



Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática.

**Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para
Análisis y Gestión de Riesgos de Seguridad de la Información.**

Tesis de grado previo a la obtención del título de Ingeniera de Sistemas y Telemática

Autora: Geovanna Cordero Torres.

Director: MBA. Esteban Crespo.

Cuenca, Ecuador

2015

Dedicatoria

El presente trabajo va dedicado a mis abuelas Rosa e Inés.

A mis hermanas, Amanda e Isabella.

A mis primas y primos que son como mis hermanos: Diana, Jhoanna, Nathaly, Verónica, Nancy, Stephanie, Amy, Mauricio, Vinicio.

A mis dos tías que más que eso siempre han sido como unas madres para mí: Carmen y Yolanda, que cada instante me dieron su apoyo en este largo camino, brindándome sus consejos y dándome ánimo para no desvanecer en este arduo trabajo.

A mi hermana Pamela, la cómplice de cada uno de mis triunfos, la compañera que siempre está allí para brindarme su apoyo incondicional.

A mi querido esposo que cada día me brinda su apoyo incondicional para ir avanzando en esta difícil senda.

A mis amigos que estuvieron conmigo en todos los momentos, apoyándonos unos a otros para seguir adelante hasta culminar con esta extensa tarea. Hemos compartido y vivido experiencias que estoy segura que siempre las recordaremos.

Agradecimiento

En primer lugar quiero dar gracias a Dios por permitirme cumplir una meta más y llenar mi vida de personas y sucesos enriquecedores.

Quiero agradecerles a mi mami Chochi y a mi mami Carmen que sin el apoyo de ellas nunca hubiera llegado donde el día de hoy me encuentro.

A mi hermana Pamela y a mi esposo, por siempre estar a mi lado, darme fuerzas cuando más las necesito.


Quiero agradecer a mi profesor, Esteban Crespo, por el apoyo brindado a lo largo de mi trabajo de fin de carrera.

Resumen

El presente trabajo pretende realizar un estudio comparativo entre las metodologías MAGERIT y CRAMM , utilizadas para el análisis y gestión de riesgos de la Seguridad de la Información, en base a los mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo.

ABSTRACT

This paper aims to conduct a comparative study between CRAMM (CCTA Risk *Analysis* and Management Method), and MAGERIT (Methodology for Information Systems Risk Analysis and Management); both of which are used for the analysis and management of Information Security Risks, based on mechanisms identification of assets, identification of vulnerabilities, probability functions, variable risk measurement, and risk calculation.


Lourdes Crespo
UNIVERSIDAD DEL
AZUAY
Dpto. Idiomas

Lourdes Crespo
Translated by,
Lic. Lourdes Crespo

Índice de contenidos

Dedicatoria	I
Agradecimientos	II
Resumen	III
Abstract	IV
Introducción	- 1 -
Objetivos	- 2 -
Objetivo general.....	- 2 -
Objetivos específicos.....	- 2 -
Metodología	- 2 -
Capítulo 1	- 3 -
Seguridad informática.....	- 3 -
Definición.....	- 3 -
Principios de la seguridad informática.....	- 3 -
❖ Confidencialidad.....	- 3 -
❖ Integridad.....	- 3 -
❖ Disponibilidad.....	- 3 -
Actores de la seguridad informática.....	- 3 -
Vulnerabilidad.....	- 4 -
Identificación de vulnerabilidades.....	- 4 -
Amenazas.....	- 4 -
Riesgo.....	- 4 -
Activo.....	- 4 -
Impacto.....	- 4 -
Seguridad de la información.....	- 4 -
Involucrados de la Seguridad de la información.....	- 5 -
Gestión de riesgos.....	- 5 -
ISO 27001.- Tecnologías de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI).....	- 6 -
Establecimiento y gestión del SGSI.....	- 9 -
Implementar y operar el SGSI.....	- 10 -

Monitorizar y revisar el SGSI	- 11 -
ISO/IEC 27002:2005: Tecnologías de la información, técnicas de seguridad - código de buenas prácticas para la gestión de la seguridad de la información.	- 11 -
ISO / IEC 27005:2011: Tecnología de la información, técnicas de seguridad, información de gestión de riesgos de seguridad.	- 16 -
ISO 31000:2009: Gestión de riesgo, principios y directrices.....	- 17 -
MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información..	- 17 -
Objetivos de MAGERIT	- 18 -
CRAMM: (Risk Analysis and Management Methodology) Metodología para el análisis y la gestión de riesgos	- 19 -
Objetivo.....	- 19 -
CAPÍTULO 2.....	- 20 -
Estudio de la metodología MAGERIT	- 20 -
Objetivos de la metodología.....	- 22 -
Mecanismos de identificación de activos de información.....	- 23 -
Funciones de probabilidad	- 24 -
Variable de medición de riesgo	- 24 -
Cálculo de riesgo.....	- 24 -
Alineación con el estándar ISO27001	- 25 -
Alineación con el estándar ISO27002	- 26 -
Alineación con el estándar ISO27005	- 26 -
Alineación con el estándar ISO31000.....	- 27 -
CAPÍTULO 3.....	- 29 -
Estudio de la metodología CRAMM.....	- 29 -
Mecanismos de identificación de activos	- 31 -
Identificación de vulnerabilidades.....	- 31 -
Funciones de probabilidad a desarrollar.....	- 31 -
Variable de medición de riesgo	- 32 -
Cálculo de riesgo.....	- 32 -
Alineación con el estándar ISO27001	- 32 -
Alineación con el estándar ISO27002	- 33 -
Alineación con el estándar ISO27005	- 33 -
Alineación con el estándar ISO31000.....	- 34 -
CAPÍTULO 4.....	- 35 -

Análisis comparativo entre MAGERIT y CRAMM	- 35 -
CONCLUSIONES	- 43 -
RECOMENDACIONES	- 46 -
Bibliografía	- 47 -
ANEXOS	- 52 -

Introducción

El presente trabajo pretende realizar un estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para el análisis y gestión de riesgos de la Seguridad de la Información, en base a los mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo basándose en las ISO 27001, 27002, 27005 y 31000.

Fue desarrollado con la finalidad de identificar cuál de las dos metodologías es la que más se apega a la realidad de las pequeñas, medianas y grandes empresas. En donde se busca concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la gran necesidad de mitigar cada una de las vulnerabilidades que día a día se van presentando en el sistema.

Es por ello que se realiza una comparación entre las metodologías para poder decidir cuál de las dos es la que más se apega a la realidad de la PYMES. Dichas Metodologías fueron desarrolladas para la Gestión y Seguridad de la Información. Siendo aplicables para empresas de diferente naturaleza y dimensión. En este caso nos orientamos al Análisis y Gestión de las empresas PYMES.

Objetivos

Objetivo general: Realizar un estudio comparativo entre las metodologías MAGERIT y CRAMM para el análisis y gestión de riesgo tecnológico.

Objetivos específicos:

- Fundamentar y analizar teóricamente el concepto de análisis y gestión de riesgo basado en las normativas ISO 27001, 27002, 27005 y 31000.
- Comparar las metodologías MAGERIT y CRAMM utilizadas en el análisis y gestión de riesgo informático, en base a mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo.
- Emitir un documento comparativo entre las metodologías MAGERIT y CRAMM.

Metodología

La metodología que se va a utilizar es la investigativa-deductiva, basándose en un proceso de razonamiento, que intenta no sólo describir cada hecho, sino también ir dando explicaciones de cada uno.

Alcances y resultados esperados

El proyecto pretende emitir un documento del análisis comparativo de las metodologías MAGERIT y CRAMM en base a mecanismos para la identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo y cálculo de riesgo.

Capítulo 1

Marco Teórico

Seguridad informática

Definición: Es un conjunto de normas y procedimientos que son aplicados para salvaguardar un sistema informático. Su finalidad es garantizar que todos los recursos que conforman el sistema informático sean utilizados para el fin que fueron creados sin ninguna intromisión (Alcidez Germán, 2009)

Principios de la Seguridad Informática

- ❖ **Confidencialidad.-** Es la capacidad que posee el sistema para evitar que personas y organizaciones no autorizadas puedan acceder a la información (González Julián, 2010).

- ❖ **Integridad.-** Hace referencia a la validez y consistencia de cada elemento de información que se encuentra almacenada en un sistema informático.

- ❖ **Disponibilidad.-** Es una característica de la información que nos garantiza que esta se encuentra disponible, en el momento que sea requerida, para quien tiene la autorización de acceder a la información (González Julián, 2010).

Actores de la Seguridad Informática

Los actores son todos los individuos que de una u otra forma están involucrados con el manejo de la información, dentro de una organización.

Vulnerabilidad.- Son todas las debilidades que existen en un sistema de información, las mismas que permiten que este sea fácilmente atacado, violando el control de acceso y la confidencialidad de los datos y las aplicaciones existentes.

Identificación de vulnerabilidades

Cada una de las vulnerabilidades debe ser identificadas y valorizadas. (Burgos Jorge, Campos Pedro, 2010).

Amenazas.- Todo elemento o acción que sea capaz de dañar de una u otra forma la seguridad de la información. Pueden ser encontradas a partir de la existencia de vulnerabilidades dentro de un sistema informático.

Riesgo.- Es la probabilidad que tiene una amenaza para poder originarse produciendo un ataque a la organización.

Activo.- Hace referencia a todo lo que represente algún valor para la empresa y debe ser protegido.

Impacto.- Las consecuencias de la ocurrencia de las amenazas dentro de la organización.

Seguridad de la Información

Es un conjunto de reglas, planes y acciones que permiten asegurar la información existente en un sistema de información. (Martínez Cristina, 2005).

Involucrados de la Seguridad de la Informática.

Talento Humano.- Se encuentra constituido por personas que tienen los conocimientos especializados para planificar, organizar y administrar los sistemas informáticos.

Tecnología.- Constituida por: software, hardware, sistemas operativos, gestión de base de datos, redes.

Procesos.- Según Avendaño Gabriel, 2014, es una unidad de actividad que se caracteriza por ejecutar una secuencia de instrucciones, posee un estado actual y se encuentra relacionado con un conjunto de recursos de sistemas relacionados.

Riesgos informáticos.- Son exposiciones tales como atentados y amenazas a los sistemas de información. Existen tres tipos:

- Riesgos de datos.
- Riesgos de control.
- Riesgos estructurales.

Gestión de riesgos.- Permite seleccionar y establecer las medidas de seguridad apropiadas que ayudarán a controlar o eliminar los riesgos identificados dentro de nuestro sistema informático (Jaén Daylis, Pinedo Francisco; 2012).

ISO 27001.- Tecnologías de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI).

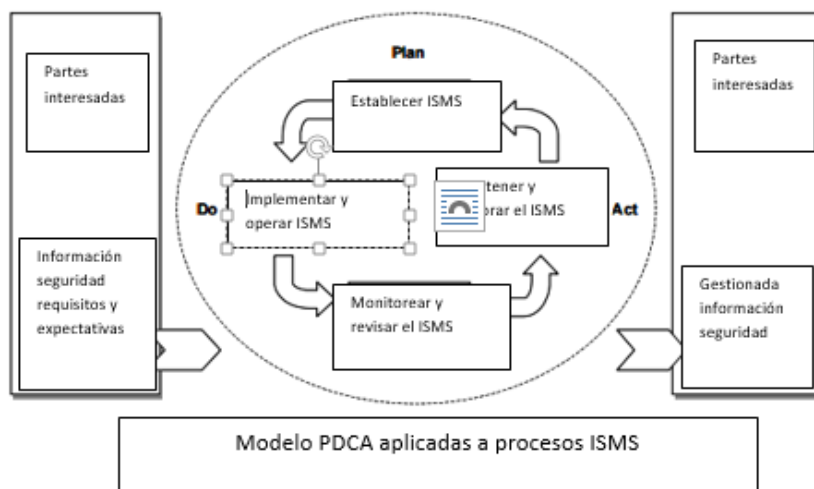
Publicada el 15 de octubre de 2005. Esta normativa es la principal de la serie de las normas ISO. Se ha preparado para proporcionar un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar SGSI. La normativa es aplicable a todas las organizaciones y puede ser utilizada por entidades internas o externas para evaluar la conformidad. Garantiza que se pueda satisfacer todas las necesidades de la organización.

La ISO 27001 proporciona altos niveles de seguridad en temas de datos confidenciales. Especifica los requerimientos para establecer, implantar, documentar, revisar, mantener y evaluar un sistema de gestión de la seguridad de la información. Anima a que los usuarios hagan hincapié en la importancia de (López, Rapha, 2014):

- ❖ La comprensión de los requisitos de seguridad de la información de una organización, la necesidad de establecer políticas y objetivos para la seguridad de la información.
- ❖ La aplicación y los controles de operación para gestionar los riesgos de la seguridad de información de una organización.
- ❖ El seguimiento y la revisión del rendimiento, la eficacia de SGSI.
- ❖ Mejora continua basada en mediciones objetivas.

La norma está basada en el modelo de proceso plan-Do-Check-Act.

Gráfico No 1
Esquema del plan Do-Check-Act



Fuente: Aranda José, 2005.

<https://www.dspace.espol.edu.ec/bitstream/123456789/8080/1/Implementaci%C3%B3n%20del%20primer%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf>

Plan: Establecer políticas, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información (López, Rahpa, 2014).

Hacer: Implementar y operar las políticas, controles procedimientos y procesos SGSI (Aranda José, 2005).

Revisar: Evaluar y donde sea posible medir el desempeño del proceso en comparación con la política (Aranda José, 2005; López, Rahpa, 2014).

Actuar: Tomar acciones correctivas y preventivas, basadas en los resultados de las auditorías (López, Rahpa, 2014).

Esta normativa propone que para el intercambio de información con terceros, se debe estimar las responsabilidades y procedimientos del envío, transferencia, recepción y confirmación de la información. (García Manuel, Quispe Carlos, Páez Luis, 2003)

Está constituida por dominios:

Dominio Política de Seguridad. Su objetivo es garantizar el soporte y gestión necesarios para la seguridad según los requisitos institucionales y normativos (ISOTools, 2014).

Dominio organización de la Seguridad de la Información. Su finalidad es instaurar un marco de referencia para la implementación y control de la seguridad de la información (ISOTools, 2014).

Dominio gestión de activos. Tiene como objetivo realizar una protección adecuada de los activos de la organización (ISOTools, 2014).

Dominio seguridad de los recursos humanos. Su objetivo es fijar las medidas necesarias para controlar la seguridad de la información, que sea manejada por los recursos humanos (ISOTools, 2014).

Dominio seguridad física y del ambiente. Nos permite proteger a las instalaciones de la organización y a toda la información que maneja (ISOTools, 2014).

Dominio gestión de las comunicaciones y operaciones. El objetivo es determinar el procedimiento y responsabilidades de las operaciones que realiza la organización (ISOTools, 2014).

Dominio control de acceso. Con él se asegura el acceso autorizado a los sistemas de información de la organización (ISOTools, 2014).

Dominio adquisición, desarrollo y mantenimiento de los sistemas de información. Está dirigido a aquellas organizaciones que desarrollen software internamente o que tengan un contrato con otra organización que sea la encargada de desarrollarlo. Se tiene que establecer los requisitos en la etapa de implementación o desarrollo del software para que sea seguro (ISOTools, 2014).

Dominio gestión de incidentes en la seguridad de la información. Se aplica un proceso de mejora continua en la gestión de percances de seguridad de la información (ISOTools, 2014).

Dominio gestión de la continuidad del negocio El objetivo es asegurar la continuidad operativa de la organización. Se requiere aplicar controles que eviten o reduzcan los incidentes de las actividades desarrolladas por la organización que puedan generar un impacto (ISOTools, 2014).

Dominio cumplimiento. Su finalidad es asegurar que los requisitos legales de seguridad referidos al diseño, operación, uso y gestión de los sistemas de información se cumplan. (Aranda José, 2005; García Manuel, Quispe Carlos, Páez Luis, 2003).

Establecimiento y gestión del SGSI

Según Robles Ramón y Rodríguez de la Roa Alvaro, 2006, sirve para definir el alcance y los límites del SGSI en términos de las características propias de la empresa. Se debe:

- ❖ Definir una política de SGSI: Esta política está constituida por marco de establecimiento de objetivos, se alinea con el contexto de la gestión del riesgo. Establece criterios con los cuales se evaluará el riesgo. Esta política debe ser aprobada por la dirección (Robles Ramón y Rodríguez de la Roa Alvaro, 2006).
- ❖ Definir el enfoque de evaluación de riesgos de la organización.
- ❖ Identificar los riesgos (Robles Ramón y Rodríguez de la Roa Alvaro, 2006).
- ❖ Analizar y evaluar los riesgos (Robles Ramón y Rodríguez de la Roa Alvaro, 2006).
- ❖ Identificar y evaluar las opciones para el tratamiento de los riesgos.
- ❖ Seleccionar los objetivos de control y controles para el tratamiento de los riesgos.
- ❖ Obtener la aprobación de gestión de los riesgos residuales propuestos.

Implementar y operar el SGSI

Para su implementación se debe:

- ❖ Formular un plan de tratamiento de riesgos que identifique la acción adecuada de la gestión de recursos, responsabilidades y prioridades para SGSI.
- ❖ Poner en práctica el plan de tratamiento de riesgos con el fin de alcanzar los objetivos de control previamente identificados. Aquí está incluido el examen de la financiación y la asignación de funciones y responsabilidades.
- ❖ Implementar los controles seleccionados para cumplir con los objetivos de control.
- ❖ Definir la forma de medir la eficacia de los controles o grupos de controles previamente seleccionados. (Calderón Diana, Estrella Martín, Flores Manuel; 2011)

Monitorizar y revisar el SGSI

Para la correcta monitorización del SGSI, se debe:

- ❖ Ejecutar el seguimiento y la revisión de los procedimientos y otros controles con el fin de detectar los errores en los resultados del procesamiento e identificar rápidamente las infracciones y de los incidentes de seguridad.

- ❖ Llevar a cabo revisiones periódicas de la eficacia del SGSI.

ISO/IEC 27002:2005: Tecnologías de la información, técnicas de seguridad - código de buenas prácticas para la gestión de la seguridad de la información.

Esta norma internacional establece directrices y principios generales para la iniciación, implementación, mantenimiento y mejora de la gestión de seguridad de la información en una organización. Se resume en una guía de buenas prácticas que describen los objetivos de control y controles recomendables en cuanto tiene que ver con la seguridad de la información. Se encuentra constituida por 39 objetivos de control y 133 controles, agrupados en 11 dominios que cubren aspectos específicos de la seguridad de la información. Se encuentra estructurada en 16 capítulos (27001 academy , 2015):

- **Capítulo 0.** Conceptos generales de seguridad de la información y SGSI.

- **Capítulo 1. Campo de aplicación:** Se especifica el objetivo de la norma y su campo de aplicación (27001 academy , 2015).

- **Capítulo 2. Términos y definiciones:** Breve descripción de los términos más usados en la norma (27001 academy , 2015).

- **Capítulo 3. Estructura del estándar:** Descripción de la estructura de la norma.

- **Capítulo 4. Evaluación y tratamiento del riesgo:** Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

- **Capítulo 5. Política de seguridad:** Tiene como objetivo establecer controles que permitan orientar con todo lo referente a la seguridad de la información a la alta dirección, de acuerdo con los requisitos propios de cada negocio. Permite elaborar un documento de políticas de seguridad que puede ser aprobado o modificado según sus necesidades. Este documento debe darse a conocer a toda la organización tanto interna como externa (27001 academy , 2015).

- **Capítulo 6. Aspectos organizativos de la seguridad de la información:** Su objetivo es establecer controles a través de los cuales se pueda gestionar la seguridad de la información dentro de la organización y mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas (27001 academy , 2015).

Organización interna. Está integrada por:

- ❖ Compromiso de la dirección con la Seguridad de la Información.
- ❖ Coordinación de la Seguridad de la Información.
- ❖ Asignación de responsabilidades relativas a la seguridad de la información.
- ❖ Proceso de autorización de recursos para el tratamiento de la información.
- ❖ Acuerdos de confidencialidad.
- ❖ Contacto con las autoridades.
- ❖ Contacto con grupos de especial interés.
- ❖ Revisión independiente de la seguridad de la información.

Terceros.

- Identificación de los riesgos derivados del acceso de terceros.
- Tratamiento de la seguridad en la relación con los clientes.
- Tratamiento de la seguridad en contratos con terceros.

- **Capítulo 7. Gestión de activos:** Este dominio busca establecer controles que permitan lograr y mantener la protección adecuada de los activos de la organización, definiendo responsabilidad sobre los activos (inventario de activos, propiedad de los activos, uso aceptable de activos) y realizando clasificación de la información (directrices de clasificación, etiquetado y manipulado de la información) (27001 academy , 2015).

- **Capítulo 8. Seguridad ligada a los recursos humanos:** Con este dominio se pretende establecer controles que conduzcan a asegurar que los empleados, contratistas y usuarios de terceras partes, entiendan sus responsabilidades y sean aptos para las funciones para las cuales están considerados y reducir el riesgo de robo, fraude, o uso inadecuado de las instalaciones (27001 academy , 2015).

Antes del empleo: Funciones y responsabilidades; investigación de antecedentes; términos y condiciones de contratación.

Durante el empleo: Responsabilidades de la dirección, concienciación, formación y captación en seguridad de la información, proceso disciplinario.

Cese del empleo o cambio de puesto de trabajo: Responsabilidad de cese o cambio; devolución de activos: retirada de los derechos de acceso.

- **Capítulo 9. Seguridad física y ambiental:** Busca establecer controles que permitan evitar el acceso físico no autorizado, el daño o la interferencia en las instalaciones y a la información de la organización, de igual forma evitar la pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización (27001 academy , 2015).

Seguridad de los equipos. Se adquiere con:

- ❖ Emplazamiento y protección de equipos.
- ❖ Instalaciones de suministro.
- ❖ Seguridad del cableado.
- ❖ Mantenimiento de los equipos.
- ❖ Seguridad de los equipos fuera de las instalaciones.
- ❖ Reutilización o retirada segura de equipos.
- ❖ Retirada de materiales propiedad de la empresa.

- **Capítulo 10. Gestión de comunicaciones y operaciones:** Está orientado al establecimiento de controles que permitan asegurar la operación correcta y segura de los servicios de procesamiento de información e implementar y mantener un grado adecuado de seguridad de la información de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros (27001 academy , 2015).

- **Capítulo 11. Control de acceso:** Su objetivo es permitir controlar el acceso a la información de la organización con base en los requisitos de seguridad y del negocio, asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

- **Capítulo 12. Adquisición, desarrollo y mantenimiento de los sistemas de información:** Busca establecer controles que permitan: mantener la seguridad en los procesos de adquisición, mantenimiento y desarrollo del software, garantizando que la seguridad es parte integral de los sistemas de información; evitar errores, pérdidas, modificaciones no

autorizadas o uso inadecuado de la información en las aplicaciones; proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos; garantizar la seguridad de los archivos del sistema, y de la información de los sistemas de aplicaciones (27001 academy , 2015).

- **Capítulo 13. Gestión de incidentes de seguridad de la información:** El objetivo de este dominio es establecer controles que permitan asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información, se comunican de forma tal que permitan tomar las acciones correctivas oportunamente (27001 academy , 2015).

- **Capítulo 14. Gestión de la continuidad del negocio:** Busca establecer controles orientados a contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallos importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna (27001 academy , 2015).

- **Capítulo 15. Cumplimiento:** El objetivo de este dominio es el establecimiento de controles tendientes a evitar el incumplimiento de cualquier ley, de obligaciones estatutarias reglamentarias o contractuales y de cualquier requisito de seguridad (27001 academy , 2015).

ISO / IEC 27005:2011: Tecnología de la información, técnicas de seguridad, información de gestión de riesgos de seguridad.

Esta norma brinda directrices para la gestión del riesgo de la seguridad de la información. Suministra soporte a los conceptos generales de la ISO/IEC 27001. Contiene la descripción de los procesos para la gestión del riesgo en la seguridad de la información. Proporciona directrices para seguridad de la información de gestión de riesgos. Fue diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en el riesgo. Puede ser aplicada en todo tipo de organizaciones que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización (Ormella, 2014).

Contribuye a:

- La identificación de los riesgos.
- La valoración de los riesgos en términos de las consecuencias para el negocio y la probabilidad de su ocurrencia.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.
- Monitoreo y revisión del riesgo.

ISO 31000:2009: Gestión de riesgo, principios y directrices

La norma surge como remplazo de la norma AS/NZS 4360:2004, estándar australiano para la gestión de riesgos.

Existe una gran variedad, complejidad y naturaleza de los principios por lo que la ISO 31000 propone unas pautas sobre cómo gestionar los riesgos de la forma sistemática y transparente, para poder dar solución a cada uno de estos riesgos. Esta norma proporciona directrices sobre cómo se debe establecer y mantener un marco de gestión de riesgos, el mismo que puede ser adoptado por cualquier organización. (Serra Carlos, 2009)

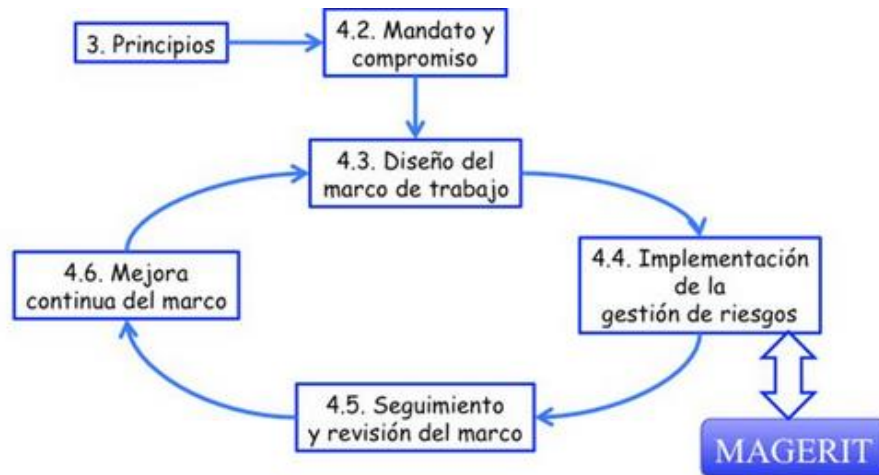
El objetivo del marco de trabajo es estructurar las actividades para la implementación continua de todos los procesos para la gestión de riesgos.

La normativa determina algunos principios para una eficaz gestión de riesgos. Se encuentra integrada en los procesos de una organización. Forma parte de la toma de decisiones. Es dinámica, interactiva y sensible al cambio. Facilita la mejora continua de la organización. Con el cumplimiento de todos estos principios, busca incrementar la posibilidad de alcanzar los objetivos trazados dentro de cada organización y fomentar una gestión proactiva (Ormella, 2014).

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Su creación está directamente relacionada con la generalización del uso de las tecnologías de la información. Es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad de España, proporcionando los principios básicos y requisitos mínimos para la protección de la información (Dirección General de Modernización Administrativa, 2012).

Gráfico No 2
Esquema del funcionamiento del programa MAGERIT



Fuente: Dirección General de Modernización Administrativa, 2012.

Objetivos de MAGERIT

- ❖ Concienciar a los responsables de todas las organizaciones de la existencia de riesgos, dando a conocer la necesidad de gestionar los mismos.
- ❖ Ofrecer un método sistemático para analizar los riesgos (Dirección General de Modernización Administrativa, 2012).
- ❖ Ayudar a descubrir y planificar el tratamiento oportuno en caso de que los riesgos ataquen los activos de información.
- ❖ Preparar a cada organización para procesos de evaluación, auditoría o certificación ISO 27001 (Dirección General de Modernización Administrativa, 2012).

CRAMM: (Risk Analysis and Management Methodology) Metodología para el análisis y la gestión de riesgos

Esta metodología fue desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones. (Seguridad Informática, 2015). Está destinado a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y sus activos.

CRAMM puede definirse como una metodología para el análisis y gestión de riesgos, orientado a proteger la confidencialidad, la integridad y disponibilidad de un sistema y sus activos. Puede ser aplicable en todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad, donde el alto nivel del riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones. Durante el análisis detallado del negocio y de entornos técnicos donde los problemas de seguridad o contingencia asociados con la opción tomada pueden ser investigados o refinados. Antes de la ejecución, para garantizar que todos los requerimientos físicos, el personal, técnicas y contramedidas de seguridad se han identificado e implementado, (Seguridad Informática, 2015).

Objetivo

- Identificar las amenazas, vulnerabilidades y evaluar los niveles de riesgos, dando orientación a los responsables de la seguridad para evitar los riesgos individuales, reduciéndolos a un nivel aceptable en las siguientes etapas:

1. Identificación y valoración de activos.
2. Evaluación de amenazas y vulnerabilidad
3. Selección y recomendación de contramedidas.

CAPÍTULO 2

Estudio de la metodología MAGERIT

Introducción.

En este capítulo se podrá conocer más a fondo a la metodología MAGERIT, con la finalidad de identificar los aspectos más relevantes de la misma, facilitando el estudio comparativo con la otra metodología propuesta en este trabajo de investigación.

Objetivos del capítulo:

- ❖ Encontrar mecanismos de identificación de activos.
- ❖ Identificar vulnerabilidades.
- ❖ Determinar funciones de probabilidad.
- ❖ Establecer variables de medición de riesgo.
- ❖ Determinar cálculo de riesgo.

De esta manera se podrá realizar la comparación con las normativas de la familia ISO relacionadas con la seguridad de la información y la gestión de riesgos 270001, 270002, 270005 y la 31000.

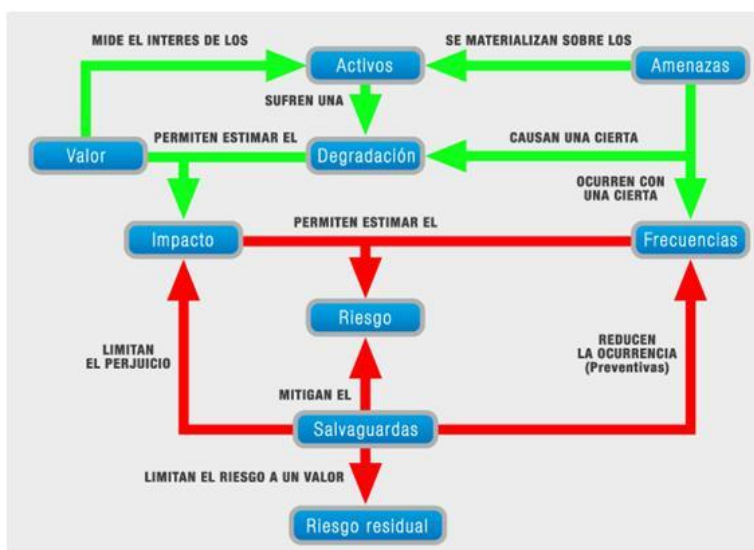
La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica y publicada por el entonces Ministerio de Administraciones Públicas de España, hoy en día Ministerio de Hacienda y Administraciones Públicas.

Es un método formal que sirve para investigar los riesgos que soportan los sistemas de información existentes en cada una de las organizaciones para recomendar las medidas apropiadas que poco a poco deberían adoptar todas las organizaciones (Portal de administración electrónica de España, 2013).

La primera versión se publicó en 1997. En 2006 se publicó la versión 2.0 y en el 2012 sale a la luz la última versión 3.0 que introduce los siguientes cambios con respecto a la versión anterior: Mejor alineamiento con la normativa ISO, buscando una integración de las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno. Esta es una metodología abierta, de uso generalizado en la Administración Pública Española. Dispone de una herramienta de soporte, PILAR II.

Pilar II: Es una herramienta que soporta el análisis y la gestión de riesgos de un sistema de información, siguiendo como base la metodología MAGERIT. Está conformada por una biblioteca estándar de propósito general, es capaz de realizar calificaciones de seguridad respecto de las normas ISO 27002). Sirve para normalizar las siguientes actividades: MAR (Método de Análisis de Riesgos), PAR (Proyecto de Análisis de Riesgos) y PS (Plan de seguridad) (Dirección General de Modernización Administrativa, 2012).

**Gráfico No 3
Función Pilar II**



Fuente: Seguridad informática, 2010.

<https://seguridadinformaticaufps.wikispaces.com/PILAR+->

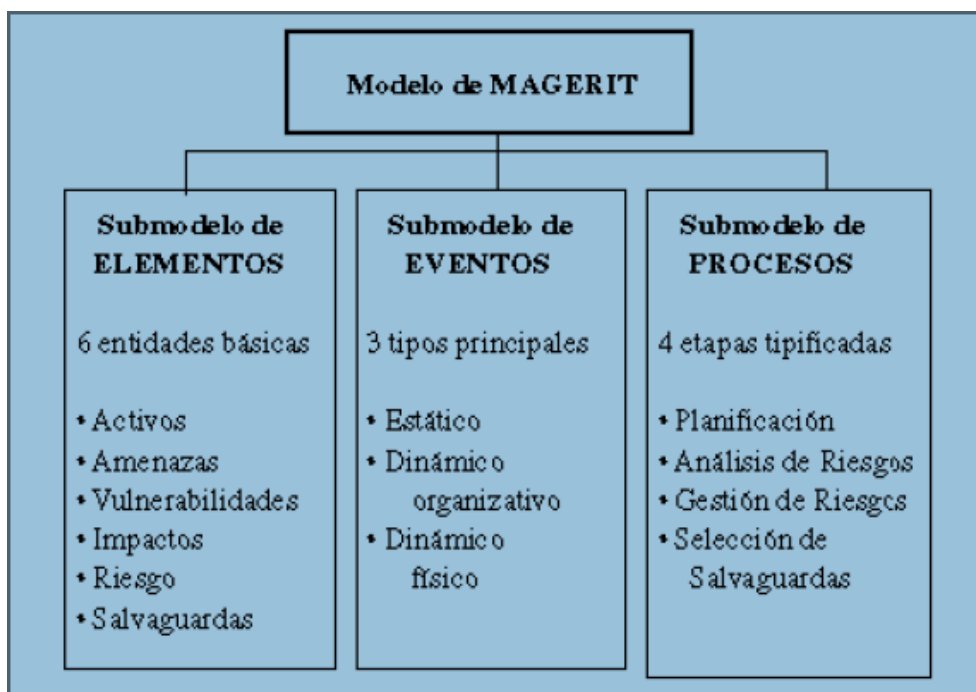
+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos

Objetivos de la metodología

La metodología MAGERIT busca:

- ❖ Estudiar todos los riesgos que día a día atacan a la mayoría de organizaciones.
- ❖ Propone la realización de un análisis de cada uno de los riesgos.
- ❖ Recomendar las medidas que deberían apropiarse en las organizaciones para conocer, prevenir, impedir y reducir o controlar los riesgos identificados dentro de la organización, de esta manera poder disminuir al mínimo sus posibles perjuicios.
- ❖ Preparar mecanismos de evaluación, homologación y certificación de seguridad de todos los sistemas de información, en cada una de las organizaciones, todos ellos a largo plazo.

Gráfico No 4
Estructura del programa MAGERIT



Fuente: Portal de Administración Electrónica de España, 2015.

Mecanismos de identificación de activos de información

Todos los activos de información son los recursos del Sistema de información o relacionados con el mismo, necesarios para que la organización funcione correctamente o alcance de una forma satisfactoria sus objetivos planteados .

MAGERIT presenta cinco grandes categorías de activos de información.

El entorno o soporte del Sistema de Información, que comprende activos tangibles.

La propia información requerida, soportada o producida por el Sistema de Información que incluye los datos informatizados, entrantes y resultantes, así como su estructuración.

Las funcionalidades del Dominio que justifican al Sistema de Información, incluido desde el personal usuario a los objetivos propuestos por la dirección del Dominio.

Otros Activos, de naturaleza muy variada, por ejemplo la imagen de la organización, la confianza que inspire, el fondo de comercio, la intimidad de las personas, etc. (Dirección General de Modernización Administrativa, 2012)

Los activos de información pueden ser identificados mediante estas cinco categorías, y dentro de esta se construyen los árboles de activos.

Una vez listos los árboles de activos se puede ir encontrando las dependencias existentes entre cada uno de ellos. Con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores.

Una vez identificados todos los activos de la organización se debe dar una valorización a cada uno de ellos y tomar en cuenta que un activo no es más importante para la organización por lo que cuesta si no por lo que vale. Esta valorización está dada por la necesidad de proteger cada uno de los activos.

Funciones de probabilidad

En esta metodología la probabilidad de ocurrencia a veces se modela cualitativamente por medio de alguna escala nominal.

También se puede modelar numéricamente como una frecuencia de ocurrencia. Es habitual usar un año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra.

Tabla No 1
Probabilidad de ocurrencia

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: Dirección General de Modernización Administrativa, 2012.

Variable de medición de riesgo

El riesgo crece con el impacto y con la frecuencia. Si se conoce el impacto de las amenazas sobre cada uno de los activos se puede derivar el riesgo teniendo en cuenta la frecuencia de ocurrencia.

Cálculo de riesgo

Para MAGERIT el riesgo es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, se deriva el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia. Sobre cada activo podemos tener riesgo acumulado, riesgo repercutido agregación de riesgos.

Riesgo acumulado: Es el riesgo que se calcula para un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza.

Riesgo repercutido: Es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la amenaza. Este riesgo se calcula sobre cada uno de los activos, por cada amenaza y en cada dimensión de valorización, teniendo como función del valor propio, la degradación causada y la frecuencia de la amenaza.

$$\text{Riesgo} = \text{Valor del activo} \times \text{Vulnerabilidad} \times \text{Impacto}$$

Alineación con el estándar ISO27001

MAGERIT se basa en el dominio de administración de recursos de la norma ISO 27001 tomando sus propias pautas al momento de realizar el inventario de activos. El estándar clasifica sus activos, mediante software y hardware físicos, que son claramente identificados y se clasifican en sentido de su valor, de sensibilidad y de criticidad a la organización. De la taxonomía del softwar se deriva una subcategorización: desarrollo propio, desarrollo a medida, estándar, navegador web, servicios de prestaciones, cliente de correo electrónico, servidor de correo electrónico, sistema de gestión de base de datos, ofimática, entre otros.

Otra de las clasificaciones de los activos de MAGERIT se basa en la ISO 27001, que es hardware, que también tiene subcategorías: equipos, grandes equipos, medios, informática personal, informática móvil, agendas electrónicas, equipos virtuales, equipamiento de respaldo, periféricos, medios de impresión, soporte de red, dispositivos de frontera, conmutadores, encaminadores, cortafuegos entre otros.

Dentro de la clasificación de los activos de información se puede identificar, tanto en la ISO como en MAGERIT: red telefónica, red digital, red de datos, punto a punto, comunicación de radio, red inalámbrica, telefónica móvil, por satélite, red local, red metropolitana e internet. (Portal de administración electrónica de España, 2013).

Tanto en la metodología como en el estándar se clasifica a los RRHH en: usuarios externos, usuarios internos, operadores, administradores de sistemas, administradores de comunicaciones, administradores de BBDD¹, de seguridad, desarrolladores, proveedores.

El estándar como la norma busca proteger los activos y cumplir con: disponibilidad, integridad, confidencialidad y trazabilidad.

Alineación con el estándar ISO27002

Para identificar la alineación que tiene MAGERIT con respecto a esta norma, se debe dejar en claro que ésta es una guía de implementación que colabora en la certificación de la ISO 27002.

MAGERIT tiene una clara alineación con esta norma al momento de identificar las amenazas. El estándar clasifica las amenazas de una forma que sean fácil de identificar e indica a qué tipo de activos pueden afectar, dando a conocer la disponibilidad o dimensión de la misma. Estas amenazas pueden ser de índole: natural, origen industrial, error y fallos no intencionados, ataques intencionados y nuevas amenazas.

Alineación con el estándar ISO27005

MAGERIT, al igual que con las ISO 27001 y 27002 se alinea con esta norma en la identificación y valorización de los activos de información. Identifica las amenazas que pueden dañar los activos y las vulnerabilidades que existen.

Ambos identifican el impacto que puede tener en la organización si pasara algo con alguno de los activos de la misma.

¹ Base de datos.

MAGERIT gestiona los riesgos mediante la aplicación de salvaguardas, las mismas que se clasifican en: protecciones generales, protección de claves, protección de los servicios, protección del software, hardware y comunicaciones (Portal de Administración Electrónica de España, 2015).

Alineación con el estándar ISO31000

Se nota claramente la alienación de MAGERIT con respecto a la norma en la determinación del contexto. Documenta el entorno externo en el que está operando la organización: social política y cultural. También se analiza el contexto interno de la institución. Identifica una relación entre los posibles puntos de peligro, obteniendo los riesgos identificados y si no ocurre la identificación se quedan como riesgos ignorados.

Mediante la identificación del riesgo, su principal función es encontrar los riesgos potenciales que tiene cada organización o empresa sobre cada uno de sus activos; para esta identificación se puede utilizar varios métodos o técnicas: método Delphi, árboles de fallos, árboles de eventos, entre otros.

Una vez identificados los riesgos se pueden calificar mediante el análisis cuantitativo y cualitativo.

La evaluación de los riesgos aquí presente, los factores de percepción, de estrategia y de políticas permitiendo tomar decisiones de que riesgos son aceptados y cuáles no, identificando las circunstancias en las que se pueden aceptar o en las que hay que buscar un tratamiento a dicho riesgos.

El tratamiento de riesgos recopila todas las actividades que están encaminadas a modificar la situación de riesgo.

MAGERIT permite que una vez concluido el análisis de riesgos, los resultados obtenidos se pongan en práctica para evitar incidentes dentro del entorno (Portal de Administración electrónica de España, 2013).

Conclusiones del capítulo

- ❖ MAGERIT es una metodología formal para el análisis y gestión de riesgos, que fue creada con el fin de concienciar a todos los responsables de los sistemas de información de la existencia de riesgos y la necesidad de prevenir los mismos (Portal de administración electrónica de España, 2013).
- ❖ MAGERIT está basada en las normas ISO. De cada uno de estos estándares esta metodología ha ido tomando algo importante para su desarrollo.
- ❖ MAGERIT al igual que las normas identifican los activos, valoran los activos, identifican amenazas y vulnerabilidades.
- ❖ Esta metodología es gratuita y puede ser utilizada en todas las organizaciones.
- ❖ MAGERIT es una metodología que poco a poco se ha ido acoplando para satisfacer las necesidades de muchas organizaciones.
- ❖ MAGERIT colabora en la certificación de ISO 27001.

CAPÍTULO 3

Estudio de la metodología CRAMM

Introducción del capítulo

El capítulo tres permitirá conocer a la metodología CRAMM, buscando identificar los aspectos más relevantes de la misma para facilitar el estudio comparativo con MAGERIT.

Los objetivos de este capítulo son:

- ❖ Encontrar mecanismos de identificación de activos.
- ❖ Identificar vulnerabilidades.
- ❖ Determinar funciones de probabilidad.
- ❖ Establecer variables de medición de riesgo.
- ❖ Calcular riesgos.

Se realizará la comparación de la metodología con las normativas de la familia ISO relacionadas con la seguridad de la información y la gestión de riesgos 270001, 270002, 270005 y la 31000.

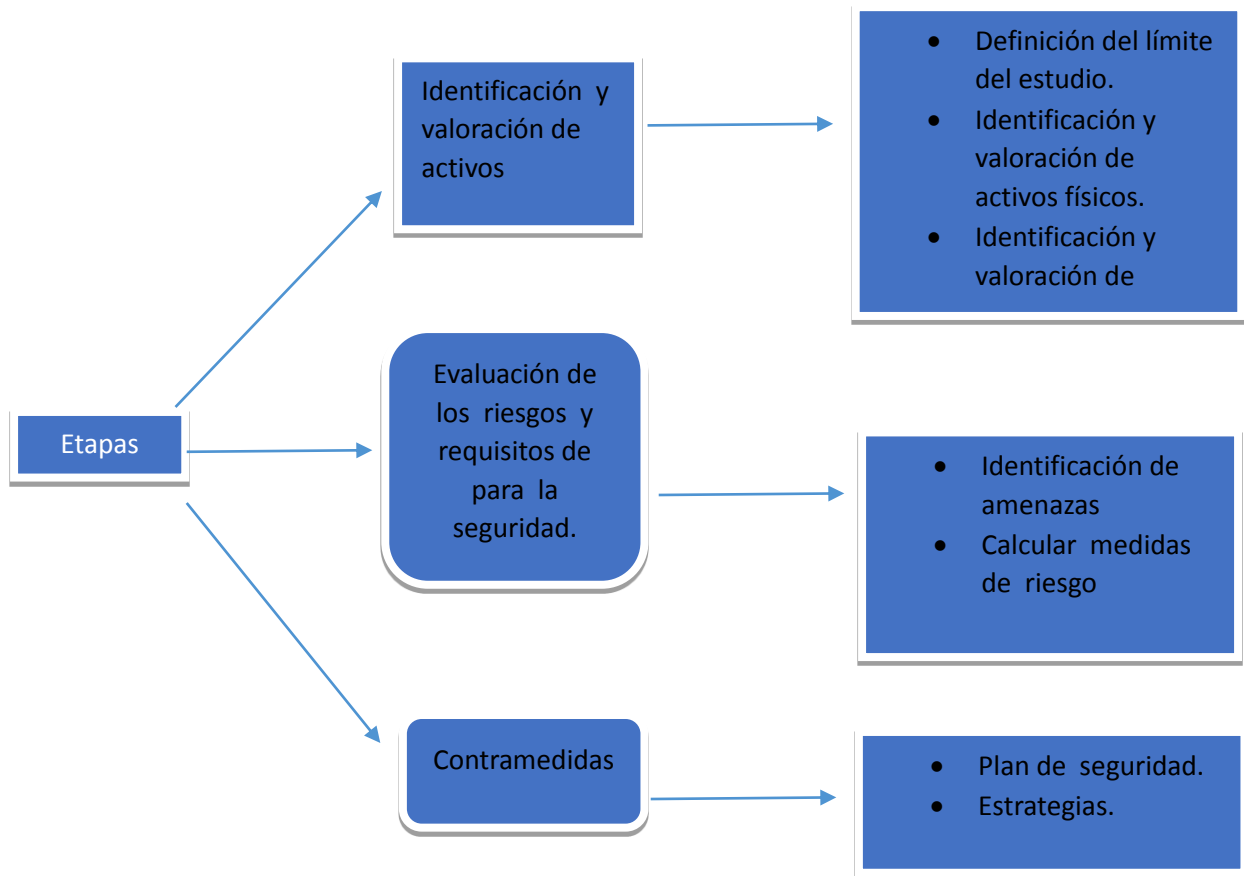
Introducción a CRAMM

Esta metodología de análisis de riesgo fue desarrollada por el Centro de Informática y la Agencia Nacional de Telecomunicaciones del Gobierno del Reino Unido en 1987. La versión vigente es la 5.2. (Huerta Antonio, 2012).

CRAMM puede definirse como una metodología para el análisis y gestión de riesgos. Está orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos. Esta metodología es compatible con las ISO 27001 (Huerta Antonio, 2012).

Dentro de CRAMM se tienen 3 grandes etapas.

Gráfico No 5
Etapas de CRAMM



Fuente: Fernández Manuel, 2003.

http://rodin.uca.es/xmlui/bitstream/handle/10498/16805/Metodolog%C3%ADas%20de%20seguridad_2.pdf?sequence=1

Mecanismos de identificación de activos

CRAMM permite identificar hardware, software, datos y activos de localización que componen el sistema de información. Cada uno de estos puede ser valorado. Esta identificación se da en el módulo de identificación y valoración de activos.

Los activos físicos se valoran en términos de costo de reemplazo, los datos y activos de software son valorados en términos del impacto que sufrirá si la información fuera a estar disponible para cualquiera, destruida, divulgada o modificada (Fernández Manuel, 2003).

Identificación de vulnerabilidades

Identifica y evalúa el tipo y el grado de amenazas que pueden afectar al sistema mediante un enfoque organizado y sistemático que conjuga software, hardware, aspectos físicos, ambientales y humanos. Se puede utilizar dos métodos para determinar las vulnerabilidades:

- ❖ Método Cualitativo: Mediante lluvias de ideas, entrevistas con expertos, foros y debates con los involucrados.

- ❖ Método Cuantitativo: asignando valores de probabilidad de ocurrencia.

Funciones de probabilidad a desarrollar

La función de probabilidad está determinada en la metodología por la frecuencia de ocurrencia de los incidentes que es evaluada por cada organización de acuerdo a sus reglas.

Variable de medición de riesgo

Las variables de medición para CRAMM son: magnitud de daño y la probabilidad de las amenazas.

Cálculo de riesgo

Se basa en una combinación de la valoración de los activos, y los niveles de amenaza y los niveles de vulnerabilidades que se han obtenido durante la identificación de vulnerabilidad y amenazas. El cálculo del riesgo se realiza en una escala del 1 al 7 considerando uno como la línea de más baja seguridad y 7, como la más alta (Huerta Antonio, 2012).

Alineación con el estándar ISO27001

CRAMM al igual que el estándar realiza un inventario de activos de la información sean estos de software, hardware e infraestructura física que brinda soporte a las tecnologías de información y comunicaciones. El estándar clasifica sus activos mediante software, hardware. Estos activos son claramente identificados y se clasifican en: Sentido de su valor, sensibilidad, criticidad a la organización.

CRAMM clasifica a sus activos en:

- Hardware: considerando también la infraestructura física de la organización.
- Software: Tomando en cuenta las aplicaciones, los sistemas y los datos de la organización.

Dentro de la metodología, los activos físicos son valorados en términos de coste de reemplazo, mientras que los datos y software son valorados en términos del impacto, disponibilidad e integridad de la información. El estándar como la norma busca proteger los activos y que estos cumplan con las normas de confidencialidad y trazabilidad (Fernández Manuel, 2003).

CRAMM toma aspectos que son concordantes con el estándar ISO 27001 como evaluación de los activos y sus dependencias, evaluación del impacto empresarial, identificación de amenazas y vulnerabilidades, evaluación de riesgos, identificación de controles.

Alineación con el estándar ISO27002

La alineación de CRAMM con la ISO 27002 es notoria al momento de identificar las amenazas. Detectando el problema potencial investiga que tan probable es que esto ocurra. Cubre toda la gama de amenazas deliberadas o accidentales que puedan afectar a los sistemas de información, incluyendo hacking, virus, fallos de equipo o software, daños intencionales o el terrorismo y errores humanos.

La metodología está alineada con el estándar en la gestión de activos constituyendo esta administración como un imperativo en los dos casos.

La gestión de activos tanto en el estándar como en la metodología busca clasificar los recursos físicos y lógicos de los sistemas de información que conforman las organizaciones.

Alineación con el estándar ISO27005

La alineación de CRAMM con este estándar se da en la identificación de amenazas, vulnerabilidades, obtenidas a partir del análisis de activos, incidentes y catálogos de amenazas externas.

Tanto el estándar como la metodología identifican los activos de la organización como el hardware, el software, recursos humanos y físicos, la finalidad es enfocar el análisis y estudio sobre los recursos críticos y descartar los activos irrelevantes.

La metodología CRAMM se alinea con el estándar ISO 27005 en su fase de planificación donde se realiza la identificación y evaluación del riesgo (Matalobos Juan Manuel, 2009).

Alineación con el estándar ISO31000

Tanto el estándar como la metodología buscan implementar contramedidas para cada uno de los riesgos que asechan a cada organización, pero la metodología lo que hace es ver si el riesgo es tan grande que vale la pena implementar una contramedida. La metodología se ayuda de su propia herramienta para realizar contramedidas a las amenazas y riesgos encontradas.

Conclusiones del capítulo

- ❖ CRAMM es una metodología para el análisis y gestión de riesgos.

- ❖ Esta metodología nos permite definir el marco de gestión del riesgo, identificar riesgos, identificar propietarios de los riesgos, evaluar riesgos, definir niveles aceptables de riesgo, identificar respuestas adecuadas al riesgo, implantar respuestas, obtener garantías de la efectividad, monitorizar y revisar.

- ❖ CRAMM se alinea con las normas ISO tomando de cada una algo relevante.

- ❖ Tanto la normativa como los estándares se preocupan por implementar contramedidas en caso de descubrir que existen riesgos o amenazas que pueden poner en riesgo a los activos de información. (Huerta Antonio, 2012; Matalobos Juan Manuel, 2009)

CAPÍTULO 4

Análisis comparativo entre MAGERIT y CRAMM

Introducción al capítulo.

En este capítulo se realizará la comparación de las metodologías MAAGERIT y CRAMM con la norma ISO 31000. Para identificar cuál de las dos es la que más se alinea a la realidad de las PYMES.

ISO 31000	MAGERIT	CRAMM	Satisfactorio
1. Comunicación	<p>Permite tener un contacto fluido con varios Actores:</p> <ul style="list-style-type: none">• Órganos de gobierno y decisión.• Los usuarios y técnicos del sistema. <p>Debido a que si se necesita realizar un cambio o no se debe tomar en cuenta todos los cambios que esto puede producir dentro de la organización .</p>	<p>Permite tener contacto con los actores de la organización.</p>	MAGERIT
2. Establecer el contexto.	<p>Lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para la Gestión de los Riesgos.</p> <p>Elementos a destacar:</p> <ul style="list-style-type: none">• Alcance del análisis.• Obligaciones propias y obligaciones contraídas,• Relaciones con otras Organizaciones (Intercambio de información y servicio, servicios subcontratos). <p>Documentar el entorno en el que opera la organización.</p>	<p>Permite determinar los alcances de la Organización.</p>	MAGERIT

	<p>Identificar las obligaciones legales, reglamentos y contractuales.</p> <p>Identificar el contexto interno en el que se desenvuelve las actividades de la organización: Política interna, compromisos con los accionistas y con los trabajadores.</p> <p>La identificación del contexto en el proceso de gestión de riesgos debe ser objeto de una revisión continua.</p> <p>Determinar:</p> <ul style="list-style-type: none"> • Política de seguridad y normas. • Requisitos de cumplimiento normativo. • Obligaciones contractuales. • Roles y funciones. • Criterios de valoración de información y servicios. • Criterios de valoración de riesgos. • Criterios de aceptación de riesgos. • Contingencias o riesgos de los activos <p>En la parte de Contexto de Riesgos:</p> <ul style="list-style-type: none"> • Árboles de ataques. Permite modelar las diferentes formas de alcanzar un mismo objetivo dentro de la organización. • Nodos con atributos: Indican varias formas de alcanzar un objetivo dentro de la organización 		
--	---	--	--

<p>3. Identificación.</p>	<p>Los activos de La organización se identifican de acuerdo a su función dentro de la organización, por medio de un levantamiento de procesos, identificando cada activo relevante cada departamento de la organización, tomando en cuenta su criticidad dentro de la organización .</p> <p>Luego se categorizan los activos en :</p> <p style="padding-left: 40px;">Activos Fundamentales</p> <ul style="list-style-type: none"> • Información <p style="padding-left: 40px;">Activos Secundarios</p> <ul style="list-style-type: none"> • Servicios • Aplicaciones Informáticas. • Hardware • Redes • Instalaciones • Personas <p>Utilizando los siguientes métodos.</p> <p>Modelo de Apéndice:</p> <ul style="list-style-type: none"> • Activos con código, nombre descriptivos. <p>Modelo cuantitativo:</p> <ul style="list-style-type: none"> ○ En una cierta dimensión es un número mayor a cero. <p>Modelo cualitativo.</p> <ul style="list-style-type: none"> ○ Cada activo recibe en cada dimensión un valor de la escala V. • Identificación de bajo qué tipo cabe clasificar el activo. • Identificar las dependencias entre los activos. • Valoración de los activos en diferentes dimensiones. • Valor acumulado. <p>Riesgos:</p> <ul style="list-style-type: none"> • Situación: Activo-tiempo-amenaza. 	<p>Identifica los activos: Tres tipos de activos que componen la información son Identificadas: datos, software de aplicación y los activos físicos.</p> <ul style="list-style-type: none"> • Físicos • Software (Aplicaciones) • Datos (Información contenida en los sistemas de información). 	<p>MAGERIT</p>
---------------------------	--	--	----------------

	<ul style="list-style-type: none"> • Riesgo Acumulado • Riesgo Repercutido. 		
4. Análisis.	<ul style="list-style-type: none"> • Cualitativo Riesgos: Saber qué es lo que hay, sin cuantificar con precisión. Trabajando sobre una escala discreta de valores. Se basa en tablas de impacto y probabilidad.... • Cuantitativo de Riesgo. Identificando que es lo que hay, cuantificando con precisión. Trabajando con números reales. • Modelo escalonado. Determina una serie ordenada de escalones de valoración. <p>Está basado en:</p> <ul style="list-style-type: none"> ▪ Impacto. Valorado según sea el caso en MA,A,M,B y MB ▪ Probabilidad ▪ Nivel de Necesidad de Salvaguardas. 	CRAMM no realiza este procedimiento	MAGERIT
4.1. Técnicas específicas para el análisis de riesgos	<p>Mediante Tablas.</p> <p>Sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas. Utilizando una escala para calificar los valores de activos.</p> <ul style="list-style-type: none"> • MB: muy bajo • B: bajo • M: medio • A: alto • MA: muy alto <p>Análisis algorítmico. puede ser un análisis cualitativo .- se busca saber qué es lo que hay sin cuantificarlo con precisión , se trabaja sobre una escala discreta de valores.</p>		

	<p>Análisis cuantitativo se busca cuantificar todos los aspectos posibles. Se trabaja con números reales.</p> <p>árboles de ataque.- nos ayudan a modelar de varias formas el cómo alcanzar nuestros objetivos.</p>		
4.2. Técnicas generales	<p>Técnicas Gráficas. Se centra en cómo algunas representaciones gráficas de los elementos de un proyecto AGR pueden apoyar a dicho proyecto, tanto como soporte a presentaciones, como en la toma de decisiones.</p> <p>sesiones de trabajo: entrevistas, reuniones y presentaciones.- estas sesiones de trabajo están destinadas a la obtención de información, se puede obtener de una forma individual o en conjunto.</p> <p>valoración Delphi.- Es una técnica netamente cualitativa que relativamente permite tratar con alta precisión problemas técnicamente complejos</p>	CRAMM no realiza este procedimiento	
5. Evaluación	<ul style="list-style-type: none"> ○ Riesgo Intrínseco. Medida del daño probable sobre un sistema sin considerar las salvaguardias. ○ Riesgo Residual. Medida del daño, una vez consideradas las salvaguardias. <p>Riesgo Efectivo medida del daño probable al que está sometido el activo tras la valoración de las salvaguardias y tomando en cuenta el valor propio de cada activo.</p> <ul style="list-style-type: none"> ○ Sobre la eficacia de las salvaguardias. Las salvaguardias son 	CRAMM no realiza este procedimiento	MAGERIT

	<p>evaluadas según su eficacia reduciendo el riesgo de cada activo que protege.</p>		
6. Tratamiento.	<ul style="list-style-type: none"> ▪ Eliminación. Se pueden eliminar varias cosas siempre y no se altere la esencia de la Organización. ▪ Mitigación. <ul style="list-style-type: none"> ○ Reducir la degradación causada por una amenaza. ○ Reducir la probabilidad de que una amenaza se materializa. ▪ Compartición del riesgo. <ul style="list-style-type: none"> ○ Riesgo cualitativo. se comparte por medio de la externalización de componentes del sistema. ○ Riesgo cuantitativo: se comparte por medio de la contratación de seguros ▪ Financiación. Una vez aceptados los riesgos la organización reservara un dinero en casa de que el riesgo llegue a concretarse. 	CRAMM no realiza este procedimiento	MAGERIT

Tanto MAGERIT como CRAMM establecen como objetivo principal la gestión y análisis de riesgo.

Un beneficio que nos presentan las dos metodologías es el presentarse de forma gratuita al público en idioma Inglés, MAGERIT nos presenta un plus más al estar disponible en idioma Español.

Las dos metodologías se apoyan con herramientas para la gestión de riesgos, en el caso de la Metodología CRAMM sus dos herramientas CRAMM Expert, CRAMM Express son comerciales en el caso de la Metodología MAGERIT la herramienta EAR es comercial pero la herramienta PILAR es Gratuita.

Cada metodología está alineada a estándares internacionales. MAGERIT adopta las mejores prácticas de la ISO 27001, 15408, 17799, y 13335. Sin embargo para la gestión de riesgos se alinea correctamente a los requerimientos de la ISO 27005 e ISO 31000. CRAMM, a su vez, tiene un enfoque más práctico, pues su base de referencia es la ISO 27002, contemplando además los fundamentos de la ISO 27005 e ISO 31000.

El ciclo de la metodología CRAMM está basado en identificar primero los riesgos y luego estimar la frecuencia de presentación de los mismos. Por otra parte el ciclo de MAGERIT inicia con la identificación de los activos de información, luego identifica las amenazas lógicas y de entorno, estima las frecuencias y el impacto para inmediatamente pasar a las salvaguardas y gestionar finalmente el riesgo residual.

Dentro de la metodología CRAMM se considera como activos de información solamente a los datos. Por otro lado la metodología MAGERIT considera como activos de información al hardware, software, información electrónica, personas, instalaciones, medios de soporte y elementos de comunicación de datos.

CRAMM para la identificación de riesgos y amenazas utiliza solamente métodos cualitativos y cuantitativos; además de valorar los activos en términos de costo de reemplazo, y por dimensiones de disponibilidad, integridad y confidencialidad. MAGERIT además de los dos métodos también utiliza el método mixto. Determina el valor de los activos considerando la dimensión de disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad, y estableciendo una escala de valoración en seis niveles: Muy alto, alto, medio, bajo, muy bajo

y despreciable, esta metodología analiza el impacto determinando el valor de los activos, el impacto acumulado lo calcula considerando el valor acumulado del activo y las amenazas a las que se afronta, y el impacto repercutido considerando el valor propio y las amenazas.

Conclusiones del capítulo

- ❖ Tanto MAGERIT como CRAMM son metodologías bastante similares para la gestión de riesgos.
- ❖ Las dos metodologías ayudan a identificar los riesgos y a la vez tomar medidas de salvaguardia obteniendo como resultado la disminución de tiempo.
- ❖ Ambas sobrellevan a una identificación de los activos, inventarios de los mismos, amenazas, impacto y probabilidad obteniendo como resultado salvaguardias para minimizar el riesgo.
- ❖ Tanto MAGERIT como CRAMM aportan con las ISOS, MAGERIT tiene una clara alineación con la ISO 27001 y CRAMM se alinea con la 27002.
- ❖ Tomando en cuenta que la 27001 sirve para certificar, se determina que entre las dos metodologías la mejor es la MAGERIT.

CONCLUSIONES

- El riesgo es intrínseco a cada organización y la organización o la empresa es afectada directamente por el proceso de seguridad de la información.
- La tecnología debe ser tomada como una estrategia para la seguridad de la empresa.
- Los activos de la información se debe considerar como críticos dentro de una organización y su seguridad debe ser integral y holística, comprometiendo todos los recursos y todos los participantes en los diferentes departamentos de la organización.
- La seguridad de la información está basada en las personas ya que las mismas tienen el control de todas las fases.

MAGERIT es una metodología formal para el análisis y gestión de riesgos, que fue creada con el fin de concienciar a todos los responsables de los sistemas de información de la existencia de riesgos y la necesidad de prevenir los mismos (Portal de administración electrónica de España, 2013).

- MAGERIT está basada en las normas ISO. De cada uno de estos estándares esta metodología ha ido tomando algo importante para su desarrollo.
- MAGERIT, al igual que las normas identifican los activos, valoran los activos, identifican amenazas y vulnerabilidades.

- MAGERIT es gratuita y puede ser utilizada en todas las organizaciones.
- MAGERIT paulatinamente se ha ido acoplado para satisfacer las necesidades de empresas y organizaciones.
- MAGERIT colabora en la certificación de ISO 27001.
- Tanto MAGERIT como CRAMM son metodologías bastante similares para la gestión de riesgos.
- Las dos metodologías ayudan a identificar los riesgos y a la vez tomar medidas de salvaguardia. Obteniendo como resultado la minoría de tiempo.
- MAGERIT y CRAMM sobrellevan a una identificación de los activos, inventarios de los mismos, amenazas, impacto y probabilidad. Obteniendo como resultado salvaguardias para minimizar el riesgo.
- Ambas aportan con las normas ISO. MAGERIT tiene una clara alineación con la ISO 27001 y al contrario CRAMM se alinea con la norma 27002.
- La diferencia principal que existe entre MAGERIT y CRAMM está en que la primera desarrolla procesos para su implementación dentro de la planificación y lanzamiento de un proyecto dando resultados de pérdida o ganancia económica y CRAMM se aplica directamente para las organizaciones y los resultados se evalúan en una tabla con ponderación de 1 a 7.

- CRAMM es una metodología para el análisis y gestión de riesgo, que permite: Definir un marco de gestión del riesgo, identificar riesgos, identificar los propietarios de los riesgos, evaluar riesgos, definir niveles aceptables de riesgo, identificar respuestas adecuadas al riesgo, implantar respuestas, obtener garantías de la efectividad, monitorizar y revisar.
- CRAMM se alinea con las normas ISO tomando de cada una algo relevante. Tanto la normativa como los estándares se preocupan por implementar contramedidas en caso de descubrir que existen riesgos o amenazas que pueden poner en riesgo a los activos de información.
- En el contexto de las PYMES ecuatorianas, MAGERIT es la metodología que podría ser aplicada. La ventaja principal es que primero busca “que” se quiere proteger, luego establece el “de qué” se quiere proteger, para finalmente decidir el “como” se debe proteger. Sin embargo es inconclusa, ya que llega solamente a las pautas a considerar para establecer las contramedidas. Es importante mencionar que la implementación de un sistema de gestión de seguridad de la información debería introducir a las políticas de seguridad y considerar la continuidad del negocio en un ciclo infinito de planificación, ejecución, verificación y actuación.

RECOMENDACIONES

- Que las organizaciones deben ser más conscientes de la necesidad de identificar, evaluar y realizar un tratamiento adecuado de los riesgos.
- Se debe implementar políticas de seguridad de la información alineadas a la ISO 27002 en donde las metodologías recomendadas para las PYMES ecuatorianas son MAGERIT y CRAMM.
- Cuando se realicen proyectos enfocados al desarrollo de las tecnologías de la información y las comunicaciones se recomienda utilizar la metodología MAGERIT ya que esta brinda un método para la implementación y nos dará un referencia de pérdida o ganancia monetaria.
- La metodología CRAMM es ideal para el análisis de riesgos de las pequeñas y medianas empresas para su mejora continua por lo que se recomienda su uso.
- Se recomienda tomar en cuenta e implementar el no repudio de la información ya que ninguna de las metodologías lo consideran.

Bibliografía

- ALCIDES, Gemán. Seguridad informática. Antioquía, Colombia. Universidad de Antioquia, 2009. Disponible en la web en la siguiente dirección: <http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=16&ved=0CEIQFjAFOAo&url=http%3A%2F%2Fbiblioteca.udea.edu.co%2Fmanuales%2Fseguridad.pps&ei=beKCVZ26CZDlsAStkoE4&usg=AFQjCNETJIK15wXY9yFwqksPPTVQNzviBA>

- ARANDA SEGOVIA, José Alonso. Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, Certificado bajo la Norma ISO27001. Quito – Ecuador, 2005. Disponible en la web en la siguiente dirección: <https://www.dspace.espol.edu.ec/bitstream/123456789/8080/1/Implementaci%C3%B3n%20del%20primer%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf>

- Auditoría Informática. Fraudes, CAATTs. (07 de 08 de 2014). Obtenido de <http://fraudit.blogspot.com/2008/07/la-familia-iso-27000.html>

- AVENDAÑO ALVAREZ, Gabriel. Tipos de procesos informáticos. 13 de enero de 2014. Disponible en la web en: https://prezi.com/1_mz-a4qcqsq/tipos-de-procesos-informaticos/

- BURGOS SALAZAR, Jorge; CAMPOS, Pedro. Modelo Para Seguridad de la Información en TIC. Concepción, Chile. Disponible en la web en la siguiente dirección: <http://ceur-ws.org/Vol-488/paper13.pdf>

- CALDERÓN ONOFRE, Diana; ESTRELLA OCHOA, Martín; FLORES VILLAMARÍN, Manuel. Escuela superior politécnica del litoral. Implementación de un sistema de gestión de seguridad de la información aplicada a los recursos humanos, 2011. Disponible en la web en la siguiente dirección:

<http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.dspace.espol.edu.ec%2Fbitstream%2F123456789%2F24204%2F1%2F1PROYECTO%2520DE%2520GRADUACION%2520IMPLEMENTACION%2520DE%2520SGSI%2520A%2520LA%2520EMPRESA.docx&ei=oSSDVbC3CMr9-AHVu67QBQ&usg=AFQjCNF3KGTcr6stmlW1TtDWcP5UhWh4-Q&bvm=bv.96041959.d.cWw>

- CGEIT, C. C. (20 de 09 de 2014). CIGRAS. Obtenido de <http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf>

- Dirección General de Modernización Administrativa, P. e. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid.

- FERNANDEZ, Manuel. Universidad de Cádiz. Estrategia para la implantación de los sistemas de gestión en la seguridad de la información. 2003. Disponible en la web en: http://rodin.uca.es/xmlui/bitstream/handle/10498/16805/Methodolog%C3%ADas%20de%20seguridad_2.pdf?sequence=1

- G2D. (22 de 09 de 2014). GR2DEST.ORG. Obtenido de <http://gr2dest.org/metodologia-de-analisis-de-riesgos-magerit/>

- GARCIA, Manuel; QUISPE, Carlos; PAEZ, Luis. Mejora continua de la calidad de los procesos, 2003, México. Disponible en la siguiente dirección electrónica:
http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pdf/mejora.pdf

-Gestión de la información. (s.f.). Obtenido de <http://arelyromero.blogspot.com/2012/11/de-nuevo-nos-concentramos-en-el.html>

- GONZALEZ, Julián. Seguridad Informática. Madrid - España. Disponible en la web en la siguiente dirección:
http://www.fsc.ccoo.es/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf

- HUERTA, Antonio. Introducción al análisis de riesgos – Metodologías. 30 de marzo de 2012. Disponible en la siguiente dirección electrónica:
<http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/>

- ISO. (s.f.). Obtenido de http://www.iso.org/iso/catalogue_detail?csnumber=43170. Ltd, I. (s.f.). Information security standards. Obtenido de <http://www.iso27001security.com/html/27005.html>.

- ISOTools, ISO 27001: Cumplimiento de los requisitos legales en Seguridad de la Información, 16 de Diciembre del 2014 .Disponible en la siguiente dirección electrónica:<https://www.isotools.org/2014/12/16/iso-27001-cumplimiento-requisitos-legales-seguridad-informacion/>.

- JAEN, Daylis, PINEDO, Francisco. Universidad Católica Santa María, la antigua. Seguridad informática y gestión de riesgos, 2012. <http://es.scribd.com/doc/262596174/seguridadinformaticaygestionderiesgos-120929075238-phpapp02#scribd>

- MARQUINA, Edgar. Escuela Politécnica Nacional. Análisis y gestión de riesgos para el servidor Radius. Quito – Ecuador. Mayo, 2010. Disponible en la web en: <http://bibdigital.epn.edu.ec/bitstream/15000/2500/1/CD-3203.pdf>

- MARTINEZ, Cristina. Guía de implantación de sistemas de gestión de la seguridad de la información, 21 diciembre del 2005. Disponible en: <http://dspace.ups.edu.ec/bitstream/123456789/573/3/CAPITULO1.pdf>

- Ministerio de seguridad de Uruguay. ISO31000: 2009. Herramienta para evaluar la gestión de riesgos. Montevideo – Uruguay, 2011. Disponible en la web en: <http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf>

- MATALOBOS, Juan Manuel. Universidad politécnica de Madrid. Análisis de riesgos de la seguridad de la información. Madrid – España. Mayo 2009. Disponible en la web en: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

- MORALES, R. (25 de 07 de 2014). RETRIC. Obtenido de RETRIC: <http://retico.gt/2013/10/09/principios-de-la-seguridad-informatica-2/>

- LÓPEZ, Rapha. COPY OF NORMA ISO 27000, 3 de febrero de 2014. Disponible en la web en: <https://prezi.com/fam9idqrhmr7/copy-of-norma-iso-27000/>.

- ORMELLA, I. C. (22 de 09 de 2014). Norma ISO 31000 de Riesgos Corporativos. Obtenido de http://www.criptored.upm.es/descarga/ISO_31000_riesgos_corporativos.pdf

- PEREIRA, José. Universidad autónoma de Barcelona. Plan de implementación de la norma ISO/IEC 27001, 2005. Madrid – España, 2013. Disponible en la siguiente dirección electrónica:

<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23704/7/jaurelaTFM0613memoria.pdf>

- Portal de Administración Electrónica de España, 2013. Disponible en la siguiente dirección electrónica:

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VYQ8BkZRLRs

- Portal Administración Electrónica de España. (22 de 01 de 2015). Obtenido de

<http://administracionelectronica.gob.es/ctt/magerit#.VMGxmpbRbHQ>

- ROBLES, Ramón; RODRÍGUEZ DE ROA, Alvaro. Comité de Entidades de Certificación de la AEC. Gestión Informática. Junio, 2006. Disponible en la web en la siguiente dirección:

http://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

- SUSCERTE. (07 de 08 de 2014). Obtenido de

http://www.sunai.gob.ve/images/stories/PDF/Ponencias/EF/3_Daniel_sandoval.pdf

ANEXOS

Anexo A: Normativo

Objetivos de control y controles

Tabla No 3
Políticas de seguridad de la información

Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con las empresas requisitos y disposiciones legales y reglamentarias pertinentes.	
Documento de la política de seguridad de la información	CONTROL: Un documento de política de seguridad de la información deberá ser aprobado por gestión, y publicado y comunicado a todos los empleados y partes externas pertinentes.
Revisión de la información de la política de seguridad	CONTROL: La política de seguridad de la información será revisado por lo planificado intervalos o si ocurren cambios significativos para asegurar su continua conveniencia, adecuación y eficacia.
Organización de seguridad de la información	
Organización Interna	
Objetivo: Gestionar seguridad de la información dentro de la organización.	
Compromiso de la dirección de la seguridad de la información.	CONTROL: Gestión apoyará activamente a la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, explícita asignación, y el reconocimiento de seguridad de la información

	responsabilidades.
Coordinación de seguridad de información.	CONTROL: Actividades de seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con relevantes roles y funciones de trabajo.
Asignación de la información a responsables de seguridad.	CONTROL: Todas las responsabilidades de seguridad de la información deben estar claramente definidas.
Proceso de autorización para procesamiento de la información de comodidades.	CONTROL: Un proceso de autorización de la administración para la nueva información de instalaciones de procesamiento será definido e implementados.
Acuerdos de confidencialidad	CONTROL: Requisitos para los acuerdos de confidencialidad o de no divulgación que refleja las necesidades de la organización para la protección de la información se identificará y revisará periódicamente.
Contacto con las autoridades.	CONTROL: Se mantendrán los contactos apropiados con las autoridades pertinentes.
Contacto con grupos de especial interés.	CONTROL: Los contactos pertinentes con los grupos de interés especial o de otro especialista. Se mantendrán foros de seguridad y asociaciones profesionales.
Revisión independiente de seguridad de la información.	CONTROL: El enfoque de la organización para la gestión de seguridad de la información y sus objetivos aplicación (es decir, de control, controles, políticas, procesos y procedimientos para la seguridad de la información) serán revisado de forma independiente a intervalos planificados, o cuando significativamente se producen cambios en la implementación de la seguridad.
Las partes externas	
Objetivo: Mantener la seguridad de la información y de procesamientos de información sobre las instalaciones de la organización que son visitadas, procesadas, comunicadas, o gestionadas por terceros externos.	
Identificación de los riesgos relacionados a partes externas.	CONTROL: Los riesgos para la información y procesamiento de información sobre las instalaciones de la organización de los procesos de negocio relacionados con partes externas deberán ser identificados y controlados apropiados implementados antes de conceder el acceso.
Abordar la seguridad cuando se trata de clientes.	CONTROL: Todos los requisitos de seguridad identificados deberán dirigirse antes de dar a los clientes acceso a la información o de los activos de la organización.
Abordar la seguridad en terceros.	CONTROL: Acuerdos con terceros que impliquen el acceso, tratamiento, la comunicación o la gestión de instalaciones de procesamiento de información o la información de la organización, o la adición de productos o servicios a instalaciones de procesamiento de información deberán cubrir la totalidad de seguridad pertinentes requisitos.
Gestión de activos	
Responsabilidad de los activos	
Objetivo: Lograr y mantener la protección adecuada de los activos de la organización.	
Inventario de activos	CONTROL: Todos los activos deberán estar claramente identificados y un inventario de todos los importantes activos establecimiento y el mantenimiento

La propiedad de los activos	CONTROL: Toda la información y los activos asociados con el procesamiento de la información de instalaciones serán "propiedad" de una parte designada de la organización.
El uso aceptable de los activos	CONTROL: Normas para el uso aceptable de la información y los activos asociados a las instalaciones de procesamiento de información deben ser identificadas, documentados e implementados.
Clasificación de la información	
Objetivo: Garantizar que la información recibe un nivel adecuado de protección.	
Guías de Clasificación	CONTROL: La información se clasificará en función de su valor, los requisitos legales, la sensibilidad y criticidad a la organización.
Información y etiquetado manejo	CONTROL: Un conjunto apropiado de los procedimientos para el etiquetado de la información y la manipulación se desarrollará y ejecutará de conformidad con el sistema de clasificación adoptado por la organización.
Seguridad de los recursos humanos	
Antes de empleo	
Objetivo: Asegurar que los empleados, contratistas y terceros usuarios comprendan sus responsabilidades, y sean adecuados para las funciones que se consideran, y para reducir el riesgo de robo, fraude o mal uso de las instalaciones.	
Roles y responsabilidades	CONTROL: Los roles de seguridad y las responsabilidades de los empleados, contratistas y terceros usuarios serán definidas y documentadas de acuerdo con información de la política de seguridad de la organización.
Proyección	CONTROL: Controles de verificación de antecedentes de todos los candidatos a empleo, contratistas y usuarios de terceras partes se llevarán a cabo de acuerdo con las leyes, regulaciones y ética, y proporcional a los requerimientos del negocio, la clasificación de la información que se acceda, y los riesgos percibidos.
Términos y condiciones de empleo	CONTROL: Como parte de sus obligaciones contractuales, empleados, contratistas y usuarios de terceras partes lo acuerden y firmar los términos y condiciones de su contrato de trabajo, en el que expondrá sus responsabilidades y la de la organización para la seguridad de la información.
Durante el empleo	
Objetivo : Asegurar que todos los empleados , contratistas y usuarios de terceras partes son conscientes de las amenazas de seguridad de información y preocupaciones, sus responsabilidades y obligaciones , y están equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de error humano.	
Responsabilidades de la administración	CONTROL: Gestora deberá exigir a los empleados , contratistas y usuarios de terceras partes para aplicar la seguridad de conformidad con las políticas y procedimientos de la organización establecidas
Concienciación sobre la seguridad de la información, la educación y la formación	CONTROL: Todos los empleados de la organización y, en su caso , los contratistas y terceros usuarios deberán recibir una capacitación adecuada conciencia y actualizaciones periódicas en las políticas y procedimientos de la organización , como relevantes para su función de trabajo .
Proceso disciplinario	CONTROL: Habrá un proceso disciplinario formal para los empleados

	que hayan cometido una infracción de seguridad
Terminación o cambio de empleo	
Objetivo : Asegurar que los empleados , contratistas y terceros usuarios salen de una organización o cambian de empleo de una manera ordenada	
Responsabilidades de terminación	CONTROL: Responsabilidades para realizar la terminación del empleo o cambio de empleo, deberán estar claramente definidas y asignadas.
Categorías de los activos	CONTROL: Todos los empleados, contratistas y usuarios de terceras partes deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.
La eliminación de los derechos de acceso	CONTROL: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a las instalaciones de procesamiento de la información y de información deberán ser retirados a la terminación de su empleo, contrato o convenio, o ajustarse a cambio.
Seguridad física y ambiental	
Áreas seguras	
Objetivo: Impedir el acceso físico no autorizado, el daño y la interferencia a las instalaciones de la organización e información.	
Perímetro de seguridad física	CONTROL: Perímetros de seguridad (barreras, como paredes, puertas de entrada de tarjetas controlada o mostradores de recepción tripulados) se utilizan para proteger áreas que contienen las instalaciones de procesamiento de la información y de la información.
Controles de entrada físicas	CONTROL: Áreas seguras se protegerán mediante controles de entrada adecuados a garantizar que se permite el acceso sólo el personal autorizado.
Asegurar oficinas, salas y comodidades	CONTROL: La seguridad física para oficinas, salas e instalaciones deberá ser diseñada y aplicada.
La protección contra externa y amenazas ambientales	CONTROL: La protección física contra los daños causados por incendios, inundaciones, terremotos, explosiones, disturbios civiles, y otros tipos de catástrofes naturales o de origen humano se diseñó y aplicó.
Trabajar en zonas seguras	CONTROL: Protección física y directriz para el trabajo en las áreas de seguridad deberá ser diseñada y aplicada.
El acceso del público, la entrega y zonas de carga	CONTROL: Los puntos de acceso como las zonas de entrega y de carga y otros puntos en los que personas no autorizadas puedan entrar en los locales deberán ser controlados y, si es posible, aislado de procesamiento de la información instalaciones para evitar el acceso no autorizado.
Seguridad de los equipos	
Objetivo: Para evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la organización.	
Equipo emplazamiento y protección	CONTROL: El equipo deberá estar situado o protegido para reducir los riesgos de amenazas y peligros ambientales , y las oportunidades para el acceso no autorizado .
Apoyo a los servicios públicos	CONTROL: El equipo debe ser protegido de fallas de energía y otros Interrupciones causadas por fallas en el apoyo a los servicios públicos.

Seguridad del cableado	CONTROL: Servicios de transporte de datos o soporte de información de energía y telecomunicaciones de cableado deben estar protegidos contra la interceptación o daños.
El mantenimiento del equipo	CONTROL: El equipo debe mantenerse correctamente para asegurar su disponibilidad e integridad continua.
Seguridad de off premises equipo	CONTROL: Seguridad se aplicará a los equipos de fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
La eliminación segura o la reutilización de equipo	CONTROL: Todos los artículos de equipos que contengan soportes de almacenamiento deberán ser evaluados para verificar que los datos sensibles y software con licencia ha sido eliminado o sobrescrito de forma segura antes de su eliminación.
La eliminación de la propiedad	CONTROL: Equipos, información o software no se tendrán fuera de sitio sin autorización previa.
Comunicaciones y operaciones de gestión	
Procedimientos y responsabilidades operacionales	
Objetivo: Para garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.	
Operativos documentados	CONTROL: Los procedimientos de operación deberán ser documentados, mantenidos y puestos a disposición de todos los usuarios que los necesitan.
Gestión del cambio	CONTROL: Los cambios en las instalaciones y sistemas de procesamiento de información deben ser controladas.
La segregación de funciones	CONTROL: Deberes y áreas de responsabilidad deben estar separados para reducir oportunidades para la modificación no autorizada o accidental o mal uso de los activos de la organización.
Separación del desarrollo, Instalaciones de ensayo y operacionales	CONTROL: Desarrollo, prueba e instalaciones operativas estarán separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.
Gestión de la prestación de servicios de terceros	
Objetivo: Implementar y mantener el nivel adecuado de seguridad de la información y la prestación de servicios en línea con los acuerdos de prestación de servicios de terceros.	
La prestación de servicios	CONTROL: Se velará por que los controles de seguridad, las definiciones de servicios y niveles de envío incluidos en el tercer acuerdo de prestación de servicios de terceros se implementan, operado y mantenido por el tercero.
Seguimiento y revisión de servicios de terceros	CONTROL: Los servicios, informes y registros proporcionados por el tercero serán controlados periódicamente y revisados , y las auditorías se llevarán a cabo con regularidad.
Gestión de cambios a tercera servicios para fiestas	CONTROL: Los cambios en la prestación de servicios, incluido el mantenimiento y la mejora de la seguridad de información políticas, procedimientos y controles existentes, serán gestionados, teniendo en cuenta la criticidad de los sistemas y procesos de negocio involucrados y reevaluación de riesgos.

Planificación y aceptación del sistema	
Objetivo: Para minimizar el riesgo de fallas en los sistemas.	
Gestión de la capacidad	CONTROL: El uso de los recursos será supervisado, afinado , y proyecciones hecho de las futuras necesidades de capacidad para garantizar el funcionamiento del sistema requerido .
Aceptación del sistema	CONTROL: Los criterios de aceptación para los nuevos sistemas de información, actualizaciones y nuevas versiones serán establecidos y las pruebas adecuadas del sistema (s) llevó a cabo durante el desarrollo y antes de la aceptación .
Protección contra código malicioso y móvil	
Objetivo: Proteger la integridad del software y de la información.	
Controles contra malicioso código	CONTROL: Detección, prevención y control de recuperación de protección contra código malicioso y procedimientos apropiados de sensibilización usuario será implementado.
Controles contra móvil	CONTROL: Cuando se autorice el uso de código móvil, la configuración se asegurará de que el código móvil autorizado funciona de acuerdo con una política de seguridad claramente definido, y el código móvil no autorizado puede ser impedido de ejecutar.
Back-up	
Objetivo: Mantener la integridad y la disponibilidad de las instalaciones de procesamiento de la información y de la información.	
Información copias de seguridad	CONTROL: Se tendrán copias de seguridad de la información y software y probado periódicamente de acuerdo con la política de copia de seguridad convenido.
Gestión de la seguridad de red	
Objetivo: Garantizar la protección de la información en las redes y la protección de la infraestructura de apoyo.	
Controles de red	CONTROL: Redes serán gestionados adecuadamente y controlados, con el fin de protegerse de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones de red , incluyendo la información en tránsito.
Seguridad de los servicios de red	CONTROL: Las características de seguridad , niveles de servicio y los requisitos de gestión de todos los servicios de red serán identificados e incluidos en cualquier acuerdo de servicios de red , si estos servicios son prestados en la empresa o subcontratados
Manejo del soporte	
Objetivo: Para evitar la divulgación no autorizada, modificación, eliminación o destrucción de bienes, y la interrupción de actividades empresariales.	
Gestión de soportes extraíbles	CONTROL: Habrá procedimientos para la gestión de medios extraíbles.
La eliminación de los medios de comunicación	CONTROL: Medios deberán ser desechados de forma segura y con seguridad cuando ya no se necesiten, utilizando procedimientos formales.

Tratamiento de la información procedimientos	CONTROL: Los procedimientos para el manejo y almacenamiento de la información serán establecidos para proteger esta información contra su divulgación o uso no autorizado.
Seguridad del sistema de documentación	CONTROL: Documentación del sistema estará protegida contra el acceso no autorizado.
Intercambio de información	
Objetivo: Mantener la seguridad de la información y software cambiar dentro de una organización y con cualquier entidad externa.	
Intercambio de información políticas y procedimientos	CONTROL: Los acuerdos se establecieron para el intercambio de información y software entre la organización y las partes externas.
Los acuerdos de intercambio	CONTROL: Los acuerdos se establecieron para el intercambio de información y software entre la organización y las partes externas.
Medios físicos en tránsito	CONTROL: Los medios que contienen información deberán estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante el transporte más allá de los límites físicos de una organización.
Información de negocios de sistemas	CONTROL: Las políticas y procedimientos deben ser desarrollados e implementados para proteger la información asociada a la interconexión de los sistemas de información de negocios.
Mensajería electrónica	CONTROL: Protección a todos los mensajes.
Servicios de comercio electrónico	
Objetivo: Garantizar la seguridad de los servicios de comercio electrónico, y su uso seguro.	
El comercio electrónico	CONTROL: Informaciones involucradas en el comercio electrónico que pasa por encima del público redes deberán estar protegidas de la actividad fraudulenta, disputa de contrato, y la divulgación no autorizada y modificación.
Transacciones en línea	CONTROL: Información involucrada en las transacciones en línea estarán protegidos a prevenir la transmisión incompleta, errónea enrutamiento, alteración mensaje no autorizado, revelación no autorizada, la duplicación de mensajes no autorizados o la repetición.
Información Públicamente Disponible	CONTROL: La integridad de la información está disponible en un público disponible del sistema deberá estar protegido para evitar la modificación no autorizada.
Monitoreo	
Objetivo: Detectar las actividades de procesamiento de información no autorizadas.	
El registro de auditoría	CONTROL: Los registros de auditoría registran las actividades del

	usuario, excepciones y eventos de seguridad de información se producen y se mantienen durante un período acordado para ayudar en futuras investigaciones y monitoreo de control de acceso.
El uso del sistema de monitoreo	CONTROL: Procedimientos para el uso de vigilancia de las instalaciones de procesamiento de información se establecerán y los resultados de las actividades de vigilancia revisados regularmente.
Protección de la información de registro	CONTROL: Registro de las instalaciones y la información de registro estarán protegida contra la manipulación y acceso no autorizado.
Administrador y operador de registros	CONTROL: Se registrarán administrador del sistema y las actividades del operador del sistema.
El registro de fallos	CONTROL: Fallas se registrarán, analizarán, y tomarán las medidas correspondientes.
Sincronización de la hora	CONTROL: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de un dominio de organización o de seguridad estarán sincronizados con un recurso de hora exacta acordado.
Control de acceso	
Requerimiento de negocio de control de acceso	
Objetivo: Controlar el acceso a la información.	
Política de control de acceso	CONTROL: Se establecerá una política de control de acceso, documentado, y revisado en base a los requisitos empresariales y de seguridad para el acceso.
Gestión de acceso de usuario	
Objetivo: Garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.	
Registro de usuarios	CONTROL: Habrá un registro de usuarios y de-registro formal procedimiento para otorgar y revocar el acceso a todos sistemas y servicios de información.
Gestión de privilegios	CONTROL: La asignación y uso de los privilegios serán restringidas y controladas.
La administración de contraseñas de usuario	CONTROL: La asignación de contraseñas se controla a través de un proceso de gestión formal.
Revisión de los derechos de acceso de usuario	CONTROL: La dirección revisará los derechos de acceso de los usuarios a intervalos regulares mediante un proceso formal.
Responsabilidades del usuario	
Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o el robo de información y procesamiento de la información instalaciones.	
Utilización Contraseña	CONTROL: Se exigirá a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de contraseñas.
Equipos de usuario desatendida	CONTROL: Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada.

Política de Escritorio y Pantalla limpia	CONTROL: Se adoptará una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política clara pantalla para las instalaciones de procesamiento de información.
Control de acceso de red Objetivo: Para prevenir el acceso no autorizado a los servicios en red.	
Política sobre el uso de la red de servicios.	CONTROL: Los usuarios sólo deberán disponer de acceso a los servicios que han sido autorizados específicamente para su uso.
La autenticación del usuario para conexiones externas	CONTROL: Métodos de autenticación apropiados se utilizan para controlar el acceso de usuarios remotos.
Identificación del material en redes	CONTROL: Identificación automática equipo se considerará como un medio para autenticar las conexiones desde ubicaciones y equipos específicos.
Diagnóstico de remoto y protección de puerto de configuración	CONTROL: Se controlará el acceso físico y lógico a los puertos de diagnóstico y configuración.
La segregación en las redes	CONTROL: Grupos de servicios de información, los usuarios y los sistemas de información deben estar separados de las redes.
Sincronización de la hora	CONTROL: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de un dominio de organización o de seguridad estarán sincronizados con un recurso de hora exacta acordado.
Control de la conexión de red	CONTROL: Para las redes compartidas, especialmente aquellas que se extienden a través de los límites de la organización, la capacidad de los usuarios para conectarse a la red se limitarán, en línea con la política y los requisitos de las aplicaciones de negocio (véase 11.1) de control de acceso.
Control de encaminamiento de red	CONTROL: Controles de enrutamiento se aplicarán a las redes para garantizar que las conexiones informáticas y de los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.
Control de acceso del sistema operativo Objetivo: Para prevenir el acceso no autorizado a los sistemas operativos.	
Inicio de sesión seguro procedimientos	CONTROL: El acceso a los sistemas operativos se controla mediante un procedimiento de inicio de sesión seguro.
Identificación de usuario y autenticación	CONTROL: Todos los usuarios deben tener un identificador único (ID de usuario) exclusivamente para su propio uso personal, y una técnica de autenticación adecuados serán elegidos para corroborar la identidad declarada de un usuario.
La gestión de contraseñas	CONTROL: Sistemas de gestión de contraseñas deberán ser

	interactivos y velarán contraseñas de calidad.
Uso de las utilidades del sistema	CONTROL: El uso de programas de utilidad que podría ser capaz de anular sistemas y aplicaciones controles tendrán carácter reservado y bien.
Sesión de tiempo de espera	CONTROL: Sesiones inactivas se apague después de un período definido de inactividad.
Limitación de tiempo de conexión	CONTROL: Restricciones en los tiempos de conexión se utilizan para proporcionar seguridad adicional para aplicaciones de alto riesgo.
Aplicación y acceso a la información de control	
Objetivo: Para prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.	
Restricción al acceso a la información	CONTROL: El acceso a las funciones de información y sistemas de aplicaciones por los usuarios y el personal de apoyo se limitará de acuerdo con la política de control de acceso definido.
Aislamiento del Sistema Sensible	CONTROL: Sistemas sensibles tendrán un (aislado) informática dedicada medio ambiente.
Informática móvil y teletrabajo	
Objetivo: Garantizar la seguridad de información al utilizar instalaciones informáticas y de teletrabajo móviles.	
La informática móvil y comunicaciones	CONTROL: Una política formal deberá estar en su lugar, y se adoptará las medidas de seguridad apropiadas para proteger contra los riesgos del uso de los recursos informáticos y de comunicaciones móviles.
Teletrabajo	CONTROL: Una política, planes y procedimientos operativos se desarrollaron e implementó para las actividades de teletrabajo.
Sistemas de información de adquisición , desarrollo y mantenimiento	
Los requisitos de seguridad de los sistemas de información	
Objetivo: Garantizar que la seguridad es una parte integral de los sistemas de información.	
Los requisitos de seguridad análisis y especificación	CONTROL: Declaraciones de los requerimientos del negocio para los nuevos sistemas de información, o mejoras de los sistemas de información existentes deberán especificar los requisitos para los controles de seguridad.
Procesamiento correcto en aplicaciones	
Objetivo: Para evitar errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.	
La validación de datos	CONTROL: La entrada de datos a las aplicaciones será validada para asegurar que esos datos son correctos y adecuados.
El control de procesamiento interno	CONTROL: Comprobaciones de validación deberán ser incorporadas en las aplicaciones para detectar cualquier corrupción de información a través de los errores de procesamiento o actos deliberados.
Integridad de los mensajes	CONTROL: Requisitos para garantizar la autenticidad y la protección

	de la integridad del mensaje en aplicaciones serán identificados y los controles adecuados identificados e implementados.
La validación de datos de salida	CONTROL: La salida de datos desde una aplicación deberá ser validada para asegurarse de que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias.
Controles criptográficos	
Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.	
Política sobre el uso de controles criptográficos	CONTROL: Una política sobre el uso de controles criptográficos para la protección de la información deberá ser desarrollada e implementada.
La gestión de claves	CONTROL: Gestión de claves estará en el lugar para apoyar el uso de la organización de las técnicas criptográficas.
La seguridad de los archivos del sistema	
Objetivo: Garantizar la seguridad de los archivos del sistema.	
El control de software operativo	CONTROL: Habrá procedimientos para controlar la instalación de software en sistemas operativos.
Protección de los datos de prueba del sistema	CONTROL: Los datos de prueba deben seleccionarse cuidadosamente y protegidos y controlados.
Control de acceso al código fuente del programa	CONTROL: El acceso al código fuente del programa será restringido.
Seguridad en los procesos de desarrollo y soporte	
Objetivo: Mantener la seguridad del software del sistema de aplicación y la información.	
Cambie los procedimientos de control	CONTROL: La implementación de los cambios será controlado por el uso de los procedimientos normales de control de cambios.
Revisión técnica de solicitudes después de cambios en el sistema operativo	CONTROL: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio serán revisados y probados para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.
Las restricciones a los cambios en los paquetes de software	CONTROL: Las modificaciones a los paquetes de software se pondrán trabas, limitada a los cambios necesarios, y todos los cambios deben ser estrictamente controlados.
Fuga de información	CONTROL: Se impedirá Oportunidades para la fuga de información.
Desarrollo de software externalizado	CONTROL: Desarrollo de software externalizado será supervisado y monitoreado por la organización.
Gestión de Vulnerabilidades Técnica	
Objetivo: Reducir los riesgos derivados de la explotación de las vulnerabilidades técnicas publicadas.	
El control de las vulnerabilidades técnicas	CONTROL: La información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan se obtendrá, la exposición de la organización a tales vulnerabilidades evaluada, y

	tomarse medidas adecuadas para hacer frente a los riesgos asociados.
Información de gestión de incidentes de seguridad	
Comunicación de los incidentes de seguridad de información y debilidades	
Objetivo: Garantizar los eventos de seguridad de la información y debilidades asociadas con los sistemas de información se comunican de una manera que permite acciones correctivas oportunas que deban tomarse.	
Comunicación de los incidentes de seguridad de información	CONTROL: Los eventos de seguridad de la información deben ser reportados a través apropiado canales de gestión lo más rápido posible.
Informes debilidades de seguridad	CONTROL: Todos los empleados, contratistas y terceros usuarios de la información se exigirán a los sistemas y servicios de observar y reportar cualquier deficiencia de seguridad que observen o sospechen en sistemas o servicios.
Gestión de incidentes de seguridad de la información y mejoras	
Objetivo: Garantizar un enfoque coherente y eficaz es aplicada a la gestión de incidentes de seguridad de la información.	
Responsabilidades y procedimientos	CONTROL: Responsabilidades y procedimientos de gestión se establecerán para garantizar una respuesta rápida, eficaz y ordenada a la información de los incidentes de seguridad.
Aprender de la información incidentes de seguridad	CONTROL: No habrá mecanismos para permitir a los tipos, volúmenes y costos de los incidentes de seguridad de la información para ser cuantificados y controlados.
El acopio de pruebas	CONTROL: Cuando una acción de seguimiento contra una persona u organización después de una incidente seguridad de la información implica la acción jurídica (civil o penal) , se percibirá la evidencia , retuvo , y se presentó a cumplir con las reglas de pruebas establecido en la jurisdicción correspondiente.
La continuidad del negocio y evaluación de riesgos	CONTROL: Eventos que pueden causar interrupciones en los procesos de negocio deben ser identificados, junto con la probabilidad y el impacto de estas interrupciones y sus consecuencias para la seguridad de la información.
Desarrollo e implementación de planes de continuidad incluyendo seguridad de la información	CONTROL: Los planes deberán desarrollarse y aplicarse para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas siguiente interrupción, o el fracaso de los procesos críticos de negocio.
Marco de planificación de la continuidad del negocio	CONTROL: Deberá mantenerse un único marco de planes de continuidad de negocio para asegurar que todos los planes son coherentes, para abordar sistemáticamente los requisitos de seguridad de la información, e identificar prioridades para pruebas y mantenimiento.
Pruebas, mantenimiento y reevaluación de planes de continuidad de negocio	CONTROL: Los planes de continuidad de negocios deberán ser probados y actualizados regularmente para asegurarse de que están al día y eficaz.
Conformidad	

Cumplimiento de los requisitos legales	
Objetivo: Evitar las infracciones de cualquier ley, las obligaciones legales, reglamentarias o contractuales, y de cualquier requisito de seguridad.	
Identificación de la legislación aplicable	CONTROL: Los requisitos reglamentarios y contractuales y el enfoque de la organización para cumplir con estos requisitos se definen explícitamente, documentados, y se mantienen al día para cada sistema de información y la organización.
Derechos de propiedad intelectual (DPI)	CONTROL: Procedimientos apropiados se aplicarán para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales sobre el uso de material para la que puede haber propiedad intelectual derechos y en el uso de productos de software privativo.
Protección de los registros de la organización	CONTROL: Registros importantes estarán protegidos contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, reglamentarios, contractuales y de negocio.
Protección de datos y privacidad de la información personal	CONTROL: Protección de datos y privacidad se garantizará como se requiere en la legislación pertinente, los reglamentos, y si las cláusulas contractuales aplicables.
Prevención del uso indebido de instalaciones de procesamiento de información	CONTROL: Los usuarios se decidan a utilizar las instalaciones de procesamiento de información para fines no autorizados.
Reglamento de controles criptográficos	CONTROL: Controles criptográficos se utilizarán de conformidad con todos los pertinentes convenios, leyes y reglamentos.
Cumplimiento de las políticas de seguridad y las normas y el cumplimiento técnico.	
Objetivo: Garantizar el cumplimiento de los sistemas con las políticas y estándares de seguridad de la organización.	
Cumplimiento de la seguridad, políticas y normas	CONTROL: Los gerentes se asegurarán de que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad.
Verificación del cumplimiento técnico	CONTROL: Los sistemas de información deberán ser revisados regularmente por el cumplimiento de las normas de aplicación de la seguridad.
Sistemas de información consideraciones de auditoría	
Objetivo: Maximizar la eficacia y minimizar la interferencia a / desde el proceso de auditoría de sistemas de información.	
Auditoría de los sistemas de información	CONTROL: Requisitos y actividades de control de los sistemas operativos de auditoría deben ser cuidadosamente planificadas y acordadas para reducir al mínimo el riesgo de interrupciones de los procesos de negocio.
Protección de la información, herramientas de auditoría de sistemas	CONTROL: El acceso a las herramientas de auditoría de sistemas de información estará protegida de prevenir cualquier posible uso incorrecto o el compromiso.

Fuente: Matalobos Juan, 2009.

http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Anexo B

Tabla No 4
OCDE principios y norma internacional

Principio de la OCDE	Correspondiente proceso de SGSI y fase PDCA
Conciencia: Los miembros deben ser conscientes de la necesidad de seguridad de los sistemas y redes de información y de su mejoría.	Esta actividad forma parte de la fase de Do.
Responsabilidad: Todos los miembros son responsables de la seguridad de los sistemas.	Esta actividad forma parte de la fase de Do.
Respuesta: Los participantes deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes de seguridad.	Esto es en parte una actividad de supervisión Comprobar fase y una fase ley. Puede estar cubierto por algunos aspectos del Plan y comprobar fases.
Evaluación de Riesgos: Los participantes deben	Esta actividad forma parte de la fase del Plan y la

llevar a cabo las evaluaciones de riesgos.	reevaluación del riesgo es parte de la fase de Check.
Diseño de seguridad y aplicación: Los miembros deben incorporar la seguridad como un elemento esencial de los sistemas y redes informáticos.	Evaluados los riesgos, los controles son seleccionados para su tratamiento como parte de la fase del Plan. La fase Do y luego cubre la ejecución y uso operativo de estos controles.
Gestión de la seguridad: Los participantes deberán adoptar un enfoque integral para gestión de la seguridad.	La gestión de riesgos es un proceso que incluye la prevención, detección y respuesta a incidentes, en curso, mantenimiento, revisión y auditoría. Todos estos aspectos están englobados en el plan, Do, Check y la ley fases.
Revaloración: Los participantes deben revisar y reevaluar la seguridad de sistemas de información y redes, y hacer las modificaciones pertinentes a las políticas de seguridad, prácticas, medidas y procedimientos.	Nueva evaluación de seguridad de la información es una parte de la fase de Check, donde las revisiones periódicas deben realizarse para comprobar la eficacia del SGSI y la mejora de la seguridad es parte de la ley.

Fuente: Marquina Edgar, 2010. <http://bibdigital.epn.edu.ec/bitstream/15000/2500/1/CD-3203.pdf>.

DOCTOR ROMEL MACHADO CLAVIJO,
SECRETARIO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION
DE LA UNIVERSIDAD DEL AZUAY,

C E R T I F I C A:

Que, el H, Consejo de Facultad de Ciencias de la Administración en sesión del 15 de julio de 2014, conoció la petición de la señorita **KARLA GEOVANNA CORDERO TORRES** (46021) que denuncia su trabajo de titulación denominado: **"ESTUDIO COMPARATIVO ENTRE LAS METODOLOGIAS MAGERIT Y CRAMM UTILIZADAS PARA EL ANALISIS Y GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION"** presentado como requisito previo a la obtención del Grado de Ingeniera de Sistemas y Telemática. El Consejo acoge el informe de la Junta Académica y aprueba la denuncia. Designa como Director del trabajo al ingeniero Esteban Crespo Martínez y como miembros del Tribunal Examinador a los ingenieros Paúl Ochoa Arévalo y Rubén Ortega López. De conformidad con la disposición general tercera del Reglamento de Régimen Académico, el peticionario tiene un plazo equivalente a dos períodos académicos ordinarios (semestres) para desarrollar y terminar su trabajo de titulación, esto es hasta el 15 de julio de 2015.-

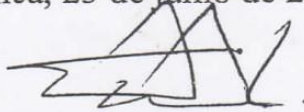
Cuenca, julio 18 de 2014



CONVOCATORIA

Por disposición de la Junta Académica de Ingeniería de Sistemas y Telemática **CONVOCO** a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación denominado: **“ESTUDIO COMPARATIVO ENTRE LAS METODOLOGIAS MAGERIT Y CRAMM UTILIZADAS PARA EL ANALISIS Y GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION”** presentado por la señorita **KARLA GEOVANNA CORDERO TORRES (46021)**, previa a la obtención del grado de Ingeniera de Sistemas y Telemática, para el día **MARTES 1 SDE JULIO DE 2014, a las 18h30**

Cuenca, 25 de junio de 2014



Dr. Romel Machado Clavijo
Secretario de la Facultad

Ing. Esteban Crespo Martínez

Ing. Paúl Ochoa Arévalo

Ing. Rubén Ortega López



convocob
2014

Oficio Nro. 063-2014-DIST-UDA

Cuenca, 23 de Junio de 2014

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 13 de Junio del 2014, recibió el proyecto de monografía titulado "Estudio comparativo entre las metodologías MAGERIT y CRAMM utilizadas para el análisis y gestión de riesgos de Seguridad de la Información", presentada por el estudiante Karia Cordero, estudiante de la Escuela de Ingeniería de Sistemas y revisado por el Ing. Esteban Crespo, previo a la obtención del título de Ingeniero de Sistemas.

La Junta solicita por su digno intermedio notificar al tribunal designado y determinar lugar, fecha y hora de sustentación.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Esteban Crespo y como miembros del Tribunal a los Ing. Paúl Ochoa Arévalo y Ing. Rubén Ortega.



Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

Sustentación del Diseño de Tesis (Doctor Romel Machado Clavijo)

Fecha: 24-06-2014

ESCUELA DE INGENIERIA DE SISTEMAS

Diseños de Tesis

Escuela de Sistemas

Estudiante: Karla Geovanna Cordero Torres con código 46021.

Tema: "ESTUDIO COMPARATIVO ENTRE LAS METODOLOGIAS MAGERIT Y CRAMM UTILIZADAS PARA EL ANALISIS Y GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION"

Para: La obtención del título de Ingeniero en Sistemas

Director: Ing. Esteban Crespo.

Tribunal: Ing. Paúl Ochoa Arévalo

Tribunal: Ing. Rubén Ortega

DIA: *MARTE*

FECHA: *1 Julio*

HORA: *18h30.*



ACTA SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

- 1.1.1 Nombre del estudiante: KARLA GEOVANNA CORDERO TORRES
- 1.1.2 Código 46021
- 1.1.3 Director sugerido: Ing. Esteban Crespo M.
- 1.1.4 Codirector (opcional): _____

1.2 Tribunal: Ings. Rubén Ortega y Paúl Ochoa Arévalo

1.3 Título propuesto: ESTUDIO COMPARATIVO ENTRE LAS METODOLOGIAS MAGERIT Y CRAMM UTILIZADAS PARA EL ANALISIS Y GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

1.4 Resolución:

1.4.1 Aceptado sin modificaciones _____

1.4.2 Aceptado con las siguientes modificaciones:

REALIZAR, EN EL CAPITULO I, UNA INTRODUCCION Y ANALISIS A ISO27001, ISO27002, ISO27005, ISO3100

MODIFICAR EL OBJETIVO I. MODIFICACION DEL ALCANCE. REVISAR Y REAJUSTAR EL CRONOGRAMA.

1.1.1 Responsable de dar seguimiento a las modificaciones (designado por la Junta Académica de entre los Miembros del Tribunal): Ing. Esteban Crespo

1.1.2 No aceptado
• Justificación:

Tribunal

.....
Ing. Esteban Crespo M.

.....
Ing. Paul Ochoa Arévalo

.....
Ing. Rubén Ortega López

.....
Srta. Karla G. Cordero T.

.....
Secretario de Facultad

Fecha de sustentación: 1ro JULIO 2014



RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: KARLA GEOVANNA CORDERO TORRES

1.1.1. Código 46021

1.1.2. 1.2 Director sugerido: Ing. Esteban Crespo M.

1.3 Codirector (opcional):

1.4. Título propuesto: ESTUDIO COMPARATIVO ENTRE LAS METODOLOGIAS MAGERIT Y CRAMM UTILIZADAS PARA EL ANALISIS Y GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

1.1 1.5 Revisores (tribunal): Ings. Rubén Ortega y Paúl Ochoa Arévalo

1.2 1.6 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	✓			
Título Propuesto				
2. ¿Es informativo?	✓			
3. ¿Es conciso?	✓			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	✓			
5. ¿Describe la teoría en la que se enmarca el trabajo	✓			
6. ¿Describe los trabajos relacionados más relevantes?	✓			
7. ¿Utiliza citas bibliográficas?	✓			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	✓			
9. ¿Tiene relevancia profesional y social?	✓			
Hipótesis (opcional)				
10. ¿Se expresa de forma clara?	✓			
11. ¿Es factible de verificación?				
Objetivo general				
12. ¿Concuerda con el problema formulado?	✓			
13. ¿Se encuentra redactado en tiempo verbal infinitivo?	✓			
Objetivos específicos				
14. ¿Concuerdan con el objetivo general?	✓			
15. ¿Son comprobables cualitativa o cuantitativamente?	✓			
Metodología				



16. ¿Se encuentran disponibles los datos y materiales mencionados?	/			
17. ¿Las actividades se presentan siguiendo una secuencia lógica?	/			
18. ¿Las actividades permitirán la consecución de los objetivos específicos planteados?	/			
19. ¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	/			
Resultados esperados				
20. ¿Son relevantes para resolver o contribuir con el problema formulado?	/			
21. ¿Concuerdan con los objetivos específicos?	/			
22. ¿Se detalla la forma de presentación de los resultados?	/			
23. ¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	/			
Supuestos y riesgos				
24. ¿Se mencionan los supuestos y riesgos más relevantes?	/			
25. ¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	/			
Presupuesto				
26. ¿El presupuesto es razonable?	/			
27. ¿Se consideran los rubros más relevantes?	/			
Cronograma				
28. ¿Los plazos para las actividades son realistas?		/		
Referencias				
29. ¿Se siguen las recomendaciones de normas internacionales para citar?	/			
Expresión escrita				
30. ¿La redacción es clara y fácilmente comprensible?	/			
31. ¿El texto se encuentra libre de faltas ortográficas?	/			

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,



- Obligatorio cuando cumple parcialmente y NO cumple.

.....
.....
.....
.....

Ing. Esteban Crespo Martínez

Ing. Paúl Ochoa Arévalo

Ing. Rubén Ortega López

Cuenca. 4 de julio del 2014



Señor Ingeniero

Xavier Ortega Vasquez

Decano de la Facultad de Ciencias de la Administración

De mis consideraciones,

Luego de enviarle un cordial saludo, me permito informarle que luego de la sustentación del diseño de tesis de la Sra. **Karla Giovanna Cordero Torres** con tema de *"Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de Seguridad de la Información"*, se procedió con la aprobación del mismo una vez que se realice la siguiente modificación: Al contenido, incluir el análisis de las normativas ISO27001, ISO27002, ISO27005 e ISO31000; modificar el primer objetivo específico a manera de que se pueda fundamentar teóricamente las normativas anteriormente indicadas y, al alcance, hacer que el mismo se alinee al proyecto de investigación de la Universidad.

He procedido con la verificación de que se haya superado la observación emitida por los miembros del tribunal, por cuanto certifico, como director de tesis, que el cambio del objetivo general ha sido modificado.

Para los fines pertinentes, suscribo de Usted.

Atentamente,




Ing. Esteban Crespo Martínez, MBA

DOCTORA JENNY RIOS COELLO SECRETARIA, DE LA FACULTAD DE
CIENCIAS DE LA ADMINISTRACIÓN DE LA UNIVERSIDAD DEL AZUAY

CERTIFICA:

Que, la Señorita Karla Geovanna Cordero Torres, registrada con código 46021 perteneciente a la Escuela de Ingeniería de Sistemas, luego de cumplir con todas las asignaturas de su Pensum de estudios, egresó de la Facultad el día 01 de Febrero de 2014.

Cuenca, Junio 23 del 2014


UNIVERSIDAD DEL AZUAY
FACULTAD DE INGENIERÍA DE SISTEMAS
ADMINISTRACIÓN DE LA FACULTAD
SECRETARÍA

Derecho 101608

vcf.-



Cuenca, 24 de junio de 2014.

Ing.

Xavier Ortega Vásquez, MBA.

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION

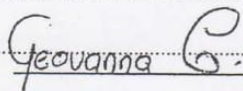
Ciudad

De mis consideraciones:

Karla Geovanna Cordero Torres con código 46021, egresado de la Escuela de Ingeniería de Sistemas y Telemática de la facultad de Ciencias de la Administración, solicito a usted de la forma más comedida y por su intermedio al Consejo de Facultad, la aprobación del diseño de tesis con el tema "Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de Seguridad de la Información", previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Me permito sugerir el nombre del Ing. Esteban Crespo, MBA como director de tesis, puesto que he recibido asesoramiento y cuento con su aprobación.

Atentamente,



Karla Geovanna Cordero Torres

0104245147

Cuenca, 24 de junio de 2014

Ing.

Xavier Ortega Vásquez, MBA

Decano de la Facultad de Ciencias de la Administración

Presente

De mi consideración:

Por la presente, me permito informarle que he revisado el diseño de tesis presentado por la estudiante **Karla Geovanna Cordero Torres** con el tema *"Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de Seguridad de la Información"*, como requisito previo para la obtención del título de Ingeniero de Sistemas y Telemática.

Al respecto, el diseño de tesis presenta una estructura teórica, metodológica y técnica coherente, cuyo objetivo es comparar las dos metodologías, a manera de poder seleccionar la que más se aplica al contexto ecuatoriano, formando parte de uno de los objetivos de investigación de un proyecto de Seguridad de la Información que se está planteando en la escuela de Sistemas y Telemática.

Por lo expuesto, emito informe favorable y recomiendo su aprobación.



Ing. Esteban Crespo Martínez, MBA

Oficio Nro. 063-2014-DIST-UDA

Cuenca, 23 de Junio de 2014

**Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Presente.-**

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 13 de Junio del 2014, recibió el proyecto de monografía titulado "Estudio comparativo entre las metodologías MAGERIT y CRAMM utilizadas para el análisis y gestión de riesgos de Seguridad de la Información", presentada por el estudiante Karla Cordero, estudiante de la Escuela de Ingeniería de Sistemas y revisado por el Ing. Esteban Crespo, previo a la obtención del título de Ingeniero de Sistemas.

La Junta solicita por su digno intermedio notificar al tribunal designado y determinar lugar, fecha y hora de sustentación.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Esteban Crespo y como miembros del Tribunal a los Ing. Paúl Ochoa Arévalo y Ing. Rubén Ortega.



Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay



UNIVERSIDAD DEL
AZUAY



UNIVERSIDAD DEL
AZUAY

**GUIA PARA LA ELABORACIÓN Y PRESENTACIÓN DE LA
DENUNCIA/PROTOCOLO DE TRABAJO DE TITULACIÓN**

1. DATOS GENERALES

1.1 Nombre del estudiante: Cordero Torres Karla Geovanna

1.1.1 Código: 46021

1.1.2 Contacto: teléfonos:

1.1.3 Convencional: 2072810133

1.1.4 Celular: 0984384794

1.1.5 Correo Electrónico: geovas7_5@hotmail.com

1.2 Director sugerido: Ingeniero Crespo Martínez Paul Esteban.

1.2.1 Contacto: Teléfonos:

1.2.1.1 Convencional: 4091000

1.2.1.2 Celular : 0996804562

1.2.1.3 Correo Electrónico: ecrespo@uazuay.edu.ec

1.3 Tribunal designado: (de acuerdo a la normativa interna de cada Facultad).

1.4 Aprobación: fecha de Junta Académica y fecha de Consejo Facultad.

1.5 Línea de Investigación de la carrera:

1.5.1 Código UNESCO: 1203

1.5.2 Tipo de trabajo:

El trabajo de titulación está basado en Proyectos técnicos relacionados con la Gestión de Seguridad de la Información.

1.6 Área de estudio: Seguridad de la Información

1.7 Título propuesto: Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de Seguridad de la Información.



1.8 Estado del proyecto: La propuesta iniciará con un estudio comparativo entre dos metodologías, utilizadas para el análisis y gestión de riesgos de Seguridad informática. Este estudio permitirá alcanzar el objetivo que plantea el proyecto de investigación de seguridad de la información que propone la escuela de Ingeniería de Sistemas y telemática: "Desarrollar una metodología ecuatoriana para el análisis y gestión de riesgo informático en las empresas del sector MPYME".

2. CONTENIDO

2.1 Motivación de la investigación: Actualmente no existe un estudio comparativo que indique cuál de las metodologías existentes para el análisis y gestión de riesgos de la Seguridad de la Información es la más adecuada para las mPYMES ecuatorianas.

2.2 Problemática: Existen varias metodologías internacionales para el análisis y gestión de riesgos de Seguridad de la Información pero en muchos casos, éstas no pueden ser alineadas a la realidad de cada nación. El proyecto de investigación de la Universidad requiere un análisis de las metodologías más nombradas a fin de poder definir y proponer una que se adapte al escenario ecuatoriano, alineándose a las normativas vigentes.

2.3 Pregunta de investigación: ¿Cuál de las dos metodologías para análisis y gestión de riesgos, MAGERIT o CRAMM, es la más viable para implementarse en las organizaciones mPYMES ecuatorianas?

2.4 Resumen: El presente trabajo pretende realizar un estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para el análisis y gestión de riesgos de la Seguridad de la Información, en base a los mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo.

2.4.1 Estado del Arte y marco teórico

2.4.1.1 Análisis de riesgos:

- A. Identificar los peligros
- B. Decidir quién y/ o que puede ser dañado y como
- C. Evaluar los riesgos y decidir las precauciones
- D. Registrar sus hallazgos e implementarlos
- E. Revisar su análisis y poner al día si es necesario (Gómez, 2014)

2.4.1.2 Gestión de riesgos:



UNIVERSIDAD DEL
AZUAY

Es la estructuración de las acciones de seguridad que nos ayudan a satisfacer las necesidades que se pueden detectar a lo largo del análisis (Candau, 2012).

2.4.1.3 MAGERIT

Es una metodología que fue elaborada por el Consejo Superior de Informática. La razón de ser está directamente relacionada con la generalización del uso de todos los medios electrónicos, informáticos y telemáticos de una organización. (PAE, 2014)

2.4.1.4 CRAMM

Es la metodología de análisis de riesgos desarrollado por el Centro de Informática y la Agencia Nacional de Telecomunicaciones (CCTA) del gobierno del Reino Unido.

El significado del acrónimo proviene de CCTARisk Analysis and Management Method. Su versión inicial data de 1987 y la versión vigente es la 5.2. (Enisa, 2003)

2.4.1.5 ISO 27001

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre del 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. (El portal de ISO 27001 en Español, 2014).

2.4.1.6 ISO 27002

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. (El portal de ISO 27001 en Español, 2014).

2.4.1.7 ISO 27005

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. (El portal de ISO 27001 en Español, 2014)

2.4.1.8 ISO 31000



La ISO 31000 está destinada a ser una familia de normas relativas a la gestión de riesgos. El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices genéricas sobre la gestión de riesgos. (El portal de ISO 27001 en Español, 2014)

2.5 Objetivo: Realizar un estudio comparativo entre las metodologías MAGERIT y CRAMM para el análisis y Gestión de Riesgo Tecnológico.

2.6 Objetivos específicos:

- Fundamentar y analizar teóricamente el concepto de análisis y gestión de riesgo basado en las normativas ISO 27001, 27002, 27005 y 31000
- Comparar las metodologías MAGERIT y CRAMM utilizadas en el análisis y gestión de riesgo informático, en base a mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo.
- Emitir un documento del estudio comparativo entre las metodologías MAGERIT y CRAMM en base a los mecanismos mencionados.

2.7 Metodología:

La metodología que se va a utilizar es la investigativa-deductiva, basándose en un proceso de razonamiento, que intenta no solo describir cada hecho, sino también ir dando explicaciones de cada uno.

2.8 Alcances y resultados esperados:

El proyecto pretende emitir un documento de la comparativa de las metodologías MAGERIT y CRAMM en base a mecanismos para la identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo y cálculo de riesgo, a fin de poder determinar cuál de ellas es la más viable a utilizar en el Proyecto de investigación de la Universidad del Azuay.

2.9 Supuestos y riesgos:

Describe los puntos críticos del trabajo que pueden afectar la realización adecuada del mismo en el tiempo propuesto y deja planteadas posibles alternativas de solución.



UNIVERSIDAD DEL AZUAY

- No contar con acceso a la información de CRAMM. Con MAGERIT no existe problema ya que la metodología está disponible gratuitamente en el portal del Instituto de Hacienda de España.
- Tener que adquirir las normativas ISO

2.10 Presupuesto: El presupuesto para el proyecto de titulación será de 150 Dólares.

	Costo USD (detalle)	Justificación ¿para qué?
Gastos varios	150	Gastos de impresión para revisiones, Gastos de transporte. Gastos de internet

2.11 Financiamiento: Financiamiento propio.

2.12 Esquema tentativo

ABSTRACT

INTRODUCCION

OBJETIVOS

CAPÍTULO 1: Marco teórico:

1.1 Seguridad de la información vs. Seguridad Informática

1.2 Riesgo informático

1.3 Gestión de Riesgos

1.4 ISO 27001

1.5 ISO 27002

1.6 ISO 27005

1.7 ISO 3100

1.8 MAGERIT

1.9 CRAMM

CAPÍTULO 2: Estudio de la metodología Magerit

2.1 Introducción del Capítulo.

2.2 Mecanismos de identificación de activos

2.3 Identificación de vulnerabilidades

2.4 Funciones de probabilidad

2.5 Variable de medición de riesgo

2.6 Cálculo de riesgo



UNIVERSIDAD DEL AZUAY

- 2.7 Alineación con el estándar ISO27001
- 2.8 Alineación con el estándar ISO27002
- 2.9 Alineación con el estándar ISO27005
- 2.10 Alineación con el estándar ISO31000
- 2.11 Conclusiones del capítulo

CAPÍTULO 3: Estudio de la metodología CRAMM

- 3.1 Introducción del capítulo
- 3.2 Mecanismos de identificación de activos,
- 3.3 Identificación de vulnerabilidades,
- 3.4 Funciones de probabilidad,
- 3.5 Variable de medición de riesgo,
- 3.6 Cálculo de riesgo
- 3.7 Alineación con el estándar ISO27001
- 3.8 Alineación con el estándar ISO27002
- 3.9 Alineación con el estándar ISO27005
- 3.10 Alineación con el estándar ISO31000
- 3.11 Conclusiones del capítulo

CAPÍTULO 4: Análisis comparativo entre Magerit y CRAMM

- Introducción al capítulo
- Cuadro comparativo de las metodologías
- Conclusiones del capítulo

- Conclusiones
- Recomendaciones
- Bibliografía

2.13 Cronograma: detalla las actividades y el tiempo previsto, en base a la

Objetivo Específico	Actividad	Resultado Esperado	Tiempo (Semanas)
1. Fundamentar y analizar teóricamente el concepto de análisis y gestión de riesgo basado en las normativas ISO 27001, 27002, 27005 y 3100	1. Fundamentar los conceptos de Análisis y Gestión de Riesgo Tecnológico	* Tener fundamentados teóricamente los conceptos de Análisis y Gestión de Riesgo	14 semanas



2. Estudiar las metodologías Magerit y CRAMM para realizar un estudio comparativo entre ellas.	1. Estudiar detalladamente cada una de las dos metodologías con las que estamos haciendo el estudio comparativo	* Tener un conocimiento detallado de cada una de las dos metodologías	12 semanas
3. Emitir un documento informe de la comparativa de las dos metodologías	1. Emitir un documento de todo el estudio comparativo de las dos metodologías	* Obtener un documento de la comparación realizada entre las dos metodologías.	8 semanas

2.14 Referencias:

(21 de 04 de 2014). Obtenido de Wikipedia:

http://es.wikipedia.org/wiki/Gesti%C3%B3n_de_riesgos

El portal de ISO 27001 en Español. (02 de 07 de 2014). Obtenido de

<http://iso27000.es/iso27000.html#section3b>

Candau, J. (2012). *Magerit 3.0*. Madrid.

Enisa. (2003). *European Union Agency for Network and Information Security*. Obtenido de

European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_cramm.html

Gómez. (2014). *Monografias.com*. Obtenido de Monografias.com:

<http://www.monografias.com/trabajos83/analisis-riesgo/analisis-riesgo.shtml>

Huerta, A. (30 de Marzo de 2012). *Security A(!)twork*. Obtenido de

<http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/>



UNIVERSIDAD DEL
AZUAY

PAE. (2014). *Portal administracion electronica*. Obtenido de Portal administracion electronica:
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U4j9nPI5OAK

Palisade. (s.f.). *@Risk*. Obtenido de <http://www.palisade-lta.com/risk/>

Administración, C. S. (13 de 12 de 2013). *PAE*. Obtenido de
http://administracionelectronica.gob.es/pae_Home/pae_Organizacion/pae_Ambit_o_Administracion_General_del_Estado_-_Organizacion/pae_CSAE_-_Organizacion_v2.html#.UqvArvTuKSo

Avellaneda, J. C. (7 de 3 de 2005). *Ilustre colegio de ingenieros de informática en la región de Murcia*. Obtenido de http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php

Matalobos, J. M. (5 de 2009). *oa.upm.es*. Obtenido de Trabajo de fin de carrera, análisis de riesgos de seguridad de información:
http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

PÚBLICAS, M. D. (2006). *MAGERIT, versión*. Madrid.

Wikipedia. (29 de 11 de 2013). Obtenido de
http://es.wikipedia.org/wiki/ISO/IEC_27001

GIS, G. (s.f.). *GRASS GIS- Introducción*.
<http://www.um.es/geograf/sigmur/yerba/intro.html>: [Último Acceso: 14-12-2013].

2.15 Firma de responsabilidad (estudiante)

Geovanna C

Geovanna Cordero T

0104245147



UNIVERSIDAD DEL
AZUAY

2.16 Firma de responsabilidad (director sugerido)

Ing Esteban Crespo Martinez, MBA

2.17 Fecha de entrega: 04 de julio de 2014

