UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCAS DE LA ADMINISTRACION.

ESCUELA DE SISTEMAS Y TELEMATICA

COMPARACIÓN ENTRE METODOLOGÍAS DE GESTIÓN DE RIESGO INFORMÁTICO.

TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN SISTEMAS Y TELEMATICA.

AUTORES: DAVID MARCELO LÓPEZ JARAMILLO.

SANTIAGO ANDRÉS VÁSQUEZ MEJÍA.

DIRECTOR: CRESPO MARTÍNEZ PAÚL ESTEBAN, MBA.

CUENCA, ECUADOR

2016

Dedicatoria.

En la consecución de este ideal, el eslabón trascendental es el hogar, lumbre constante de ejecutorias plenas para quien dedico esta tesis:
A Dios, por darme la oportunidad y fuerza necesaria para abordar esta etapa educativa que hoy culmino con éxito, a mis padres y familia por su apoyo incondicional, a mi enamorada la cual ha estado apoyándome, a mis amigos y compañeros que me motivan constantemente a cumplir mis objetivos, y por ultimo a mis profesores por haberme enseñado todo lo que ahora sé.
"La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar". Thomas Chalmers

David M. López Jaramillo.

Este trabajo está dirigido a todos mis seres queridos principalmente a mis padres por su afecto, paciencia, entusiasmo y apoyo infinito e incondicional, a mis hermanos Fátima y Fernando, que con su constante y experto consejo me guiaron en la búsqueda de mi ideal, a mis sobrinos Carlos, Dagmar, Juan Fernando y Fernando José, que con alegría e inocencia supieron disipar mis penas y rabietas.

A mis amigos y compañeros presentes y ausentes David, Santiago, Manolo, Cesar, Andrés, Francisco y Darío por prestarme una mano amiga para hacer realidad mis objetivos y mi anhelo con fe y coraje.

Santiago Andrés Vásquez M.

Agradecimientos.

Es muy importante saber, pero más importante es saber enseñar.
En este sentido nuestra gratitud y agradecimientos a:
Dios por darnos la vida y sabiduría para el desarrollo de esta tesis, la misma que nos permitirá alcanzar nuestros sueños y metas, a la Universidad del Azuay y a los profesores de la escuela de Ingeniería en Sistemas y Telemática porque nos sirvieron de marco al compartirnos todas sus enseñanzas para culminar la carrera, especialmente al Ing. Esteban Crespo y al Ing. Francisco Salgado, director y tutor de nuestro trabajo, quienes responsable y eficientemente orientaron esta investigación, propiciando: “El aprender a aprender”.

Contenido

Índice de Imágenes.

Índice de Tablas.

Resumen.

El riesgo informático para cualquier organización del sector MPYME ecuatoriano es inminente. Para contrarrestarlo, buscan apegarse a ciertos estándares establecidos por normas y metodologías internacionales, que sugieren mecanismos, procesos y alternativas para la gestión de riesgos. Sin embargo, debido a la incompatibilidad, el costo de implementarlos, o a la complejidad de ejecutarlo, para muchas lograrlo se vuelve inalcanzable. Este documento realiza una comparación entre las metodologías "Security Risk Managment Guide de Microsoft", OCTAVE, y su alineación con las normativas ISO 27001, 27002, 27005, y 31000 en base a lineamientos para la identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variables de medición de riesgos y cálculo de riesgos, a fin de identificar la más adecuada para el análisis y gestión de riesgo informático en las MPYMES ecuatorianas.

ABSTRACT

Information Technology risk is imminent for any organization of the Ecuadorian SME sector. In order to counter this situation, they seek to adhere to certain standards established by international regulations and methodologies that suggest mechanisms, processes and alternatives for risk management. However, due to incompatibility, implementation costs, or the complexity of its execution, it becomes unreachable for many businesses. This paper makes a comparison between "Microsoft Security Risk Management Guide, and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodologies, and their alignment with ISO 27001, 27002, 27005 and 31000 standards, based on guidelines for the identification of assets, identification of vulnerabilities, probability functions, risk measurement variables and calculation of risks in order to identify the most suitable for IT risk analysis and management in the Ecuadorian MSMEs.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by:
mar-8-2016

Introducción:

Estado del proyecto.

La propuesta realizará un estudio comparativo entre la metodología Security Risk Managment Guide de Microsoft y OCTAVE, y su relación con las normativas 27001, 27002, 27005, y 31000 utilizadas para el análisis y gestión de riesgos de seguridad de la información. Este estudio se inserta en la línea propuesta en 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".*

Motivación de la investigación.

Se trata de realizar un estudio comparativo que nos permita recomendar cuál de las metodologías existentes para el análisis y gestión de riesgos de la seguridad de la información sería adecuada para las MPYMES ecuatorianas.

Problemática.

Existen muchas metodologías internacionales, pero es necesario adaptarles a las condiciones propias de nuestro país. Este trabajo contribuirá a la solución de este problema realizando un estudio comparativo para análisis y gestión de riesgos de seguridad de la información.

CAPÍTULO 1: INDAGACIÓN EXPLORATORIA:

1.1 Situación de la MPYMES ecuatorianas en relación a la seguridad de información.

MPYME hace referencia a las micro, pequeñas y medianas empresas las cuales para el Ecuador se definen a continuación:

Microempresa: Este tipo de empresa está comprendida de escasos ingresos y está compuesta de 1 a 6 empleados involucrados exclusivamente. Las microempresas tienen los siguientes criterios:

- El número de empleados es igual o menor a 10 personas.
- El volumen anual de negocio no supera los 20 mil dólares.

Este tipo de empresa tiene la ventaja de ser flexibles, es decir que pueden adaptarse fácilmente a los cambios del mercado. (Muñoz, 2012)

Pequeña empresa: Es una entidad independiente, creada para generar rentabilidad, su ritmo de crecimiento es superior al de la microempresa y puede ser mayor al de la mediana o grande y cumplen con los siguientes criterios:

- El número de empleados es mayor a 50 personas.
- El volumen anual de negocio supera los 20 mil dólares.

(Muñoz, 2012)

Mediana Empresa: Las medianas empresas se caracterizan a que el capital es suministrado por sus propietarios, su tamaño es relativamente pequeño dentro del sector en el que se desarrolla, estas empresas aseguran el mercado de trabajo mediante la descentralización de obra.

- Alberga entre 50 a 99 obreros
- Su capital fijo no debe sobrepasar los 120 mil dólares.

(Muñoz, 2012)

Las MPYMES se desarrollan en su mayoría en las provincias de Guayas, Pichincha, Manabí, Azuay y Tungurahua, en sectores productivos tales como: textil, madera, productos alimenticios, cuero, entre otros. Prevaleciendo la mayoría de las MPYMES

como compañía limitadas y manteniendo una estructura cerrada o de tipo familiar. (Cadena, Triviño, y Aranda, 2011)

La falta de conciencia sobre como las Tecnologías de la Información - TI pueden ayudar a mejorar el desempeño de sus negocios, así como el no tener recursos suficientes para invertir en software y hardware, y la falta de acceso a servicios técnicos, hacen que las organizaciones no crezcan tanto a nivel económico, como a nivel de conocimientos e información. (Cadena, Triviño, y Aranda, 2011)

Una parte importante de las TI es el Internet, ya que es el medio por el cual se puede unir con todo mundo, compartir información, tener acceso a los últimos avances tecnológicos; pero así, como se consigue obtener beneficios de este medio, también se puede ser víctimas y, por consiguiente, poner en riesgo la preciada información. (Cadena, Triviño, y Aranda, 2011)

El Internet en las MPYMES ecuatorianas está siendo utilizado en un porcentaje del 100%, haciendo que el crimen cibernético se incremente de manera evidente, así como también el uso de servidores de correo electrónico; lo que hace inminente la adopción de mecanismos y metodologías que aporten a la seguridad de la información, y que sea ejecutada bajo parámetros estandarizados. (Cadena, Triviño, y Aranda, 2011)

Un estudio realizado por (Cadena, Triviño, y Aranda, 2011) que tuvo por objetivos definir el Estado del arte de la seguridad informática en el Ecuador, identificar el nivel de aceptación por mercados de los servicios de gestión de seguridad e identificar oportunidades de emprendimiento utilizando técnicas estadísticas (Encuestas), y clasificando al estado ecuatoriano en tres grupos (Home, MPYMES, Corporativo); obtuvo los siguientes resultados:

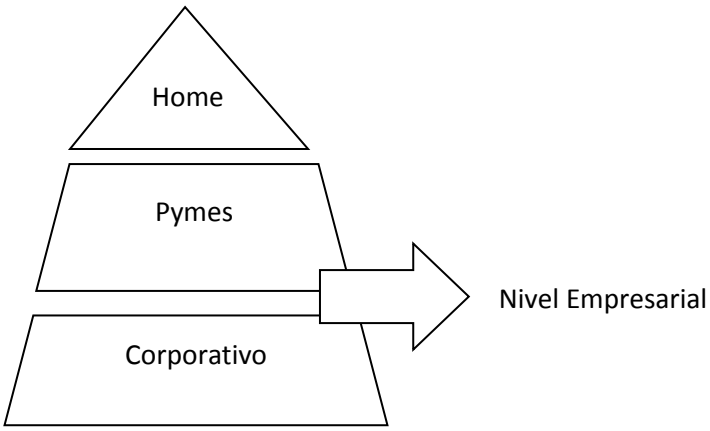


Imagen 1: Mercado Ecuatoriano.

Fuente: (Cadena, Triviño, y Aranda. s.f.)

1. La Seguridad Informática en el Ecuador aun no alcanza el nivel de madurez que garantice y proporcione confianza a los administradores del sector empresarial sobre el resguardo de la información, lo que hoy en día constituye uno de los activos más importantes, y, cada día con el avance tecnológico y penetración del Internet en el país, las organizaciones están más expuestas a ser víctimas del cibercrimen. (Cadena, Triviño, y Aranda, 2011)

2. En las MPYMES ecuatorianas se cree que no se debe tener un departamento especializado en Seguridad de Información e Informática. (Cadena, Triviño, y Aranda, 2011)

3. Las organizaciones ecuatorianas han dedicado tiempo a crear y mantener sistemas de protección eléctrica de alta disponibilidad, pero han dejado de lado los sistemas de control de acceso físico a los recursos que impidan el uso de los sistemas de información no autorizados. (Cadena, Triviño, y Aranda, 2011)

4. La mayoría de las organizaciones mantienen copias de seguridad de la información, pero no cuentan con procedimientos estructurados y automatizados para la obtención de copias de seguridad, haciendo que estén propensas al error humano; además de que carecen de un lugar apropiado y de acceso restringido para el almacenamiento. (Cadena, Triviño, y Aranda, 2011)

5. Muchas organizaciones cuentan con mecanismos de identificación y autenticación para garantizar que solo los usuarios autorizados puedan hacer uso de los sistemas de

información, de igual manera se suman los controles de acceso físico y biométrico. (Cadena, Triviño, y Aranda, 2011)

6. Siendo el malware uno de los desafíos de todos los sistemas de la seguridad informático, las organizaciones ecuatorianas toman medidas contra este inconveniente, pero no siempre son las adecuadas. (Cadena, Triviño, y Aranda, 2011)

Existen varias empresas ecuatorianas que se dedican a la venta de productos y servicios tecnológicos, aprovechando el avanzado desarrollo de la industria de las TI y el aumento del acceso a Internet por parte de los usuarios en el país. Según Cadena y colaboradores (2011), en la encuesta que ellos realizan encuentran que el 100% de las organizaciones tienen contratado un servicio de internet. Por lo tanto, se requiere ofrecer productos de seguridad informática que estén adecuados para el entorno nacional y que vayan a la par con el desarrollo tecnológico.

Dentro de la cartera de productos y servicios que se ofrecen en Ecuador, se pueden mencionar los siguientes:

Ítem	Productos y Servicios
1	Seguridad Perimetral Gestionada
2	Análisis de tráfico
3	Análisis de riesgo
4	Test de penetración
5	*Ethical Hacking*
6	Informática Forense
7	Diagnóstico de seguridad de los sistemas
8	Diagnóstico de vulnerabilidades y Riesgos
9	Planeación y Administración de la Seguridad Informática
10	Planeación Estratégica de Sistemas de Información
11	Asesoría en implantación normativa ISO 27001
12	Auditorías de Seguridad de Información
13	Auditoría TI
14	Software de Seguridad Informática

15	Planes para contingencias y Seguridad de información
16	Capacitaciones
17	Seguridad en redes

Tabla 1: Productos y servicios de seguridad informática que se ofrecen en Ecuador.

Fuente: (Cadena, Triviño, y Aranda. 2011)

1.2 Seguridad de la información vs. Seguridad informática.

La palabra "seguridad" se enfoca a la protección lógica de los activos de información de las organizaciones. (Ugas Luis, 2002, pág. 2). Se habla de una seguridad efectiva y completa cuando se permite perturbar la mayor cantidad de posibles ataques informáticos. Es de gran importancia que una organización guarde la seguridad de la información que posee, de igual manera el manejo y conocimiento pleno de todos los métodos para detectar y reparar los posibles ataques provocados que afecten a los datos de la organización.

1.2.1 Seguridad Informática.

La Seguridad informática es conocida como una "área de la informática que tiene como objetivo proteger la infraestructura computacional, es decir los equipos de computación". (Gualando y Moscoso, 2011, pág. 6)

Se ha creado software que fomenta la seguridad, pero han resultado poco factibles o incluso ineficaces para nuestro medio, se debe proteger a los equipos en su totalidad o como se los denomina "activos de información".

La Seguridad Informática abarca también software, bases de datos, archivos y todo aquello que brinde algún tipo de información, es decir que se pueda catalogar como un activo y estos estén disponibles a todos sus usuarios manteniendo la plena confidencialidad. (Gualando y Moscoso, 2011, pág. 6)

> "*El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable."* (Voutssas Juan, 2010, pág. 132)

En la actualidad existen estándares a seguir para un correcto manejo de los riesgos en cada uno de los activos de información valorados por la organización. La utilización de estándares para controlar sistemas complejos de información alertan posibles irregularidades en donde las respuestas sean inmediatas y efectivas.

1.2.2 Seguridad de la Información.

La Seguridad de la información "es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales". (Norma ISO/IEC, 2005, pág. 8)

Se intenta que las organizaciones en su afán de protección a la información no la pongan en riesgo a pesar de tener un sistema de resguardo, he ahí donde se encuentra el dilema, de que no existe ningún mecanismo cien por ciento efectivo, a pesar de ello los estándares, metodologías y/o plataformas empleadas intentan lograr un control de vulnerabilidad y en comparación con años atrás se evidencia grandes avances en este campo.

El objetivo de la seguridad de la información es el de proteger la información manteniendo la confidencialidad, integridad y disponibilidad de la misma, es entonces como a continuación se contextualiza la terminología empleada.

1. **Activo:** Se denomina activo a todo bien o recurso tangible o intangible, valorado por la organización.
2. **Confidencialidad:** Es una propiedad que debe tener la información, es decir que siempre esté disponible y que no sea de conocimiento general para personas, organizaciones sin autorización.
3. **Integridad:** Se refiere a que la información sea completa y pueda ser eliminada, actualizada solo por el personal autorizado.
4. **Autenticidad:** La información debe ser legitima es decir que dicha información debe ser creada por la misma organización, persona.
5. **Disponibilidad:** La información debe estar siempre disponible para el acceso del personal autorizado. (Gualando y Moscoso, 2011, pág. 6)

1.3 Riesgo informático.

La seguridad de la información y la seguridad informática buscan minimizar a lo que llamamos la "Riesgo Informático".

Mario Simón define al riesgo como la probabilidad de eventos que se presentan afectando el avance del proyecto y el cumplimiento de los objetivos planteados, estos riesgos pueden existir en cada uno de los activos de información presentes.

Relacionado con la tecnología el riesgo "se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una perdida". (Leonardo y Simón Mario, 2004, pág. 2)

El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas, en el riesgo informático intervienen variables que ayudarán al cálculo del riesgo que podrán tener los activos de información afectados, tales como: Probabilidad, Amenazas, Vulnerabilidades, Activos, Impacto. (Voutssas Juan, 2010)

Probabilidad: Es un método para analizar con qué frecuencia una amenaza se presenta, este método se puede realizar de manera cualitativa y/o cuantitativa.

Amenaza: "Fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización." (Voutssas Juan, 2010)

Existen 4 categorías de amenazas descritas a continuación:

Categoria	**Descripción.**
Interrupción	Disponibilidad de una parte o total del sistema.
Intercepción	Confidencialidad
Modificación	Ataque contra la integridad.
Fabricación	Autenticidad.

Tabla 2: Categoría de Amenazas.

Fuente: (Voutssas, 2010)

Vulnerabilidad: "característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza." (Voutssas Juan, 2010)

Impactos: Hace referencia a las consecuencias que existen cuando una amenaza se allá presentado, por lo general son impactos negativos tales como perdida de dinero para la organización, daño de equipos, entre otros.

Para calcular el riesgo viene dado por la siguiente ecuación:

*Riesgo = Probabilidad de ocurrencia * Impacto*. (Voutssas, 2010).

1.3.1 Análisis del Riesgo Informático.

Debido a que el activo más importante que toda organización posee es la "Información", deben existir técnicas que aseguren el resguardo de esta, sin olvidar de la protección de los equipos en los que se almacenan.

Estas técnicas brindan una seguridad que aplica barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas de una organización autorizadas para hacerlo. (Ulloa S. J., 2015)

"Los medios para conseguirlo son:

1. Restringir el acceso (de persona dentro de la organización y de las que no) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo." (Ulloa S. J., 2015, pág. 18)

1.3.2 Ataques informáticos.

Existen dos tipos de ataques informáticos:

1. **Ataque pasivo:** Se refiere a realizar el ataque a datos, pero no modificar su estructura.

2. **Ataque activo:** Al contrario de ataque pasivo este es realizado con el fin de realizar un daño alterando o modificando la información obtenida de dicho ataque.

Para poder realizar un ataque se debe tener conocimiento de 4 etapas tales como:

Descubrimiento	Etapa donde se realiza una recopilación de la información necesaria para realizar el ataque.
Exploración	Identificación de las posibles víctimas.
Evaluación	Búsqueda de vulnerabilidades de los datos obtenidos
Intrusión	La acción de realizar el ataque a través de las vulnerabilidades encontradas.

Tabla 3: Ataques activos.

Fuente: (Voutssas, 2010).

1.4 Gestión de riesgos.

Cada activo está expuesto a amenazas, para lo cual se debe analizar el riesgo para reducirlo y posteriormente realizar la gestión del mismo.

La gestión de riesgos hace referencia a una serie de normas a seguir para que los riesgos sean identificados, clasificados, evaluados, controlados, en su totalidad y con ello la protección de los activos de información.

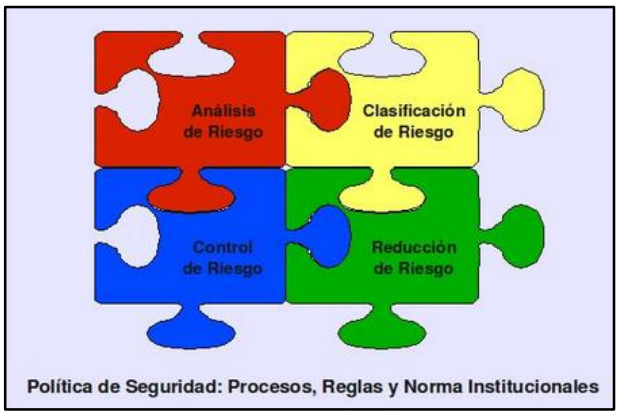


Imagen 2: Políticas de Seguridad, procesos, reglas y normas institucionales.

Fuente: (Ulloa S. J., 2015)

La gestión de riesgos está formada por cuatro partes:

- **Análisis de Riesgo:**

"Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo." (Ulloa S. , 2015), teniendo como objetivo establecer una valoración y priorización de los riesgos en base de información obtenida en el proceso de identificación y de esta manera establecer el nivel de riesgo y las acciones que se deben implementar en el siguiente proceso. En este punto la probabilidad de ocurrencia y el impacto son valores necesarios que deben establecerse en escala de valoraciones sean estas cuantitativas o cualitativas. (UTE, 2013)

- **Clasificación de riesgos.**

En esta etapa, una vez analizados los riesgos existentes, se clasifican dependiendo de la magnitud de impacto y probabilidad de ocurrencia. Esta clasificación se realiza para dar prioridades a los riesgos y tomar acciones para cada uno de ellos. (UTE, 2013)

- **Control de Riesgos.**

Son acciones que se tomarán y realizarán para controlar los riesgos y minimizar perdidas, analizando el funcionamiento, la efectividad y el cumplimiento de las medidas a

evaluar. “Existen riesgos que pueden ser aceptados y aquellos que no lo son, se los mitigará, transferirá o evitará mediante un análisis costo–beneficio y dentro de los parámetros técnico–legales.” (UTE, 2013)

- **Reducción de Riesgos.**

Después del control de los riesgos, se tiene una idea clara de cuáles de los riesgos identificados anteriormente, pueden ser mitigados, es decir, no considerados debido a su impacto.

Existen varias metodologías que gestionan el riesgo, a continuación, se listan algunas metodologías.

Metodología	**Descripción**	**Organización**	**País**
CMMI	*Capability Maturity Model Integration.*	*SEI (Software Enginereing Institute).*	Estados Unidos
SPICE	*Software Process Improvement and Capability Determination.*	*ISO (International Organization for Standardization)*	International (Suiza)
PMBOOK	*Project Management Body of Knowledge*	*PMI (Project Management Institute)*	Estados Unidos.
COBIT	*Control Objectives for Information and related Technology*	*ISACA (Information Systems Audit and Control Association)*	Estados Unidos.
OCTAVE	*Operationally Critical Threat*	*Carnegie Mellon SEI (Software*	Estados Unidos.

	Asset and Vulnerability Evaluation.	*Engineering Institute) y CERT (Computer Emergency Response Team)*	
MAGERIT	Metodología de Análisis y Gestión de Riesgos de IT.	MAP (Ministerio de Administraciones Públicas)	España
SECURITY RISK MANAGMENT GUIDE	Administración de Riesgos de Seguridad.	Microsoft.	Estados Unidos.

Tabla 4: Metodologías de control de riesgos.

Fuente: (UTE, 2013).

De la tabla anterior, el presente documento hará énfasis en las metodologías OCTAVE y SECURITY RISK MANAGMENT GUIDE.

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

Aprobada el 15 de octubre del 2005, es una norma que permite certificar los Sistemas de Gestión de Seguridad de la Información que adopta el modelo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar), y proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización. (Yamila y Aneyty, 2012) (Cordero, 2015)

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

Hacer: Implementar y operar las políticas, controles procedimientos y procesos SGSI.

Revisar: Evaluar y donde sea posible medir el desempeño del proceso en comparación con la política.

Actuar: Tomar acciones correctivas y preventivas, basadas en los resultados de las auditorias.

Hace referencia sobre la importancia de:

- Entender los requerimientos de seguridad de información que satisfacen las necesidades de la organización.
- Implementar y manejar los controles de para manejar los riesgos de seguridad, 113 controles generales, 11 áreas de seguridad física, ambiental y de recursos humanos.
- Monitorear y revisar el desempeño y la efectividad del SGSI.

Esta norma específica los requisitos para implantar el SGSI. (Ulloa, 2015) (Cordero, 2015)

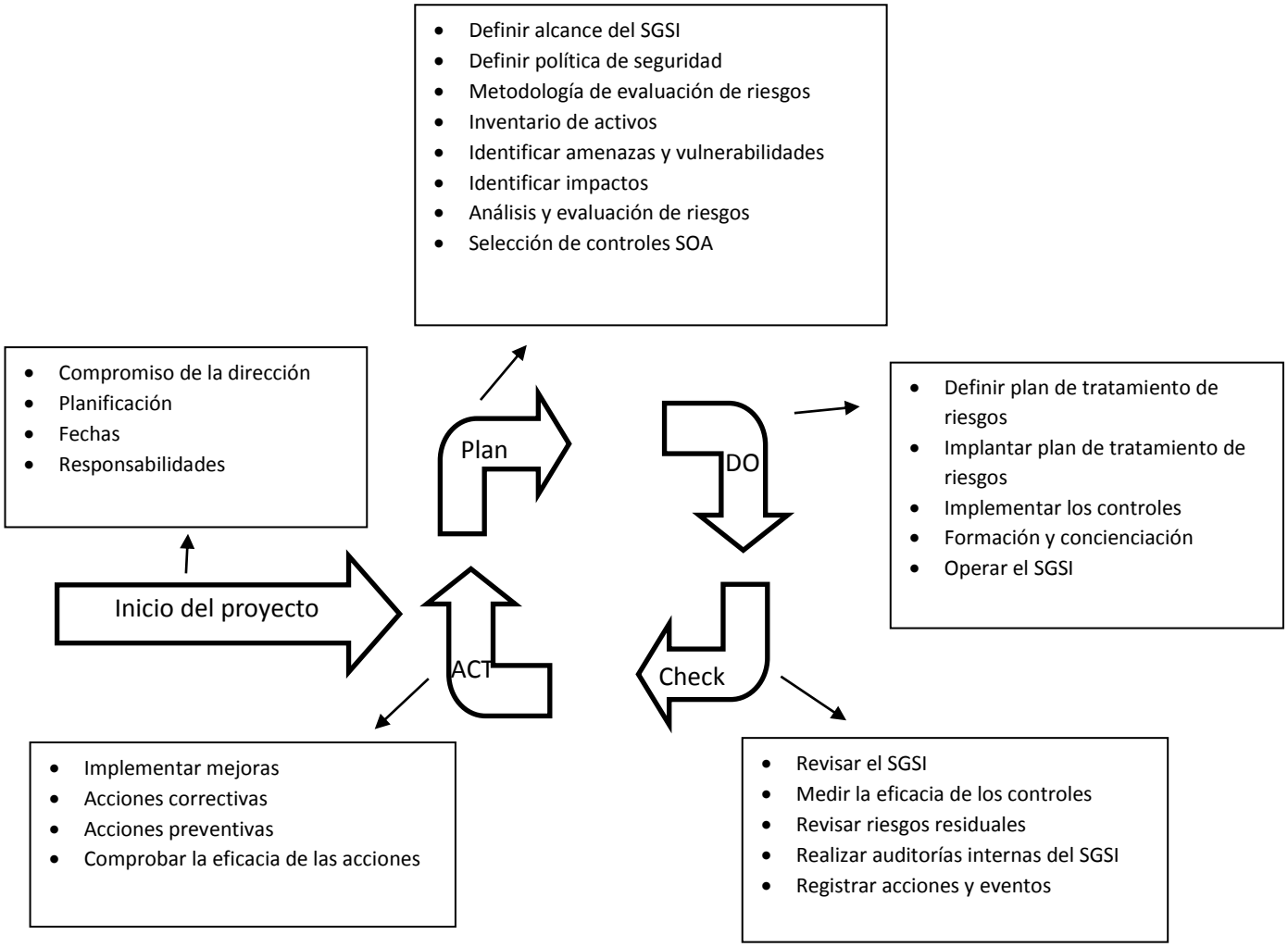


Imagen 3: Ciclo PDCA.

Fuente: http://www.iso27000.es/doc_iso27000_all_archivos/image002.gif

"El objetivo es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) y proteger la confidencialidad, integridad y disponibilidad de la información revisando cuáles son sus potenciales problemas (identificación de riesgos), para luego evitar que estos problemas ocurran (control de riesgos)". (Ulloa, 2015)

"El propósito de un sistema de gestión de la seguridad de la información es, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías." (Ulloa, 2015)

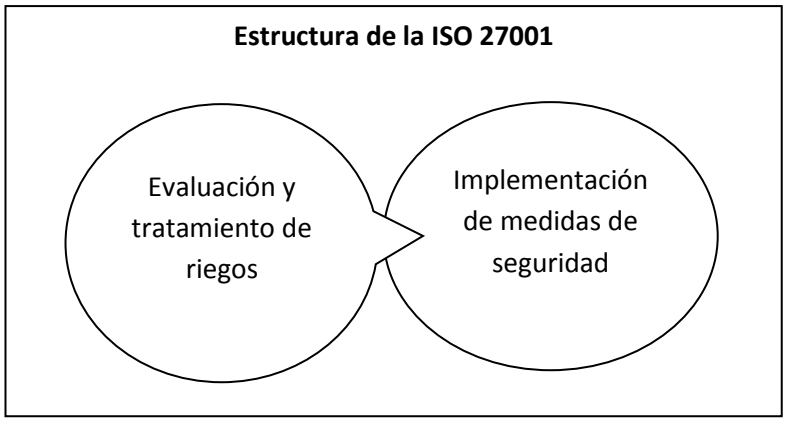


Imagen 4: Estructura de ISO 27001

Fuente: (Ulloa S. J., 2015)

Existen 4 ventajas esenciales para una organización si adoptan la implementación de esta norma:

- Cumplir con los requerimientos legales.
- Menores costos.
- Una mejor organización.
- Obtener una ventaja comercial.

(Ulloa S. J., 2015), (Cordero, 2015)

La norma ISO 27001 consta de 11 secciones más al anexo A, las tres primeras secciones son introductorias, es decir, no son necesariamente obligatorias implementarlas. A partir de la sección 4 lo que implica que la organización debe aplicar obligatoriamente para poder cumplir con la norma.

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. (Cordero, 2015)

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. (Cordero, 2015)

Dominio gestión de activos: Tiene como objetivo realizar una protección adecuada de los activos de la organización. (Cordero, 2015)

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. (Cordero, 2015)

Dominio seguridad física y del ambiente: Nos permite proteger a las instalaciones de la organización y a toda la información que maneja. (Cordero, 2015)

Dominio gestión de las comunicaciones y operaciones: El objetivo es determinar el procedimiento y responsabilidades de las operaciones que realiza la organización.

Dominio control de acceso: Con él se asegura el acceso autorizado a los sistemas de información de la organización. (Cordero, 2015)

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. (Cordero, 2015)

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. (Cordero, 2015)

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. (Cordero, 2015)

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. (isotools, 2013) (Cordero, 2015)

1.5.1 Plan: Establecer con planificación

Según (Ulloa S. , 2015) define el alcance y límites de un Sistema de Gestión de Seguridad de Información (SGSI), se debe:

- Definir el enfoque de evaluación de riesgos de la organización.
- Identificar los riesgos.
- Analizar y evaluar los riesgos.
- 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.

1.5.2 Hacer: Implementar y utilizar 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.

(Ulloa S. , 2015)

1.5.3 Verificar: Monitorizar y Revisar

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.

1.6 ISO 27002 Tecnologías de la información, técnicas de seguridad - código de buenas prácticas para la gestión de la seguridad de la información.

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información. Es una norma que permite crear principios para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información, posee objetivos de control se implementan para satisfacer los requisitos analizados por la evaluación de riesgos. (Cordero, 2015)

Los objetivos de esta norma vienen dados por "satisfacer los requisitos identificados por la evaluación de los riesgos." Contiene once secciones conformadas por treinta y nueve categorías principales de seguridad. (Ulloa S. , 2015), (Cordero, 2015)

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 (iso27001Academi, 2015), (Cordero, 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.**

- **Capítulo 2. Términos y definiciones:** Breve descripción de los términos más usados en la norma.

- **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.

- **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.

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).

- **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.

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.

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.

- **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.

- **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.

- **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.

- **Capítulo 15. Cumplimiento:** El objetivo de este dominio es el establecimiento de controles tendentes a evitar el incumplimiento de cualquier ley, de obligaciones estatuarias reglamentarias o contractuales y de cualquier requisito de seguridad

(iso27001Academi, 2015), (Cordero, 2015)

1.6.1 Dominios de controles de la normativa ISO/IEC 27002

Los dominios de control están resumidos a continuación:

Objetivos de Control y Controles

Edición 2005		Objetivos	Controles
5	Política de seguridad	1	2
6	Aspectos organizativos para la seguridad	2	11
7	Gestión de los Activos	2	5
8	Seguridad de los recursos humanos	3	9
9	Seguridad física del entorno	2	13
10	Gestión de comunicaciones y operaciones	10	32
11	Control de accesos	7	25
12	Adquisición, Desarrollo, y mantenimiento de sistemas	6	16
13	Gestión de incidentes de seguridad de la información	2	5
14	Gestión de continuidad del negocio	1	5
15	Conformidad	3	10
Totales		39	133

Tabla 5: Objetivos de control y controles.

Fuente: (Moscoso Montalvo & Guagalando Vega, 2011)

1.7 ISO 27005 Tecnología de la información, técnicas de seguridad, información de gestión de riesgos de seguridad.

Contiene técnicas de seguridad para la administración de riesgos en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO 27001,

está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Esta norma consta con las siguientes etapas:

- Establecimiento de plan de comunicación interno y externo.
- Definición del contexto organizacional interno y externo.
- Valoración de riesgos tecnológicos.
- Tratamiento de riesgos tecnológicos.
- Monitoreo y mejora continua del proceso de gestión.

(Ulloa S. J., 2015), (Cordero, 2015)

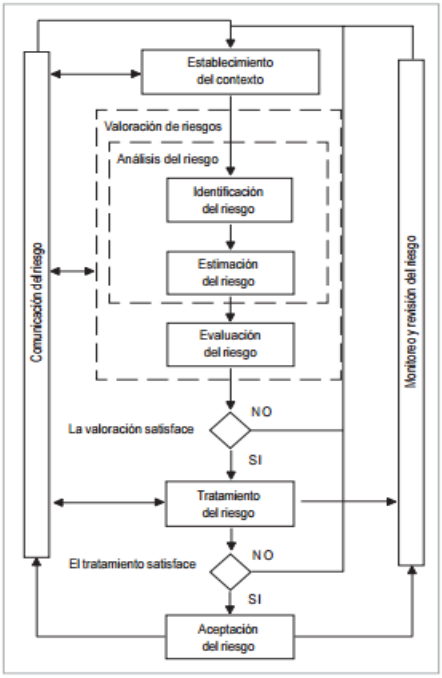


Imagen 5: Proceso para la gestión de riesgos de acuerdo ISO 27005.

Fuente: (Elizabeth, 2014)

1.7.1 Establecimiento de plan de comunicación interno y externo.

Este es un plan que se realiza a nivel interno (empleados, directivos, socios) y externo (distribuidores, clientes), realizando charlas informativas, presentaciones, circulares, capacitaciones. Se deberá crear conciencia en seguridad y evidencia la existencia de riesgos tecnológicos.

Esta propuesta contiene tres etapas:

1. **Comunicación inicial:**

Donde se definen los conceptos de lo que se refiere a riesgos, implicaciones que tienen dichos riesgos, ventajas de la gestión, entre otros.

2. **Comunicación sobre la marcha.**

Presentar los avances que se obtienen a cada uno de los miembros de la organización para que pueda existir una retroalimentación.

3. **Comunicación de resultados.**

Presenta resultados aplicando restricciones de información al público objetivo, es decir que la información no será de conocimiento público.

1.7.2 Definición del contexto organizacional interno y externo.

En este plan el objetivo es conocer a la organización para poder saber que les puede afectar tanto a nivel interno como externo, también saber qué es lo que quieren proteger y como se realiza esta protección.

1.7.3 Valoración de riesgos tecnológicos.

En esta etapa lo que se recomienda es identificar los activos de información que se protegerán, así como sus debilidades y amenazas.

Para una correcta valoración se debe priorizar los activos incluyendo procesos, información, datos y activos de soporte.

Sin olvidar de que se debe identificar los tipos de amenazas, los daños que implican cada una de estas amenazas, perdidas que causan los riesgos en términos de impacto y un análisis sobre el negocia más conocido como BIA (*Bussines Impact Analysis).*

1.7.4 Tratamiento de riesgos tecnológicos.

En esta etapa lo que se implementan las acciones (reducir, aceptar, eliminar, transferir) a tomar para mitigar los riesgos anteriormente analizados.

Estas acciones junto con un plan de tratamiento en donde se definen recursos, responsabilidades se debe documentar para finalmente definir las políticas a seguir.

1.7.5 Monitoreo y mejora continua del proceso de gestión.

En esta fase el elemento necesario es el control de cambios, el monitoreo se realiza sobre los activos identificados, vulnerabilidades, procesos, amenazas, documentación, políticas y procedimientos con el fin de establecer acciones ante algún cambio.

Lo que se busca con el monitoreo es mantener a los riesgos controlados y ante la posibilidad de que aparezcan después nuevos riesgos poderlos controlar antes de que realicen algún daño a los activos de información.

(Ramírez y Ortiz, 2011)

1.8 ISO 31000.

Incluye los principios y directrices, marco y procesos para la gestión de riesgos. En toda organización grande o MPYME en capacidad y ganancias, enfrentan riesgos que se presentan en cada una de las actividades presentes y en los activos de información.

Esta normativa fue publicada en noviembre del 2009 y creada por un grupo de trabajadores, incluidos tutores técnicos de más de 20 países. Nace a partir del estándar de riesgo de Nueva Zelanda/Australia (AS NZS 4360:2004) para que pueda ser usado por una gran variedad de organizaciones sin importar su tipo, tamaño, operación, etc. (Dorothy y Peter, 2011)

La norma ISO 3100:2009 “tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a gestionar el riesgo con efectividad.” (Castro M.)

Lo importante de esta norma es que puede ser aplicada a cualquier tipo de organización con o sin fines de lucro y ante cualquier riesgo existente. Esta norma recomienda que las organizaciones puedan desarrollar, implementar, y mejorar continuamente un marco de trabajo (*framework*) “cuyo objetivo es integrar el proceso de gestión de riesgos.” (Castro M.)

1.8.1 Principios básicos para la gestión de riesgos

Para que la norma ISO 31000 obtenga la mayor eficacia, la gestión de riesgos debe tener en cuenta los siguientes principios:

a) Crea valor.
b) Está integrada a los procesos de organización.

c) Forma parte de la toma de decisiones.

d) Trata explícitamente la incertidumbre.

e) Es sistemática, estructurada y adecuada.

f) Hecha a la medida.

g) Hace énfasis en los factores humanos y culturales.

h) Basada en la mejor información disponible.

i) Es transparente e inclusiva.

j) Dinámica, iterativa y sensible al cambio.

k) Facilita la mejora continua de la organización.

Mientras que el enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos:

1. Principios de gestión de riesgo.
2. El marco de trabajo (*framework*) para la gestión de riesgo.
3. El proceso de gestión de riesgo.

A continuación se muestra la relación existente entre los principios de gestión, el marco de referencia, así como el proceso de gestión de riesgo mencionado anteriormente. (Castro, M., s.f.)

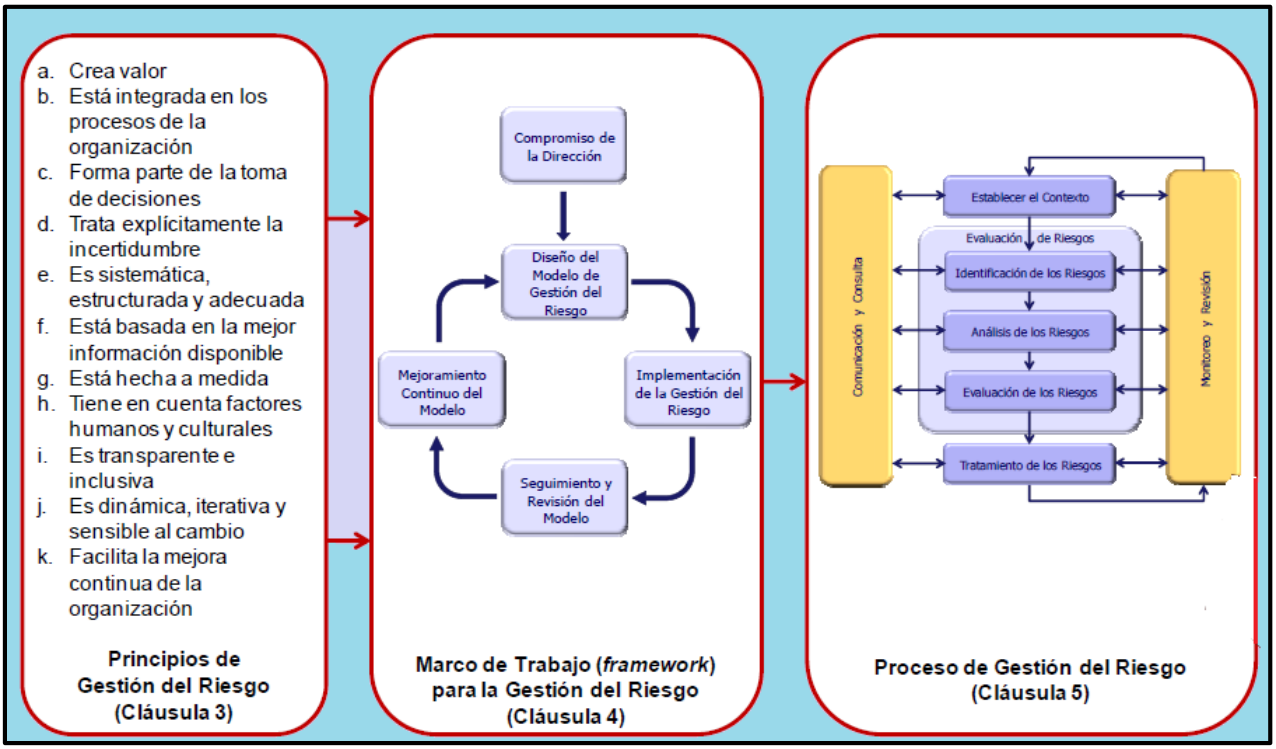


Imagen 6: Relación de principios, Marco de Trabajo, Proceso de Gestión de Riesgos.

Fuente de (Castro, M, s.f.)

1.8.2 Beneficios de la ISO 31000.

Ayuda a las organizaciones a:

- Aumentar la probabilidad de lograr sus objetivos.
- Mejorar la gobernabilidad.
- Mejorar la información financiera.
- Ser conscientes de la necesidad de identificar y tratar al riesgo en toda la organización.
- Mejorar en la identificación de amenazas y oportunidades.
- Mejorar los controles.
- Mejorar la eficacia y eficiencia laboral.
- Minimizar perdidas.
- Mejorar la capacidad de recuperación de la organización. (Castro M.)

1.9 Security Risk Managment (Microsoft)

(Microsoft, 2006. Pag 2, 3) menciona que "*su objetivo es ofrecer una orientación clara sobre cómo implementar un proceso de gestión de riesgos de seguridad que ofrece una serie de beneficios, incluyendo:*

- *Mover los clientes a una postura de seguridad proactiva y liberándolos de un proceso reactivo, frustrante.*
- *Realización de seguridad medible mostrando el valor de los proyectos de seguridad.*
- *Ayudar a los clientes a mitigar eficazmente los riesgos más grandes en sus entornos en lugar de aplicar los recursos escasos para todos los riesgos posibles."*

1.9.1 Resumen de la Guía

Debido a que las organizaciones conocen la función principal que desempeñan las tecnologías de información (TI) en el cumplimiento de los objetivos de negocio, adoptadas en un entorno cada vez más hostil; los ataques, infiltraciones y robos de información se realizan con mayor frecuencia, requiriendo un tiempo de reacción mucho más rápido; por lo tanto, las organizaciones no pueden tomar acción ante las nuevas técnicas que amenazan la seguridad de la infraestructura de información antes de que afecten a su negocio. (Microsoft, 2006)

La guía Gestión de Riesgo de Microsoft ofrece a la organización una forma clara y de fácil entendimiento para organizar y asignar prioridades a cada recurso (activo de información), con el fin de identificar y gestionar adecuadamente los riesgos de los cuales son víctimas, se puede decir también que esta guía crea ventajas, las cuales se aprecian únicamente al implementar los controles propuestos, ya que ayudan a reducir el riesgo a un nivel aceptable. (Microsoft, 2006).

1.9.2 La función de Microsoft en la administración de riesgos de seguridad

Security Risk Managment es la primera guía normativa publicada por Microsoft que se centra por completo en la administración de riesgos de seguridad. Está basada en las experiencias propias de Microsoft y en las de sus clientes, esta guía ha sido probada y revisada por clientes, socios y revisores técnicos durante su desarrollo. (Microsoft, 2006)

1.9.3 Información general de la guía

La Guía de administración de riesgos de seguridad consta de seis capítulos, que se describen brevemente a continuación. Cada capítulo se basa en una práctica completa necesaria para iniciar y poner en funcionamiento de forma eficaz un proceso de administración de riesgos de seguridad continuo en la organización. (Microsoft, 2006)

Capítulo 1: Introducción a la Guía de administración de riesgos de seguridad

En este capítulo se presenta la guía y se ofrece una breve descripción de cada capítulo para dar a conocer al usuario la administración de riesgos. (Microsoft, 2006)

Capítulo 2: Estudio de prácticas de administración de riesgos de seguridad

El establecimiento de un buen proceso de administración de riesgos de seguridad responde a una necesidad que se ha evidenciado mediante la revisión de las distintas formas de

manejo que las organizaciones han realizado en el pasado. Es de gran importancia estudiar de los puntos tanta fuertes como débiles de los enfoques proactivo y reactivo de la administración de riesgos, posteriormente se realiza el analisis el concepto de madurez de la administración de riesgos para luego valorar y contrastar la administración de riesgos cualitativa y cuantitativa, pues estos son métodos tradicionales. En sintesis el mencionado proceso presenta un equilibrio entre estas formas de evaluación de riesgos que ha demostrado eficacia en Microsoft. (Microsoft, 2006.)

Capítulo 3: Información general acerca de la administración de riesgos de seguridad

Dentro de este capítulo Microsoft realiza un análisis más minucioso del proceso de administración de riesgo de seguridad y da conocer conceptos, claves para aselas recomendaciones que presenta van encaminadas a un planeamiento eficaz y la creación de un equipo de administración de riesgos de seguridad estable con funciones y cargas bien definidas. (Microsoft, 2006)

Capítulo 4: Evaluación del riesgo

En este capítulo se explica tendidamente la evaluación de este proceso, en donde se realiza un planeamiento, la recopilación de datos facilitados y la asignación de prioridades a los riesgos. Se asigna prioridad a los riesgos de resumen, entonces, el equipo de administración de riesgos de seguridad utiliza un enfoque cualitativo para clasificar la lista completa de riesgos de seguridad para poder identificar los más importantes y someterlos a un mayor análisis.

Posteriormente, los riesgos principales se someten a un análisis detallado mediante técnicas cuantitativas cuyo resultado son métricas detalladas que el equipo puede utilizar para tomar decisiones sensatas durante la siguiente fase del proceso. (Microsoft, 2006)

Capítulo 5: Apoyo a la toma de decisiones

Se detalla como el equipo de administración de riesgos de seguridad da posibles soluciones a los riesgos más relevantes de manera eficaz y asequible. El equipo identifica los controles, determina costos asociados con la adquisición, implementación y soporte de cada control, además evalúa la reducción del nivel de riesgo que logra cada control para finalmente trabajar con el comité directivo de seguridad para determinar que controles se

implementarán. Como resultado final se crea un plan claro y aplicable para controlar o aceptar cada uno de los riesgos principales identificados. (Microsoft, 2006)

Capítulo 6: Implementación de controles y medición de la efectividad del programa

Las dos fases finales: implementación de controles que se encarga en crear y ejecutar planes en función de la lista de soluciones de control para mitigar los riesgos identificados en la fase de evaluación de riesgos y la medición de la efectividad del programa. La segunda fase es un proceso continuo en el que el equipo de administración de riesgos de seguridad comprueba habitualmente que los controles implementados durante la fase anterior están ofreciendo la protección prevista.

Finalmente hace referencia a la importancia de vigilar los cambios en el medio informático, como la adición, eliminación de sistemas y aplicaciones; también la aparición de nuevas amenazas y vulnerabilidades preparando a la organización protegerse de riesgos nuevos o cambiantes. (Microsoft, 2006).

Todos los capítulos, apéndices, herramientas y plantillas provistas por la metodología se estudiarán más a detalle, en el capítulo siguiente.

1.9.4 Organización por niveles de defensa en profundidad

Los responsables de la evaluación del riesgo son aquellos encargados en almacenar considerables cantidades de información. En la actualidad se cuenta con el modelo de Defensa de Profundidad y es utilizado por la empresa Microsoft, esta ayuda al equipo de administración de riesgos de seguridad a recopilar información en el ámbito de seguridad a la organización, también proporciona una adecuada estructura.

Como un modelo y ejemplo de debate de riesgo se establecen niveles de defensa en profundidad y es entonces que se presenta el siguiente gráfico:

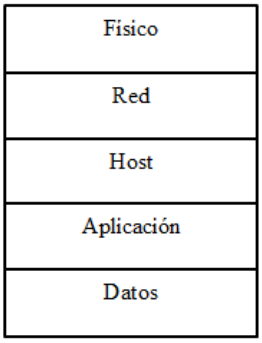


Imagen 7: Modelo de defesa en profundidad.

Fuente: (Microsoft, 2006)

Hay que entender de una manera objetiva las finalidades de la "*Defensa en Profundidad*" y es entonces que se habla de un diseño e implantación de seguridad en varios niveles, disminuyendo de una manera considerable futuros ataques, pero teniendo en cuenta que si los mismos persisten es necesario, se incluyan medidas adicionales que dificulten y retrasen el acceso a la información confidencial, entre otros tipos. (Vieites, 2011)

El nivel de seguridad interna en los sistemas informáticos debe contar con un control constante, el cual sea reforzado a través de la configuración de servidores, analizando parches y eliminando todo tipo de vulnerabilidades. Para su efectivo desenvolvimiento el equipo de seguridad debe desactivar aquellos servicios que son innecesarios, contando siempre con un cambio de contraseñas periódico. Con este modelo se llega a comprobar que los atacantes solo se atreven a lidiar con sistemas informáticos débiles. (Vieites, 2011)

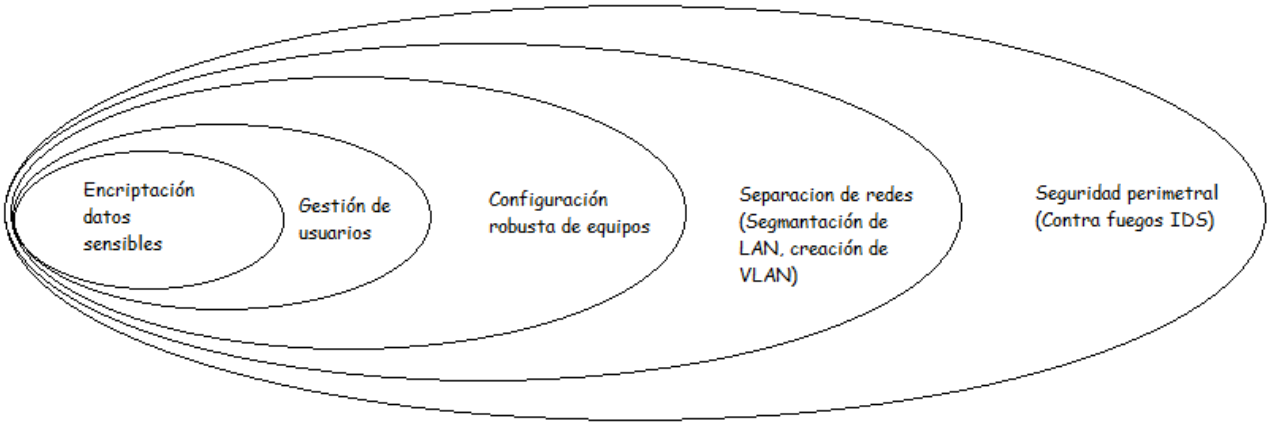


Imagen 8: Principio de defensa de seguridad.

Fuente: (Vieites, 2011).

1.10 OCTAVE.

El conocer sobre los marcos de referencias existentes no necesariamente asegura que el proceso de gestión de los riesgos se lleve de una forma correcta, para ello se necesita de la ayuda metodologías que "de manera eficaz y eficiente aplique los marcos de referencias exitosamente en la labor del análisis de riesgos de TI". (Gómez, Pérez, Donoso, y Herrera, 2011) Estas metodologías puede ser: MAGERIT, OCTAVE, MEHARI, CRAMM, EBIOS, entre otros.

En este estudio se analizará detalladamente una de estas metodologías listadas, llamada OCTAVE.

"La metodología OCTAVE evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa. Equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que, a partir de estos, los entes empresariales puedan tomar decisiones de protección de información basados en los principios de la seguridad de la información." (Ana y Jhon A, 2013, pág. 42)

Esta metodología se focaliza en el trabajo diario de las organizaciones, identificando primero los activos de información, siendo un proceso común para el resto de metodologías. OCTAVE estudia y analiza como estos activos influyen en la tarea diaria de la organización. Para que la organización cumpla con sus metas y objetivos, OCTAVE considera que es fundamental que todos los empleados de diferentes niveles de organización deben conocer sobre estos activos y saber que tan importantes son y como poderlos proteger frente a alguna amenaza inminente.

Para realizar el estudio se debe crear un grupo conformado por personas de las áreas de negocio y del área de TI (Tecnología de la Información), llamado por OCTAVE **"el equipo de análisis"**. Este grupo es de gran importancia ya que al contar con integrantes bien relacionados con la organización pueden identificar inmediatamente los activos de información más importantes y como se usan estos en el día a día; por otra parte, los integrantes del área de TI ayudan a ver las debilidades que poseen estos activos.

Lo primero que realiza este equipo es analizar los activos de información importantes para la organización, es decir que garanticen la continuidad de la operación. Una vez analizados dichos activos, se da una priorización y así saber en cuál de los activos se realizará el estudio enfocándose en los más críticos, en sus vulnerabilidades y amenazas de

seguridad. Por último, se realiza un plan de mitigación de estos riegos y una estrategia basada en prácticas para el mejoramiento organizacional y así poder reducir el riesgo en los activos de la organización.

(Gómez, Pérez, Donoso, y Herrera, 2011)

1.10.1 Desarrollo de la evaluación.

Para poder realizar este levantamiento de información, el "equipo de análisis" adelanta el mismo, y lo realiza dividiendo al proceso en tres fases:

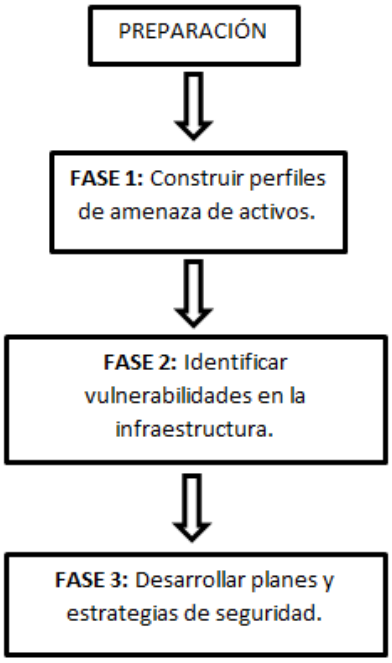


Imagen 9: Fases para el desarrollo de la evaluación OCTAVE.

Fuente: http://www.securityartwork.es/wp-content/uploads/2012/03/1.jpg

Fase 1: Construir perfiles de amenazas basados en los activos.

Esta fase comprende cuatro etapas, donde las tres primeras son talleres en los cuales cada uno de los miembros del equipo contribuyen dando sus puntos de vista sobre los activos de información que son los más críticos, la manera de utilizarlos, los mecanismos de protección, las amenazas identificadas sobre cada uno de los activos, el impacto que tienen las mismas y por último los requerimientos de seguridad. Además, eligen los que son de mayor importancia, "describen los requerimientos de seguridad y se crea un perfil de amenazas para cada activo crítico". (Gómez, Pérez, Donoso, y Herrera, 2011)

Para la cuarta etapa se consolida la información recopilada en las etapas anteriores "verificando aspectos como la completitud, coherencia y diferencias de apreciación en los diferentes niveles de la organización". (Gómez, Pérez, Donoso, y Herrera, 2011)

Como resultado de esta fase podemos encontrar los siguientes productos:

- **Activos críticos:** Se identifican a cada uno de los activos de información con un nivel alto de criticidad para la organización. Ejemplo: máquinas, equipos de cómputo, información clave, entre otros.

- **Requerimientos de seguridad para los activos críticos:** Se identifican los aspectos que se requieren para la seguridad de cada uno de los activos críticos tales como: confidencialidad, integridad y disponibilidad.

- **Perfiles de amenazas:** "Un perfil de amenaza es una manera estructurada de mostrar las diferentes amenazas que se presentan sobre cada activo crítico".

(Gómez, Pérez, Donoso, y Herrera, 2011)

En los perfiles de amenazas se debe identificar al "actor" que genera la amenaza, así como el motivo y el objetivo de realizarla, como podría acceder al activo, cuál sería el impacto de la amenaza con respecto al activo y a la organización, entre los impactos que se pueden ocasionar tenemos: modificación, eliminación, perdida, interrupción, vulnerabilidad de la confidencialidad, entre otros.

Cabe recalcar que OCTAVE identifica cuatro perfiles principales: acceso a través de red, acceso físico, problemas del sistema y otros problemas.

- **Prácticas actuales de seguridad:** OCTAVE tiene una serie de catálogos de prácticas de seguridad que son aplicadas en los distintos talleres.

Fase 2: Identificar vulnerabilidades en la infraestructura.

En esta fase el equipo evalúa los diferentes componentes organizacionales para identificar vulnerabilidades tecnológicas, que darían lugar a acciones no autorizadas contra los activos críticos.

Como salidas, se tienen:

- **Componentes claves:** Los componentes claves son los que están relacionados con los activos críticos, tales como firewall, servidores, routers y sistemas de almacenamiento de información.

- **Vulnerabilidades tecnológicas actuales:** Se evalúa cada uno de los activos críticos, mediante diferentes técnicas o herramientas de análisis de vulnerabilidades, una de ellas, utilizada como escáner de vulnerabilidades, es OPENVAS. Al ser una actividad sumamente técnica, se podría realizar el mismo con empresas subcontratadas.

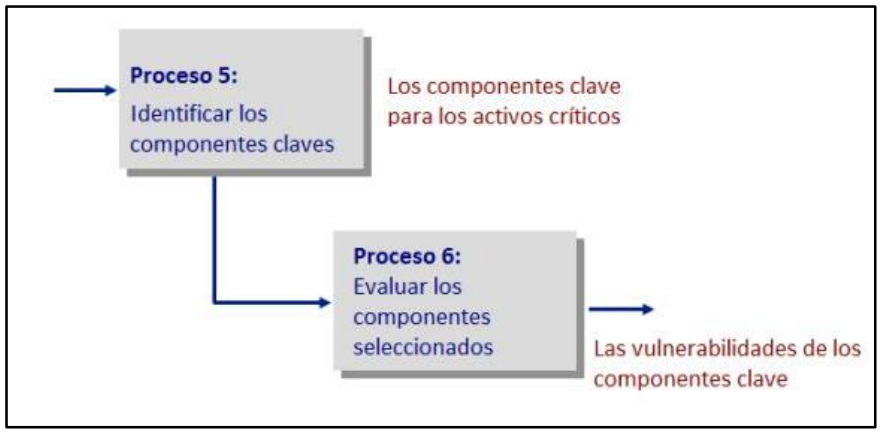


Imagen 10: Fase dos, desarrollo de la evaluación.

Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/fase2octave.JPG/374127226/fase2octave.JPG

Fase 3: Desarrollar estrategias y planes de seguridad.

En esta última etapa el equipo de análisis identifica los riesgos que existen sobre los activos críticos identificados anteriormente para establecer las estrategias a tomar, creando planes de mitigación de riesgos basada en información recopilada.

Las salidas de esta fase son las siguientes:

- **Identificación y evaluación de riesgos:** Esta toma información recopilada en etapas anteriores, se recopilan los riesgos y se evalúa el impacto en términos de escala predefinida tal como: alto, medio y bajo de acuerdo a criterios que deben definirse durante las fases anteriores.

• **Estrategia de protección y planes de mitigación del riesgo:** Se desarrollan planes de mejora y pasos para la protección de los activos críticos de información de la organización.

(Gómez, Pérez, Donoso, y Herrera, 2011)

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.

OCTAVE es una metodología definida para grandes empresas, a su vez existe una división:

- OCTAVE allegro que permiten analizar riesgos con mayor enfoque en activos de información.

- OCTAVE-S que se enfoca para pequeñas empresas.

CAPÍTULO 2: Estudio de la metodología Security Risk Managment Guide de Microsoft.

2.1 Introducción

La correcta administración de la seguridad se ha convertido en el principal objetivo de los departamentos de tecnologías de información. Muchas organizaciones están obligadas por la ley a llevar un nivel de control mínimo de seguridad, y si esta no se administra de forma proactiva, se exponen a riesgos que conllevan a consecuencias negativas, e inclusive, legales. (Microsoft, 2006)

Security Risk Managment Guide o Guía de Administración de Riesgos de Seguridad, es la primera guía normativa publicada por Microsoft creada para la gestión de riesgos. Esta guía se basa por completo en experiencias propias de Microsoft y en la de todos sus clientes; la misma que ha sido probada y revisada por sus desarrolladores y técnicos durante su desarrollo, con el fin de ofrecer un camino claro y entendible de cómo implementar un correcto proceso de administración de riesgos de seguridad, dentro de las cuales se obtienen numerosas ventajas, entre ellas se señalan:

- Hace que los clientes desarrollen conciencia sobre la seguridad, y los independiza al momento de realizar procesos repetitivos y frustrantes.
- Poder cuantificar la seguridad.
- Ayuda a mitigar de forma eficaz los riesgos de mayor prioridad, en lugar de asignar todo el esfuerzo a riesgos posibles.

(Microsoft, 2006)

La guía está diseñada especialmente para consultores, ingenieros en sistemas, informáticos, arquitectos de redes y profesionales de las tecnologías de información, debido a que son las personas responsables durante la planeación e implementación de aplicaciones y/o infraestructuras de varios proyectos de TI, de los cuales incluyen funciones de trabajos comunes:

- Diseñadores que son responsables de infraestructura y arquitectura de los proyectos.

- Miembros de grupos de trabajo de seguridad de información y de seguridad informática, los cuales se especializan en dar seguridad a todos los departamentos de una organización.
- Auditores de seguridad de TI, quienes tiene la responsabilidad de proteger los activos de información de las organizaciones.
- Analistas de sistemas y de negocios responsables de la toma de decisiones cruciales que necesitan el apoyo de TI.
- Consultores de negocios.

(Microsoft, 2006)

Esta guía de administración de riesgos de seguridad consta de seis capítulos que se enumeran a continuación, y que fueron detallados en el capítulo 1:

- Capítulo 1: Introducción a la Guía de administración de riesgos de seguridad.
- Capítulo 2: Estudio de prácticas de administración de riesgos de seguridad.
- Capítulo 3: Información general acerca de la administración de riesgos de seguridad.
- Capítulo 4: Evaluación del riesgo.
- Capítulo 5: Apoyo a la toma de decisiones.
- Capítulo 6: Implementación de controles y medición de la efectividad del programa.

2.2 Mecanismos de identificación de activos

Todos los recursos de un Sistema de Información que ayuden al correcto funcionamiento de la organización o al cumplimiento de los objetivos planteados, es conocido como Activos de Información. (Cordero, 2015)

Security Risk Managment Guide de Microsoft clasifica a los Activos de Información en tres grupos:

1. Activos Tangibles.
2. Activos Intangibles.
3. Servicios de TI.

Esta lista de clases no es definitiva, ya que, no siempre puede ser respetada dentro del entorno de la organización, por lo tanto, es de gran importancia personalizarla o

acoplarla durante la evaluación de los riesgos de los activos. A continuación se presenta esta lista como referencia para facilitar la identificación de los activos:

Clase de Activo	**Entorno de TI Global**	**Nombre del activo**	**Clasificación del Activo**
	Máximo nivel de descripción del activo	*Definición de siguiente nivel*	*Clasificación de valor de activo (grupo 1 - 5)*
Tangible	Infraestructura física	Centro de datos	5
Tangible	Infraestructura física	Servidores	3
Tangible	Infraestructura física	Equipos de escritorio	1
Tangible	Infraestructura física	Equipos móviles	3
Tangible	Infraestructura física	PDA	1
Tangible	Infraestructura física	Teléfonos móviles	1
Tangible	Infraestructura física	Software de aplicación de servidor	1
Tangible	Infraestructura física	Software de aplicación final	1
Tangible	Infraestructura física	Herramientas de desarrollo	3
Tangible	Infraestructura física	Enrutadores	2
Tangible	Infraestructura física	Conmutadores de red	2
Tangible	Infraestructura física	Equipos de fax	1
Tangible	Infraestructura física	PBX	3
Tangible	Infraestructura física	Medios extraíbles (cintas, disquetes, CD-ROM, DVD, discos duros, portátiles, dispositivos de almacenamientos PC Card, dispositivos de almacenamiento USB, etc.)	1
Tangible	Infraestructura física	Fuentes de alimentación	3
Tangible	Infraestructura física	Sistemas de alimentación ininterrumpida	3
Tangible	Infraestructura física	Sistemas contra incendios	3
Tangible	Infraestructura física	Sistemas de aire acondicionado	3
Tangible	Infraestructura física	Sistemas de filtrado de aire	1

Tangible	Infraestructura física	Otros sistemas de control medioambiental	3
Tangible	Datos de intranet	Código fuente	5
Tangible	Datos de intranet	Datos recursos humanos	5
Tangible	Datos de intranet	Datos financieros	5
Tangible	Datos de intranet	Datos de publicidad	5
Tangible	Datos de intranet	Contraseñas de empleados	5
Tangible	Datos de intranet	Claves de cifrado privadas de empleado	5
Tangible	Datos de intranet	Claves de cifrado de sistema informático	5
Tangible	Datos de intranet	Tarjetas inteligentes	5
Tangible	Datos de intranet	Propiedad intelectual	5
Tangible	Datos de intranet	Planes estratégicos	3
Tangible	Datos de intranet	Informes de crédito de clientes	5
Tangible	Datos de intranet	Registros médicos	5
Tangible	Datos de intranet	Identificadores biométricos de empleados	5
Tangible	Datos de intranet	Datos de contactos de negocios de empleados	1
Tangible	Datos de intranet	Datos de contacto personales de empleados	3
Tangible	Datos de intranet	Datos de pedidos	5
Tangible	Datos de intranet	Diseño de infraestructura de red	3
Tangible	Datos de intranet	Sitios web internos	
Tangible	Datos de extranet	Datos etnográficos de empleados	3
Tangible	Datos de extranet	Datos de contratos con socios	5
Tangible	Datos de extranet	Datos financieros de socios	5
Tangible	Datos de extranet	Datos de contacto de socios	3
Tangible	Datos de extranet	Aplicación de colaboración de socios	3

Tangible	Datos de extranet	Claves de cifrado de socios	5
Tangible	Datos de extranet	Informes de crédito de socios	3
Tangible	Datos de extranet	Datos de pedidos de socios	3
Tangible	Datos de extranet	Datos de contrato con proveedores	5
Tangible	Datos de extranet	Datos financieros de proveedores	5
Tangible	Datos de extranet	Datos de contacto de proveedores	3
Tangible	Datos de extranet	Aplicación de colaboración de proveedores	3
Tangible	Datos de extranet	Claves de cifrado de proveedores	5
Tangible	Datos de extranet	Informes de crédito de proveedores	3
Tangible	Datos de extranet	Datos de pedidos de proveedores	3
Tangible	Datos de internet	Aplicación de ventas de sitio web	5
Tangible	Datos de internet	Datos de publicidad de sitios web	3
Tangible	Datos de internet	Datos de tarjetas de crédito de clientes	5
Tangible	Datos de internet	Datos de contacto de clientes	3
Tangible	Datos de internet	Claves de cifrado publicas	1
Tangible	Datos de internet	Notas de prensa	1
Tangible	Datos de internet	Notas del producto	1
Tangible	Datos de internet	Documentación del producto	1
Tangible	Datos de internet	Materiales de cursos	3
Intangible	Reputación		5
Intangible	Buena Voluntad		3
Intangible	Moral de empleados		3

Intangible	Productividad de empleados		3
Servicios de TI	Mensajería	Correo electrónico / programación (por ejemplo Microsoft Exchange)	3
Servicios de TI	Mensajería	Mensajería instantánea	1
Servicios de TI	Mensajería	Microsoft Outlook Web Acces (OWA)	1
Servicios de TI	Infraestructura Básica	Microsoft Active Directory	3
Servicios de TI	Infraestructura Básica	Sistema de nombres de dominio (DNS)	3
Servicios de TI	Infraestructura Básica	Protocolo de configuración Dinámica de Host (DHCP)	3
Servicios de TI	Infraestructura Básica	Herramientas de administración empresarial	3
Servicios de TI	Infraestructura Básica	Uso compartido de archivos	3
Servicios de TI	Infraestructura Básica	Almacenamiento de datos	3
Servicios de TI	Infraestructura Básica	Accesos telefónico remoto	3
Servicios de TI	Infraestructura Básica	Telefonía	3
Servicios de TI	Infraestructura Básica	Acceso a red privada virtual (VPN)	3
Servicios de TI	Infraestructura Básica	Servicio de nombres de Internet de Microsoft (WINS)	1
Servicios de TI	Otra infraestructura	Servicios de colaboración (Por ejemplo, Microsoft SharePoint)	1

Tabla 6: Activos comunes del Sistema de Información

Fuente: (Microsoft, 2006)

En la evaluación de riesgos se definen las áreas de la organización que se utilizarán para la identificación de los activos, posteriormente se realiza un estudio acerca de los riesgos que se puedan presentar. Esto incluye los activos intangibles como la reputación de la empresa, también la información digital y los activos tangibles como la infraestructura física. El o los riesgos que cada activo podría ser víctima se deben estudiar claramente en reuniones

con los responsables para definir un plan de políticas para cada uno de ellos, mientras se identifica un activo también se debe asignar su responsable.

Se habla de una complejidad bastante clara, además de documentar cada actividad, esto suele resultar muy útil para la asignación de políticas y así confirmar y comunicar los riesgos directamente a los responsables de cada uno de ellos. La clasificación de cada activo también es un componente de gran importancia en la gestión de riesgos. (Microsoft, 2006)

Rango de Exposición	Confidencialidad o Integridad del Activo
5	El daño es severo o total de los activos, por ejemplo, visible desde el exterior y afecta a la rentabilidad del negocio o el éxito
4	Graves daños pero no completos, a los activos, por ejemplo, afecta a la rentabilidad del negocio o el éxito, puede ser visible desde el exterior
3	Daño o pérdida moderada, por ejemplo, afecta a las prácticas comerciales internas, provoca aumento en los costos operativos o la reducción de los ingresos
2	Bajo daño o pérdida, por ejemplo, afecta a las prácticas comerciales internas, no pueden medir aumento de los costos
1	Menor o ningún cambio en los activos

Tabla 7: Rango de exposición al riesgo

Fuente: (Microsoft, 2006)

Clasificación de exposición	Disponibilidad	Descripción
5	Parada de trabajo	Gastos de apoyo sustanciales o compromisos empresariales cancelados.
4	Interrupción de trabajo	Aumento cuantificable de los gastos de apoyo o compromisos empresariales retrasados.
3	Demoras en el trabajo	Impacto notable para apoyar los costos y la productividad. Sin impacto en el negocio medible.
2	Distracción en el trabajo	Sin impacto medible, aumentos menores en apoyo o de infraestructura costos.
1	Absorción por operaciones comerciales normales	Sin impacto medible para apoyar los costos, la productividad, o compromisos de negocios.

Tabla 8: Clasificación de la exposición

Fuente: (Microsoft, 2006)

2.2.1 Activos de información

Como ya se mencionó, la empresa *Microsoft* clasifica a los activos de dos maneras: tangible o intangible, con la finalidad de que cada responsable pueda estipular el valor del activo y establecer así el riesgo que pueda significar para la organización, es

entonces que esta clasificación requiere que se aplique estimaciones en forma de pérdidas financieras tanto directa como indirectamente.

Si resulta necesario para la organización, Microsoft determina otra clasificación de los activos denominado: *Servicio de TI*, esta es una combinación de algunos activos tangibles e intangibles como por ejemplo, el servicio de correo electrónico corporativo el cual, puede tener datos digitales confidenciales, también se incorpora el servicio de una manera objetiva ya que, un activo puede tener varios responsables tantos de datos como equipos físicos Otros activos de Servicio de TI pueden ser: archivos, almacenamiento, redes, telefonía, etc. además se considera el Servicio de TI como un activo de información.

(Microsoft, 2006).

2.2.2 Clasificación

Toda la clasificación de los activos está dentro de una clase o grupo cualitativo, lo cual facilita la definición de los impactos de los riesgos de seguridad, también ayuda a que las organizaciones centren su atención en los riesgos de mayor importancia. Security Risk Management Guide de Microsoft utiliza tres clases que ayudan a la cuantificación del valor de los activos de la organización. Estas permiten tanto administrar como reducir el tiempo de dedicación para cada clase de activo, y su definición es la siguiente:

1. Alto impacto en la organización
2. Impacto moderado en la organización
3. Bajo impacto en la organización

Según sea necesario, se pueden cuantificar los riesgos en pequeñas reuniones para luego asignar políticas y prioridades, esto, con el fin de reducir el número de riesgos que necesitan más análisis. (Microsoft, 2006)

Alto impacto en la organización:

En esta clasificación, los riesgos como: confidencialidad, integridad o la disponibilidad de los activos, provocan pérdidas de mucho valor graves, o inclusive catastróficas para la organización. Los impactos se expresan netamente en términos financieros y reflejar pérdidas inconscientes, robos, falta de productividad, daños a la reputación o responsabilidad legal. (Microsoft, 2006)

Impacto moderado en la organización:

Los impactos en la integridad, confidencialidad y disponibilidad de estos activos generan consecuencias moderadas para la organización, es decir, constituyen pérdidas catastróficas y altera las funciones organizativas hasta que es necesario realizar controles tempranos para minimizar el impacto. (Microsoft, 2006)

Bajo impacto en la organización:

Los activos que tiene una repercusión baja en la organización no contienen requisitos de protección, tampoco controles adicionales. Simplemente cuenta con algunas prácticas recomendadas para proteger la infraestructura. Estos activos suelen ser normalmente de dominio público como por ejemplo la estructura de la organización, páginas web, información básica en los que una mala difusión puede generar problemas legales para la organización. (Microsoft, 2006)

El modo para realizar recolección de los activos de información se presenta en la siguiente plantilla:

Plantilla para recolección de datos

Identificar los activos que su grupo es responsable del desarrollo, la gestión, el apoyo, o el mantenimiento.

Nombre del Activo	Clasificación de Activos (Alto, Medio o Bajo Impacto en el Negocio)
1.	

Nombre del Activo	Clasificación de Activos (Alto, Medio o Bajo Impacto en el Negocio)
2.	

Tabla 9: Recolección de datos Activos de información

Fuente: (Microsoft, 2006)

2.3 Identificación de Vulnerabilidades

La información que se expone con el tema acerca de las vulnerabilidades resulta una prueba técnica, la cual es utilizada para asignar prioridades entre los riesgos de una empresa; en la misma puede existir personal que no esté familiarizado con conocimientos técnicos y que afecten de una manera directa a la organización. Este es un espacio de gran valor en donde una investigación es de gran necesidad para determinar tanto responsables como los riesgos del entorno. (Microsoft, 2006)

Para resolver la falta de conocimiento previo del personal técnico, es necesario realizar un debate de riesgos en donde resulte beneficioso traducir las vulnerabilidades en términos mucho más manejables y conocidos. Esta problemática es un punto débil dentro del o los activos que una amenaza pueda atacar como por ejemplo la falta de revisión de los *Host* pueden afectar a la información financiera de las organizaciones. (Microsoft, 2006)

Hay que tomar en cuenta que no solo las vulnerabilidades técnicas son riesgos centrales, ya que, las de gran importancia surgen de la falta de un proceso o control adecuado de la seguridad de información, así también en el aspecto organizativo y de liderazgo durante el proceso de recopilación de datos. Citando uno de los problemas más comunes, es el control claro y aplicación de políticas de seguridad de información en el ámbito organizativo de muchas organizaciones; finalmente se debe tener en cuenta el seguimiento respectivo para evaluar los riesgos en cuestión. (Microsoft, 2006)

En la siguiente tabla se detallan todas aquellas vulnerabilidades que posiblemente puedan afectar a la organización, esta tabla es solo de referencia que se puede adaptar al medio quitando aquellas vulnerabilidades que no son relevantes y agregando las que se identifiquen a lo largo de la gestión de riesgos:

Clase de vulnerabilidad	**Vulnerabilidad**	**Ejemplo**
Clase de vulnerabilidad de alto nivel	*Breve descripción de la vulnerabilidad*	*Ejemplo específico (si es aplicable)*
Física	Puertas sin seguro	
Física	Acceso no permitido a las instalaciones informáticas	

Física	Sistemas contra incendios insuficientes	
Física	Diseño deficiente de edificios	
Física	Construcción deficiente de edificios	
Física	Materiales inflamables utilizados en la construcción	
Física	Materiales inflamables utilizados en el acabado	
Física	Ventanas sin seguro	
Física	Paredes que se pueden asaltar físicamente	
Física	Paredes interiores que no sellan la sala por completo tanto en el techo como en el suelo	
Natural	Instalación situada sobre una línea de error	
Natural	Instalación situada en una zona de inundaciones	
Natural	Instalación situada en un área de avalanchas	
Hardware	Faltan revisiones	
Hardware	Firmware obsoleto	
Hardware	Sistemas configurados incorrectamente	
Hardware	Sistemas sin proteger físicamente	

Hardware	Protocolos de administración permitidos en interfaces públicas	
Software	Software antivirus obsoleto	
Software	Faltan revisiones	
Software	Aplicaciones escritas deficientemente	Secuencias de comandos entre sitios
Software	Aplicaciones escritas deficientemente	Inserción de SQL
Software	Aplicaciones escritas deficientemente	Vulnerabilidades de código como desbordamientos de buffer
Software	Vulnerabilidades colocadas deliberadamente	Puertas traseras del proveedor para administración o la recuperación del sistema
Software	Vulnerabilidades colocadas deliberadamente	Programas espía como aplicaciones de captura del teclado
Software	Vulnerabilidades colocadas deliberadamente	Troyanos
Software	Vulnerabilidades colocadas deliberadamente	
Software	Errores de configuración	Creación manual que provoca configuraciones incoherentes
Software	Errores de configuración	Sistemas no protegidos
Software	Errores de configuración	Sistemas no auditados
Software	Errores de configuración	Sistemas no supervisados
Medios	Interferencia eléctrica	

Comunicaciones	Protocolos de red sin cifrar	
Comunicaciones	Conexiones a varias redes	
Comunicaciones	Se permiten protocolos innecesarios	
Comunicaciones	Sin filtrado entre segmentos de red	
Humana	Procedimientos definidos deficientemente	Preparación insuficiente para la respuesta a incidencias
Humana	Procedimientos definidos deficientemente	Creación manual
Humana	Procedimientos definidos deficientemente	Planes de recuperación de desastres insuficientes
Humana	Procedimientos definidos deficientemente	Pruebas de sistemas de producción
Humana	Procedimientos definidos deficientemente	Infracciones no comunicadas
Humana	Procedimientos definidos deficientemente	Control de cambios deficiente
Humana	Credenciales robadas	

Tabla 10: Vulnerabilidades

Fuente: (Microsoft, 2006)

2.4 Funciones de Probabilidad

La información, acerca de las estimaciones de las posibles repercusiones de los activos organizativos deben ser facilitados por cada uno de los participantes, en donde, después de una evaluación de riesgos, se obtengan las suficientes opiniones que permitan de este modo cerrar el debate acerca de los riesgos y aquellos puedan comprender de una manera objetiva el proceso de identificación de los riesgos de seguridad. Se establecerá un

grupo de seguridad de información, el cual estará a cargo de la decisión final a cerca de la estimación de probabilidad que produzcan los impactos en la organización.

Microsoft determina como referencia ciertos indicadores que permiten valorar la probabilidad de cada uno de los riesgos, amenazas y vulnerabilidades que se pueden apreciar en los ya mencionados debates:

- **Alta**: muy probable, previsión de uno o varios ataques en un año.
- **Media**: probable, previsión de ataque en dos a tres años.
- **Baja**: no probable, no se prevé ningún ataque en tres años.

Estos indicadores se deben debatir entre cada uno de los participantes en la medida en que se pueda apreciar la importancia de la seguridad y el proceso de administración de riesgos al nivel global.

Clase de impacto	Valor de la clase de impacto (V)
AI	10
IM	5
BI	2

AI: Alto Impacto

IM: Impacto Medio

BI: Bajo impacto

Para describir el nivel de exposición de a los riesgos, *Security Risk Managment Guide* ofrece la siguiente información de rangos:

Clasificación del rango de exposición	Factor de exposición (EF)	Rango de impacto (V * EF)	Impacto	Niveles resumen y comparación
5	100%		7 - 10	Alto
4	80%		4 - 6	Medio
3	60%		0 - 3	Bajo
2	40%			
1	20%			

Tabla 11: Funciones de probabilidad de riesgos

Fuente: (Microsoft, 2006)

Como un claro ejemplo se puede considerar a la organización *Microsoft*, cuyo modelo de proceso de administración de riesgos de seguridad determina intervalos de un año aproximadamente para establecer la categoría de probabilidad alta, esto debido a que los

controles de seguridad de información suelen ser periodos largos, y, tarda en implementarse. Tanto los participantes como el equipo encargado de la seguridad de la información deben exigirse un trabajo conjunto y direccionado, el mismo que pueda llegar a tomar decisiones eficaces y oportunas acerca de la mitigación del siguiente ciclo presupuestario, lo mismo que ayudará a la concientización y responsabilidad de estimar la probabilidad de los impactos.

Posteriormente es necesario que los participantes emitan opiniones en donde, el debate a realizar sea el producto de una objetiva lluvia de ideas y de esta manera no se rechace ninguna; es así que la premisa principal del mismo es demostrar todos los componentes de riesgo con los que cuenta la organización, y así facilitar la comprensión a cada uno de los usuarios. Los participantes deben tener claro que la noción de reducción de probabilidad de riesgo es uno de los fundamentos de mayor importancia para controlarlo en niveles aceptables. (Microsoft, 2006)

2.5 Variable de medición del riesgo

Se habla de una plantilla o modelo de discusión de riesgos la cual es incluida en la sección de herramientas, ya que esta hace más asimilable el trabajo de los asistentes y así llegar a una comprensión directa. También es de gran ayuda para el responsable de registro de evaluación de riesgos, ya que ayuda a obtener eficazmente la información pertinente y coherente en las reuniones o debates. (Microsoft, 2006)

Este modelo sugiere seguir una secuencia para ayudar a los participantes del debate a entender los componentes de riesgo y revelar más información, considerando:

- ¿Qué activo se va a proteger?
- ¿Cuál es el valor del activo para la organización?
- ¿Qué se intenta evitar que le suceda al activo (amenazas conocidas y posibles)?
- ¿Cómo se pueden producir la pérdida o las exposiciones?
- ¿Cuál es el alcance de la exposición potencial para el activo?
- ¿Qué se está haciendo actualmente para reducir la probabilidad o el alcance del daño en el activo?
- ¿Cuáles son las acciones que se pueden adoptar para reducir la probabilidad en el futuro?

Los cuestionamientos antes presentados, hacen referencia a una terminología y categorías de evaluación de riesgos específicas, las mismas que ayudarán a establecer un orden de prioridad a las vulnerabilidades presentadas. No se excluye la posibilidad de que en el transcurso del proceso se tome la decisión de cambiar ciertas terminaciones para hacer más asimilable el trabajo de los encargados de la seguridad; esto no va en detrimento de la calidad del debate; al contrario, brinda a los participantes eliminar todo tipo de intimidación al hablar de estos conocimientos técnicos. Es importante considerar que quien esté a cargo de la evaluación de riesgos deberá esperar a la terminación del debate para esclarecer dudas de las definiciones y terminología de los riesgos. (Microsoft, 2006)

2.6 Calculo de riesgo

Al hablar específicamente de la clasificación de los riesgos, se manifiesta que la misma es producto de la clasificación de efecto (con valores del 1 a 10) y los intervalos de clasificación de probabilidad (con valores de 0 a 10), generando de esta manera un intervalo de 0 a 100 y de esta manera se pueden detallar los riesgos de forma cualitativa, es decir, Alto, Medio, y Bajo.

Clasificación de riesgo * Clasificación de probabilidad = Nivel de riesgo				
Intervalos de clasificación de efecto		*****	**Intervalos de probabilidad**	
Alto	10 -- 7		10 – 7	
Medio	6 -- 4		6 – 3	
Bajo	3 -- 0		3 – 0	

	H	10	0	10	20	30	40	50	60	70	80	90	100
		9	0	9	18	27	36	45	54	63	72	81	90
		8	0	8	16	24	32	40	48	56	64	72	80
		7	0	7	14	21	28	35	42	49	56	63	70
Impact		6	0	6	12	18	24	30	36	42	48	54	60
	M	5	0	5	10	15	20	25	30	35	40	45	50
		4	0	4	8	12	16	20	24	28	32	36	40
		3	0	3	6	9	12	15	18	21	24	27	30
		2	0	2	4	6	8	10	12	14	16	18	20
	L	1	0	1	2	3	4	5	6	7	8	9	10
			0	1	2	3	4	5	6	7	8	9	10
			L					M					H
							Probability						

Clasificación	**Nivel de riesgo**
41-100	Alto
20-40	Medio
0-19	Bajo

Imagen 11: Hoja de trabajo de análisis de riesgos: Clasificación cualitativa

Fuente: (Microsoft, 2006)

> *"El equipo de administración de riesgos de seguridad debe comunicar a la organización por escrito el significado de riesgos altos, medios y bajos. El proceso de administración de riesgos de seguridad de Microsoft solo constituye una herramienta para identificar y administrar los riesgos en la organización de un modo coherente y progresivo."* (Microsoft, 2006)

2.7 Alineación con el estándar ISO27001

Security Risk Management Guide, al igual que este estándar, adopta el Plan de Mejora Continua (Planificar, Hacer, Verificar, Actuar). La guía este plan está denominado como: "Las cuatro fases del proceso de administración de riesgos de seguridad de Microsoft", las mismas que se enumeran a continuación:

1. **Evaluación del Riesgo:** Identifica y asigna las prioridades a los riesgos de la organización.
2. **Apoyo a la toma de decisiones:** en este punto se identifican y se toman decisiones, es decir, implementa políticas según el proceso definido costo – beneficio.
3. **Implementación de controles:** Se pone en funcionamiento las políticas o soluciones para reducir el riesgo de la organización.
4. **Medición de la efectividad del programa:** Analiza la efectividad del proceso de administración de riesgos

(Microsoft, 2006)

La metodología de *Microsoft* propone que la clasificación de los *Activos de información,* sea tangibles e intangibles, y según sea necesario para la organización, Activo de Servicio de TI, al igual que el estándar, clasifica a los activos mediante software y hardware.

Clasificación de Activos			
Security Risk Management		**ISO27001**	
Tangible	Infraestructura, servidores, computadores	**Hardware**	Infraestructura física
Intangible	Datos - Información digital	**Software**	Aplicaciones - Sistemas de datos
Servicios de TI	Correo electrónico		

Tabla 12: Tabla comparativa de la clasificación de activos SRM e ISO 27001

Fuente: (Microsoft, 2006), (Cordero, 2015)

Para la evaluación de los activos, *Security Risk Management* también toma aspectos importantes del estándar como la valoración del riesgo, el impacto para la organización, definición de vulnerabilidades, apoyo a la toma de decisiones e implementación de controles.

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 1".*

2.8 Vinculación con el estándar ISO27002

La relación que existe entre la guía de administración de riesgos de seguridad y este estándar se da al momento de identificar las amenazas y establecer políticas. *Microsoft* las denomina: Implementación de controles y apoyo a la toma de decisiones. Es muy similar al estándar, ya que, brinda indicaciones del como evaluar, tratar los riesgos de seguridad, realizar la gestión de los activos, clasificar la amenazas y buscar la seguridad de la organización tanto física como ambiental además de proteger los recursos humanos y la seguridad de los equipos. (Microsoft, 2006)

Así como el estándar sugiere una lista de objetivos de control y controles, *Security Risk Management* también consta de un llamado "Proceso de respuesta a incidencias" las cuales sirven de ayuda de cómo implementar un exitoso sistema de gestión de riesgos de seguridad para la organización. Este proceso se detalla en el siguiente diagrama:

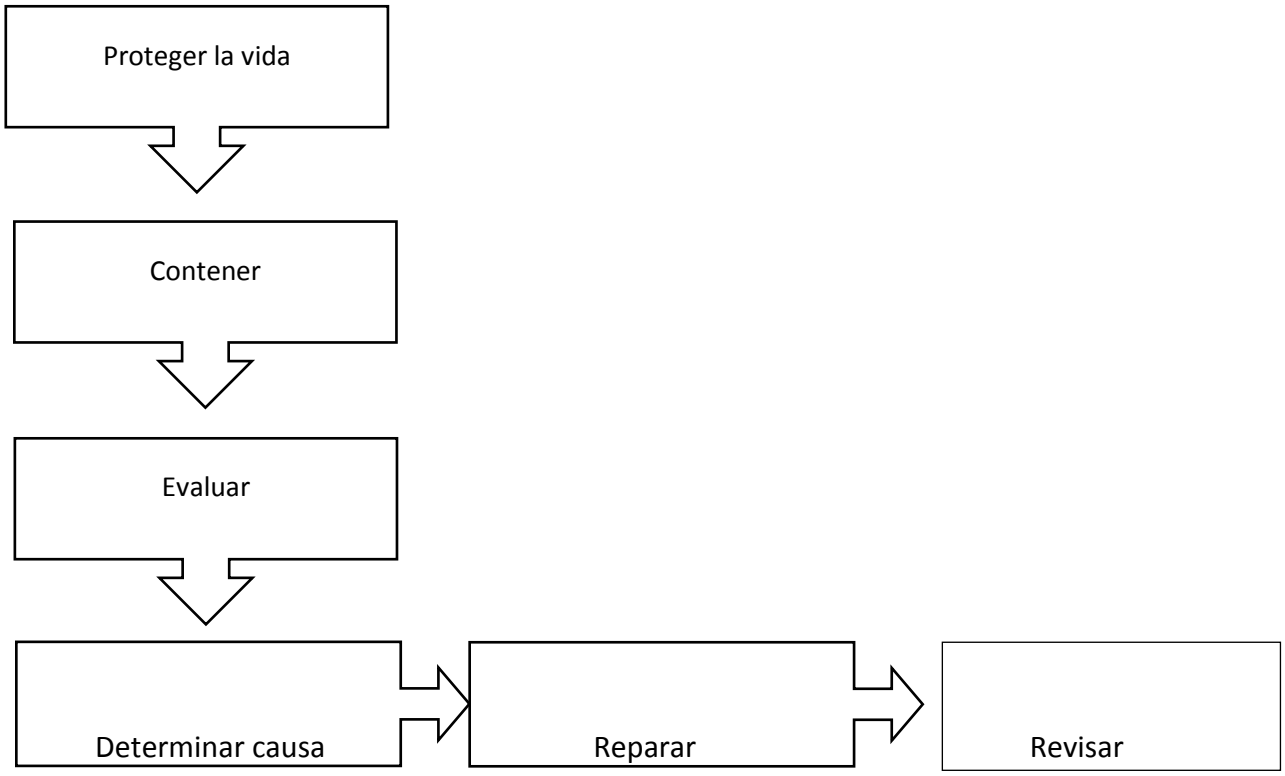


Imagen 12: Proceso de respuesta a incidencias

Fuente: (Microsoft, 2006)

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 1".*

2.9 Relación con el estándar ISO27005

Security Risk Management tiene una clara alineación con este estándar en el momento que identificar las vulnerabilidades y amenazas con resultados detallados y fácilmente justificables mediante la combinación de la simplicidad con un proceso único y eficaz para la administración de riesgos de seguridad; este proceso consta de cuatro faces que tienen similitud con el estándar.

1. Medición de efectividad del programa.
2. Evaluación de riesgo.
3. Apoyo a la toma de decisiones.
4. Implementación de controles.

Estas fases de la administración de riesgos son similares con el estándar al momento de:

1. Realizar la evaluación de riesgos de seguridad
2. Dar tratamiento a los riesgos de la seguridad de la información
3. Admisión de riesgos de seguridad de información

4. Comunicación de riesgos y seguridad de información.
5. Seguimiento y revisión del riesgo.

(Microsoft, 2006)

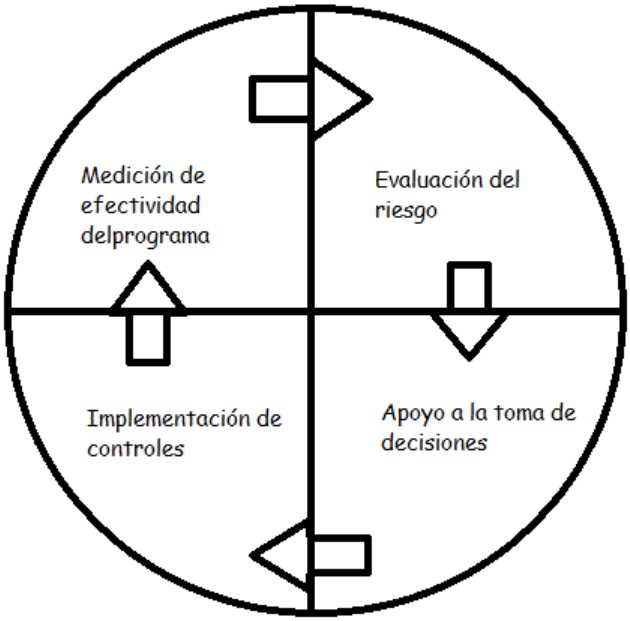


Imagen 13: Faces del proceso de administración de riesgos de seguridad de "Microsoft" Fuente: (Microsoft, 2006)

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 1".*

2.10 Alineación con el estándar ISO31000

Security Risk Management tiene varias similitudes al momento de realizar la administración de riesgos de seguridad proponiendo una seria de fases basadas en este estándar analizando conocimientos previos, requisitos y tareas de este proceso, las cuales se detallan a continuación:

- Tener en claro la diferencia entre administración y evaluación de riesgos.
- Notificación clara del riesgo.
- Analizar el grado de madurez que la organización posee para la gestión del riesgo.
- Definir claramente las funciones y las responsabilidades del proceso.

(Microsoft, 2006)

Esta guía al igual que el estándar, definen al proceso de gestión de riesgo como un proceso global en toda organización hasta que alcance un nivel aceptable. Como se habló

anteriormente esto se realiza en cuatro fases (evaluación de riesgos, apoyo a la toma de decisiones, implementación de controles y medición a efectividad del programa). (Microsoft, 2006)

Luego de haber identificado los riesgos los califica realizando el análisis cualitativo y cuantitativo.

Security Risk Management una vez que concluye la identificación de riesgos inicia su fase de apoyo a la toma de decisiones que se vinculan en la práctica al momento de:

1. Definir requisitos.
2. Identificar soluciones de control.
3. Revisar las soluciones propuestas.
4. Calcular la reducción del nivel de riesgo.
5. Calcular el coste de cada solución.
6. Seleccionar la estrategia de mitigación de riesgos.

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 1".*

2.11 Conclusiones del capítulo

Se puede deducir del capítulo presentado que, *Security Risk Management Guide* es una alternativa viable desarrollada por: técnicos, clientes y especialistas computacionales cuya finalidad es la concientización de posibles riesgos informáticos, la cuantificación de dicha problemática y el proceso de investigación de riesgos que se llevará a cabo en cada una de las organizaciones. Dentro de las empresas debe existir una plantilla de recolección de datos de los activos la cual, ayudará a gestionar información, facilitar estudios y análisis.

Los resultados del trabajo mencionado será una herramienta fundamental para reuniones futuras, en donde se deberá diseñar un plan de políticas a seguir con la finalidad de contrarrestar y combatir la problemática de la seguridad de información y la seguridad informática. Las reuniones deben ser basadas en debates direccionados, considerando un control y monitoreo constante y adecuado del sistema informático, que deben finalizar con evaluaciones dadas por cada uno de los participantes.

En cada una de las reuniones debe asistir todo el personal que tenga a su cargo algún tipo de información fundamental de la empresa, si en dicho conversatorio surgen terminologías

desconocidas o aspectos que no forman parte de la organización, estas pueden ser reemplazadas por un lenguaje más asimilable, ya que no siempre dichos términos son familiares o conocidos. De esta manera se incentiva a cada uno de los miembros a que sean partícipes del proceso de identificación de riesgos de seguridad y que puedan dar, como resultado, indicadores que permitan valorar la posible probabilidad de riesgo de una manera cualitativa, es decir, alta, media y/o baja que finalmente deben tener un debido seguimiento.

Se habla también de una escala de riesgos que involucra a los activos tangibles e intangibles, los mismos tienen un valor específico que está dado por un rango y una clasificación determinada. El primero hace referencia al daño o afección que pueden sufrir tanto los equipos como la información, posteriormente el segundo trata la probabilidad de que ocurra y a los efectos que causan los riesgos para organización.

Security Risk Management Guide se basa en las normas ISO, ya que toma de cada uno de los estándares puntos que son de gran importancia para su desarrollo, como por ejemplo la identificación de activos y su valoración, y la detección de vulnerabilidades y amenazas.

Esta metodología está para la disposición de cualquier organización de forma gratuita, y a pesar de que no ha sido actualizada desde el año 2006, puede utilizarse en cualquier entorno, ya que se acopla a las necesidades de muchas empresas.

CAPÍTULO 3: Estudio de la metodología OCTAVE-S.

3.1 Introducción del capítulo.

En este capítulo se estudia la metodología OCTAVE-S debido a que fue enfocada para MPYMES.

Para el desarrollo de esta, se debe como primer punto, encontrar mecanismos para la identificación de los activos, definiendo activo como: "todo bien o recurso tangible o intangible, valorado por la organización". (Moscoso Montalvo & Guagalando Vega, 2011, pág 6-7); una vez identificados los activos de la organización se procede con la identificación de vulnerabilidades, determinar funciones de probabilidad, establecer variables de medición del riesgo, y por último, determinar el cálculo del riesgo de la organización.

OCTAVE-S fue escogida para este estudio comparativo porque:

- Recurre a personal de la misma organización, ya que son los que conocen exactamente donde se encuentran los puntos más críticos, y esto reduce los costos para la implementación del mismo.

OCTAVE-S consta de tres fases:

- **Fase uno:** Construir perfiles de amenaza basada en activos.
- **Fase dos:** Identificar vulnerabilidades de la infraestructura.
- **Fase tres:** Desarrollo de planes y estrategias de seguridad.

Para utilizar o implementar esta metodología, se debe tener en cuenta que se necesita un equipo interdisciplinario de 3 a 5 personas que tengan una visión amplia de los procesos de la organización, llamándolo OCTAVE-S como "***equipo de análisis***".

Como se puede observar en la imagen 11, OCTAVE-S consta de tres fases para su correcto desarrollo e implementación.

Imagen 14: Fases de la metodología OCTAVE-S.

Fuente: (Flores y Melo, 2013)

Principalmente, antes de comenzar con la primera fase de la metodología, se debe iniciar con una fase de preparación donde se construye el ***"equipo de análisis",*** donde los integrantes deben ser personas que pertenezcan y conozcan de manera cercana a la organización. Al ***"equipo de análisis"*** también pueden integrar personal externo. (Flores y Melo, 2013)

Nombre Miembro	**Función en la evaluación.**

Tabla 13: Modelo para el registro del equipo de análisis.

Este es el modelo de tabla a llenar para construir el ***"equipo de análisis,*** donde se debe colocar el nombre del miembro, seguido de la función que este realiza en la empresa.

Roles y responsabilidades del equipo de análisis:

- Trabajar con los directivos en el alcance de la evaluación, selección de participantes y cuando se llevarán a cabo cada una de las actividades pertenecientes a cada proceso de la metodología.
- Coordinar con los altos directivos las respectivas evaluaciones de las vulnerabilidades.
- Recopilar, analizar y mantener datos y resultados durante los procesos de la metodología.

- Proveer de soporte logístico.

Selección de alto directivos:

> **“**Deben tener la capacidad y conocimientos necesarios para identificar correctamente los activos de información más importantes, las distintas amenazas para estos, los requerimientos de seguridad de cada activo, las estrategias de protección y las vulnerabilidades organizacionales.” (Alejandro Sebastian, 2014)

Selección de directivos de Áreas Operativas:

> “Deben estar asociados con la operación, mantenimiento y desarrollo de la infraestructura computacional de la organización; son requeridos para identificar los activos de información que posee la organización, las distintas amenazas para estos activos, los requerimientos de seguridad de cada activo, las estrategias de protección y las vulnerabilidades organizacionales”.

3.2 Fase 1: Construir perfiles de amenaza basada en activos.

Según la tabla descrita a continuación, se describe los procesos, actividades y pasos que sigue la fase 1.

Fase 1	**Proceso**	**Actividad**	**Pasos**
Fase 1: Construir perfiles de amenaza basada en activos.	Proceso S1: Identificar la información organizacional.	S1.1 Establecer los criterios de evaluación.	1
		S1.2 Identificar activos.	2
		S1.3 Evaluar las prácticas de seguridad.	3,4
	Proceso S2: Crear perfiles de amenaza.	S2.1 Seleccionar activos críticos.	5,6,7,8,9
		S2.2 Identificar requerimientos de seguridad.	10,11

		S2.3 Identificar amenazas a los activos.	12,13,14,15,16

Tabla 14: Procesos, Actividades y Pasos de la Fase 1, OCTAVE-S.

Fuente: (Flores y Melo, 2013)

3.2.1 Proceso S1: Identificar la información organizacional.

3.2.1.1 Actividad S1.1: Establecer los criterios de evaluación.

Como primer paso se debe definir los rangos de potencial impacto, los cuales pueden ser: (alto, medio y bajo), que afectan a los activos de información de las organizaciones en las áreas que propone OCTAVE-S:

- Reputación/Confianza de los clientes.
- Financiera.
- Productividad.
- Seguridad de las personas/Salud.
- Multas/Sanciones legales.
- Sistemas.

A continuación se presenta ejemplos de hojas de trabajo para establecer los criterios de evaluación:

Reputación/Confianza de los clientes			
Tipo de impacto	**Bajo**	**Medio**	**Alto**
Reputación	La reputación de la organización se afecta en un mínimo porcentaje, poco o nada de esfuerzo o gasto es necesario para recuperarse si se presenta la	La reputación de la organización se daña, necesitando esfuerzo y un poco de gasto económico para poder recuperarse.	La reputación de la organización está irremediablemente destruida o dañada.

	situación de pérdida de confianza del cliente.		

Tabla 15: Hoja de trabajo: Impacto de los criterios de evaluación: Confianza de los clientes.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005)

Financiera			
Tipo de Impacto	**Bajo**	**Medio**	**Alto**
Costos Operativos	Aumento de menos de 2% anual en costos operativos.	Gastos anuales de costos operativos aumentan del 2% al 10%.	Anualmente los costos operativos aumentan el 10%.
Pérdida de ingresos	Menos del 5% de pérdida de ingresos anuales.	Del 5% al 12% de pérdida de ingresos anuales.	Mayor al 12% de pérdida de ingresos anuales.
Perdida financiera	Pérdida de menos de $5000	Pérdida de $5000 a $15000	Pérdida mayor a $15000

Tabla 16: Hoja de trabajo: Impacto de los criterios de evaluación: Financiera.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

Productividad.			
Tipo de Impacto	**Bajo**	**Medio**	**Alto**
Horarios del personal.	Se incrementan un 5% en 28 días.	Se incrementa del 5% al 20% en 28 días.	Se incrementa en más de un 20% en los 28 días.

Tabla 17: Hoja de trabajo: Impacto de los criterios de evaluación: Productividad.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

Seguridad/Salud.			
Tipo de Impacto	**Bajo**	**Medio**	**Alto**
Vida.	No existe amenaza significativa en la	Se ve afectada, pero se recuperan	Pérdida de vidas del personal.

	vida del personal.	después de haber recibido tratamiento médico.	
Salud.	Degradación mínima, inmediatamente tratable de la salud de los miembros del personal con un tiempo de recuperación dentro de cuatro días	Discapacidad temporal o recuperable de la salud de miembros del personal.	Deterioro permanente de la salud del personal.
Seguridad.	Seguridad cuestionada.	Seguridad afectada.	Seguridad violada.

Tabla 18: Hoja de trabajo: Impacto de los criterios de evaluación: Seguridad/Salud.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

3.2.1.2 Actividad S1.2: Identificar activos.

Luego de haber establecido el **"*equipo de análisis*",** y definidos los rangos de valoración de impacto, el siguiente paso es identificar los activos de información críticos (sistemas, aplicaciones, información y personas).

Se toma como punto de partida la experiencia del **"*equipo de análisis*",** que debe recolectar activos de información críticos desde un punto vista organizacional, para posteriormente evaluarlos con mayor profundidad, entre 3 a 5 de ellos. (Flores y Melo, 2013)

Información, Sistemas y Aplicaciones.			
Sistemas. ¿Qué sistemas la gente necesita para realizar su trabajo?	**Información** ¿Qué información la gente necesita para realizar su	**Apliacaciones y Servicios.** ¿Qué aplicaciones y servicios la	**Otros.** ¿Qué otros activos estan relacionados directamente con

	trabajo?	gente necesita para realizar su trabajo?	estos activos?

Tabla 19: Hoja de trabajo. Identificaciones de los activos organizacionales. Información, Sistemas y Aplicaciones.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005)

Gente			
Gente. ¿Qué personas tienen una habilidad y conocimiento especial que es vital para su organización y puede ser muy difícil de reemplazar?	**Habilidades y Conocimiento.** ¿Cuáles son sus habilidades y conocimientos?	**Sistemas Relacionados.** ¿Qué sistemas utilizan estas personas?	**Activos Relacionados.** ¿Qué otros activos usan estas personas?

3.2.1.3 Actividad S1.3: Evaluar las prácticas de seguridad.

En esta actividad se desarrolla el paso 3 y 4, descritos en la tabla 7, en el cual, el paso 3 se subdividirá en los procesos 3a y 3b, donde en el proceso 3a, se analiza hasta qué punto, cada una de las prácticas de seguridad son aplicadas en las organizaciones, y en el proceso 3b, se registra lo que la organización realiza correctamente (prácticas de seguridad) y en lo que falla (vulnerabilidades organizacionales).

OCTAVE-S propone 15 prácticas de seguridad:

1. Concienciación y formación en seguridad: No divulgar información sensible a terceros, capacidad suficiente para el manejo de hardware y software, reportar incidentes, cursos de capacitación (interna o externa) de seguridad de la información.
2. Estrategia de Seguridad.

3. Gestión de Seguridad: Dar soluciones a problemas de seguridad que se presenten en cada una de las áreas de trabajo.
4. Políticas y Regulaciones de Seguridad: Tener procedimientos que se deben realizar cuando se presenta algún incidente de seguridad de la información, con ello solucionar dichos incidentes.
5. Gestión de Seguridad Colaborativa: Tener políticas y procedimientos para proteger la información cuando se trabaja con organizaciones externas y a su vez estas organizaciones cumplan con sus necesidades y requerimientos.
6. Planes de Contingencia/ Recuperación de desastres: Tales como:
    - Seguridad de la instalación.
    - Disponibilidad de recursos (hardware y software).
    - Políticas y procedimientos de respaldo de información.
    - Recuperación de información.
7. Control de Acceso Físico: Determinar los mejores controles de seguridad física para proteger los activos de la organización, tales como:
    - Accesos restringidos a las áreas donde existe activos de información.
    - Proteger los computadores con claves personales.
    - Cámaras de circuito cerrado.
    - Utilización de sistemas biométricos para el control de acceso.
8. Monitoreo y Auditoria de Seguridad Física. Asegurar que todos los equipos, dispositivos e información estén asegurados, saber quién es el responsable y manteniendo un monitoreo constante de cada uno de ellos.
9. Gestión de Sistemas y Redes: Poseer herramientas para gestionar la seguridad y almacenamiento de los datos.

10. Monitoreo y Auditoria de Seguridad de TI. Para realizar un correcto procedimiento de monitoreo y auditoria de los sistemas, de la red y la información, es necesario poseer herramientas que ayuden al desarrollo del mismo, al igual se debe contar con políticas documentadas.
11. Autenticación y Autorización. Se debe implementar mecanismos de control de acceso a los usuarios que accedan a los activos de información, sin olvidar de la respectiva autorización otorgada por su jefe(a) inmediato(a), o al personal encargado de dicho activo de información.

12. Gestión de Vulnerabilidades. Documentar procedimientos y políticas de cómo desarrollar un análisis y gestión de vulnerabilidades de los sistemas.
13. Encriptación: Hace referencia a una manera de proteger la información de gran importancia de la organización contra los ataques informáticos.
14. Diseño y Arquitectura de Seguridad. Poseer documentación del diseño de la red informática, con ello se puede tomar acciones y crear planes de seguridad.
15. Gestión de Incidentes. Documentación para saber como reaccionar en caso de surgir algun incidente, ademas guias de como realizar respaldos de información y recuperación de datos. (Flores y Melo, 2013)

Para el paso número 4, se asigna un estado de semáforo (verde, amarillo y rojo), en cada una de las prácticas de seguridad.

Verde: Hace referencia a que la organización cumple correctamente con las prácticas de seguridad.

Amarillo: La organización cumple hasta cierto punto las prácticas de seguridad con espacio a mejora.

Rojo: No cumple con las prácticas de seguridad propuestas.

Nombre de la Práctica de Seguridad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización no está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementando las prácticas en esta área?**
Existen diferentes enunciados para cada una de las Prácticas de	Si Algo No No se sabe			Rojo Amarillo Verde No aplica

Seguridad.				

Tabla 20: Hoja de trabajo. Prácticas de Seguridad.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

3.2.2 Proceso S2: Crear perfiles de amenaza.

En este proceso se seleccionan los activos críticos de entre los activos identificados previamente. Luego se identifican los requerimientos de seguridad para esos activos y se determina las amenazas presentes en contra de ellos.

3.2.2.1 Actividad S2.1: Seleccionar los activos críticos.

En esta actividad se desarrollan los pasos del 5 al 9 donde:

Paso 5: Se selecciona de 3 a 5 activos críticos dentro de los activos identificados anteriormente.

Paso 6: Se identifica al activo crítico por su nombre.

Paso 7: Se describe la razón por la cual se le considera un activo crítico.

Paso 8: Se registra quien usa y quien es el responsable del activo crítico.

Paso 9: Se registra cuales otros activos están relacionados con el activo crítico. (Flores y Melo, 2013)

Selección de activos críticos.	
Preguntas a considerar: Que activo tendría un efecto adverso en la organización si: - ¿Es divulgado a personas no autorizadas? - ¿Es modificado sin autorización? - ¿Se pierde o es destruido? - ¿El acceso al activo es interrumpido?	
Nombre Activo crítico:	**Notas:**

Tabla 21: Hoja de trabajo. Selección de activos críticos.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

3.2.2.2 Actividad S2.2: Identificar los requerimientos de seguridad.

En esta actividad se desarrollan los pasos 10 y 11, mencionados en la tabla 7.

Paso 10: Se identifican los requerimientos de seguridad para cada activo crítico.

OCTAVE-S propone varios requerimientos de seguridad descritos a continuación:

- **Confidencialidad:** La información se encuentre accesible solamente para el personal autorizado.
- **Integridad:** Garantiza que cierta información pueda ser modificada solamente por el personal autorizado.
- **Disponibilidad:** La información esté disponible siempre para el personal que la necesite.
- Otros. (Flores y Melo, 2013)

Paso 11: Se determinan los requerimientos más importantes de seguridad de cada activo.

Información de activos críticos.				
Activo Critico. Nombre del activo crítico seleccionado.	**Justificación de la selección.**	**Descripción del Sistema.** ¿Quién usa el sistema? ¿Quién es responsable del sistema?	**Requerimientos de Seguridad.**	**Requerimiento de Seguridad más importante.**
			Se escoge y describe los requerimientos de seguridad propuestos por OCTAVE-S que la organización ha elegido para dicho activo crítico.	De los requerimientos escogidos se selecciona el más importante. (Confidencialidad, Disponibilidad, Integridad y Otros).

Tabla 22: Hoja de trabajo. Información de activos críticos.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005)

3.2.2.3 Actividad S2.3: Identificar las amenazas a los acticos críticos.

En esta actividad se describen y realizan los pasos 12, 13, 14, 15 y 16.

Paso 12: Se completa el árbol de amenazas propuesto por OCTAVE-S, para cada activo crítico, tomando en cuenta las siguientes categorías de amenazas:

1. Actores humanos usando acceso a la red.
2. Actores humanos usando acceso físico.
3. Problemas del sistema.
4. Otros. (Alberts, Dorofee, Stevens, y Woody, 2005)

Paso 13: Se determina cuáles son los actores que representa la mayor amenaza para cada uno de los activos críticos, tomando en cuenta las siguientes combinaciones:

- Internos actúan por accidente.
- Internos actúan deliberadamente.
- Externos actúan por accidente.
- Internos actúan deliberadamente.

Nota: Este paso solo se debe realizar con actores con acceso a la red o acceso físico.

(Alberts, Dorofee, Stevens, y Woody, 2005)

Paso 14: En este paso se anota la opinion del "***equipo de analisis"*** sobre la intensidad de la motivacion del actor a realizar un ataque y el grado de confianza en esa estimación, tomando en cuenta las siguiente combinaciones:

- Internos actuan deliberadamente.
- Externos actuan deliberadamente.

Al igual que el anterior paso solo se puede realizar para las siguientes categorias de amenazas.

- Actores humanos con acceso a la red.
- Actores humanos con acceso físico.

Paso 15: Se debe revisar cualquier tipo de dato objetivo de la organización tales como (registros, datos de insidente, documentación de problemas), tambien revisar datos subjetivos (lo que el personal o el equipo de analisis puede recordar).

Paso 16: Para este paso se describe escenarios reales de como las amenazas especificas pueden afectar a cada uno de los activos criticos.

(Alberts, Dorofee, Stevens, y Woody, 2005)

<table>
<tr><td colspan="5">Actores con acceso a la red y físico.</td><td></td></tr>
<tr><td colspan="5">Amenaza.
¿Para cual rama hay una posibilidad no desdeñable de una amenaza a un activo? Marcar estas ramas en el árbol.
¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marcar estas ramas.</td><td>Actores de amenazas.
¿Qué actores planean las mayores amenazas para el sistema a través de la red?</td></tr>
<tr><td>Activo</td><td>Acceso</td><td>Actor</td><td>Motivo</td><td>Resultado</td><td></td></tr>
<tr><td>Nombre del activo critico elegido.</td><td>- Red.
- Físico</td><td>- Adentro.
- Afuera.</td><td>- Accidental.
- Premeditado.</td><td>- Revelación.
- Modificación
- Perdida
- Interrupción.</td><td>Describir si los actores internos como externos actúan deliberadamente o por accidente.</td></tr>
</table>

Tabla 23: Hoja de trabajo. Actores con acceso a la red y físico.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

Motivo	**Historia**

¿Qué tal fuerte es el motivo del actor?			¿Qué tan confiado esta de este estimado?			¿Con que frecuencia ha ocurrido esta amenaza en el pasado?	¿Qué tal exacto son estos datos?		
Alto	**Medio**	**Bajo**	**Muy**	**Algo**	**Nada**		**Muy**	**Algo**	**Nada**

Tabla 24: Hoja de trabajo. Actores con acceso a la red y físico.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

Problemas del sistema						
Amenaza. ¿Para cual rama hay una posibilidad no desdeñable de una amenaza a un activo? Marcar estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marcar estas ramas.			**Historia.** ¿Con que frecuencia ha ocurrido esta amenaza en el pasado?	¿Qué tal exacto son estos datos?		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
Nombre del activo critico elegido.	- Defectos de software. - El sistema se cae. - Defectos de hardware. - Código malicioso.	- Revelación. - Modificación - Perdida - Interrupción.				

Tabla 25: Hoja de trabajo. Problemas del sistema.

Fuente: (Alberts, Dorofee, Stevens, y Woody, 2005).

3.3 Fase 2: Identificar vulnerabilidades en la infraestructura.

Según la tabla presentada a continuación, se describe los procesos, actividades y pasos que sigue la fase 2.

Fase	Proceso	Actividad	Pasos
Fase 2: Identificar vulnerabilidades de la Infraestructura	Proceso S3: Examinar la infraestructura computacional en relación con los activos críticos.	S3.1 Examinar rutas de acceso.	17,18
		S3.2 Analizar procesos relacionados con la tecnología.	19,20,21

Tabla 26 Procesos, Actividades y Pasos de la Fase 2, OCTAVE-S.

Fuente: (Flores y Melo, 2013)

3.3.1 Proceso S3: Examinar la infraestructura computacional en relación con los activos críticos.

3.3.1.1 *Actividad S3.1: Examinar rutas de acceso.*

En esta actividad se desarrollan los pasos 17 y 18 descritos a continuación:

Paso 17: Principalmente se debe determinar cuál es el sistema que está más estrechamente ligado a cada activo crítico, y así poder identificar cual es el sistema de interés.

Paso 18: Según se lo necesite este paso puede ser sub dividido en 5 sub pasos.

Como primer punto se debe examinar cuales son las rutas de acceso a la información, para continuar determinando que clase de componentes se utilizan para transmitir información desde el sistema de interés.

Otro sub paso es determinar qué clase de componentes pueden utilizar las personas (usuarios, atacantes) para acceder al sistema de interés.

Para terminar, se analiza cuáles son los componentes que se utilizan para respaldar la información del sistema de interés.

3.3.1.2 *Actividad S3.2: Analizar procesos relacionados con la tecnología.*

En esta actividad se desarrollan los pasos 19, 20 y 21 descritos en la tabla 26 del capítulo.

Paso 19: Se determina la clase de componentes que están vinculados o tienen con los activos críticos analizados anteriormente.

Paso 20: Asignamos la responsabilidad de quien mantiene y se encarga de cada clase de componente en la red.

Paso 21: En el último paso de la fase 2 para la implementación de la metodología de gestión de riesgos informáticos OCTAVE-S, se debe estimar un grado en el que la seguridad es considerada en los procesos de configuración y mantenimiento de los componentes de la red.

3.4 Fase 3: Desarrollo de planes y estrategias de seguridad.

En la última fase es donde se realizan los planes de seguridad y se toman las mejores decisiones con respecto a los resultados obtenidos.

Según la tabla presentada a continuación, se describe los procesos, actividades y pasos que sigue la fase 3.

Fase	Proceso	Actividad	Pasos
Fase 3: Desarrollo de estrategias y planes de seguridad	Proceso S4: Identificar y analizar los riesgos	S4.1 Evaluar el impacto de las amenazas.	22
		S4.2 Establecer criterios de evaluación probabilística.	23
		S4.3 Evaluar probabilidades de amenazas.	24
	Proceso S5: Desarrollar estrategias de protección y planes de mitigación.	S5.1 Describir las estrategias de protección actuales.	25
		S5.2 Seleccionar aproximaciones de mitigación.	26,27
		S5.3 Desarrollar planes de mitigación de riegos.	28

		S5.4 Identificar cambios en las estrategias de protección.	29
		S5.5 Identificar los siguientes pasos.	30

Tabla 27 Procesos, Actividades y Pasos de la Fase 3, OCTAVE-S.

Fuente: (Flores y Melo, 2013)

3.4.1 Proceso S4: Identificar y analizar los riesgos.

El proceso se centra en la evaluación de impacto y la probabilidad que tienen las amenazas en los activos críticos, también se establece los criterios de evaluación de la probabilidad.

Para ello consta de varias actividades seguidamente descritas:

3.4.1.1 Actividad S4.1: Evaluar el impacto de las amenazas.

Paso 22: Se debe analizar el impacto que tiene cada uno de los activos críticos identificados en las diferentes áreas de la organización.

Las áreas que propone OCTAVE-S en sus hojas de trabajo son:

- Reputación/Confianza del cliente.
- Financiera.
- Productividad.
- Multas.
- Seguridad.
- Otros.

3.4.1.2 Actividad S4.2: Establecer criterios de evaluación probabilística.

Paso 23: Definir las medidas para calcular la probabilidad de ocurrencia de una amenaza, basándose en la frecuencia con la que estos eventos han ocurrido anteriormente.

Estas probabilidades son estimadas basándose en los datos objetivos y experiencia del grupo de análisis.

Cabe recalcar que es una actividad opcional.

3.4.1.3 Actividad S4.3: Evaluar probabilidades de amenazas.

Paso 24: Para poder desarrollar este paso, se necesita de los criterios de evaluación de probabilidad definidos en el paso 23, estos criterios nos servirán para asignar un valor de probabilidad (alta, media, baja) para cada amenaza.

3.4.2 Proceso S5: Desarrollar estrategias de protección y planes de mitigación.

El proceso además de desarrollar estrategias de protección y planes de mitigación, realiza actividades para la toma de decisiones mediante los resultados obtenidos de la evaluación de la metodología OCTAVE-S.

3.4.2.1 Actividad S5.1: Describir las estrategias de protección actuales.

Paso 25: Se trasfiere el estado de semáforo de cada área de prácticas de seguridad. Para cada área identificamos el enfoque actual de la organización para hacer frente a las amenazas presentadas.

OCTAVE-S divide a las 15 prácticas de seguridad en dos áreas:

Área de práctica de seguridad estratégica.	**Área de práctica de seguridad operacional.**
1. Concienciación y formación en seguridad. 2. Estrategias de seguridad. 3. Gestión de seguridad. 4. Políticas y regulaciones de seguridad. 5. Gestión de la seguridad colaborativa. 6. Planes de contingencia.	7. Control de acceso físico. 8. Monitoreo y auditoria de seguridad física. 9. Gestión de sistemas y redes. 10. Monitoreo y auditoria de seguridad TI. 11. Autenticación y autorización. 12. Gestión de vulnerabilidades. 13. Encriptación 14. Diseño y arquitectura de seguridad. 15. Gestión de incidentes.

Tabla 28 Áreas de las prácticas de seguridad.

Fuente: (Flores y Melo, 2013)

Para el correcto desarrollo de este paso se debe tomar en cuenta varios puntos:

- El estado del semáforo.
- El grado en que cada práctica de seguridad se refleja en la organización en cada área de la misma.
- Lo que la organización está realizando bien o mal actualmente en cada área.

3.4.2.2 Actividad S5.2: Seleccionar aproximaciones de mitigación.

En esta actividad se desarrollaran los pasos 26 y 27.

Paso 26: En este paso transferimos el estado de semáforo para cada área de práctica de seguridad, con ello se tiene una visión global de la interacción de los árboles de amenaza con las áreas de prácticas de seguridad.

Paso 27: Para terminar la actividad se debe seleccionar las áreas de prácticas de seguridad a las que se va implementar actividades de mitigación, estas áreas son conocidas también como "áreas de mitigación".

OCTAVE-S recomienda seleccionar 3 áreas con ello centrarse en mitigar los riesgos más importantes. Para poder seleccionar estas áreas no existe algún método, sino se basa en el criterio del equipo de análisis.

3.4.2.3 Actividad S5.3: Desarrollar planes de mitigación de riesgos.

Paso 28: Se desarrollará los planes de mitigación de riesgos para las áreas seleccionadas en el paso anterior.

Un plan de mitigación de riesgos tiene como objetivo reducir el riesgo a un activo crítico, y generalmente incorporan actividades o medidas para contrarrestar las amenazas a los activos.

3.4.2.4 Actividad S5.4: Identificar cambios en las estrategias de protección.

Paso 29: En este paso se revisa cada una de las áreas seleccionadas y se verifica si existe un cambio que se presente en la estrategia de protección para la respectiva área de práctica de seguridad.

Estos cambios generalmente surgen en los cambios de roles y responsabilidades

3.4.2.5 Actividad S5.5: Identificar los siguientes pasos.

Paso 30: En este último paso se determina un conjunto de actividades para facilitar la implementación de los resultados obtenidos, es decir pasos para la toma de decisiones.

Estos pasos o actividades según propone OCTAVE-S son las siguientes:

- Relación de las evaluaciones posteriores.
- Monitoreo de la implementación del plan.
- Aplicación de las actividades de mitigación.
- El apoyo por parte de los altos funcionarios.

3.5 Alineación con el estándar ISO27001.

OCTAVE-S al igual que el estándar ISO 27001, adopta el ciclo de Deming o Plan de Mejora Continua (Planear, Hacer, Verificar y Actuar).

La clasificación de los activos de información, la metodología lo realiza clasificando en Sistemas, Aplicaciones, Información y Personas, al igual que el estándar ISO 27001 lo clasifica en Software y Hardware.

Otros aspectos importantes que se basa la metodología OCTAVE-S con el estándar ISO 27001 son:

- Identificación de los riegos.
- Propiedad de los activos críticos.
- Identificación y evaluación de los impactos.
- Gestiones de cambios.

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 2".*

3.6 Vinculación con el estándar ISO27002.

Al igual que con el estándar anterior, existe una cierta relación con la metodología OCTAVE-S, dándose al momento de realizar la evaluación de los impactos que tienen las amenazas en la organización y desarrollando planes de mitigación de riesgos. OCTAVE-S lo denomina como una fase llamada "Desarrollo de estrategias y planes de seguridad,

siendo en gran parte muy similar al estándar, ya que, brinda indicaciones del como evaluar, tratar los riesgos de seguridad, realizar la gestión de los activos, clasificar la amenazas y buscar la seguridad de la organización tanto física como ambiental.

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 2".*

3.7 Relación con el estándar ISO27005.

OCTAVE-S tiene relación con este estándar en la identificación de los activos de información, identificación, evaluación y control de los riesgos, realizando una serie de procesos bien detallados y fáciles de implementar, con la ayuda del "**grupo de análisis**", el cual recolecta toda la información a utilizar.

Un proceso y no menos importante que tiene relación con este estándar es el "*Crear perfiles de amenaza*", llamado así por la metodología OCTAVE-S, en donde se desarrollan los criterios de evaluación de los riesgos los cuales son monitoreados, estos criterios pueden ser Confidencialidad, Integridad y Disponibilidad.

Por último, el desarrollo de planes de mitigación de los riesgos para la toma de decisiones.

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 2".*

3.8 Alineación con el estándar ISO31000.

Siendo de igual manera un estándar internacional para la gestión del riesgo, posee varias similitudes con la metodología OCTAVE-S, proponiendo una serie de fases tales como:

- Identificación de los riesgos: donde se identifica la fuente y el área donde afectan los riesgos identificados, así como determinar las causas y consecuencias potenciales.
- Monitoreo y Revisión.
- Analizar el grado de madurez que la organización posee para la gestión del riesgo.
- Definir claramente las funciones y las responsabilidades del proceso.

Principalmente este estándar se alinea con la OCTAVE-S realizando un monitoreo y revisión de los planes de seguridad para un correcto control del riesgo y la toma de decisiones.

Nota: *Para ver el cuadro comparativo más detallado ver "Anexo 2".*

3.9 Conclusiones del capítulo.

Se deduce del capítulo presentado que, la metodología OCTAVE-S es una alternativa viable para evaluación de riegos informáticos, ya que considera tanto temas organizacionales como técnicos, examinando la forma en la que la gente emplea la infraestructura a diario.

Para la implementación de la metodología mencionada, se necesita de un grupo llamado el ***"equipo de análisis",*** de entre 3 a 5 personas que entienda la amplitud y profundidad de la organización, para que, en equipo trabajen enfocados a las necesidades de seguridad, balanceando dos aspectos: Riesgos operativos y Prácticas de seguridad.

Este equipo desarrolla la recopilación de información sobre los elementos importantes, los requisitos de seguridad, las amenazas y prácticas de seguridad, que luego permitirán el desarrollo de cada una de las fases con sus respectivas hojas de trabajo.

OCTAVE-S se basa en tres grandes fases o procesos, donde se examina temas organizacionales y tecnológicos. Se compone de reuniones organizadas y llevadas a cabo por el equipo de análisis. Las fases son:

1. Identificar los elementos críticos y las amenazas de los activos.
2. Identificación de las vulnerabilidades.
3. Desarrollo de estrategias y planes de seguridad.

Cada una de las fases está sub divididas en actividades y pasos a seguir, cada uno con sus hojas de trabajo para obtener información de la organización y tomar decisiones en cada una de las reuniones que se tengan.

OCTAVE-S solo incluye una exploración limitada de la infraestructura informática. Las pequeñas empresas con frecuencia externalizan sus procesos de TI por completo y no tienen la capacidad de ejecutar o interpretar los resultados de las herramientas de vulnerabilidad.

Uno de los puntos importantes del capítulo, es la alineación que tiene esta metodología con las normativas ISO, ya que toma de cada uno de los estándares o normativas puntos que son de gran importancia para su desarrollo, tales como: la identificación y selección de los

activos críticos, criterios de la evaluación de impacto, identificar amenazas de los activos críticos entre otros.

OCTAVE-S es una metodología que se puede implementar de preferencia en pequeñas organizaciones de forma gratuita, ya que posee procesos y actividades de fácil desarrollo e implementación.

CAPÍTULO 4: Análisis comparativo entre las normativas Security Risk Managment Guide de Microsoft y OCTAVE – S

Introducción:

Luego de haber estudiado a fondo las mencionadas normativas tanto en su funcionamiento e implementación, el siguiente paso es realizar una comparación entre las dos metodologías estudiadas, para poder sugerir la más apropiada para el mercado meta (MPYMES ecuatorianas). Entre los principales procesos a comparar y de manera general se mencionan: establecer los criterios de evaluación de impacto, identificación de activos de información, prácticas de seguridad, identificación de riesgos, amenazas y vulnerabilidades y la evaluación de los mismos, identificación de procesos tecnológicos, etc. Luego de analizar los ya mencionados puntos, se hace la comparación de las tareas de: definir planes de protección a incidencias, definir políticas internas de control, establecer planes de mitigación de riesgos.

Finalmente, las metodologías realizan las actividades que servirán para: seleccionar una estrategia de mitigación, calcular el costo de cada solución, cálculo del nivel de riesgo, así como su reducción, verificación del programa de control (el más efectivo), además de realizar el "cálculo del riesgo residual" el cual se basa en el cómputo del nivel del riesgo inherente dividido para la eficacia del control, dando como resultado la valoración de este riesgo.

Resultados de la comparación

Luego de haber evaluado cada una de las metodologías y su alineación con las normativas ISO utilizadas en la gestión de riesgo, el siguiente paso consiste en comparar Secure Risk Management con OCTAVE, a manera de extraer los aspectos más relevantes de estas dos metodologías.

A continuación, se presenta una tabla en donde se muestran las actividades y/o procesos correspondientes, identificando similitudes y diferencias que servirán para la gestión de riesgos de seguridad.

El cuadro comparativo detallado se lo puede ver en la sección "Anexo 3".

Conclusiones del trabajo

Como bien se sabe los riesgos tanto de seguridad informática como los de seguridad de información afectan a cada organización o empresa ya sea directa o indirectamente, esto debido a que la gran mayoría no tiene creado un plan de administración de riesgos de seguridad. Se debe tener en cuenta que los activos de información son la parte fundamental dentro de las organizaciones, y la gestión de riesgos de estos activos compromete a todos y cada uno de los departamentos con sus respectivos integrantes. Toda la información que se maneja en una organización es responsabilidad directa del equipo de trabajo, es decir de las personas, ya que tienen el acceso y el control total con sus debidas excepciones cuando la requieran.

La empresa *Microsoft* pone a disposición de forma gratuita y en español una metodología formal denominada "*Security Risk Management Guide*" – "Guía de Administración de Riesgos de Seguridad", la cual proporciona las directrices para realizar la gestión o la administración de los riesgos de seguridad de las organizaciones, con el fin de proteger al activo más importante de las empresas que es la información. Esta metodología implementa varios procesos que ayudan al equipo de administración de riesgos a gestionar las amenazas, así como las vulnerabilidades que afectan a cada activo de información, además de crear conciencia para con los responsables y de cómo prevenir que sucedan.

Security Risk Management Guide está basada en los estándares ISO, entre los cuales se destacan: ISO 27001, 27002, 27005 y 31000, los mismos que han sido previamente estudiados, y que hablan sobre la gestión de riesgos de seguridad. De cada una de estas normativas, *Security Risk Management Guide* ha ido tomando puntos importantes para poder desarrollar una metodología que sea de fácil entendimiento para el departamento responsable de la gestión de la seguridad de información.

Security Risk Management Guide no ha sido actualizada desde el año 2006 pero desde su lanzamiento y luego del estudio realizado se adapta a las MPYMES Ecuatorianas, esto con algunos cambios recomendados por la normativa por ejemplo, en sus tablas, ya que la normativa explica que son simplemente de referencia, pero no sucede lo mismo con el valor que da a cada activo, amenaza y vulnerabilidad porque las clasifica en varias escalas que utiliza para realizar los respectivos cálculos de administración del riesgo a excepción del valor del impacto del riesgo ya que, deja en libertad para que el equipo de administración de riesgos tome sus propias decisiones. Además, provee herramientas de

ayuda y plantillas de relleno para facilitar las tareas de cada proceso. Un problema encontrado es que estas herramientas solo se han podido encontrar en el idioma inglés, aunque en la página oficial de *Microsoft* – España se desarrolla la metodología paso a paso, completamente en español.

OCTAVE-S es también una de las metodologías existentes para el análisis y control de los riesgos de seguridad de la información, proponiendo un plan de mitigación de los mismos en una organización. Para el desarrollo e implementación de OCTAVE-S, cuenta con tres grandes fases o procesos a desarrollar donde el **"equipo de análisis"** participa en todos ellos, estando conformado este equipo de 3 a 5 personas las cuales deberán conocer de manera amplia los procesos y actividades que se realizan en la organización.

Las fases y procesos de esta metodología, ayudan a gestionar las amenazas, así como las vulnerabilidades que afectan a cada activo de información, con la finalidad de crear conciencia en los responsables de cada activo de información.

OCTAVE-S por la forma y manera de implementación estudiadas, la metodología es adaptable a las condiciones de las MPYMES ecuatorianas, se puede realizar cambios en cada una de las fases conforme a lo que necesite y se pueda realizar en la organización donde se implementa la metodología. En cuanto a la toma de decisiones, el **"equipo de análisis"** se encarga de ello, con la ayuda de las plantillas adaptables al entorno de cada organización.

De igual manera que la metodología *Security Risk Management Guide,* OCTAVE-S se basa también en las normativas ISO con sus respectivos procesos, los cuales la metodología OCTAVE-S ha ido basándose en ellos y así conseguir una metodología con el estándar y calidad requerido.

Entre las metodologías *Security Risk Management Guide* y *OCTAVE – S* existen varias similitudes entre los procesos y las tareas para la gestión de riesgos de seguridad, tanto los mecanismos de identificación y valoración de: activos, riesgos, amenazas y vulnerabilidades, e inclusive, las valoraciones de los impactos son muy similares tanto en su desarrollo como en su implementación, con lo que se podrán establecer contramedidas que permitirán mitigar el riesgo.

A diferencia de *Security Risk Management Guide, OCTAVE – S* no proporciona herramientas estandarizadas para la gestión del riesgo. Esta última tiene una clasificación

adicional al momento de realizar el proceso de identificación de activos de información, denominada: “Identificación de Activos Organizacionales”, que los clasifica en: Sistemas, Aplicaciones, Información y Personas. *Security Risk Management Guide* lo realiza de manera general, identificando a los activos de información en tres grupos: Hardware, Software y Servicios de TI.

La metodología *OCTAVE – S* realiza, a manera de auditorías, un proceso denominado “Evaluar las prácticas de seguridad organizacionales”, el cual consiste en medir cada una de las áreas de la organización y verificar su grado de cumplimiento, con el fin de documentar los resultados obtenidos. Además, examina las rutas de acceso que poseen los activos de información, determinando sus componentes, y asignando responsabilidades a las personas que los administran.

En lo que hace referencia a la valoración de la probabilidad de las amenazas, la herramienta *OCTAVE – S* asigna de manera cualitativa un grado de ocurrencia (alto, medio, bajo) de amenazas a cada uno de los activos críticos, a diferencia de *Security Risk Management Guide* que deja en libertad al grupo de trabajo realizarlo mediante un debate, en el que se discute sobre la valoración para cada activo de información, la propuesta de soluciones y estimar el costo para cada una.

Luego de haber mencionado los puntos a favor como en contra de las dos metodologías estudiadas, a criterio personal de los autores de este trabajo, se puede recomendar la herramienta *Security Risk Management Guide* de la organización *Microsoft* para la correcta gestión de riesgos informáticos de las MPYMES, esto debido a que la metodología mencionada es más rápida, de fácil implementación, de menor costo y en forma general, se acopla de mejor manera al entorno de este tipo de organizaciones.

Referencias

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S. Implementation Guide, Version 1.0.*

Alejandro Sebastian, M. (2014). DISEÑO DE MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA ERP DE EP PETROECUADOR DE ACUERDO A LA NORMA ISO/IEC 27002 Y COBIT 5 . Sangolquí.

Cadena, L. S., Triviño, J. R., & Aranda, A. (2011). Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/24298/1/Articulo%20de%20Tesis%20Estudio%20del%20Estado%20del%20Arte%20de%20La%20Seguridad%20Informatica%20en%20el%20Ecuador.pdf

Castro, M. (s.f.). *surlatina*. Obtenido de surlatina: http://www.surlatina.cl/contenidos/archivos_articulos/13-el%20nuevo%20estandar%20iso%20para%20la%20gestion%20del%20riesgo.pdf

ciifen. (s.f.). Obtenido de ciifen: http://www.ciifen.org/index.php?option=com_content&view=category&id=84&layout=blog&Itemid=111&lang=es

Cordero, G. (2015). Estudio comparativo de las tecnologías MAGERIT y CRAMM, utilizadas para análisis y gestión de de riesgos de seguridad de la información. Cuenca, Azuay, Ecuador.

Dorothy, G., & Peter, M. (Marzo de 2011). *atlantis*. Obtenido de atlantis: http://www.atlantis-press.com/php/download_paper.php?id=4406

dspace. (s.f.). Obtenido de dspace: http://dspace.ups.edu.ec/bitstream/123456789/1442/5/Capitulo%202.pdf

Elizabeth, M. R. (1 de Agosto de 2014). Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/8499/1/CD-5741.pdf

Erb, M. (27 de Septiembre de 2011). *Protejete*. Obtenido de https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Flores, H., & Melo, D. (2013). *Diagnostico y Diseño de un plan de seguridad de la información de la empresa MANPOWER.* Quito.

iso27001Academi. (2015). Obtenido de iso27001Academi: http://www.iso27001standard.com/es/que-es-iso-27001/

isotools. (03 de Octube de 2013). Obtenido de isotools: https://www.isotools.org/2013/10/03/iso-27001-dominios/

Microsoft. (15 de Octubre de 2006). Obtenido de Microsoft: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.mspx

Moscoso Montalvo, P. E., & Guagalando Vega, R. N. (Agosto de 2011). *espe*. Obtenido de espe: http://repositorio.espe.edu.ec/bitstream/21000/4279/1/T-ESPE-032634.pdf

Muñoz, D. C. (24 de Febrero de 2012). *dspace*. Obtenido de space: http://dspace.ups.edu.ec/bitstream/123456789/1442/5/Capitulo%202.pdf

Sandoval, D. (s.f.). *sunai*. Obtenido de sunai: http://www.sunai.gob.ve/images/stories/PDF/Ponencias/EF/3_Daniel_sandoval.pdf

slideshare. (15 de Mayo de 2008). Obtenido de http://es.slideshare.net/guest4a7714/clasificacion-de-empresas

TORRES, S. A. (Octubre de 2014). *unimilitar*. Obtenido de unimilitar: http://repository.unimilitar.edu.co:8080/bitstream/10654/12262/1/IMPORTANCIA%20DE%20IMPLEMENTAR%20EL%20SGSI%20EN%20UNA%20EMPRESA%20CERTIFICADA%20BASC.pdf

Ulloa, S. (Febrero de 2015). *Seguridad de informática para la red de datos en una cooperativa.*

Ulloa, S. J. (Febrero de 2015). *uta*. Obtenido de uta: http://repositorio.uta.edu.ec/bitstream/123456789/8654/1/Tesis_t975si.pdf

UTE. (Diciembre de 2013). *Enfocate Revista Cientifica.*

Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Infomática.* México: AlfaOmega.

Voutssas, J. (06 de Abril de 2010). *scielo*. Obtenido de scielo: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Anexos:

Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay,

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 05 de noviembre de 2015, conoció la petición del (los) estudiante(s) **David Marcelo López Jaramillo y Santiago Andrés Vásquez Mejía** con código(s) **61044 y 46169 respectivamente**, registrado(s) en la Unidad de Titulación Especial, quien(es) denuncia(n) su trabajo de titulación denominado: **"COMPARACION ENTRE METODOLOGIAS DE GESTION DE RIESGO INFORMATICO"**en la modalidad: Proyecto de investigación y presentado como requisito previo a la obtención del título de Ingenieros de Sistemas y Telemática .-El Consejo de Facultad acoge el informe de la Junta Académica y aprueba la denuncia. Designa como Director(a) a Ing. Esteban Crespo Martínez y como miembro del Tribunal Examinador a Ing. Francisco Salgado Arteaga. De conformidad con el cronograma de la Unidad de Titulación el (los) peticionario(s) debe presentar su trabajo de titulación hasta el 11 de marzo de 2016.

Cuenca, 06 de noviembre de 2015

Dra. Jenny Ríos Coello
Secretaria de la Facultad de Ciencias de la Administración

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

Oficio Nro. 148-2015-DIST-UDA

Cuenca, 28 de Octubre de 2015

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

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 28 de octubre del 2015, recibió el proyecto de tesis titulado "Comparación entre metodologías de gestión de riesgo informático", presentado por los estudiantes David Marcelo López Jaramillo y Santiago Andrés Vásquez Mejía, estudiantes de la Escuela de Ingeniería de Sistemas y Telemática, y revisado por el Ing. Esteban Crespo, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

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 a al Ing. Esteban Crespo y como miembro del Tribunal a Francisco Salgado Ph.D.

Atentamente,

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

UNIVERSIDAD DEL AZUAY

Cuenca, 27 de Octubre de 2015

Señor Ingeniero

Xavier Ortega Vásquez

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

Su despacho

De nuestra consideración:

Nosotros, David Marcelo López Jaramillo y Santiago Andrés Vásquez Mejía, con código, 61044 y 46169, respectivamente, estudiantes de la carrera de Sistemas y Telemática, de la Facultad de Ciencias de la Administración, solicitamos comedidamente se nos apruebe el diseño del trabajo previo a la obtención del título de Ingenieros en Sistemas y Telemática.

Atentamente,

David Marcelo López Jaramillo — 61044

Santiago Andrés Vásquez Mejía — 46169

C O N V O C A T O R I A

Por disposición de la Junta Académica de Administración de Empresas, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: ***"Comparación entre metodologías de gestión de riesgo informático"***, presentado por los estudiantes **López Jaramillo David Marcelo**, con código **61044** y **Vásquez Mejía Santiago Andrés**, con código **46169,** previa a la obtención del grado de Ingeniero en Sistemas y Telemática, para el día **MARTES, 27 DE OCTUBRE DE 2015 A LAS 08:00 AM.**

Cuenca, 26 de octubre de 2015

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Esteban Crespo Martínez .....

Ing. Francisco Salgado Arteaga .....

UNIVERSIDAD DEL AZUAY

ACTA

SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** LOPEZ JARAMILLO DAVID MARCELO Y VASQUEZ MEJIA SANTIAGO ANDRES Código: 46588 y 46169
1.2 **Director sugerido**: Ing. Esteban Crespo Martínez
1.3 **Codirector (opcional)**: _____
1.4 **Tribunal:** Ing. Francisco Salgado Arteaga
1.5 **Título propuesto: (Proyectos de investigación)** "Comparación entre metodología de gestión de riesgo informático".
1.6 **Resolución**:

1.6.1 Aceptado sin modificaciones ✓

1.6.2 Aceptado con las siguientes modificaciones:

_____

_____

_____

1.6.3 Responsable de dar seguimiento a las modificaciones:
1.6.4 No aceptado
- Justificación:

_____
_____
_____

Tribunal

Ing. Esteban Crespo Martínez

Ing. Francisco Salgado Arteaga

Sr. David López Jaramillo

Sr. Santiago Vásquez Mejía

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: Martes, 27 de octubre de 2015.

1. Protocolo/Rúbrica

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: David Marcelo López Jaramillo y Santiago Andrés Vásquez Mejía
Código 61044 y 46169
1.2 Director sugerido: Ing. Esteban Crespo Martínez
1.3 Codirector (opcional):
1.4 Título propuesto: (proyectos de investigación) *"Comparación entre metodología de gestión de riesgo informático".*
1.5 Revisores (tribunal): Ing. Francisco Salgado Arteaga
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?	✓			

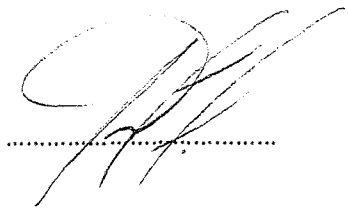
(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

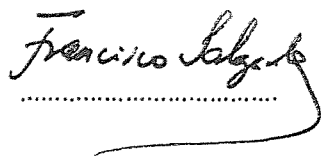
.....

.....

.....



.....



.....

.....

Universidad del Azuay.

Facultad de Ciencias de la Administración.

Escuela de Sistemas y Telemática.

"Comparación entre metodologías de gestión de riesgo informático".

Trabajo de graduación previo a la obtención del título de Ingeniero en Sistemas y Telemática.

Autor: David López – Santiago Vásquez.

Director: Crespo Martínez Paul Esteban, MBA.

Cuenca, Ecuador

2015

1. Datos generales

1.1 Nombre del estudiante: Vásquez Mejía Santiago Andrés

1.1.1 Código: 46169

1.1.2 Contacto: teléfonos: 2-841682 – 0987127710 – shanta2501@hotmail.com

1.1 Nombre del estudiante: David Marcelo López Jaramillo

1.1.1 Código: 61044

1.1.2 Contacto: teléfonos: 4110779 – 0983130176 – davidm3502@hotmail.com

1.2 Director sugerido: Crespo Martínez Paul Esteban, MBA.

1.2.1 Contacto: ecrespo@uazuayedu.ec

1.3 Asesor metodológico: Salgado Arteaga Francisco Rodrigo

1.4 Tribunal designado:

1.5 Aprobación:

1.6 Línea de Investigación de la carrera: Un proyecto integrador basado sobre la seguridad de la información.

1.6.1 Código *UNESCO*: 1203.99

1.6.2 Tipo de trabajo:

Proyecto de investigación, basado en proyectos técnicos relacionados con una gestión de seguridad de la información.

1.7 Área de estudio: Seguridad de la información.

1.8 Título propuesto: Comparación entre metodologías de gestión de riesgo informático.

1.9 Subtítulo: Evaluación de Security Risk Management Guide y OCTAVE, y su alineación con las normativas ISO 27001, 27002, 27005, y 31000.

1.10 Estado del proyecto: La propuesta realizará un estudio comparativo entre la metodología de Security Risk Managment Guide de Microsoft y OCTAVE, y su

vinculación con las normativas ISO 27001, 27002, 27005, y 31000, utilizadas para el análisis y gestión de riesgos de seguridad de la información. Este estudio se inserta en la línea propuesta en el proyecto de investigación de seguridad de la información que propone la escuela de Ingeniería de Sistemas y Telemática: "*Desarrollo de una metodología para el análisis y gestión de riesgo informático en las empresas del sector MPYME ecuatoriano*".

2. Contenido

2.1 Motivación de la investigación: Se trata de realizar un estudio comparativo que permita recomendar cuál de las metodologías existentes para el análisis y gestión de riesgos de la seguridad de la información sería adecuada para las MPYMES ecuatorianas.

2.2 Problemática: Existen muchas metodologías internacionales pero es necesario adaptarles a las condiciones propias de nuestro país. Este trabajo contribuirá a la solución de este problema realizando un estudio comparativo para análisis y gestión de riesgos de seguridad de la información.

2.3 Resumen:

En algunas empresas ecuatorianas se siguen ciertos estándares establecidos por normas que permiten introducirse en la gestión de riesgos, sin embargo para muchas de ellas el escenario se vuelve inalcanzable debido a la incompatibilidad o a la complejidad de ponerlos en marcha. En este trabajo se pretende realizar un estudio comparativo entre las metodologías "Security Risk Managment Guide de Microsoft", OCTAVE, y su alineación con las normativas ISO 27001, 27002, 27005, y 31000 en base a mecanismos para la identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo y cálculo de riesgo. El propósito final es el de recomendar una metodología para el análisis y gestión de riesgo informático adecuado para las circunstancias de las MPYMES del Ecuador.

2.4 Indagación exploratoria y base conceptual: Basado en los principios de seguridad de la información y la gestión de riesgos.

- **Seguridad de la información:** Son aquellos mecanismos que utilizan las personas, las empresas tanto pequeñas como medianas para proteger su bien más importante que es su *información.* Hay que recordar que no hay seguridad total pero se debe intentar reducir el riesgo. Existen cuatro pilares fundamentales que hacen que la información se encuentre protegida. (redusers, s.f.)
    - **Confidencialidad**

      Hace referencia a que la información puede ser accedida únicamente por la(s) persona(s) que tienen la autorización para hacerlo.

    - **Integridad**

Quiere decir que cuando se realiza alguna alteración a la información por ejemplo borrar, copiar, modificar, se debe estar seguro de que no solo se ha alterado en una pequeña parte de esta, sino también desde el origen de los datos.

- **Disponibilidad**

  Hace referencia a los métodos de precaución contra los posibles daños a la información como ataques, accidentes o general y simplemente por descuidos para poder diseñar métodos efectivos para bloquearlos.

- **Autenticidad**

  La autenticidad informa el momento y el cómo fue el acceso a la información. Aunque generalmente no se incluye este punto debido a que se suele incluir en la integridad. La autenticidad tiene tres categorías. La primera se refiere a las contraseñas, la segunda a la verificación de identidad y la última a verificación de propiedades físicas, como huellas dactilares.

- **Análisis y gestión de riesgos:**

Para una correcta gestión de riesgos el primer paso es el análisis del mismo, (Erb, 2011) "Que consiste en determinar los componentes de un sistema que necesita protección, como también sus vulnerabilidades y amenazas valorando el grado de riesgos que estos poseen".

Para el análisis de los riesgos deben tomar en cuenta que cada uno de ellos posee una característica propia, tales como:

- Dinámico y cambiante.
- Diferenciado con diferentes caracteres.
- Deben ser bien analizados con personas especialistas de diferentes elementos del sistema, (Coordinación, Administración financiera, Técnicos, Conserje, Soporte técnico externo), para que los resultados sean los correctos y esperados.

El riesgo se calcula por una formula base: Riesgo = Probabilidad de Amenaza + Magnitud de daño.

- **Security Risk Managment Guide:**

(Cobb, 2011) "Muchas de las organizaciones pequeñas dispuestos a mejorar su seguridad de la información, pero carecen de los conocimientos, ya sea en la empresa o los fondos para traer a un asesor especialista. Si bien las normas como la ISO 27001 establecen los requisitos para las mejores prácticas actuales en la seguridad de la información, no proporcionan mucha orientación sobre cómo ir sobre su aplicación, sobre todo en algunas de las áreas clave, tales como evaluaciones de riesgos.

Un kit gratuito que puede ayudar en situaciones es la Guía de Gestión de Riesgos de Seguridad de Microsoft (*Security Risk Managment Guide of Microsoft)*. El documento gratuito explica cómo planificar, construir y mantener un programa de gestión de riesgos de seguridad de éxito para medir los riesgos de seguridad y los llevan a niveles aceptables. No está dirigido únicamente a los sistemas basados en Microsoft. La guía hace referencia a muchas de las normas aceptadas por la industria para la gestión de riesgos de seguridad. Aunque no ha sido actualizado desde 2006, sigue siendo una herramienta útil y relevante, aunque parte de la información contenida en los apéndices es un poco fuera de fecha."

- **OCTAVE.**

"(Operationally Critical Threats Assets and Vulnerability Evaluation). Es una metodología de análisis de riesgos que se desarrolló en el año 2001 por la Universidad Carnegie Mellon; esta se encarga de estudiar los riesgos en base a tres principios Confidencialidad, Integridad y Disponibilidad." (Elizabeth, 2014) Al igual que la mayoría de metodologías esta evalúa vulnerabilidades y amenazas pero de recursos tecnológicos y operacionales importantes de una organización.

Hay existentes versiones de OCTAVE:

- La original OCTAVE.
- Para pequeñas empresas OCTAVE-S.
- Y una simplificada OCTAVE-ALLEGRO.

2.5 Objetivo general:

- Realizar un estudio comparativo entre las metodologías Security Risk Managment Guide de Microsoft y OCTAVE, y su relación con las normativas

ISO 27001, 27002, 27005, y 31000 para el análisis y gestión de riesgo tecnológico.

UNIVERSIDAD DEL AZUAY

2.6 Objetivos específicos:

- Sistematizar información sobre las metodologías Security Risk Managment Guide de Microsoft y OCTAVE.
- Sistematizar información sobre gestión de riesgos basado en las normativas ISO 27001, 27002, 27005 y 31000.
- Definir los atributos o variables de los sistemas a comparar.
- Comparar las metodologías Security Risk Managment Guide de Microsoft y OCTAVE y las normativas ISO 27001, 27002, 27005 y 31000, 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.

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 Security Risk Managment Guide de Microsoft y OCTAVE para la identificación de activos, vulnerabilidades, funciones de probabilidad, variable de medición y cálculo de riesgo a fin de determinar cuál es la más viable a utilizar en el proyecto de investigación de la Universidad del Azuay.

2.9 Supuestos y riesgos: No contar con acceso a la información de Security Risk Managment Guide de Microsoft y OCTAVE. Además no contar con acceso a las normativas de la familia ISO 27000 y 31000.

2.10 Presupuesto:

Rubro-Denominación	Costo USD	Justificación
Proveedor de internet	$120	Para realizar las investigaciones sobre los temas establecidos.
Impresiones	$100	Para realizar la impresión de los documentos.
Materiales de Oficina (papel, lápiz)	$10	Para realizar apuntes de cambios a realizar.
Total:	$230	

2.11 Financiamiento: Financiamiento propio.

2.12 Esquema tentativo:

ABSTRACT

INTRODUCCION

OBJETIVOS

CAPÍTULO 1: Indagación exploratoria.

1.1 Situación de la MPYMES ecuatorianas en relación a la seguridad de información.

1.2 Seguridad de la información vs. Seguridad Informática

1.3 Riesgo informático

1.4 Gestión de Riesgos

1.5 ISO 27001

1.6 ISO 27002

1.7 ISO 27005

1.8 ISO 31000

1.9 Security Risk Managment Guide de Microsoft

1.10 OCTAVE

CAPÍTULO 2: Estudio de la metodología Security Risk Managment Guide de Microsoft.

2.1 Introducción del Capítulo.

2.2 Mecanismos de identificación de activos

2.13 Cronograma:

Objetivo Específico	Actividad	Resultado esperado	Tiempo
1. Sistematizar información sobre las metodologías Security Risk Managment Guide de Microsoft y OCTAVE.	1. Organizar los conceptos de la metodología Security Risk Managment Guide de Microsoft para el Análisis y Gestión de Riesgo Tecnológico.	• Conocer teóricamente los conceptos sobre las metodologías Security Risk Managment Guide de Microsoft y OCTAVE para el Análisis Gestión de Riesgos.	**4 semanas**
2. Sistematizar información sobre gestión de riesgos basado en las normativas ISO 27001, 27002, 27005 y 31000.	1. Estudiar detalladamente las normativas ISO 27001, 27002, 27005 y 31000 con las que estamos haciendo el estudio.	• Tener un conocimiento detallado las normativas ISO 27001, 27002, 27005 y 31000.	**4 semanas**
3. Definir los atributos o variables de los sistemas a comparar.	1. Analizar que variables son las adecuadas para la comparación entre las metodologías estudiadas.	• Obtener variables o atributos para obtener una comparación adecuada.	**1 semana**
4. Comparar las metodologías Security Risk Managment Guide de Microsoft y	1. Luego de haber estudiado tanto Security Risk Managment Guide de Microsoft, OCTAVE	• Una comparación realizada entre la metodología Security Risk Managment Guide de Microsoft, OCTAVE y	**3 semanas**

OCTAVE, y su alineación con las normativas ISO 27001, 27002, 27005 y 31000, utilizadas en el análisis y gestión de riesgo informático.	y su vinculación con ISO 27001, 27002, 27005 y 31000 realizar un estudio comparativo entre la metodología y las normativas.	su vinculación con las normativas ISO 27001, 27002, 27005 y 31000.	

2.14 Referencias:

Aciar, S., Duque, N. D., & Aciar, M. (2015). Procesamiento de Opiniones de Usuarios Respecto a Objetos de Aprendizaje Basado en Ontologías y Minería de Texto. . *Conferencias LACLO*, 5 (1).

Castillo, J. J., Cardenas, M. E., Curti, A., & Casco, O. (2015). Software para asistencia en la creación de corpus para sistemas de análisis de texto no estructurado. *In XVII Workshop de Investigadores en Ciencias de la Computación.*

Cobb, M. (Mayo de 2011). *computerweekly*. Obtenido de computerweekly: http://www.computerweekly.com/tip/How-to-use-the-free-Microsoft-Security-Risk-Management-Guide

Del Fresno, M., Daly, A. J., & Supovitz, J. (2015). Desvelando climas de opinión por medio del Social Media Mining y Análisis de Redes Sociales en Twitter. *El caso de los Common Core State Standars. Revista Redes*.

Domínguez, D. C. (2010). Las Redes Sociales.Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. . *Documentación de las Ciencias de la Información*, 33, 45-68.

Elizabeth, M. R. (1 de Agosto de 2014). Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/8499/1/CD-5741.pdf

Erb, M. (27 de Septiembre de 2011). *Protejete*. Obtenido de https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Feldman, R., & Sanger, J. (2007). The text mining handbook: advanced approaches in analyzing unstructured data. . *Cambridge University Press*.

García-García, A., García-Massó, X., Ferrer-Sapena , A., González, L. M., Peset, F., Villamón, M., & Aleixandre, R. (2014). Text mining versus redes neuronales. Dos métodos de análisis aplicados al caso de las políticas de las revistas sobre datos.

Lobos, C., & Bartolome, L. (2012). Metodología de búsqueda de sub-comunidades mediante análisis de redes socialeas y minería de datos.

Mansilla, P. S., Costaguta, R., & Missio, D. (2014). Aplicación de Algoritmos de Clasificaación de Minería de Textos para el Reconocimiento de Habilidades de E-tutores Colaborativos. . *Revista Iberoamericana de Inteligencia Artificial*, 17 (53), 57-67.

McDonell, R., De la Fuente Aragón, M. V., & McDonnell, R. (2012). Minería de Datos Aplicada a la Gestión de la Información Urbanística Data Mining Applied to Urban Information Management. *In 6th Internacional Conference on Industrial Engineering and Industrial Management*, pp. 1476-1483.

redusers. (s.f.). Obtenido de redusers: http://img.redusers.com/imagenes/libros/lpcu082/capitulogratis.pdf

Rodriguez Aldape, F. (2013). Cuantificación del interés de un usuario en un tema mediante minería de texto y análisis de sentimiento. *Doctoral dissertation. Universidad Autónoma de Nuevo León*.

Tascón, M. (2013). Introducción: Big Data. Pasado, presente y futuro. . *Telos: Cuadernos de comunicación e innovación*, (95) 47-50.

2.15 Firma de responsabilidad (Estudiante)

David Marcelo López Jaramillo

Santiago Andrés Vásquez Mejía

2.16 Firma de responsabilidad (Director Sugerido).

MBA. Crespo Martínez Paúl Esteban

2.17 Fecha de entrega: 27 de Octubre del 2015.