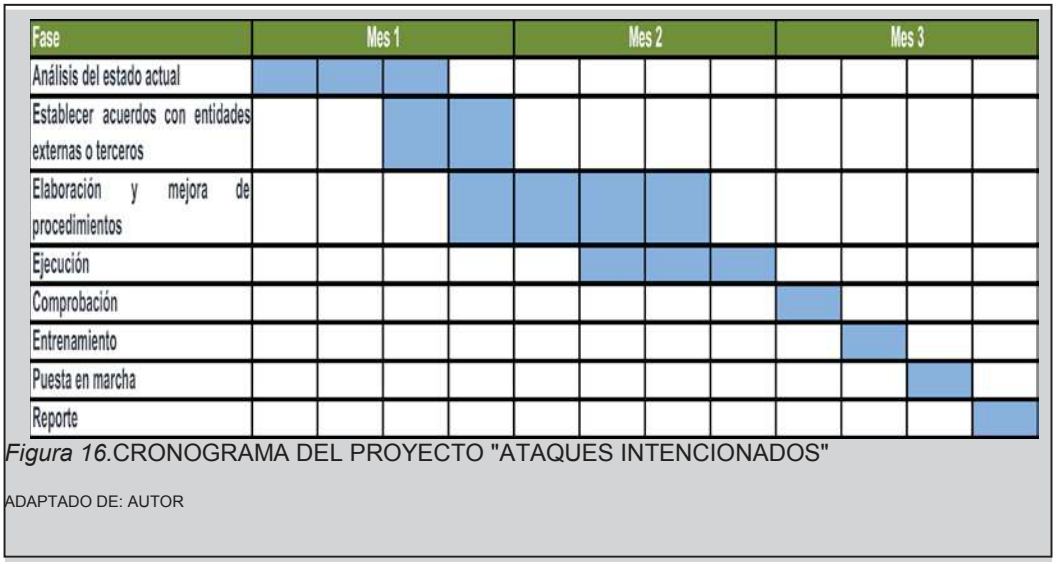

*Figura 16.*CRONOGRAMA DEL PROYECTO "ATAQUES INTENCIONADOS"

ADAPTADO DE: AUTOR

Costos

A continuación se muestran los costos del proyecto. Los precios están basados en relación a dos ofertas recibidas de empresas, de las cuales, una es nacional y la otra es del extranjero, con quién la empresa tiene convenios. Partiendo de estas cotizaciones se promedia el valor para contar con un valor estimado.

Tabla 17. COSTOS DEL PROYECTO RELACIONADO A ATAQUES INTENCIONADOS

Personal	Cantidad	Precio Unitario	Tempo de participación (meses)	Precio Total
Consultor Senior	1	$3.000,00	3	$9.000,00
Consultor Junior	3	$1.500,00	3	$4.500,00
Director de proyectos	1	$2.500,00	3	$7.500,00
Consultor CEH	1	$3.000,00	1	$3.000,00
				$24.000,00

6.4.3 Relacionados a errores involuntarios

Antecedentes

El presente proyecto se basa en la creación, implementación y fortalecimiento de controles existentes, relacionados a seguridad física, lógica complementaria y adicionalmente, involucra la creación de mecanismos de control que para el personal responsable del manejo y administración de los activos críticos de la organización.

El proyecto planteado pretende generar una cultura organizacional, a todo nivel, en el manejo y gestión de la información. Se contemplan dentro del proyecto: charlas, planes de divulgación de Seguridad de la Información y formas reducción de los riesgos a través de la culturización.

El presente proyecto pretende cubrir los activos de información como: hardware, aplicativos, personal, bases de datos, instalaciones, servicios y equipamiento informático, de forma específica en:

- Directorio Activo principal

- Servidor de Base de Datos
- Servidor de correo
- Granja de Servidores Vmware
- Servidor CRM
- Administración Vmware
- File Server
- Antivirus
- ERP
- ERP Database
- Internet
- Correo Electrónico
- Red LAN
- Red WAN
- Staff Infraestructrura y Telecomunicaciones
- Personal directivo y general

Acciones a implementar

Dentro de las acciones consideradas, se plantea la ejecución de un análisis de vulnerabilidades a nivel tecnológico y del personal tacnológico, adicional a esto, un análisis de la madurez tecnológica y de seguridad de la información enfocado en el personal administrativo, financiero, gerencial y personal en general. Partiendo de este análisis se propone que la empresa realice las siguientes acciones:

- Elaboración y divulgación de políticas de seguridad, que incluye: charlas de concientización para la utilización correcta de medios tecnológicos y protección de la información.

- Generación o revisión de una Política de Seguridad de la Información, normas para control de fugas de información y procedimientos para contratación de personal basados en análisis de perfiles.
- Hardening de equipamiento tecnológico.
- Políticas de gestión y seguridad en los activos involucrados dentro del proyecto.

Cronograma

El cronograma establecido para el proyecto tiene un tiempo de duración de cuatro meses. Este cronograma puede ser modificado de acuerdo a los tiempos que la empresa necesite.

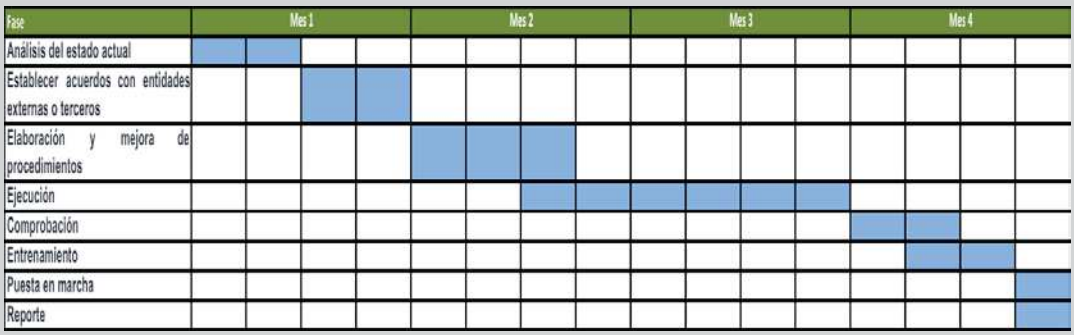

Figura17. CRONOGRAMA DEL PROYECTO "ERRORES INVOLUNTARIOS"

ADAPTADO DE: AUTOR

Costos

Los costos que se muestran a continuación están dados por una empresa extranjera, la cual mantiene un convenio con RADICAL CIA. LTDA. para trabajos en conjunto.

Tabla 18. COSTOS DEL PROYECTO RELACIONADO A ERRORES INVOLUNTARIOS

Personal	Cantidad	Precio Unitario	Tempo de participación (meses)	Precio Total
Consultor Senior	1	$3.000,00	4	$12.000,00
Consultor CEH	1	$3.000,00	1	$3.000,00
				$15.000,00

6.5 ANÁLISIS DE RIESGO Y RIESGO RESIDUAL

En base al análisis de Riesgo realizado y ponderado en base a la cuantificación establecida por la compañía, se diseñan varios mecanismos de control o medidas de mitigación, sin embargo, estos mecanismos no pueden ser suficientes para minimizar el riesgo.

El valor de Riesgo que se identifica, posterior a la implementación de los mecanismos de control, se lo denomina Riesgo Residual. Este Riesgo Residual se lo podrá mitigar a través del ciclo de mejora continua y umbrales cada vez más bajos de riesgo para disminuirlo a valores cercanos a 0% o casi nulos, aunque es un poco probable que esto suceda, ya que no se podría mantener un total control sobre las amenazas existentes que afectan a los activos de la información.

A continuación y en forma ilustrativa, se muestra el análisis del Riesgo Residual, pero por la cantidad de datos que son generados se colocan sólo un cierto grupo de activos de información. El detalle de este análisis se encuentra en el Anexo 4 - Análisis de Riesgo.

Tabla 19. ANÁLISIS DE RIESGO Y RIESGO RESIDUAL

ACTIVO		Valor del Activo de 1 a 5	AMENAZA		RIESGO	CONTROLAR	ACCIÓN	MECANISMOS DE CONTROL	REDUCCION DEL RIESGO	REDUCCIÓN	RIESGO RESIDUAL
I01	Oficinas	4	N01	Fuego	**20%**	SI	Mitigar	Sistema de supresión y protección contra incendios	70%	14%	6%
		4	N02	Daños por agua	**20%**	SI	Mitigar	Detectores de humedad	70%	6%	14%
		4	N03	Otros desastres Naturales	**20%**	SI	Transferir	Poliza de seguros	60%	8%	12%
		4	I01	Fuego	**20%**	SI	Mitigar	Sistema de supresión y protección contra incendios	70%	6%	14%
		4	I02	Daños por agua	**20%**	SI	Mitigar	Detectores de humedad	70%	6%	14%
		4	I11	Emanaciones electromagnéticas	**20%**	SI	Mitigar	Sistema de protección eléctrico	50%	10%	10%
		4	A11	Acceso no autorizado	**24%**	SI	Mitigar	Video vigilancia y tarjetas de proximidad	70%	7%	17%
		4	A26	Ataque destructivo	16%	NO		N/A	0%	0%	0%
		4	A27	Ocupación enemiga	16%	NO		N/A	0%	0%	0%
H01	Controlador de dominio principal	3	N01	Fuego	15%	NO		N/A	0%	0%	15%
		3	N02	Daños por agua	12%	NO		N/A	0%	0%	12%
		3	N03	Otros desastres Naturales	12%	NO		N/A	0%	0%	12%
		3	I01	Fuego	15%	NO		N/A	0%	0%	15%
		3	I02	Daños por agua	12%	NO		N/A	0%	0%	12%
		3	I03	Contaminacion Mecanica	12%	NO		N/A	0%	0%	12%
		3	I04	Contaminación electromagnética	6%	NO		N/A	0%	0%	6%
		3	I05	Avería de origen físico o lógico	18%	NO		N/A	0%	0%	18%
		3	I06	Corte del suministro eléctrico	18%	NO		N/A	0%	0%	18%
		3	I07	Condiciones inadecuadas de temperatura o humedad	9%	NO		N/A	0%	0%	9%
		3	I11	Emanaciones electromagnéticas	6%	NO		N/A	0%	0%	6%
		3	E02	Errores del administrador	**27%**	SI	Mitigar	Procedimientos y políticas de gestión del activo	70%	8%	19%
		3	E23	Errores de mantenimiento / actualización de equipos (hardware)	**27%**	SI	Mitigar	Procedimientos y contratos de mantenimiento preventivo	70%	8%	19%
		3	E24	Caída del sistema por agotamiento de recursos	**24%**	SI	Mitigar	Sistema de monitoreo y alertas tempranas	70%	7%	17%
		3	E25	Pérdida de equipos	**36%**	SI	Mitigar	Control de acceso fisico y pólizas de seguro	70%	11%	25%
		3	A06	Abuso de privilegios de acceso	**36%**	SI	Mitigar	Sistema de monitoreo y alertas tempranas	70%	11%	25%
		3	A07	Uso no previsto	18%	NO		N/A	0%	0%	18%
		3	A11	Acceso no autorizado	18%	NO		N/A	0%	0%	18%
		3	A15	Modificación deliberada de la información	18%	NO		N/A	0%	0%	18%
		3	A23	Manipulación de los equipos	**27%**	SI	Mitigar	Procedimientos de manipulación de equipamiento	70%	8%	19%
		3	A24	Denegación de servicio	**27%**	SI	Mitigar	Implementar políticas y equipamiento para DDoS	80%	5%	22%
		3	A25	Robo	**24%**	SI	Mitigar	Controles de acceso fisico y lógico	60%	10%	14%
		3	A26	Ataque destructivo	**36%**	SI	Mitigar	Procedimientos de backup y levantamiento de equipamiento alterno	80%	7%	29%

El nivel de criticidad establecido dentro del presente proyecto fue el considerado por los Directivos de la organización y con el cual esperan obtener un nivel de Madurez III - “Proceso Definido”, reduciendo su nivel de criticidad a los mayores a 20% en su nivel de riesgos (umbral establecido) a través de mecanismos de control propuestos, generación de procedimientos y documentación necesaria para su obtención.

Las consideraciones de cómo mitigar los riesgos establecidos son puestos a consideración de la organización, a fin de que se evalúen las alternativas y se opte por la mejor forma de mitigación.

El Riesgo Residual, mostrado en la tabla anterior (Ver Tabla 19), se desarrolló en forma ilustrativa y se considera como una supuesta situación posterior a la implementación de los proyectos ejemplares propuestos.

CAPÍTULO VII

7. ANÁLISIS DE POSIBLES RESULTADOS

7.1 ANÁLISIS DE CUMPLIMIENTO EN BASE A LA NORMA ISO/IEC 27002:2005

Para poder establecer el nivel de cumplimiento que la organización tiene en relación con la guía de mejores prácticas ISO/IEC 27002:2005, se utiliza la evaluación de cada uno de los controles en base a la siguiente tabla:

Tabla 20. ESCALA DE MADUREZ DE LOS CONTROLES

Nivel	Porcentaje	Descripción
Inexistente	0%	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
Inicial / Ad-hoc	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
Reproducible, pero intuitivo	50%	Los procesos se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
Proceso definido	90%	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
Gestionado y medible	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
Optimizado	100%	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Partiendo del nivel de cumplimiento de cada control, se pondera el nivel en cada uno de los 11 dominios o áreas de control, de forma que permita

evidenciar el nivel de madurez actual de la organización. Anexo 8 - Modelo de Madurez de la Capacidad (CMM) Inicial.

7.2 EVALUACIÓN DEL NIVEL DE MADUREZ DE LA ORGANIZACIÓN

En el siguiente cuadro y con base a los controles establecidos por la norma ISO/IEC 27002:2005 (Ver Anexo 6 - Modelo de Madurez de la Capacidad (CMM) Final) se procede con una ponderación, en base a los controles que la empresa desea implementar. A continuación se detalla un posible nivel de cumplimiento en base a los controles y se muestran sólo una parte de los mismos:

Tabla 21. NIVELES DE CUMPLIMIENTO POR CONTROLES ISO 27002:2005

CONTROLES ISO 27002:2005			Estado	% Efectividad
Clausula	**Sec**	**Control/Objetivo de Control**		
Politica de Seguridad		Política de seguridad de la información		50%
	1.1	Documento de política de seguridad de la información	Total	100%
	1.2	Revisión de la política de seguridad de la información	No será implementada inicialmente	0%
			Efectividad conjunta:	**50%**
Aspectos Organizativos de la seguridad de la información		Organización Interna		27%
	2.1	Compromiso de la máxima autoridad de la organización con la seguridad de la información	Total	100%
	2.2	Coordinación de la Gestión de la Seguridad de la Información	Parcial 1	15%
	2.3	Asignación de responsabilidades para la seguridad de la información	No será implementada inicialmente	0%
	2.4	Proceso de autorización para nuevos servicios de procesamiento de la información	No será implementada inicialmente	0%
	2.5	Acuerdos sobre Confidencialidad	Total	100%
	2.6	Contacto con las autoridades	No será implementada inicialmente	0%
	2.7	Contactos con grupos de interés especiales	No será implementada inicialmente	0%
	2.8	Revisión independiente de la seguridad de la información	No será implementada inicialmente	0%
		Terceros		0%
	2.9	Identificación de los riegos relacionados con las partes externas	No será implementada inicialmente	0%
	2.10	Consideraciones de la seguridad cuando se trata de clientes	No será implementada inicialmente	0%
	2.11	Consideraciones de la seguridad de los acuerdos con terceras partes	No será implementada inicialmente	0%
			Efectividad conjunta:	**19%**
Gestión de Activos		Responsabilidad sobre los activos.		43%
	3.1	Inventario de activos.	Total	100%
	3.2	Responsable de los activos	No será implementada inicialmente	0%
	3.3	Uso aceptable de los activos.	Parcial 2	30%
		Clasificación de la información.		50%
	3.4	Directrices de clasificación de la información	Total	100%
	3.5	Etiquetado y manejo de la información	No será implementada inicialmente	0%
			Efectividad conjunta:	**46%**

Los controles restantes se encuentran dentro del Anexo 6 - Modelo de Madurez de la Capacidad (CMM) Final.

7.3 RESULTADOS ESPERADOS

En base al análisis inicialmente efectuado, en el cual la organización se encuentra en un nivel de madurez “Inexistente”, los Directivos determinan que la organización deberá alcanzar, en los próximos ocho meses, un nivel de madurez III “Proceso Definido”.

Para obtener este nivel de madurez, la empresa determina los controles que inicialmente implementará y los cuales cuentan con tareas o actividades específicas, que permiten mejorar la efectividad de cada control y por ende del dominio. Adicionalmente se pondera el cumplimiento de cada control en relación con el dominio al que pertenece a fin de determinar, el posible nivel de cumplimiento, en relación a la norma utilizada dentro de la empresa en estudio. (Ver Anexo 6 - Modelo de Madurez de la Capacidad (CMM) Final)

A continuación se muestran los porcentajes de cumplimiento que la empresa puede alcanzar, en base a los controles a implementar por cada dominio,

Tabla 22. PORCENTAJE DE CUMPLIMIENTO POR DOMINIO

Dominio	Porcentajes de cumplimiento Inicial
Política de seguridad	50%
Organización de la SI.	19%
Gestión de activos.	46%
Seguridad en los recursos humanos	56%
Seguridad física y ambiental	21%
Gestión de comunicaciones y operaciones.	20%
Control de acceso.	32%
Adqui, desar y mant de Sist. Infor	10%
Gestión de incidentes	43%
Gestión de continuidad de negocio	0%
Cumplimiento	0%

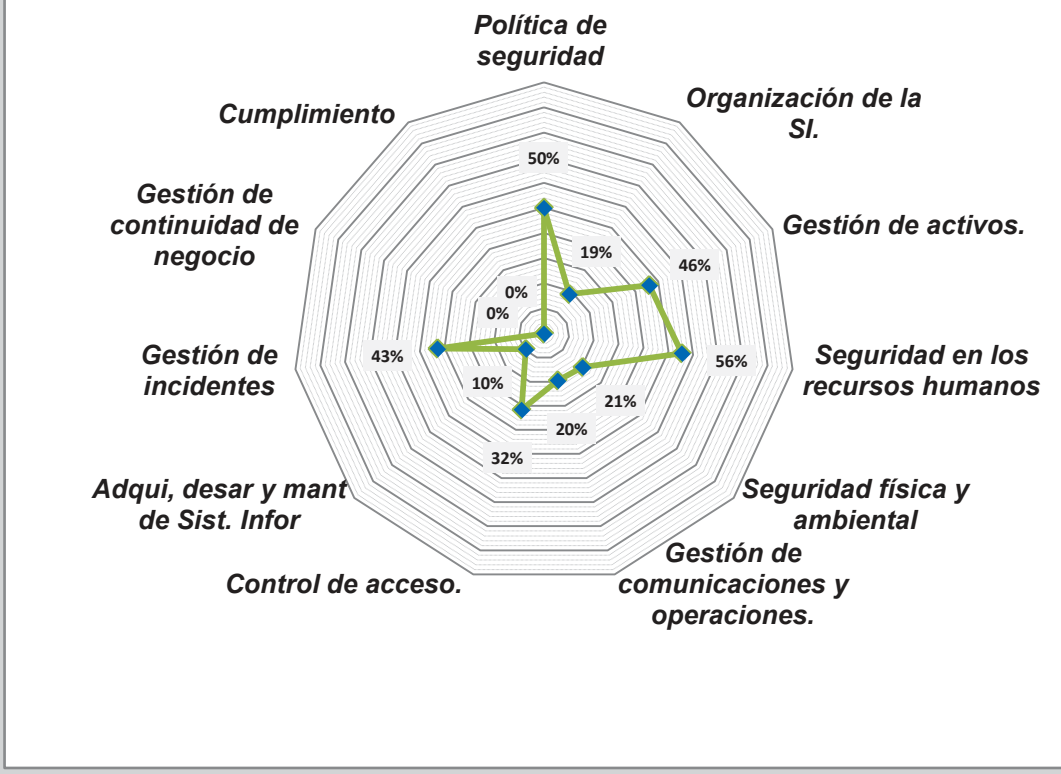

Figura 18. DIAGRAMA RADAR DE PORCENTAJES DE CUMPLIMIENTO

TOMADO DE: ISO 27000 - INFORMATION SECURITY STANDARDS

En este capítulo se demuestra que la organización debe incluir el Ciclo de Mejora Continua, a fin de alcanzar el nivel de madurez que proponen sus Directivos e implementar la totalidad de los controles propuestos acorde a los dominios. La empresa contempla que en una segunda etapa se aumentarán y mejorarán las actividades existentes hasta llegar al nivel de madurez deseado, el cual debe ser nuevamente evaluado al final de la implementación total de controles establecidos inicialmente.

Adicionalmente, se muestra el resultado del análisis de brecha realizado inicialmente, el cual está basado en los controles de la norma ISO 27002:2005 y que se encuentra dentro del Anexo 8 (Ver Anexo 8- Modelo

de Madurez de la Capacidad (CMM) Inicial), e identificar y comparar el estado inicial de la empresa y el estado que posiblemente se podrá alcanzar al finalizar la implementación total de los controles establecidos inicialmente por RADICAL CIA. LTDA.

A continuación mostraremos el resultado obtenido en base al nivel de cumplimiento de cada uno de los controles especificados en la norma ISO 27002:2005 y que se encuentra dentro del Anexo 8 - Modelo de Madurez de la Capacidad (CMM) Inicial:

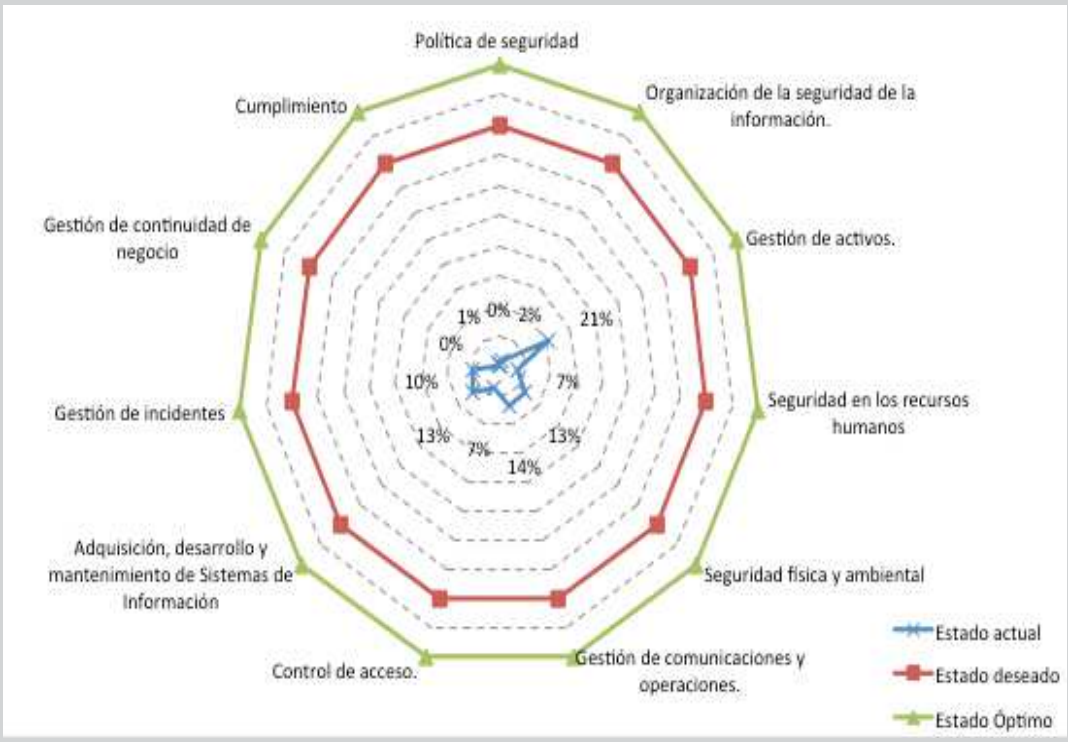

Figura 19. DIAGRAMA RADAR MADUREZ INICIAL

TOMADO DE: ISO2700 - INFORMATION SECURITY STANDARDS

Como se puede observar inicialmente el dominio de mayor efectividad a nivel de controles, realizados en forma empírica, es el de Gestión de Activos y al final de la implementación del Sistema de Gestión de

Seguridad de la Información, el dominio de mayor efectividad sería el de Seguridad de Recursos Humanos, el cual está relacionado con los riesgos identificados dentro del activo de información Personas.

CAPÍTULO VIII

8. CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

Luego de la elaboración del presente documento se han podido determinar las siguientes conclusiones:

1. Los problemas identificados inicialmente pueden ser cuantificados, gestionados y analizados, pero, sólo correspondieron a problemas que fueron percibidos por los actores de la organización. Estos problemas se encuentran atados a otros distintos, que pudieron ser identificados con la utilización del método de Marco Lógico, el cual nos permitió la identificación a mayor detalle y de la misma forma la evaluación de mecanismos de solución.
2. RADICAL CIA. LTDA. presenta varias vulnerabilidades que están atadas a sus activos de información y se constata que uno de los principales problemas identificados, que son las fugas de información, es a través del personal interno, ya que es el activo que representa un nivel de más alto de riesgo con valores entre el 30% y 60% de acuerdo a la ponderación realizada a través de sus informantes calificados.
3. Para la implementación de un Sistema de Gestión de Seguridad de la Información es imprescindible que se delimite claramente el alcance, el cual está relacionado con: el tamaño de la organización, ubicación geográfica, tiempo, recursos internos, procesos críticos, activos relacionados a los procesos y adicionalmente se contemple que es el SGSI no es un método de remediación inmediato sino evolucionario y que depende de alto nivel de compromiso.
4. Existen muchos métodos de Gestión de Riesgos, sin embargo, en base a la investigación realizada, se tomó como método de Análisis

y Gestión de Riesgos MAGERIT, el cual permitió que el análisis realizado sea más práctico y con matrices de ponderación entendibles, obviamente, permitiendo en forma efectiva y adecuada el análisis propuesto. La norma ISO 27000 establece que se puede utilizar la norma ISO 27005 para Análisis y Gestión del Riesgo de Seguridad de la Información pero no limita a que sea el único método que puede ser utilizado.

5. Se plantean tres proyectos de solución a la problemática identificada y se concluye que se deberán tomar acciones adicionales para alcanzar el Nivel de Madurez propuesto por la organización, lo que incluye el Ciclo de Mejora Continua para obtener los resultados que la empresa desea. Estas acciones conllevan a que se mejore o implemente mecanismos adicionales y que deberán ser nuevamente evaluados por la organización.
6. Es importante incluir que todas las acciones que se puedan tomar para el mejoramiento de la Seguridad de la Información, no serán factibles si no existe el compromiso del activo más importante de la organización, las personas, ya que son los gestores y responsables de los demás activos. Durante el presente análisis se evidenció que la falta de comunicación interna afecta en gran medida a la organización, por ende, es importante que el personal esté empoderado en la Seguridad. Las personas están expuestas a vulnerabilidades del tipo Ingeniería Social y si no existe una política de comunicación, acompañada de un empoderamiento probablemente, la fuga de información intencionada o por desconocimiento, conlleven a la pérdida de negocios, clientes u oportunidades de mejora empresarial.
7. El no contar con un personal responsable del área de Seguridad de la Información o un Oficial de Seguridad de la Información ha originado que la empresa desconozca de políticas o

procedimientos que permitan mitigar los riesgos a los que están expuestos los activos de la información.

8. La falta de un SGSI ha llevado a que la empresa presente pérdidas económicas o proyectos, sin dejar de lado las exigencias de algunos de sus clientes o proveedores en el cumplimiento de algún estándar en Seguridad de la Información que les garantice una correcta gestión de la información.

8.2 RECOMENDACIONES

1. Se recomienda que para proyectos en los cuales no se cuente con una visión clara de la problemática y soluciones se utilice el método del Marco Lógico, que permite obtener una visión más amplia de los objetivos a cumplir para satisfacer los problemas encontrados a través de sus recomendaciones como lo son: árbol de problemas, árbol de objetivos, informantes calificados.
2. Se recomienda la implementación de mecanismos de control y políticas para la contratación de personal, de la misma forma un análisis de perfiles profesionales y acuerdos de confidencialidad, a fin de mitigar las fugas de información que fueron ponderadas con los mayores niveles en el análisis de riesgo realizado.
3. Se recomienda determinar un alcance viable, factible y con niveles de madurez razonables para la implementación de un SGSI. Así como permitir el uso de recursos tecnológicos y personal interno como acompañamiento en la implementación para que en lo posterior pueda ser el generador de un análisis similar al realizado, sin depender de recursos adicionales.
4. Se recomienda la utilización del método MAGERIT para Gestión y Análisis de Riesgo ya que involucra atributos de la información adicionales a los de la ISO 27000:2005 como lo son: Trazabilidad y Autenticidad.

5. Se recomienda el análisis de los objetivos de los proyectos propuestos, de forma que permita la ayudar con la mitigación de los riesgos, partiendo de los ponderados con el más alto nivel.
6. Se recomienda realizar un plan de comunicación a todo el personal en Gestión de Seguridad de la Información, adicionalmente, la prioridad de realizar un test de vulnerabilidades del equipamiento tecnológico e ingeniería social, ya que permitirá a la empresa conocer aún más en detalle sus vulnerabilidades y así remediar las fugas de información.
7. Se recomienda que para cumplir con el Sistema de Gestión de Seguridad de la Información, se nombre a una persona especializada en Seguridad de la Información o se la capacite como ISO Lead Implementor o ISO Lead Auditor y se comprometa a designar y capacitar a funcionarios internos para llevar a cabo las actividades necesarias que han sido presentadas en este documento, incluyendo los planes de comunicación y la implementación de los controles propuestos, adicionalmente especificar actividades o tareas que permitan mejorar el nivel de efectividad de cada control.
8. Se recomienda la implementación del Sistema de Gestión de Seguridad de la Información, el cual deberá realizarse en el menor tiempo posible, ya que al ser una empresa dedicada a brindar servicios y productos de Seguridad Informática, le permitirá garantizar la confianza que sus clientes y proveedores necesitan, además de generar una fortaleza sobre sus competidores y, en mejor forma, si la empresa opta por una certificación.

REFERENCIAS

Alexander, A. G. (2012). Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001: 2005. Obtenido de http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf

Andes. (11 de 5 de 2012). tecno.americaeconomia.com. Obtenido de tecno.americaeconomia.com: http://tecno.americaeconomia.com/noticias/ecuador-no-hay-estadisticas-que-indiquen-perdidas-por-ataques-ciberneticos

Banda, H. (2013). Análisis de problemas y diseño de soluciones. Quito: Propia.

Broderick, J. S. (2006). ISMS, security standards and security regulations.information security technical report, 11(1), 26-31.

CONTROLES EN SISTEMAS DE INFORMACIÓN. Revista PUENTE, 6(1).

Chaves Calamita, M. E. G. (2004, December). EL LLAMADO «DELITO INFORMÁTICO». In Anales de la Facultad de Derecho (pp. 45-65).

Deming, P. (2005). Herramientas para la mejora continua. Ciclo de Deming. Disponible en: www. herramientas parapymes. com/herramienta-para-lamejora-continua-ciclodeming.

Díaz, M. (29 de octubre de 2009). www.delitosinformaticos.com. Recuperado el 16 de 2 de 2014, de www.delitosinformaticos.com:

http://www.delitosinformaticos.com/10/2009/proteccion-de-datos/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias#.U2UjTa15P8l

Economía, A. (11 de 9 de 2013). tecno.americaeconomia.com. Obtenido de http://tecno.americaeconomia.com/noticias/chile-destina-us200-millones-seguridad-informatica

Fort, J. G. (6 de 2010). http://www.iit.upcomillas.es. Obtenido de http://www.iit.upcomillas.es: http://www.iit.upcomillas.es/pfc/resumenes/4c2474cf9a017.pdf

Garay, A. D. C. Sistema para el Análisis y Gestión de Riesgos.

Giménez, G. B., Gómez, J. D. R., & Villegas, M. G. (2007). de gestión e información. Innovar, 17(29), 27-48.

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de Ingeniería Universidad de los Andes, (31), 109-118.

Guerrero Julio, M. L., & Gómez Flórez, L. C. (2013). GESTIÓN DE RIESGOS Y

Hiamnen, P. (s.f.). La ética del hacker y el espíritu de la era de la información. Obtenido de http://eprints.rclis.org/12851/1/pekka.pdf

http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf

Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES). (7 de 2005). www.ug.edu.ec. Obtenido de

www.ug.edu.ec: http://www.ug.edu.ec/dipa/senacyt/cepal_manual_marco_logico.pdf

ISO 27000, 2013, pp. 2-5 Iso 27000. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO-27000. (2009). www.iso2700.es. Recuperado el 10 de 11 de 2013, de www.iso2700.es:

León Lafebré, M., Mota Orrala, E., & Navarrete Zambrano, J. (2013). Implementación de un SGSI usando la norma ISO 27000 sobre un sitio de comercio electrónico para una nueva Institución Bancaria utilizando la metodología Magerit (Doctoral dissertation).

líderes, R. (7 de 8 de 2012). RevistaLíderes.ec. Obtenido de http://www.revistalideres.ec/tecnologia/empresas-Ecuador-registraron-incidente-Eset_0_751124909.html

Magerit. (2012). http://www.seap.minhap.gob.es. Obtenido de Ministerio de Hacienda y Administraciones Públicas de España: http://www.seap.minhap.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0/parrafo/Magerit_2012/Magerit_v3_libro1_metodo.pdf

Malave, N. (Febrero de 2007). uptparia.edu.ve. Obtenido de Universidad Politécnica Territorial de Paria: http://uptparia.edu.ve/documentos/F%C3%ADsico%20de%20Escala%20Likert.pdf

McAfee. (s.f.). McAfee-Resources.Obtenido de http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf

Mega, G. P. (2009). Tesis de Maestría.

Murillo, B. J.-D.-C. (2012). http://repository.ean.edu.co. Recuperado el 17 de 11 de 2013, de Universidad EAN: repository.ean.edu.co/bitstream/10882/2692/1/MurilloCarol2012.pdf

Norma ISO 31000 versión 2009: Gestión de Riesgos – Principios y Guías. (11 de 2009). http://www.fecoopse.com. Obtenido de http://www.fecoopse.com: http://www.fecoopse.com/files/iso_31000_-_gestion_de_riesgos_-_espaol.pdf

NTE INEN- ISO/IEC 27000. (2013). www.iso27000.es. Obtenido de www.iso27000.es: http://www.iso27000.es/download/doc_sgsi_all.pdf

NTE INEN- ISO/IEC 27005. (6 de 8 de 2011). http://www.normalizacion.gob.ec/. Recuperado el 19 de 4 de 2014, de INEN-instituto Ecuatoriano de Normalización: http://www.normalizacion.gob.ec/descargas

Orrego, V. M. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. Revista Pensamiento Americano, 4(6).

Orta, E., Ruiz, M., & Toro, M. (2009). Aplicación de las Técnicas de Modelado y Simulación en la Gestión de Servicios TI. Actas de los Talleres de las Jornadas de Ingeniería del Software y Bases de Datos, 3(1).

Pardo, C., García, F., Pino, F. J., Piattini, M., &Baldassarre, M. T. (2011). Método de integración para soportar la armonización de múltiples modelos y estándares. XVI Jornadas de Ingeniería del Software y Bases de Datos (JISBD 2011), Spain, 625-638

Peltier, T. R. (2005).Information security risk analysis. CRC press.

Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: Ingeniería, Vol. 16, No. 2, pág. 56-66.

Ramos. (6 de 11 de 2009). Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires. Recuperado el 15 de 11 de 2013, de http://www.cpciba.org.ar: http://www.cpciba.org.ar/archivos/adjuntos/seguridad.pdf

Symantec. (Abril de 2013). Symantec.com. Obtenido de https://scm.symantec.com/resources/istr18_en.pdf

Vicente, L. (6 de 2004). Redalyc.org. Obtenido de http://www.elcotidianoenlinea.com.mx/pdf/12615.pdf

Walton, M., & Deming, W. E. (1992). El método Deming en la práctica. Editorial Norma.

GLOSARIO DE TÉRMINOS Y ABREVIATURAS

- Aceptación del riesgo: Decisión de tomar o asimilar el riesgo.
- Amenaza: Causa potencial de un incidente que puede ocasionar daños a la información de una organización o la organización.
- Análisis de riesgo: Uso metódico de la información para estimar el riesgo a través de sus fuentes.
- APO: Es un dominio de COBIT 5 para Alinear, Planificar y Organizar. Sus siglas en inglés (Align, Plan and Organise, APO)
- Ataque: Intento de destrucción, alteración o inhabilitación a un sistema de información o a la información que procesa el sistema.
- Autenticidad: Es la característica o propiedad que permite la verificación de que una entidad es quien dice ser o que garantiza la fuente origen de la que procede la información.
- CEO (Chief Executive Officer): Director Ejecutivo de una organización. Es la persona que encabeza la empresa o el gobierno corporativo.
- Confidencialidad: Autorización de acceso de la información solamente por quienes se encuentren permitidos.
- Controles de seguridad: Prácticas, políticas y procedimientos realizados que permiten mantener los riesgos de seguridad por debajo del nivel de riesgo enfocado.
- Disponibilidad: Permitir y garantizar el acceso a la información en el instante que sea deseado.
- DSS: Es un dominio de COBIT 5 para Entregar, dar Servicio y Soporte. Sus siglas en inglés (Deliver, Service and Support, DSS)
- Framework: Marco de trabajo, es un conjunto de conceptos, prácticas y criterios estandarizados que sirven para resolver una problemática particular de índole similar.

- Hardening: Palabra que en inglés significa endurecimiento, y es un proceso mediante el cual se reducen los niveles de vulnerabilidades de los activos informáticos.
- Impacto: El valor que representa para una empresa cuando una amenaza se materializa sobre un activo.
- Integridad: Mantenimiento de la completitud de un dato.
- MEA: Es un dominio de COBIT 5 para Supervisar, Evaluar y Valorar. Sus siglas en inglés (Monitor, Evaluate and Assess, MEA)
- Probabilidad: Tasa de ocurrencia de que una amenaza suceda.
- Riesgo potencial: Los riesgos de los sistemas de información en un ambiente en el cual no cuenten con mecanismos de protección y sin controles.
- Riesgo residual: El nivel de riesgo que permanece posterior al tratamiento de los riesgos.
- Salvaguarda: Mecanismo o procedimiento que reduce el riesgo.
- SLA´s: Service Level Agreement o Acuerdo de Nivel de Servicio.
- Trazabilidad: Garantía de que en todo momento se podrá determinar quién realizó algo y en qué instante de tiempo lo realizó.
- Vulnerabilidad: Debilidad existe y que permite que una amenaza afecte a un activo.

ANEXOS