VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES

TESIS PREVIO A LA OBTENCION DEL TÍTULO DE MAGISTER

TEMA: MODELO DE MADUREZ PARA GESTIÓN DE SEGURIDAD DE REDES DE INFORMACIÓN APLICABLE A PYMES ECUATORIANAS

AUTOR: GUADALUPE RAMOS, MÓNICA ALEXANDRA

DIRECTOR: CRNL. CHÁVEZ, EDWIN

SANGOLQUI

2015

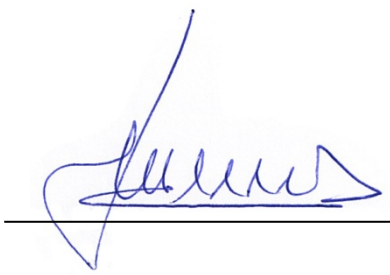
UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES

CERTIFICAN

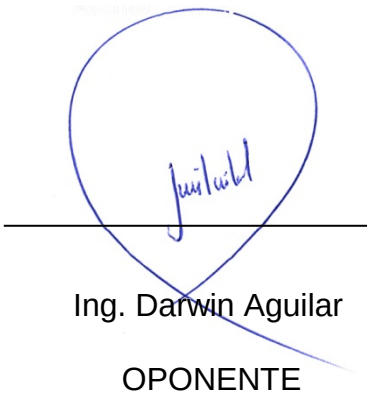
Que el trabajo titulado “MODELO DE MADUREZ PARA GESTIÓN DE SEGURIDAD DE REDES DE INFORMACIÓN APLICABLE A PYMES ECUATORIANAS” realizado por la Ing. Mónica Guadalupe ha sido guiado y revisado periódicamente y cumple con las normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerza Armadas, por lo que recomendamos su publicación.

Sangolqui, mayo del 2015



Crnl. Edwin Chávez Morillo

DIRECTOR



Ing. Darwin Aguilar

OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES

Yo, Mónica Guadalupe

DECLARO QUE:

El proyecto de grado denominado “MODELO DE MADUREZ PARA GESTIÓN DE SEGURIDAD DE REDES DE INFORMACIÓN APLICABLE A PYMES ECUATORIANAS”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolqui, mayo del 2015

Mónica Guadalupe

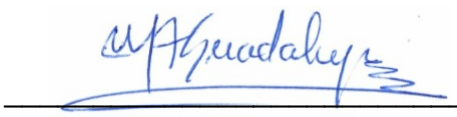
UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Mónica Guadalupe

Autorizo a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la Institución del trabajo denominado “MODELO DE MADUREZ PARA GESTIÓN DE SEGURIDAD DE REDES DE INFORMACIÓN APLICABLE A PYMES ECUATORIANAS”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolqui, mayo del 2015



Mónica Guadalupe

DEDICATORIA

A mis padres y hermanos por su valioso apoyo y motivación para mi constante crecimiento personal y académico.

Mónica

AGRADECIMIENTO

A Dios, por haberme permitido superar todos los desafíos para la consecución de un objetivo más en mi formación y superación personal.

A mi familia, por no permitir que claudique en la consecución de mis objetivos e impulsarme para cada vez llegar más lejos.

A mis maestros y compañeros de maestría, por compartir momentos de investigación, estudio y camaradería a lo largo del tiempo de estudios.

Al Crnl. Edwin Chávez, director de tesis, por su apoyo, orientación y asesoría en el desarrollo de este proyecto de tesis, además de sus acertados consejos y recomendaciones para su culminación.

Mónica

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

Esta investigación tuvo por objetivo determinar un modelo de madurez que sea base para la evaluación de la seguridad de las redes de información en las PYMES ecuatorianas. Para ello se planteó el problema y se definieron los conceptos preliminares que permitieron iniciar el estudio a través de una encuesta online. Una vez analizados los resultados de dicha encuesta se logró determinar el nivel de conocimiento, aplicación e interés de los modelos de madurez dentro del área de seguridad de las Pymes. Respaldados por la investigación bibliográfica y los resultados obtenidos en la encuesta, se determinaron los modelos de madurez que sirvieron de base para la formulación del nuevo modelo. A fin de realizar un análisis objetivo de los modelos de madurez, se establecieron los parámetros básicos que estos debían cumplir; obteniéndose una nueva propuesta basada en los modelos ampliamente aceptados: CMM e ISM3. De esta forma se proporciona una visión general inicial de este tema que incentive su estudio y aplicación en nuestro medio, especialmente en el área tecnológica y posible de ser aplicado en nuestro entorno sin la necesidad de grandes inversiones. Finalmente se establecieron las conclusiones obtenidas en el desarrollo de esta investigación y las recomendaciones de trabajo a futuro.

Palabras clave:

- **MODELO DE MADUREZ**
- **ISM3**
- **CMM**
- **SEGURIDAD DE REDES**

ABSTRACT

The purpose of this research was determined a maturity model as a basis for evaluating the information security networks in the Ecuadorian SMEs. At the beginning, the problem was propounded and preliminary concepts that allowed starting the study through an online survey were defined. After analyzing the results of this survey, the level of knowledge, application and interest maturity models within the information security area of SME's were determined. Supported by bibliographical research and survey results, maturity models that were the basis for the formulation of the new model were determined. In order to conduct an objective analysis of maturity models, the basic parameters that they had to meet were established; obtaining a new proposal based on the widely accepted models: CMM and ISM3. With this proposal an initial overview of the topic that encourages study and application in our environment, especially in the technology area and can be applied in our surroundings without the need for large investments is provided. Finally the conclusions reached in the development of this research and recommendations for future work were established.

Key words:

- **MATURITY MODEL**
- **ISM3**
- **CMM**
- **NETWORKS SECURITY**

CAPITULO I

PROBLEMÁTICA DE LA SEGURIDAD EN LAS PYMES

1.1 Antecedentes

La Información y el conocimiento constituyen el corazón de importantes cambios e innovaciones en las organizaciones. Para llegar a un conocimiento de calidad, las organizaciones deben asegurarse de la calidad de su información. Esto sólo se logra, cuando se dispone de los procesos y tecnologías con madurez suficiente para mantener la cadena de valor de la información desde los datos, hasta la generación del conocimiento, de manera que satisfagan las necesidades del negocio de acuerdo a su misión y estrategia.

Con más frecuencia las empresas se están apoyando en la automatización de los sistemas de información, en los avances de las comunicaciones y en Internet, haciéndose por lo tanto más dependientes de la tecnología. Por otro lado, una interrupción en el funcionamiento de los sistemas informáticos de una empresa (originados por cualquier causa, tales como desastres naturales, interrupción de suministro eléctrico o ataques de virus, entre otros), afectaría directamente su funcionamiento o actividades.

Lo relacionado a la seguridad informática tanto en el sector público como privado es muy importante, dado que frecuentemente es parte de la infraestructura crítica, que procesa, almacena y presenta datos personales o sensibles.

Debido al incremento en la demanda de profesionales en seguridad informática, de redes o de información, muchas organizaciones han creado programas de especialización en estas áreas; no obstante, la demanda sigue siendo alta.

Por ejemplo, con la intención de continuar mejorando la concientización sobre seguridad que al mismo tiempo ponen en riesgo la seguridad de los usuarios, año tras año Microsoft invierte alrededor de 2 mil millones de dólares (rickymartinfoundation, 2008) en investigación y educación sobre seguridad de la información; una iniciativa global para lograr una experiencia de computación más confiable.

De acuerdo al Deloitte 2010 Financial Services Global Security Study (Deloitte, 2010), las organizaciones de América Latina muestran un incremento importante en relación al estudio realizado 3 años atrás, en el que varias instituciones financieras reconocen ahora más que nunca, la importancia de las mediciones de desempeño y puntos de referencia para ayudar a administrar los sistemas y procesos complejos.

Es así que mientras en el año 2007, en América Latina los encuestados indicaron que sus Gastos en la Seguridad de la Información fueron "en plan " o "por delante de las necesidades" en un 50%, para el año 2010 este porcentaje correspondió al 58%. Sin embargo los encuestados que indicaron que “había una estrategia de seguridad de la información definida y documentada” formalmente fueron el 68% en el 2007 y en el 2010 alcanzaron un 54%, esto se justifica debido a la recesión económica mundial que obligó a muchas empresas a recortes de presupuestos, sacrificando áreas que no eran vitales para el funcionamiento del negocio.

En cuanto a nuestro país se refiere, no existen informes con evaluaciones sistemáticas o científicas que proporcionen un “feedback” sobre el estado de la seguridad en las organizaciones así como su viabilidad y beneficios. En este contexto, a pesar de la importancia que hoy en día se debe dar a la seguridad de los activos, se puede observar que la

alta gerencia no se preocupa mucho porque se evalúe e implemente mecanismos de seguridad.

En los últimos años se ha visto un incremento en los ataques a los sistemas informáticos de las empresas. Estos ataques van dirigidos a empresas, instituciones y organizaciones públicas y privadas.

Según lo describe Deloitte en su informe, las principales barreras que se enfrentaron para garantizar la seguridad de la información en el año 2010 fueron cuantificados de la siguiente manera (Deloitte, 2010):

•36%: Falta de suficiente presupuesto.

•31%: Incremento en la sofisticación de las amenazas.

•24%: Tecnologías emergentes.

•21%: Falta de visión e influencia dentro de la organización.

•19%: Falta de soporte desde las líneas de negocios.

•19%: Falta de claridad en el mandato, roles y responsabilidades.

Es evidente que el estudio demuestra que las barreras más grandes para garantizar seguridad de la información provienen de la falta de organización y compromiso internos, antes que de agentes externos solamente.

Por otro lado, han surgido múltiples metodologías y estándares para manejar la seguridad como: ISO 27001:2005 (International Organization for Standardization), CMM (Capability Maturity Model), COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library), ISM3 (Information Security Management Maturity Model), entre otros. Sin embargo, se requiere incorporar los cambios necesarios para que se ajusten a los requerimientos particulares de

cada empresa y así, permitir afianzar el proceso de seguridad personalizado para cada organización, medir su capacidad y establecer los planes de mejora que se deseen alcanzar.

1.2 Definición del Problema

Las metodologías existentes para la gestión de la seguridad y su madurez, resultan complejas, costosas y requieren de tiempos largos para su aplicación. Es por esto, que son justamente las Pymes, las que tienen mayor tasa de fracaso en la implantación de metodologías y normativas de gestión de la seguridad existente.

En la actualidad un plan estratégico bajo una perspectiva de la seguridad de la información es un factor crítico de éxito para cualquier empresa que ha adaptado y utiliza en sus actividades diarias Sistemas de Información y las Tecnologías de la Información y la Comunicación. Este plan debe poseer un enfoque sistémico, ya que para ser completo abarca aspectos relacionados con: la seguridad lógica y la seguridad física, el factor humano, el compromiso de la gerencia, la cultura y la estructura organizacional.

Se evidencia que los métodos tradicionales de seguridad, generalmente eran reactivos ante ataques; hoy en día ya no son suficientes para combatir estos ataques organizados, pudiéndose afirmar que la seguridad cobra cada día mayor importancia en el mundo. Pero, la seguridad no debe ser percibida como una respuesta meramente tecnológica, más bien debe ser vista como una estrategia con visión global, que comprende el análisis de los procesos de la organización para determinar qué mecanismos se deben desplegar y dar apoyo a las políticas definidas. Por lo tanto, se debe trabajar con un proceso estructurado apoyado en metodologías, normas y estándares.

Dentro de este contexto, son las Pymes las que mayoritariamente, tienen la necesidad de mejorar sus procesos de seguridad pero aún no saben por dónde comenzar, no cuentan con un presupuesto y en muchas ocasiones, no consiguen el compromiso de los directivos.

En este mismo orden de ideas, es necesario obtener un modelo de madurez que se transforme en una formulación teórica que sirva como herramienta para aquellos trabajadores de tecnología, encargados de la seguridad de la información, redes y/o comunicaciones y que al mismo tiempo ayude en la comprensión del problema en sus organizaciones y a disminuir la incertidumbre.

1.3 Alcance

Este proyecto comenzó con un proceso de recolección de información a través de encuestas, con el propósito de obtener datos de la utilización actual de algún tipo de modelo de madurez en el proceso de implementación y evaluación de la seguridad en redes de información dentro de organizaciones de diferentes sectores de la pequeña industria.

La presente investigación se centró en la identificación de los ejes fundamentales o relevantes de los modelos de madurez existentes a fin, de definir lineamientos con el mínimo grado de complejidad posible, que facilite su aplicación y al mismo tiempo, permita obtener el mayor nivel de automatización con una información mínima, recogida en un tiempo muy reducido, garantizando la calidad suficiente a la consecución del estudio.

Por lo tanto el alcance de este trabajo abarcó el análisis y posterior definición de un modelo de madurez “base” aplicable a todos los sectores de la Pequeña y Mediana Industria Ecuatoriana, sin pretender estructurar una normativa específica enmarcada solamente en la teoría científica, sino más

bien, articular una propuesta con orientación práctica sin descuidar la normativa existente.

Al finalizar la tesis se obtuvo una herramienta de evaluación práctica, capaz de aplicarse a cualquier entorno con la mínima inversión posible de recursos humanos, tecnológicos y financieros.

1.4 Justificación e Importancia

En la actualidad, las empresas se enfrentan a un mundo que se encuentra en un proceso de globalización, lo que hace que diariamente se estén produciendo cambios significativos en cualquier área en donde se encuentren; esto a su vez, hace necesario que las empresas sean competentes, para los cual se requiere que ésta sea evaluada por otra empresa o bien por personas certificadas que, empleando un criterio experto, certifiquen que la empresa lleva a cabo todos sus procesos de una manera adecuada lo que la lleva a que un producto o la prestación de un servicio sea de alta calidad y tenga mayor aceptación con sus proveedores y clientes.

Sin embargo, el llegar a obtener estas certificaciones acarrea consigo grandes inversiones de tiempo y recursos económicos por lo que, en la mayor parte de los casos las Pymes dejan fuera de sus objetivos el cumplir con las normativas que no reflejan de forma directa un beneficio económico.

De la necesidad de las empresas por certificarse en seguridad, es de donde se origina el requerimiento de un modelo de madurez que es una guía de evaluación de los procesos de una organización; es decir, es una especie de manual que se debe seguir para lograr de esta manera calidad, confiabilidad y seguridad.

Para una empresa el seguir un modelo de madurez trae diferentes beneficios sin importar en qué nivel se encuentre. El modelo ayuda a las empresas a entender lo que está pasando, por qué está pasando y esa comprensión de las falencias en los procesos de una empresa le ayuda a tomar acciones correctivas a los procesos que están fallando, ayuda a enfocar los esfuerzos de la empresa en lograr los objetivos planteados por la misma, a lograr que el personal trabaje de manera eficiente y desarrolle su potencial en pro al continuo crecimiento y al proceso de mejora continua de la empresa.

Por otra parte, la madurez en los procesos hace que la empresa sea mucho más exitosa y mucho más competitiva en el mercado, logrando de esta manera qué sus productos y/o servicios sean de alta calidad sin importar si se es nivel 2 o nivel 5; cada nivel significa mejora continua, en cada nivel las empresas encontraran nuevas falencias, nuevas cosas que corregir y nuevos procesos que implantar dentro de la organización. El ir avanzando por los diferentes niveles hace que las empresas adquieran un nivel de madurez mucho más elevado, hace que toda la empresa apunte a un mismo objetivo, algo que se torna casi imposible para las empresas que no optan por seguir un modelo definido.

Es decir que, los niveles de madurez facilitan, optimizan y priorizan la inversión para el aseguramiento de las redes de información.

Por lo anterior, un enfoque adecuado podría ser la implantación, no de un modelo único, sino de una combinación de modelos que, al unir sus fortalezas, se convierta en una estrategia poderosa que conduzca al mejoramiento integral de manera ordenada e incremental, de largo plazo, con hitos claros y alineados con los objetivos del negocio.

El proyecto de investigación planteado tiene objetivos claros, y pretende abordar un problema real, que actualmente se presenta en nuestras Pymes.

Y es que la seguridad, finalmente, hay que entenderla como un objetivo necesario al que toda la organización debe contribuir, ya que no es un tema netamente tecnológico. Para esto un modelo de madurez, basado en buenas prácticas, permite organizar el área de IT (Information Technology) e implementar medidas a corto y largo plazo que beneficien el funcionamiento del negocio. Además las empresas que implementan un modelo de madurez y muestran un crecimiento medido, son más propensas a adherirse con éxito a otros estándares de la industria.

1.5 Problemática de la seguridad en las PYMEs de América Latina

De acuerdo a una publicación de Universia (Universia, 2008), las Pymes constituyen entre el 90% y 98% de las unidades productivas en América Latina, generan alrededor del 63% del empleo y participan con el 35% y hasta 40% por ciento del producto total de la región, según coinciden los más recientes estudios de organismos como el Banco Mundial, el Banco Interamericano de Desarrollo y la Comisión Económica para América Latina (Cepal).

Están en todos los sectores, desde el comercio y la industria, hasta los servicios, la salud y el sistema financiero y según las estadísticas del Banco Mundial son el soporte del tejido social de todo el continente, ya que se encuentran en grandes centros urbanos, ciudades intermedias, poblaciones pequeñas y los más remotos y apartados sitios rurales, especialmente en países agrícolas como Ecuador, ya que se dedican a las más diversas actividades de la producción agropecuaria.

Sin embargo, las Pymes, padecen diversos problemas que les restan eficiencia, productividad y competitividad. “Son tantas sus dificultades como el mismo número de ellas, y aunque no existe Gobierno que las incorpore a sus políticas sociales –incluidas leyes, decretos y resoluciones-, su rezago con la gran empresa es apreciable”, afirma el presidente del Instituto

Latinoamericano de Liderazgo (Universia, 2008), consultor internacional y profesor universitario, Jorge Yarce Maya.

1.5.1 Atraso tecnológico

Las Pymes invierten poco en tecnología, y cuando lo hacen, muchas veces adquieren equipos, maquinaria y software que no son apropiados. ¿Por qué? “Porqué para modernizarse primero hay que enfocarse en el eje del negocio y después sí pensar en la tecnología”, señala Juan Carlos López, ejecutivo de la consultora multinacional de tecnología y negocios Neoris (Universia, 2008).

Como indica la Figura 1.1, el estudio de Symantec en el año 2012, muestra que a pesar de que la mayoría de ejecutivos invierten entre el 1% y 5% de su presupuesto en IT, se encuentra en porcentajes similares a los que invierten el 10%. Existe un 20% que invierte un porcentaje considerable (más del 10%) en seguridad, sin embargo, también tenemos un gran grupo que invierte menos del 1%, esto indica que la seguridad todavía es subestimada.

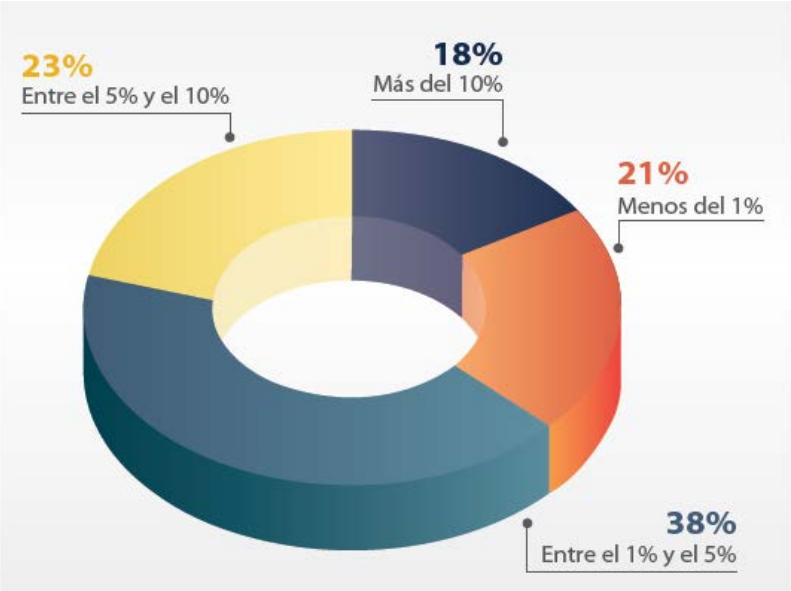


Figura 1.1 Porcentaje del presupuesto de IT para seguridad de la Información
Fuente: **(ESET, Security Report Latinoamerica 2012, 2012)**

Para este mismo estudio en el año 2014, puede apreciarse que la inversión en seguridad aumentó significativamente entre el 1% y el 20% en relación a los años 2012 y 2013, a pesar de que todavía existe un grupo de empresas que notaron disminución de presupuestos, al final el balance es positivo tal como lo indica la Fig. 1.2.

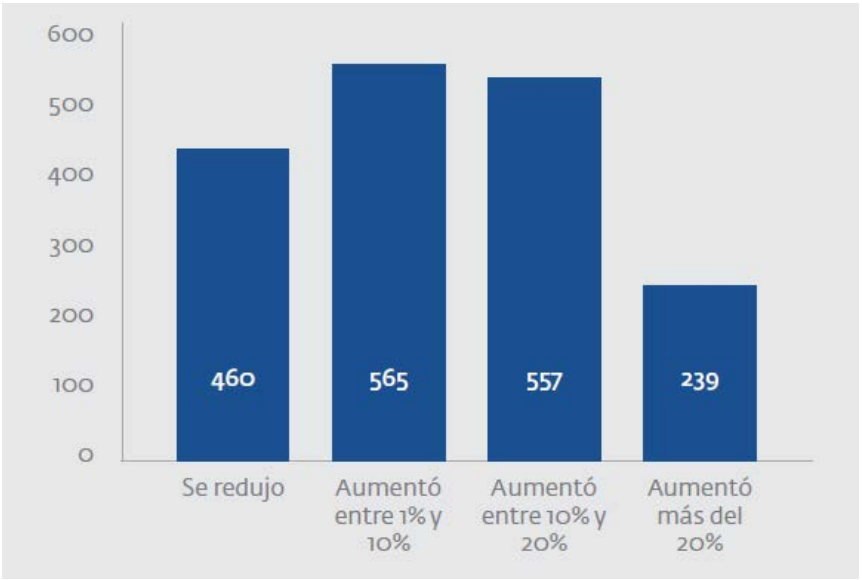


Figura 1.2 Variación del presupuesto para Seguridad Informática
Fuente: (ESET, Security Report Latinoamerica 2014, 2014)

Para Germán Andrés Camacho, coordinador del programa Zeiky, un Centro de Información y Asesoría en Comercio Exterior, promovido por la Universidad Sergio Arboleda, muchos directivos Pyme ignoran la importancia de la tecnología y las comunicaciones, un componente ineludible de la competitividad en el mundo de los negocios contemporáneos. “El gerente Pyme en América Latina generalmente es empírico y no tiene el hábito de capacitarse y actualizarse permanentemente, que es una exigencia de la sociedad de la información” (Universia, 2008), afirma Camacho, un experto en finanzas y comercio exterior, con estudios de MBA en la materia.

La Fundación para el Desarrollo Sostenible en América Latina (Fundes), presenta cifras desalentadoras: las Pymes, sobre todo las más pequeñas, solo invierten el 2% de sus presupuestos en tecnología. “Por supuesto, una empresa que no se actualice tecnológicamente, está condenada a un atraso en competitividad y productividad”, advierte Camacho. (Universia, 2008)

Generalmente cuando un administrador adquiere tecnología lo contabiliza como un gasto y no como una inversión.

1.6 Las empresas latinoamericanas y el entorno de seguridad tecnológica.

No existen estadísticas específicas de las Pymes en nuestro país y su situación en el entorno de seguridad tecnológica latinoamericana o mundial, sin embargo varias empresas realizan estudios anualmente que permiten conocer el estado de las empresas a nivel mundial, para enfrentar las amenazas que ponen en peligro su información.

Estos son algunos de los resultados de importantes estudios realizados por empresas dedicadas a desarrollar productos de seguridad y análisis de amenazas:

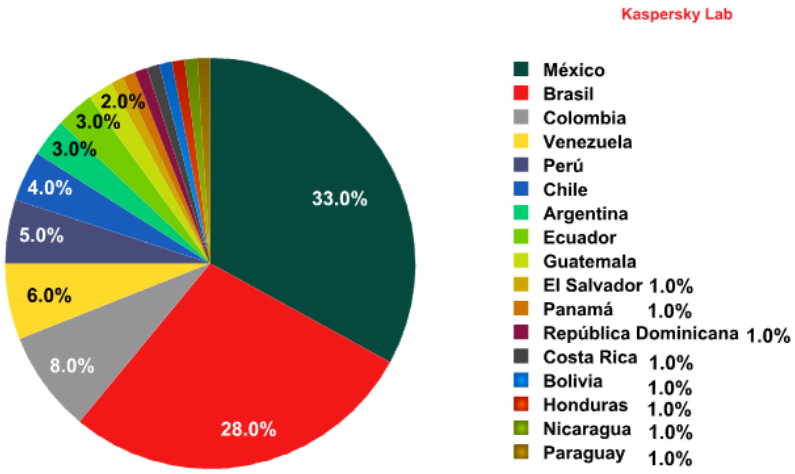


Figura 1.3 Distribución geográfica de las víctimas de ataques a la seguridad informática (2011)
Fuente: (Kaspersky, 2012)

Ranking mundial	País	% de usuarios con intentos de infección	Nº de incidentes
38	**Brasil**	32.0%	22122995
63	**Perú**	28.7%	4537175
64	**Panamá**	28.5%	929976
74	**México**	27.0%	17514481
80	**Honduras**	26.5%	458438
90	**El Salvador**	25.4%	439970
92	**Nicaragua**	24.9%	310517
95	**Ecuador**	24.6%	3157211
97	**Colombia**	24.4%	4991622
98	**Chile**	24.2%	1813276
99	**Guatemala**	24.2%	822242
112	**República Dominicana**	22.8%	435710
125	**Costa Rica**	21.6%	588932
132	**Argentina**	21.2%	1375126
148	**Uruguay**	19.6%	175873
165	**Paraguay**	17.9%	238189
232	**Cuba**	7.9%	30586

Figura 1. 4 Distribución geográfica de incidentes de ataques registrados on-line (2014)
Fuente: (Kaspersky, 2014)

Los incidentes de seguridad han ido en aumento en los países latinoamericanos, como ejemplo, en los últimos años nuestro país ha sido víctima de hackers, phising, robo de datos, casos que han sido de conocimiento público como por ejemplo: ataque de Anonymous a web

oficiales, sustracción de dinero de cuentas bancarias de miembros del Consejo de Participación Ciudadana y Control Social, entre otros.

De acuerdo al Estudio Global sobre Seguridad de las Tecnologías de la Información (TI) Empresarial 2012 (Kaspersky, 2013), realizado por Kaspersky Lab, la vulnerabilidad informática en América Latina ha ido en aumento.

Este mismo informe indica, que son precisamente las Pymes quienes menos medidas de seguridad implementan en comparación con las grandes empresas:

"El 19% de las pequeñas empresas y el 15% de las medianas son reactivas frente a los ciber-ataques, solo llegan a preocuparse por la seguridad de TI luego de que han sido víctimas de malware. En tanto, el 25% de pymes en Latinoamérica invierten en seguridad TI de forma proactiva. Por su parte, las grandes compañías son, en mayor medida, conscientes respecto a los problemas de seguridad TI". (Kaspersky, 2013)

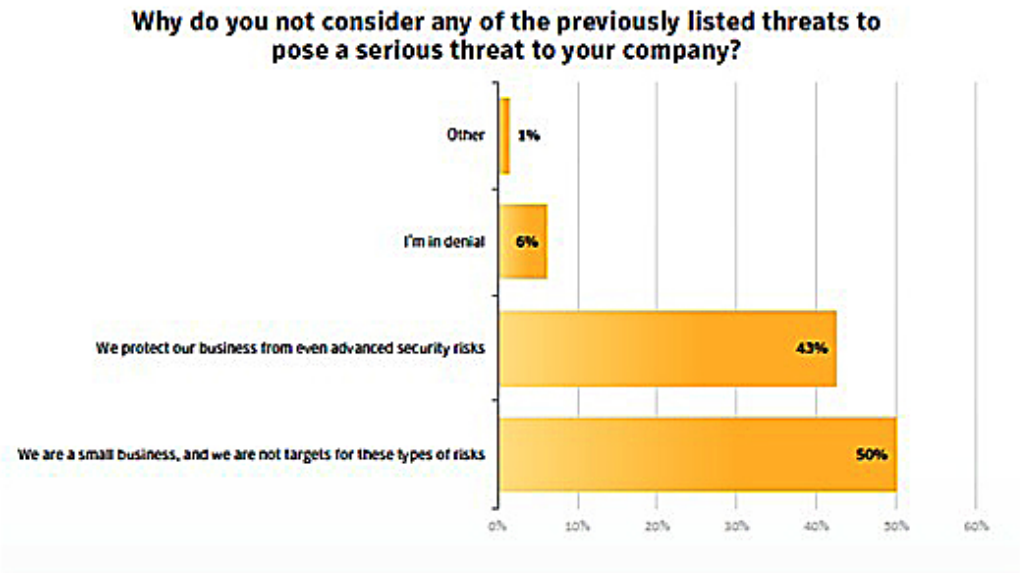


Figura 1.5 Resultado encuesta SMB Threat Awareness Poll 2011
Fuente: (Symantec, 2011)

La Figura 1.5 muestra la respuesta a una de las preguntas de la Encuesta 2011 sobre Conciencia de Amenazas entre las PyMEs, realizada por Symantec, en el que las Pymes se consideran un “blanco demasiado pequeño” para ser víctimas de ataques informáticos de cualquier tipo.

Las tareas de protección, son las más importantes tanto para las pequeñas y grandes empresas. Conforme la tecnología evoluciona, las amenazas cambian y son diferentes para cada sector, así por ejemplo: las Pymes se enfrentan a spam, virus, malware, vulnerabilidades de software; las grandes empresas deben enfrentar phishing, ingeniería social, hackers, robo de información confidencial, etc.

“Las Pymes han de concienciarse del riesgo de no contar con la protección adecuada. Es fundamental cambiar esa actitud y mejorar los niveles de seguridad IT, con el fin de mantener la empresa a salvo y segura”. (Kaspersky, 2013)

Figura 1. 6 Situación actual de las Políticas de Seguridad
Fuente: (ACIS, 2013)

La V encuesta Latinoamericana de Seguridad de la Información Tendencias 2013 (ACIS, 2013), revela que la definición de políticas de seguridad va en aumento, lo que representa el incremento de los esfuerzos de la empresa por mejorar las medidas de seguridad y la capacitación del personal responsable.

1.7 Conclusiones parciales

- Todas las empresas sin importar su tamaño, deben mejorar y controlar sus medidas de seguridad TI.

- Las amenazas a las que se enfrentan las pequeñas Pymes y las grandes empresas no son iguales por tanto la evaluación e implementación de planes de seguridad serán diferentes, tratando de conseguir un mismo objetivo.

- Para la formalización de políticas de seguridad, no es necesaria una gran inversión, inclusive con un bajo presupuesto, capacitación al personal responsable y compromiso de todo el personal se pueden aplicar medidas iniciales de seguridad TI.

- Para llegar a la determinación de estas recomendaciones, es necesario revisar la situación actual de la seguridad TI en la empresa, a fin de saber qué medidas deben aplicarse y hasta qué punto la alta gerencia está dispuesta a comprometerse en la formalización de dichas medidas.

CAPITULO II

MARCO TEÓRICO Y CONCEPTUAL

2.1 Definiciones

2.1.1 Definición de PYME

Antes de establecer un concepto de Pymes es necesario conocer el significado de estas siglas:

PYME → Pequeña Y Mediana Empresa.

Según el Servicio de Rentas Internas, SRI (SRI, 2014)**:**

"Se conoce como Pymes al conjunto de pequeñas y medianas empresas que de acuerdo a su volumen de ventas, capital social, cantidad de trabajadores, y su nivel de producción o activos presentan características propias de este tipo de entidades económicas.

Por lo general en nuestro país las pequeñas y medianas empresas que se han formado realizan diferentes tipos de actividades económicas entre las que destacamos las siguientes:

- Comercio al por mayor y al por menor.
- Agricultura, silvicultura y pesca.
- Industrias manufactureras.
- Construcción.
- Transporte, almacenamiento, y comunicaciones.
- Bienes inmuebles y servicios prestados a las empresas.

- Servicios comunales, sociales y personales.”

De acuerdo a Ecuapymes (Ecuapymes, s.f.) indica que:

“PYME es el término técnico con el que se les conoce a la Pequeña y Mediana Empresa, o Small Business en inglés”.

Es muy difícil determinar exactamente si una empresa está categorizada como una Pyme. Si nos referimos por el número de empleados, existen empresas con poco personal, pero con tecnología de punta que representa una gran inversión y alto volumen de producción, mas no estarían dentro de esta categorización debido al alcance que tienen en el mercado. Hay factores como el capital, la maquinaria, la producción, la rentabilidad y la cantidad de personal con que cuenta una empresa para catalogarla como una Pyme, y, en nuestro país, no existe una entidad que pueda determinar dicha categorización. Sin embargo, para el efecto, se engloba a las Pymes ecuatorianas como cualquier empresa proveedora de servicios y productos o insumos para otras empresas de amplia cobertura de mercado.

Entonces, una organización Pyme, es un ente productivo o de servicios, que genera empleo y productividad en el país y permiten abastecer la demanda de productos y servicios de empresas nacionales, multinacionales e industrias que mueven al Ecuador.”

Considerando la definición establecida por la Superintendencia de Compañías (Superintendencia, 2011), tenemos que:

“Para efectos del registro y preparación de estados financieros, se califica como PYMES a las personas jurídicas que cumplan las siguientes condiciones:

a) Activos totales inferiores a cuatro millones de dólares;
b) Registren un valor bruto de ventas anuales inferior a cinco millones de dólares y;

c) Tengan menos de 200 trabajadores (personal ocupado)”

Del análisis realizado a estos conceptos se puede concluir que no existe una definición exacta de Pyme pues muchos de ellos se han adaptado a las condiciones de un país o región. Incluso, en diversas ocasiones se clasifica a las empresas de acuerdo a ciertas características que pueden o no ser cumplidas en su totalidad en cada caso.

A continuación se efectúa el análisis matricial de las definiciones expuestas.

Tabla 2.1

Resumen definiciones de Pyme

Organización	Definición	Análisis
SRI	Se conoce como PYMES al conjunto de pequeñas y medianas empresas que de acuerdo a su volumen de ventas, capital social, cantidad de trabajadores, y su nivel de producción o activos presentan características propias de este tipo de entidades económicas.	Define a una empresa de acuerdo a su volumen de ventas, producción, cantidad de trabajadores y capital social.
Ecuapymes	Sin embargo, para el efecto, se engloba a las PYMES ecuatorianas como cualquier empresa proveedora de servicios y productos o insumos para otras empresas de amplia cobertura de mercado. Entonces, una organización PYME, es un ente productivo o de servicios, que genera empleo y productividad en el país y permiten abastecer la demanda de productos y servicios de empresas nacionales, multinacionales e industrias que mueven al Ecuador	La conceptualiza como un ente productivo que provee de bienes o servicios a empresas más grandes.
Superintendencia de Compañías	Para efectos del registro y preparación de estados financieros, se califica como PYMES a las personas jurídicas que cumplan las siguientes condiciones: a) Activos totales inferiores a cuatro millones de dólares; b) Registren un valor bruto de ventas anuales inferior a cinco millones de dólares y; c) Tengan menos de 200 trabajadores (personal ocupado)	Establece una definición en base al cumplimiento de ciertas condiciones financieras y contables de una empresa como: activos y ventas brutas.

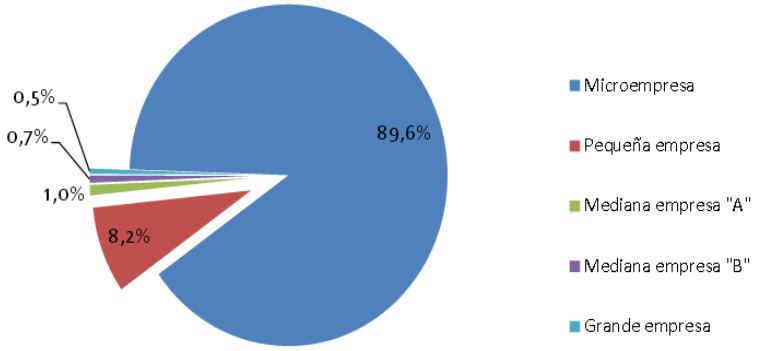
En función del análisis efectuado, se establece para la presente tesis la siguiente definición de Pymes:

Se conoce como Pyme a todo ente productivo que cumpla con las siguientes condiciones:

- Nómina de hasta 200 trabajadores
- Volumen de ventas hasta $4’999.999
- Activos totales hasta $3’999.999.
- Provea variados bienes y servicios al mercado nacional e internacional.

2.1.2 Cantidad de Pymes en el Ecuador

Conocer exactamente el número de pequeñas y medianas empresas existen en nuestro país, es complicado, sin embargo de acuerdo a las cifras del Directorio de Empresas y Establecimientos al año 2012 (INEC, 2013) realizado por el INEC publicado a mediados del año 2013, se conoce que las Pymes abarcan un amplio espectro productivo en el país, concentrándose la mayor parte de ellas en las provincias de Pichincha y Guayas, según se puede apreciar en las figuras 2.1 y 2.2.

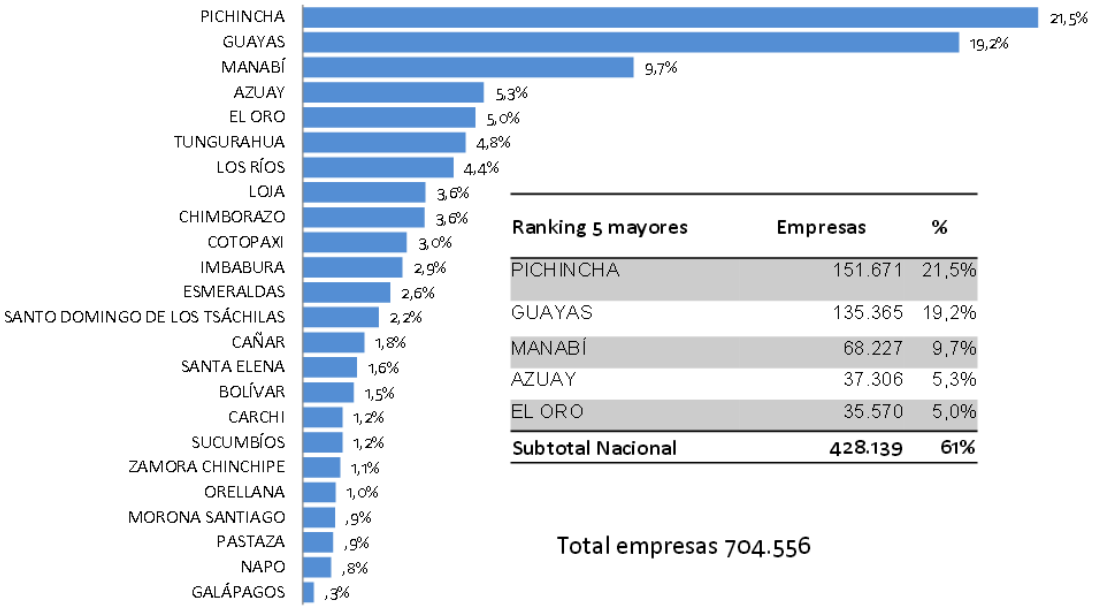


Tamaño de Empresas	Nro. Empresas	Porcentaje
Microempresa	631.430	89,6%
Pequeña empresa	57.772	8,2%
Mediana empresa "A"	6.990	1,0%
Mediana empresa "B"	4.807	0,7%
Grande empresa	3.557	0,5%
Total	704.556	100,0%

NOTA: Clasificación emitida por la Comunidad Andina de Naciones (CAN)

Figura 2.1: Clasificación de empresas según su tamaño

Fuente: (INEC, 2013)



Ranking 5 mayores	Empresas	%
PICHINCHA	151.671	21,5%
GUAYAS	135.365	19,2%
MANABÍ	68.227	9,7%
AZUAY	37.306	5,3%
EL ORO	35.570	5,0%
Subtotal Nacional	**428.139**	**61%**

Total empresas 704.556

Figura 2.2: Número de establecimientos económicos según sectores económicos por personal ocupado

Fuente: (INEC, 2013)

La existencia de este tipo de empresas permite la creación de puestos de trabajo y la diversificación de los productos y servicios ofrecidos, lo que contribuye al movimiento del motor productivo del país.

2.1.3 Definición de modelo de madurez

"Es el conjunto de procesos organizados en niveles (denominados de madurez) con los que debería contar una organización. Permite identificar fortalezas y debilidades de la organización con respecto a sus áreas de procesos" R. Arbeláez (Arbeláez Cortez, 2008)

"Un modelo de madurez, es un conjunto estructurado de elementos (buenas prácticas, herramientas de medición, criterios de análisis, etc.), que permite identificar las capacidades instaladas en dirección de proyectos en la organización, compararlas con estándares, identificar vacíos o debilidades y establecer procesos de mejora continua" Álvaro Claros L. (Claros Liendo, 2012)

Considerando lo expuesto, se definirá como modelo de madurez:

Al conjunto organizado de buenas prácticas que permita identificar debilidades y fortalezas en los procesos de una organización, permitiendo su mejora constante.

2.1.4 Propósito del modelo de madurez

Un modelo de madurez permite:

- Medirme → saber dónde estoy
- Definir → donde quiero estar
- Planear → lo que debo lograr para llegar a donde quiero estar
- Gestionar→ mi evolución

Es decir, que el Modelo de Madurez permite saber que tan preparada se encuentra una organización de acuerdo al nivel en el que se ubica y cuales son la características que requieren para avanzar al siguiente nivel.

2.2 Áreas de aplicación de los modelos de madurez

Podemos encontrar modelos de madurez aplicados en áreas como (Ramirez, 2009):

- Desarrollo de Software
- Gestión de Proyectos
- Gestión del Conocimiento
- Desarrollo de las Capacidades
- Habilidad de cambio

Y los campos de aplicación van en aumento.

2.3 Base teórica de los Modelos de Madurez

Existen varios modelos utilizados internacionalmente. Para la presente Tesis, se recurrió a investigación bibliográfica para definir los modelos más conocidos y que están siendo utilizados en diferentes áreas.

2.3.1 Modelo de Madurez COBIT

COBIT constituye un marco de referencia de buenas prácticas dirigido a la gestión de IT (gobierno de IT).

Aparece por primera vez en 1995 enfocado principalmente a la auditoría y control de los sistema de información. Desarrollado por ISACF (Information Systems Audit and Control Foundation) actualmente conocida

como ISACA (Infomation Systems Audit and Control Asociation), ha mantenido constantes actualizaciones que han permitido adaptarlo cada vez más a los objetivos del negocio.

Enfocado fuertemente en el control, COBIT ayuda a la mejor comprensión de los procesos, beneficios y riesgos tecnológicos, permitiendo una visión clara que mejora la toma de decisiones.

Con el aparecimiento del concepto de “gobierno de IT” se han desarrollado varios versiones que han sido utilizadas a nivel mundial, lo que le ha permitido mantenerse vigente y en actualización constante. Su última versión COBIT 5 liberada en julio del 2012, cubre las nuevas tendencias de gobierno y administración de IT.

COBIT aporta con un conjunto de herramientas (entre ellas un modelo de madurez) que permiten mejorar la administración de tecnología en beneficio de la empresa.

2.3.1 1 Modelo de Procesos dentro de COBIT

COBIT subdivide a IT en 34 procesos que engloban todo lo que debe ser controlado. Estos procesos son evaluados a través del modelo de madurez para identificar los procesos críticos y establecer planes de acción que permitan mejorar la capacidad de los mismos hasta llegar al nivel deseado.

El marco de trabajo de COBIT brinda soporte al gobierno de IT (Figura 2.3) ya que garantiza:

- Vínculo entre IT y los objetivos del negocio.
- Definir procesos que engloben todas las actividades de IT.
- Utilizar de manera responsable los recursos de IT asignados.
- Correcta administración de riesgos de IT.

Figura 2.3 Áreas de enfoque del gobierno de IT

Fuente: (ISACA, 2007)

2.3.1 2 Componentes de COBIT

COBIT ofrece un conjunto de herramientas de soporte conocidos como productos o componentes COBIT que permiten a la gerencia disponer de la correcta información de IT para la toma de decisiones, es decir acerca la gestión de IT a los directivos.

Los componentes y su relación se ilustran a continuación:

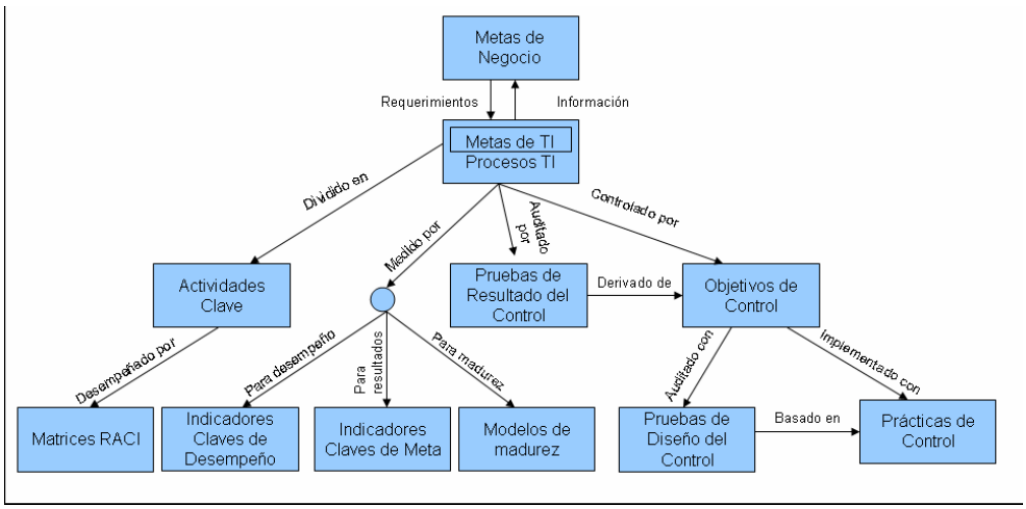


Figura 2.4 Interrelación entre los componentes COBIT

Fuente: (ISACA, 2007)

2.3.1 3 Modelo de madurez

A partir de la versión 3 de COBIT, publicada en el año 2000, aparece el Modelo de Madurez como parte de las Directivas Gerenciales.

El modelo de madurez es uno de los componentes esenciales de COBIT, que en conjunto con otros componentes, permite administrar, controlar y medir cada proceso.

A través del modelo de madurez, la empresa puede medirse y compararse con otros negocios.

COBIT aplica un modelo de madurez para administración y control de los procesos de IT, el mismo que contempla 5 niveles basados en los principios del modelo de madurez del SEI (Software Engineering Institute) para el desarrollo de software, sin embargo y a diferencia de CMM, el modelo de madurez de COBIT no pretende cumplir obligatoriamente y con exactitud todo los objetivos de cada nivel para pasar al siguiente, sino permitir la identificación de los posibles problemas y priorizar las mejoras.

Es decir que, algunos procesos pueden cumplir ampliamente las acciones o características de un nivel, mientras cumplen en menor porcentaje las acciones de otro nivel, sin que esto signifique que no está cumpliendo alguno de los 2 niveles (Figura 2.5).

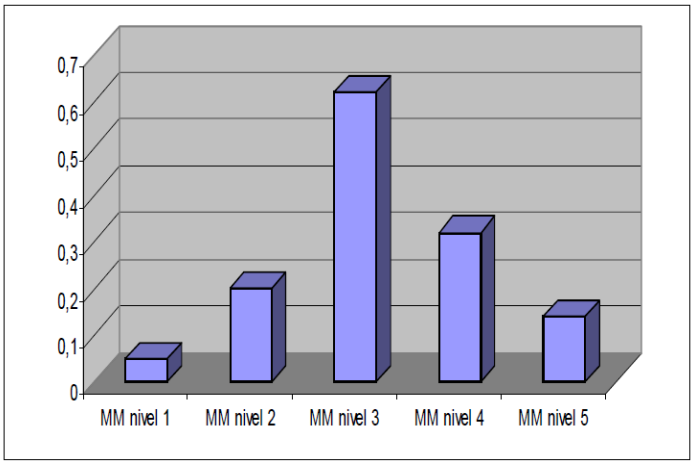


Figura 2.5 Ejemplo de evaluación del nivel de madurez basado en COBIT
Fuente: (ISACA, 2007)

Los niveles de madurez manejados por COBIT son:

Nivel 0 – No existente.- No existen procesos implementados, tampoco se han identificado problemas que afecten a la empresa.

Nivel 1 – Inicial.- La expresa manifiesta su interés por identificar y solventar los problemas que existen. La administración es desorganizada, no existen procesos implantados a nivel general.

Nivel 2 – Repetible.- Algunos procesos ya se aplican a nivel de usuarios con tareas similares, sin embargo el control y la evaluación en el cumplimiento de los procesos lo maneja cada persona.

Nivel 3 – Definido.- Existen procesos documentados y el personal a recibido capacitación sobre los mismos. Los procesos no son obligatorios sino que el personal decide si utilizarlos o no.

Nivel 4 – Administrado.- Los procesos se encuentran aplicados en toda la empresa y es posible monitorear su eficiencia y cumplimiento. En base a la retroalimentación pueden aplicarse constantes mejoras.

Nivel 5 – Optimizado.- Los procesos se han adoptado como mejor práctica, ya han superado procesos de corrección y refinamiento. Las herramientas de automatización se utilizan para ayudar a que el personal se adapte de mejor forma a la utilización de los mismos.

2.3.2 Modelo de Madurez de Capacidades o CMM

El CMM o Capability Maturity Model, es un modelo de evaluación de los procesos de una organización. Fue desarrollado en 1986 por la Universidad Carnegie-Mellon (Carnegie Mellon University, 2013) de USA para el SEI. Aplicado en procesos de desarrollo de software para evaluar la calidad del desarrollo.

Este modelo establece un conjunto de prácticas o procesos agrupados en Áreas Clave de Proceso (KPA – Key Process Area).

Para cada área de proceso define un conjunto de buenas prácticas que deberán ser:

- Documentadas.
- Provistas de los medios y formación necesarios.
- Ejecutadas de un modo sistemático, universal y uniforme.
- Medidas
- Verificadas

Según la Figura 2.6, estas áreas se agrupan en cinco “niveles de madurez”, que son:

1. **Inicial.-** Las organizaciones en este nivel no disponen de un ambiente estable. Aunque se utilicen técnicas correctas de ingeniería hace falta planificación. El resultado de los proyectos es impredecible.

2. **Repetible.-** Las organizaciones disponen de prácticas institucionalizadas de gestión de proyectos. Existen métricas básicas.

3. **Definido.-** Además de una buena gestión de proyectos, en este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos, formación de personal, técnicas de ingeniería detallada y un nivel más avanzado de métricas en los procesos. Se implementan técnicas de revisión por pares (peer reviews).

4. **Gestionado.-** Las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgo. El software resultante es de alta calidad.

5. **Optimizado.-** La organización completa está comprometida con la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

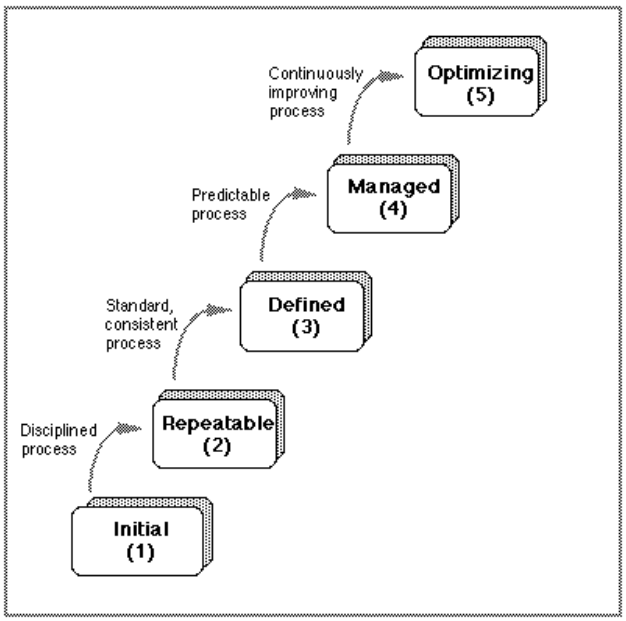


Figura 2.6 Niveles de madurez de CMM

Fuente: (Fau, 2006)

Así es como el modelo CMM establece una medida del progreso, conforme al avance en niveles de madurez. Cada nivel a su vez cuenta con un número de áreas de proceso que deben lograrse. Con excepción del primer nivel, cada uno de los restantes niveles está compuesto por un cierto número de Áreas Claves de Proceso, conocidas en la documentación de CMM por su sigla inglesa KPA. (Figura 2.7)

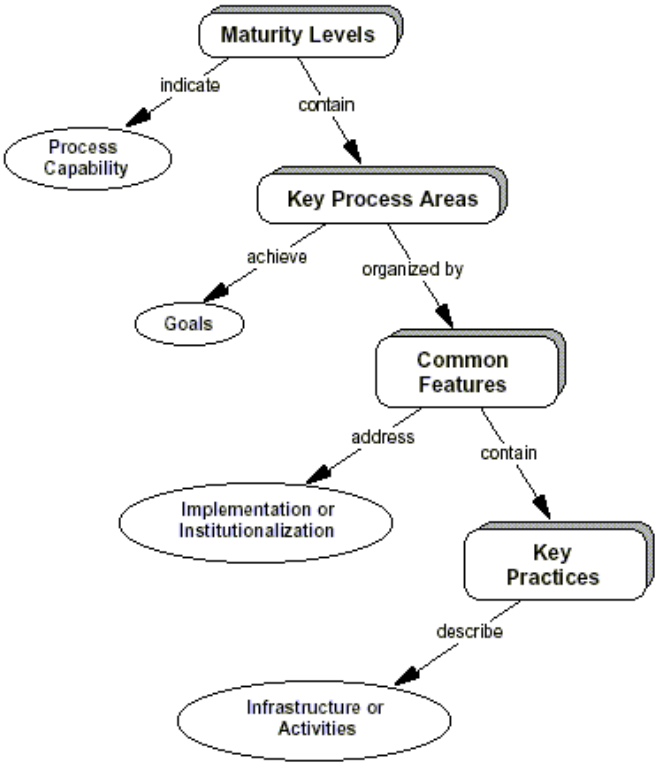


Figura 2. 7 Estructura de CMM

Fuente: (Fau, 2006)

Cada KPA identifica un conjunto de actividades y prácticas interrelacionadas, las cuales cuando son realizadas en forma colectiva permiten alcanzar las metas fundamentales del proceso. Las KPA's pueden clasificarse en 3 tipos de proceso: Gestión, Organizacionales e Ingeniería.

Hasta el año 2003, el SEI formaron evaluadores certificados, que son los encargados de evaluar el nivel de CMM en el que se encuentra una organización. Esta certificación es solicitada por el Departamento de

Defensa de los Estados Unidos, pero se ha convertido en un requisito para empresas desarrolladoras de software a nivel mundial.

A partir del 2001, se forman evaluadores en CMMI (Capability Maturity Model Integration) que es una de las variantes del modelo CMM aplicadas a diversas disciplinas como ingeniería de sistemas, integración de productos, relación con proveedores, etc.

2.3.2.1 Áreas claves para cada nivel

Nivel 1.- En este nivel se encuentran la mayoría de empresas que inician sus actividades ya que no cuentan con procesos definidos. No existe control de tiempo ni de presupuesto. No existe control sobre el estado del proyecto. Este nivel no tiene Áreas Claves del Proceso (KPA's).

Nivel 2.- La principal diferencia entre este nivel y el anterior es que el proyecto es gestionado y controlado durante el desarrollo del mismo. Se puede conocer el estado del proyecto en todo momento.

Las áreas Claves del proceso que deben cubrirse para alcanzar este nivel son:

- Gestión de requisitos
- Planificación de proyectos
- Seguimiento y control de proyectos
- Gestión de proveedores
- Aseguramiento de la calidad
- Gestión de la configuración

Nivel 3.- Alcanzar este nivel significa que la forma de desarrollar proyectos está definida, es decir establecida, documentada y existen métricas (datos objetivos) para la consecución de objetivos concretos.

Las Áreas Claves de Proceso a implantar para alcanzar este nivel son:

- Desarrollo de requisitos
- Solución técnica
- Integración del producto
- Verificación
- Validación
- Desarrollo y mejora de los procesos de la organización
- Definición de los procesos de la organización
- Planificación de la formación
- Gestión de riesgos
- Análisis y solución de toma de decisiones

Muchas empresas llegan solo a este nivel de implementación ya que se alcanzan muchos beneficios y se cubren muchas de las necesidades de la organización.

Nivel 4.- Los proyectos usan objetivos medibles para alcanzar las necesidades de los clientes y la organización. Se usan métrica para gestionar la organización.

Las Áreas Claves de Proceso para alcanzar este nivel son:

- Gestión cuantitativa de proyectos
- Mejora de los procesos de la organización

Nivel 5.- Los procesos de los proyectos y de la organización están orientados a la mejora de actividades. Mejoras de los procesos que mediante métricas son identificados, evaluados y puestos en la práctica.

Las Áreas Claves de Proceso a implantar son:

- Innovación organizacional
- Análisis y resolución de las causas

La implantación de este modelo es un proceso largo y costoso, que puede costar varios años de esfuerzo. Aún así los beneficios obtenidos por la empresa compensan todo el esfuerzo.

2.3.2.2 Otras versiones de CMM

CMM es cada vez más aceptado en diferentes áreas de aplicación, creándose versiones especializadas para cada una de ellas:

SW-CMM (Software-CMM).- CMM para software, aplicado tanto para desarrollo como para mantenimiento de software. La premisa básica de este modelo es que la mejora en la madurez del proceso de desarrollo dará como resultado un mejor desempeño del proyecto y calidad del producto.
SW-CMM cubre las prácticas de planificación, ingeniería, gestión del desarrollo y mantenimiento del software.

P-CMM (People CMM).- Introduce las directrices de CMM para mejorar la capacidad y la preparación de la fuerza laboral de una organización en el contexto del enfoque ideal para la mejora de procesos.

El método se constituye en una herramienta de diagnóstico que apoya, permite y alienta el compromiso de la organización para la mejora de su capacidad de atraer, desarrollar, motivar, organizar y retener el talento necesario para mejorar constantemente la organización.

SA-CMM (Software Acquisition CMM).- Todas las organizaciones tienen la necesidad de mejorar sus procesos internos de adquisición de software. Así como SW-CMM describe el rol del desarrollador o proveedor

de software, SA-CMM describe el rol del comprador en el proceso de adquisición.

CMMI (Capability Maturity Model Integration).- Desarrollado por el SEI con el propósito de unir en forma coherente varios modelos anteriores que eran utilizados en conjunto dentro de una organización.

CMMI es un modelo de calidad para el desarrollo y mantenimiento del software y gestión y desarrollo de proyectos.

2.3.3 ISM3

El modelo de madurez para la Gestión de la Seguridad de la Información nace como un estándar de "código libre" en el 2007, creado por un consorcio de empresas: ESTEC Systems (Canadá), First Legion Consulting y Valiant Technologies (India), Seltika (Colombia), Global 4 Ingeniería (España) y M3 Security (Estados Unidos).

El punto de partida de ISM3 es tomar las mejores ideas sobre la gestión (de sistemas y controles de ISO 9000, ITIL, CMMI) e ISO 17799/ISO 27001. "Nace con la intención de ayudar tanto a grandes como a pequeñas empresas a obtener el máximo retorno de su inversión en seguridad". (Aceituno Canal, 2004)

Este modelo se lo aplica para:

- Evaluar y mejorar el ISMS (Information Security Management System).
- Extender las disciplinas ISO 9000 hacia el ISMS.
- Proporciona otra ruta para una certificación ISMS.

ISM3 es un estándar completo que es amigable con el negocio, adaptable, acreditable, compatible, escalable y libre.

Amigable con el negocio.- El estándar alinea, la gestión de la seguridad con las necesidades del negocio a través de los objetivos del negocio, objetivos y metas de seguridad.

Los objetivos del negocio se derivan de la misión del negocio, mientras que los objetivos de seguridad se derivan de los bienes protegidos, ambientes y ciclos de vida y los recursos disponibles para la protección.

Adaptable.- ISM3 consta de 5 niveles de madurez, a través de estos niveles las compañías pueden adaptar su ISMS para obtener objetivos de seguridad realistas. Además, es posible obtener certificaciones intermedias de acuerdo al nivel en el que se encuentre ya que, alguno de los niveles puede considerarse adecuado para las necesidades de la organización y, si la organización no desea acreditarse puede aplicar los niveles de madurez como una guía para el diseño de su ISMS.

Acreditable.- Puede utilizarse ISM3 para implementar un ISMS basado en ISO 27001, ya que ISM3 es acreditable bajo ISO 9000 (International Organization for Standarization) o ISO 27001.

Fácil de implementar.- En la implementación de ISM3 es fácil definir a los responsables de cada etapa de la seguridad gracias a la división en capas, de esta forma están claramente definidos los roles de líderes, gerentes y personal técnico, pero, estableciendo objetivos en conjunto.

Compatible.- ISM3 permite utilizar la inversión actual de seguridad y puede evolucionar a partir de ésta. Al ser compatible con la norma ISO 27001 puede ayudar en la implementación de éste estándar o de ambos.

Escalable y completa.- ISM3 reconoce diferentes roles y necesidades de protección, como el entorno de usuario, producción, desarrollo, servicios de internet, etc. Los procesos en ISM3 son definidos como clases de

procesos, de esta forma diferentes procesos se aplican a diferentes ambientes, permitiendo escalabilidad desde empresas pequeñas hasta organizaciones complejas.

La aplicación del modelo cubre todos los sistemas de información críticos de la organización, no se puede certificar solo una parte de ésta, pero si se pueden “externalizar” procesos a una adecuada organización de seguridad, y con esto no es estrictamente necesario contar con todo el personal experimentado en ciertos procesos dentro de la organización.

Abierto (libre).- El modelo está publicado bajo licencia de Creative Commons, disponible gratuitamente en su versión electrónica. De uso ilimitado.

2.3.3.1 Niveles de madurez

ISM3 está dividido en 5 niveles de madurez:

ISM3 0

Pueden obtenerse ganancias a corto plazo, pero es improbable que resulte en una reducción significativa del riesgo de amenazas técnicas.

Este nivel no es recomendable para ninguna organización.

ISM3 1

Se debería apreciar una reducción significativa del riesgo de amenazas técnicas con mínima inversión en procesos ISM esenciales.

Este nivel es recomendable para organizaciones con metas de seguridad bajas en ambientes de riesgo bajo.

ISM3 2

Mayor reducción del riesgo por amenazas técnicas, inversión moderada en procesos ISM.

Recomendado para organizaciones con metas de seguridad normales en ambientes de riesgo normal.

ISM3 3

Reducción alta de riesgos por amenazas técnicas, con una importante inversión en procesos ISM.

Este nivel es recomendable para organizaciones con metas de seguridad altas en ambientes de riesgo normal o alto.

ISM3 4

En este nivel se debería obtener la mayor reducción de amenazas tanto técnicas como internas, con una inversión seria en procesos ISM.

Este nivel se recomienda para organizaciones afectadas por requerimientos específicos (suministradoras de energía y agua, instituciones financieras y organizaciones que comparten o guardan información sensible) con metas de seguridad muy altas en ambientes de riesgo normal o alto.

CAPITULO III

METODOLOGIA

3.1 Instrumentos utilizados para levantamiento de información

Para la obtención de información se utilizaron encuestas online, debido a la facilidad de difusión y aplicación. Para ello, se diseñó una encuesta en el sitio www.e-encuesta.com, la misma que estuvo publicada desde el 10 de septiembre al 15 de noviembre del 2012. (Formato de encuesta - Anexo A)

El objetivo de esta encuesta fue determinar lineamientos generales de la evaluación de seguridad en redes de información en Pymes ecuatorianas y el grado de conocimiento y difusión de los Modelos de Madurez aplicados a este campo.

Inicialmente, se solicitó la ayuda de la CAPEIPI (Cámara de la Pequeña y Mediana Empresa de Pichincha) para aplicar la encuesta a un grupo objetivo muy bien definido a través de la Base de Datos de la Cámara, lastimosamente no pudo realizarse ya que se encontraban aplicando otro cuestionario a los socios.

En busca de otra organización que trabaje directamente con Pymes o MiPymes, se contactó al Observatorio de la Pequeña y Mediana empresa de la Universidad Andina Simón Bolívar, quienes nos indicaron que la aplicación de este tipo de instrumentos de investigación solamente se debe canalizar a través de la CAPEIPI, único ente autorizado para enviarlo a los socios de la cámara y quienes cuentan con la base de datos actualizada.

Finalmente las encuestas se canalizaron a través de envío de emails directos a personas conocidas o referidas que trabajen en el área de IT.

3.2 Tabulación y análisis de resultados

Para la tabulación se utiliza un cuadro de acumulación de frecuencias lo que permite obtener el valor absoluto y relativo que representan el resultado obtenido, el mismo que luego es graficado para una mejor comprensión visual.

Pregunta 1: ¿A qué clasificación pertenece su empresa?

Tabla 3. 1

Tabulación Pregunta 1

Valor significado	Frecuencia	%
Microempresa	2	**5.41**
Pequeña y Mediana empresa	14	**37.84**
Grandes empresas	9	**24.32**
Otros	12	**32.43**
Total frecuencias	**37**	**100%**

Representación gráfica:

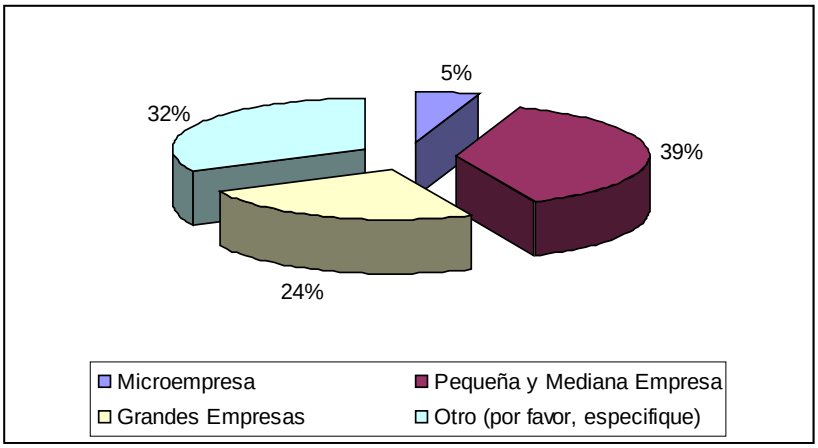


Figura 3. 1 Representación gráfica Pregunta 1

Análisis: El 37.84% de las personas que respondieron a la encuesta desarrollan sus actividades en el sector de Pymes, esto determina que la mayoría de respuestas obtenidas nos darán una visión de nuestro sector objetivo. Sin embargo es importante conocer el grado de conocimiento del tema en otros sectores como: microempresa (5%), grandes empresas (24%) y dentro del 32% de otros tenemos: colegios, empresas estatales, multinacionales y financieras.

Pregunta 2: ¿Cuenta su empresa con una persona encargada exclusivamente de seguridad IT?

Tabla 3. 2

Tabulación Pregunta 2

Valor significado	Frecuencia	%
Si	23	**62.16**
No	14	**37.84**
Total frecuencias	**37**	**100%**

Representación gráfica:

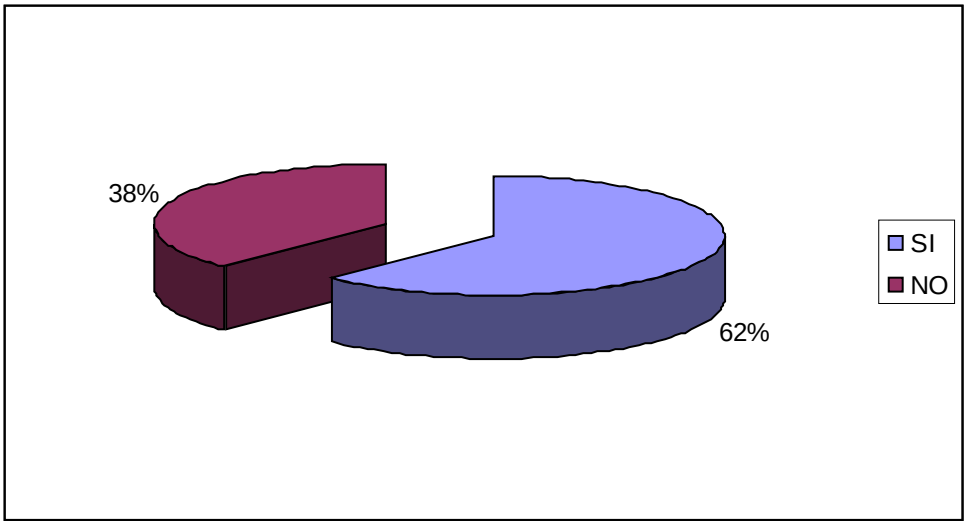


Figura 3. 2 Representación gráfica Pregunta 2

Análisis: El 62.16% de los encuestados indica que existe alguien dedicado completamente a la administración de la seguridad IT. Mientras que el 38% señala que no existe alguien exclusivamente dedicado a este tema.

Pregunta 3: La administración de seguridad de sus redes de información está a cargo de:

Tabla 3. 3

Tabulación Pregunta 3

Valor significado	Frecuencia	%
Personal interno	31	**75.61**
Proveedor	7	**17.07**
Outsourcing	2	**4.88**
Otros	1	**2.44**
Total frecuencias	**41**	**100%**

Representación gráfica:

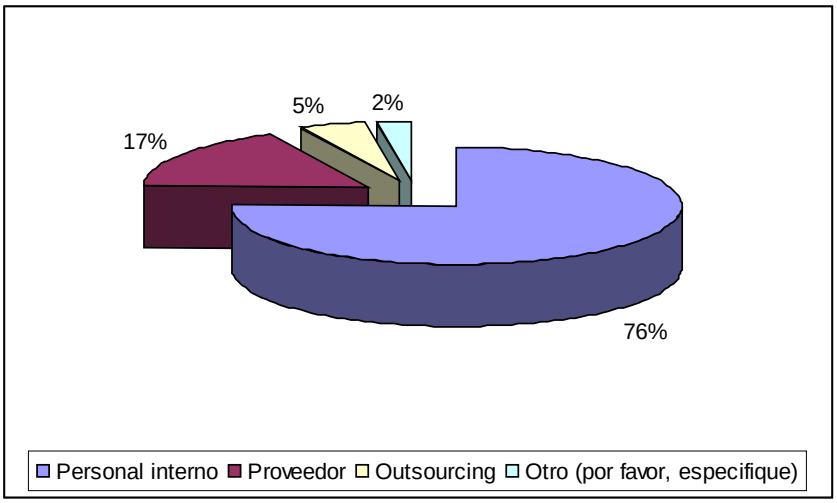


Figura 3. 3 Representación gráfica Pregunta 3

Análisis: El 75.61% indica que es el personal interno quien se encarga de la administración de la seguridad de las redes de información, un 7% delega esta tarea sus proveedores y un 2% maneja el tema a través de outsourcing.

Pregunta 4: ¿En base a qué parámetros evalúa el grado de seguridad de sus redes de información?

Tabla 3.4

Tabulación Pregunta 4

Valor significado	Frecuencia	%
Comentarios de los usuarios	18	**34.62**
Aplicación de indicadores (normativa)	8	**15.38**
Número de llamadas a Help Desk	11	**21.15**
Reportes del proveedor	9	**17.31**
Otros	6	**11.54**
Total frecuencias	**52**	**100%**

Representación gráfica:

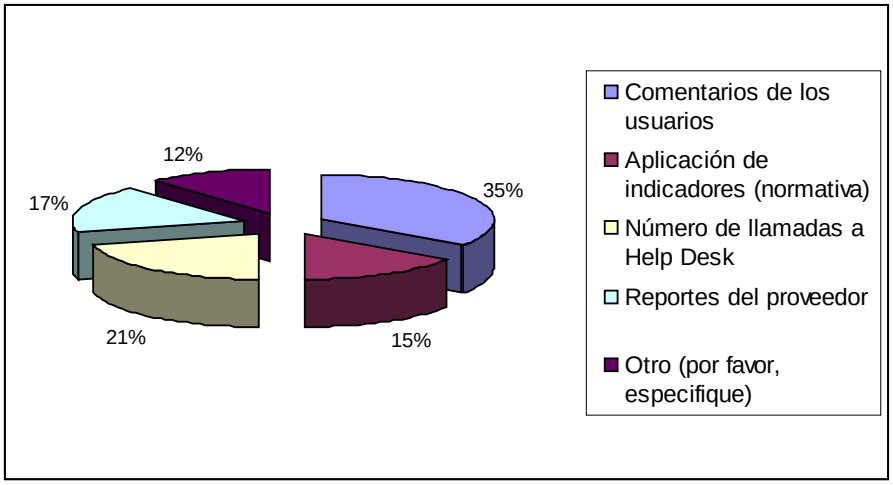


Figura 3. 4 Representación gráfica Pregunta 4

Análisis: A esta pregunta el 34.62% de las respuestas indica que el grado de seguridad de las redes de información se evalúa a través de los comentarios de los usuarios, el 21% por el número de llamadas que recibe Help Desk, el 17% en base a los reportes que reciben de su proveedor de servicios, el 15% otros (pruebas de vulnerabilidad, reportes internos, IPS) y un 12% indica que aplica algún tipo de normativa como: ISO 27000, ITIL, indicadores de gestión.

Pregunta 5: De su apreciación y experiencia indique ¿en qué nivel considera que se encuentra la seguridad de sus redes de información?

Tabla 3. 5

Tabulación Pregunta 5

Valor significado	Frecuencia	%
Inicial.- Redes inestables, hace falta planificación y proyección	10	**27.03**
Estable.- Existe planificación y mínimas métricas aplicadas	23	**62.16**

CONTINUA ⟶

Con proyección.- Se dispone de adecuados procedimientos y técnicas para la administración y se gestiona correctamente la innovación	4	**10.81**
Total frecuencias	**37**	**100%**

Representación gráfica:

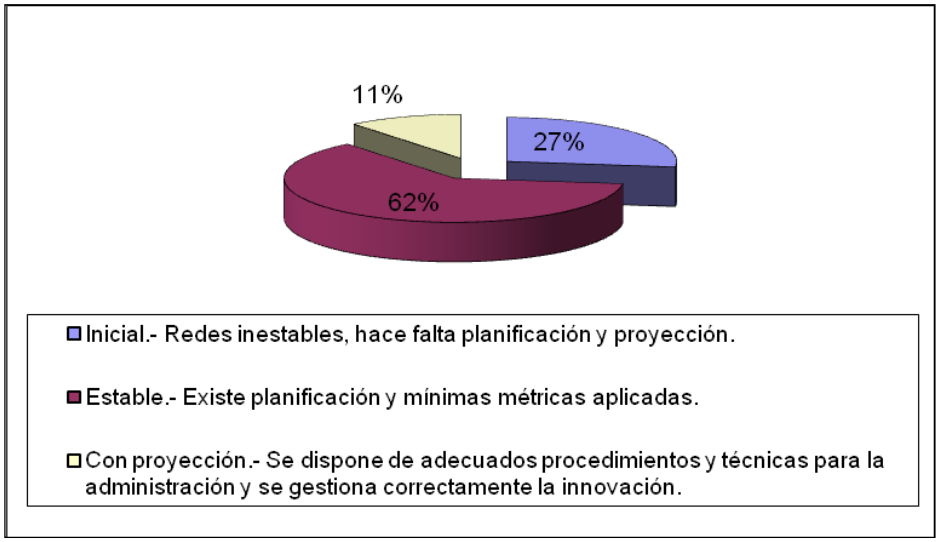


Figura 3. 5 Representación gráfica Pregunta 5

Análisis: A esta pregunta el 62% de los encuestados indica que consideran que sus redes son estables, el 27% considera sus redes en etapa inicial y un 4% indica que sus redes tienen proyección.

Pregunta 6: ¿Conoce en qué consisten los modelos de madurez?

Tabla 3. 6

Tabulación Pregunta 6

Valor significado	Frecuencia	%
Si	9	**24.32**
No	28	**75.68**
Total frecuencias	**37**	**100%**

Representación gráfica:

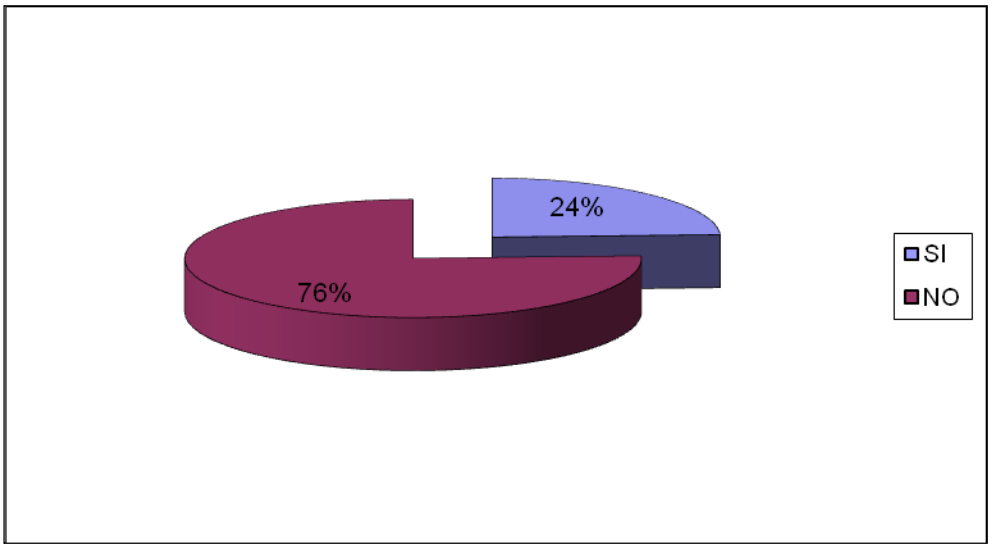


Figura 3. 6 Representación gráfica Pregunta 6

Análisis: A esta pregunta un 76% indica que no conoce de qué tratan los modelos de madurez mientras que, un 24% tiene conocimientos respecto a este tema.

Pregunta 7: ¿Aplica algún modelo de madurez para evaluar el estado de la seguridad de las redes de información?

Tabla 3. 7

Tabulación Pregunta 7

Valor significado	Frecuencia	%
Si	0	**0**
No	37	**100**
Total frecuencias	**37**	**100%**

Representación gráfica:

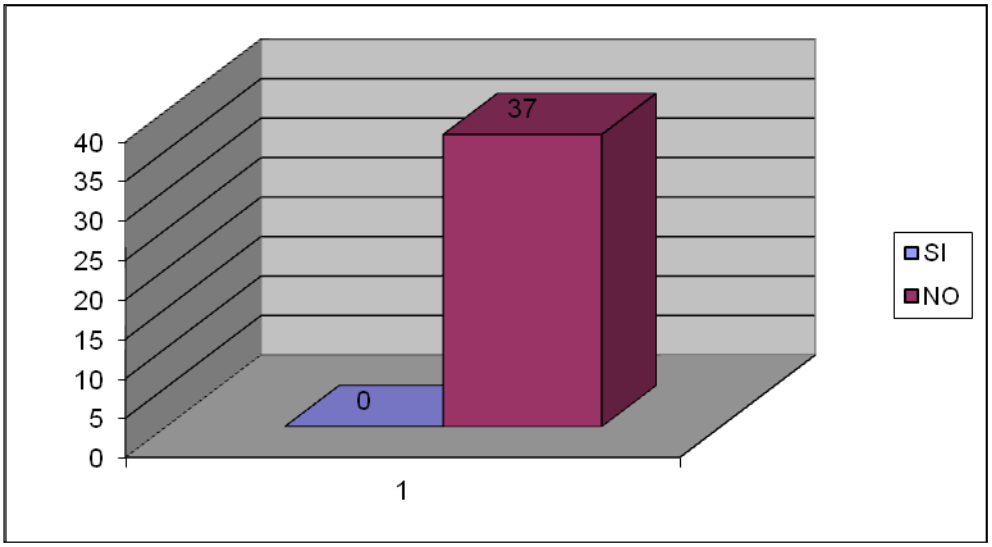


Figura 3. 7 Representación gráfica Pregunta 7

Análisis: La respuesta a esta pregunta es definitiva, el 100% de los encuestados indica que no aplica ningún modelo de madurez para evaluar sus redes de información.

Pregunta 8: ¿Aplica modelos de madurez en otros procesos de la empresa que no se relacionen con seguridad?

Tabla 3. 8

Tabulación Pregunta 8

Valor significado	Frecuencia	%
Si	3	**8.11**
No	34	**91.98**
Total frecuencias	**37**	**100%**

Representación gráfica:

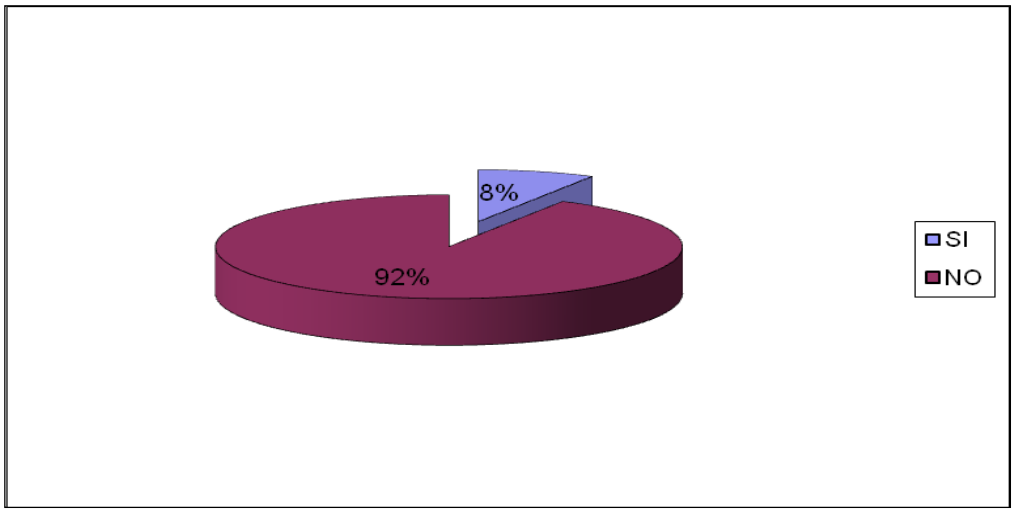


Figura 3. 8 Representación gráfica Pregunta 8

Análisis: El 91.98% responde que no aplica modelos de madurez en otros procesos de la empresa que no tienen relación con seguridad de redes, un 8% indica que si lo aplican.

Pregunta 9: ¿Considera que la aplicación de indicadores, definidos en un procedimiento documentado, ayudaría a mejorar la administración de la seguridad de sus redes de información?

Tabla 3. 9

Tabulación Pregunta 9

Valor significado	Frecuencia	%
Si	33	**89.19**
No	4	**10.81**
Total frecuencias	**37**	**100%**

Representación gráfica:

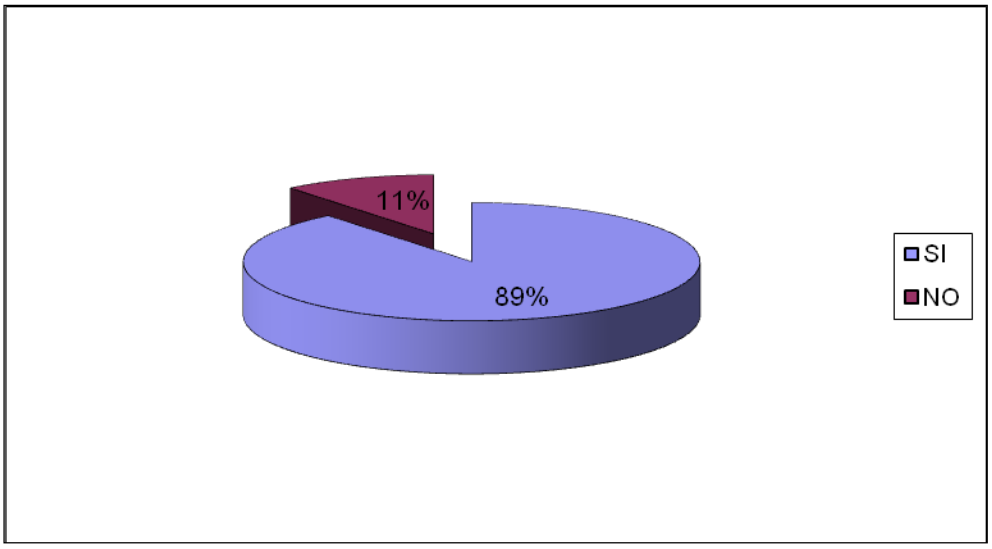


Figura 3. 9 Representación gráfica Pregunta 9

Análisis: El 89% considera que la aplicación de indicadores definidos en un documento mejoraría la administración de la seguridad de sus redes de información. Un 11% no considera que estos indicadores ayudarían en este tema.

Pregunta 10: ¿Estaría dispuesto a aplicar un modelo de madurez ajustado a nuestra realidad, pero basado en modelos aceptados internacionalmente?

Tabla 3. 10

Tabulación Pregunta 10

Valor significado	Frecuencia	%
Si	36	**97.30**
No	1	**2.70**
Total frecuencias	**37**	**100%**

Representación gráfica:

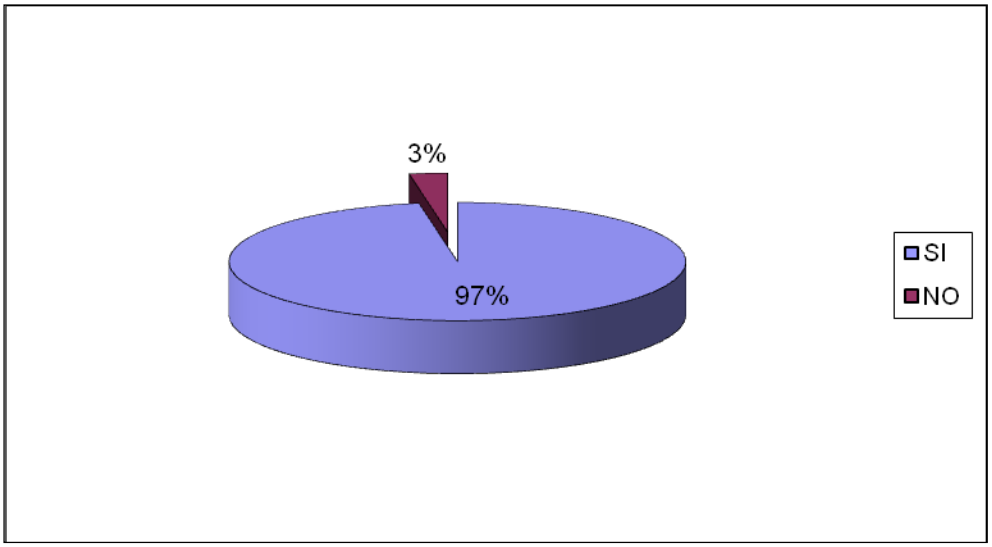


Figura 3. 10 Representación gráfica Pregunta 10

Análisis: Un 97% indica que estaría dispuesto a aplicar modelos de madurez con base en modelos aceptados internacionalmente pero adaptados a nuestra realidad. Un 3% no lo aplicarían.

3.3 Conclusiones parciales

El análisis de los resultados obtenidos permite concluir lo siguiente:

- No existe conocimiento de los modelos de madurez, por lo tanto no son aplicados en casi ningún proceso de la empresa.

- En lo que respecta a seguridad de redes de información no se aplican modelos de madurez.
- A pesar de que un reducido número de encuestados manifestaron conocer sobre los modelos de madurez, ninguno de ellos los aplica.

- La seguridad de la redes de información se evalúa en base a los comentarios del cliente, llamadas a help desk o reportes de terceros.

- Las Pymes no cuentan con herramientas de evaluación periódica que les permita conocer el nivel de madurez de las redes y aplicar correctivos o mejoras.

- Existe apertura para adoptar herramientas de evaluación de la seguridad de las redes de información, basadas en modelos ampliamente conocidos.

- La seguridad de las redes de información está a cargo de personal interno en su mayoría, por lo que es recomendable utilizar modelos de fácil acceso y aplicación, sin que se requiera la contratación de terceros que realicen este tipo de implementaciones.

- El término “modelo de madurez” en el campo de IT es nuevo en nuestro medio, aún en empresas grandes y multinacionales.

- Las redes de información se consideran estables, pero con muy pocas métricas aplicadas.

- La aplicación de indicadores y métricas se considera una herramienta de ayuda a la administración de la seguridad de redes de información.

- El único modelo de madurez mencionado en las encuestas es CMM aplicado en el desarrollo de software.

CAPITULO IV

ANALISIS DE MODELOS DE MADUREZ

4.1 Selección de los Modelos

De la investigación previa se estableció como premisa que si bien existe cierto interés por aprender sobre este tema, los modelos de madurez no son muy conocidos en nuestro medio.

En función del conocimiento establecido en el Capítulo II, se realizó un estudio comparativo de los modelos definidos como representativos en razón de ser los más conocidos, los que se están usando en otros países, los más flexibles para adecuarse al propósito que se busca en esta tesis y que tienen aplicación en el campo de la seguridad de la información.

Para la obtención de los “modelos base” se evaluaron las principales condiciones que se requieren en el modelo final; ésta evaluación se resume en la Tabla 4.1, en la que se ha valorado cada una de las características por modelo aplicando la siguiente escala:

0 = no cumple / no aplica
1 = bajo
2 = medio
3 = alto

Tabla 4.1
Matriz de análisis comparativo de selección de modelos base

CARACTERISTICAS A CUMPLIR	MODELOS DE MADUREZ		
	CMM	COBIT	ISM3
ENFOQUE	Calidad	Control	Seguridad
Flexible/Adaptable	1	1	3
Mencionado en las encuestas	3	0	0
Pionero/Modelo Base	3	0	0
Métricas de fácil aplicación	1	2	2
Conocido	2	3	2
Alineación con los objetivos del negocio	0	3	3
TOTAL	10	9	10

Del soporte bibliográfico revisado y una vez asignado un valor a los aspectos más relevantes de cada modelo, se extrajeron 2 modelos: CMM e ISM3, los cuales se constituyeron en la referencia de valor agregado para este estudio.

MODELO CMM

Se constituyó en el modelo de madurez pionero, especializado en procesos de desarrollo de software. Es ampliamente utilizado por empresas norteamericanas, quienes inicialmente se basaron en este modelo para evaluar y calificar a las empresas desarrolladoras; también es utilizado por empresas chinas, indias y latinoamericanas.

CMM tiene varias versiones y actualizaciones que son aplicadas en diferentes áreas. Algunas versiones son ampliamente usadas y adoptadas como estándar a nivel mundial, principalmente por las oportunidades de negocios con los Estados Unidos; una de sus actualizaciones es CMMI la

cual cada año tiene más empresas certificadas, tal como lo indica la Tabla 4.2:

Tabla 4.2
Cantidad de empresas certificadas en CMMI a nivel mundial año 2012

País	Certificaciones
China	**1508**
Estados Unidos	**865**
India	**382**
España	**153**
Corea del Sur	**101**
Brasil	**101**
México	**94**
Japón	**89**
Taiwán	**67**
Francia	**65**
Resto del Mundo	**606**
TOTAL	**4031**

Fuente: (CMMI en Mexico y el mundo, 2012)

CMM cumple con los siguientes aspectos:

- ✓ Pionero
- ✓ Conocido a nivel mundial
- ✓ Base de varios modelos aplicados a diferentes áreas
- ✓ Único modelo mencionado en las encuestas realizadas

MDELO ISM3

Trabaja conjuntamente con los objetivos del negocio y ha sido enfocado a la seguridad de la Información. Puede aplicarse con excelentes resultados en organizaciones con experiencia de ITIL, COBIT e ISO27001 o que deseen iniciarse en estos temas.

Es así como ISM3 cumple con los siguientes aspectos:

- ✓ Su enfoque cubre principios de seguridad
- ✓ Adaptable

- ✓ Nuevo
- ✓ Alineado con los objetivos del negocio.

No existen estadísticas exactas del uso y difusión de ISM3 a nivel mundial, sin embargo se cuentan entre los casos de éxito de este modelo las siguientes instituciones (Aceituno, vaceituno@inovement.es, 2014):

- ➢ Bankia (antes Cajamadrid)
- ➢ Fuerzas Armadas Suizas
- ➢ Banco Nacional de Panamá

La comparación de las características específicas de cada uno de ellos permitió definir:

- Cómo ellos pueden adaptarse al objetivo de este estudio.
- Qué variaciones pueden aplicarse a fin de obtener el diseño de un nuevo modelo.
- Definir que el proceso a realizar era la ejecución de un "benchmarking" de los modelos existentes.
- El "benchmarking" definiría la aplicación a las Pymes ecuatorianas.

4.2 Análisis del modelo CMM

CMM aplica conceptos de calidad total para mejorar los procesos de desarrollo de software y así lograr excelencia y calidad en el producto final. Tiene como propósito describir las prácticas de ingeniería en cada nivel de madurez; con esto se logra mejorar la productividad reflejada en la calidad, los costos y tiempos de entrega.

4.2.1 Estructura

La Figura 4.1 resume la estructura de CMM, que se compuesta de varias “sub-estructuras”, siendo la más importante el nivel de madurez ya que ella definirá la situación de la empresa. Los niveles de madurez son 5: Inicial, Repetible, Definido, Administrado, Optimizado.

Cada nivel está compuesto de KPA’s y éstas se organizan de acuerdo a características comunes.

Estas KPA’s son un conjunto de prácticas y actividades que al cumplirse indican que se puede pasar a un nivel superior. De esta forma CMM indica progreso, en función del avance en los niveles.

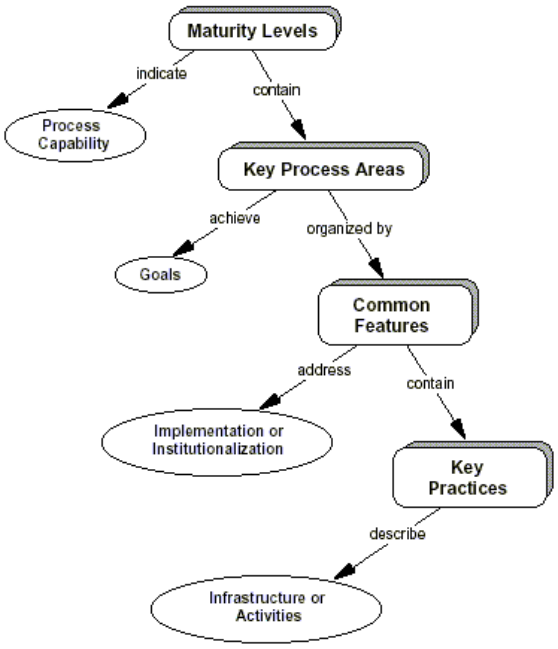


Figura 4.1 Estructura de CMM
Fuente: (Fau, 2006)

4.2.2 Niveles de madurez y KPA’s

Cada nivel de madurez es una base que irá evolucionando hasta lograr la madurez de los procesos y por tanto del producto.

Los niveles tienen por objetivo mejorar la capacidad de las empresas de desarrollo, es decir no se aplica a cada proyecto de forma individual, sino que la mejora es en todos los procesos de forma global y por ende para todos los proyectos que se ejecuten.

Tal como lo indica la Tabla 4.3, las KPA's tienen características comunes, que describen si la implementación de una KPA es efectiva, repetible y perdurable. Estas características son:

- Compromiso de realización.
- Capacidad de realización.
- Actividades realizadas.
- Mediciones y análisis.
- Verificación de implementación.

Tabla 4.3
Niveles de madurez CMM + KPA's

NIVEL	CARACTERISTICAS	KPA's
1: inicial	No provee características propicias para el desarrollo. No existe garantía de calidad en el producto.	**No aplica**
2: Repetible	Se han establecido ciertos procesos de planificación y administración. Repitiendo experiencias anteriores.	- Administración de la configuración del Software. - Aseguramiento de la Calidad del software - Seguimiento del proyecto de software. - Planificación del proyecto del software. - Administración de requerimientos. - Administración de subcontratos de software.

CONTINUA ⟶

3: Definido	Existe un proceso de desarrollo estándar, documentado e implementado en toda la organización.	- Revisiones - Coordinación de los grupos. - Ingeniería del producto de software - Administración del software integrado. - Programa de entrenamiento - Definición de los Procesos de la organización. - Enfoque de los Procesos de la organización.
4: Administrado	Se mide calidad y productividad. El cliente conocerá tanto la capacidad como el riesgo del proceso inclusive antes del inicio del proyecto. Las métricas son sumamente importantes.	- Administración de la calidad del Software. - Administración de los procesos Cuantitativos.
5: Optimizado	El mejoramiento es constante. Se previene la ocurrencia de fallas. Cada proceso debe estar completa y detalladamente definido y debe ser seguido al pie de la letra.	- Administración de los cambios de Procesos. - Administración de los cambios Tecnológicos. - Prevención de Defectos.

Las principales características que identifican a CMM se resumen en la Tabla 4.4:

Tabla 4.4
Resumen de características de CMM

Característica	Descripción
Enfoque	El modelo es Orientado a Procesos.
Medición/Evaluación	No existe información de métricas precisas
Base de su estructura	5 niveles de madurez
Alineación con otras normas y Estándares	No se conoce que su estructura sirva de base para obtener otras certificaciones.
Otros	El modelo se ha convertido en base de diversas variantes aplicadas a una amplia gama de áreas.

4.2.3 Métricas

CMM aplica métricas de procesos a partir del Nivel 4, ya que al alcanzar este nivel los procesos están documentados, son conocidos por todo el personal y aplicados en cada actividad del desarrollo de software.

Sin embargo no existe una definición clara de la métricas que deben aplicarse en este nivel y posteriores. Como norma general las métricas están orientadas a cambios en los procesos de acuerdo a la retroalimentación que conlleven a incrementar los niveles de calidad del producto. La Tabla 4.5 presenta ejemplos de las métricas utilizadas:

Tabla 4.5
Ejemplo de tipos de Métricas utilizadas en CMM

Nivel de madurez	Características	Tipos de métricas utilizadas
5. Optimización	Mejoramiento de la realimentación del proceso	Proceso más la realimentación para cambiar el proceso
4. Gestionado	Proceso de medición	Proceso más la realimentación para controlar
3. Definido	El proceso está definido y establecido	Producto
2. Repetible	El proceso dependiente de sus componentes individuales	Dirección de proyecto
1. Inicial	Desordenado	Base de comparación.

Fuente: (Belgrado, s.f.)

4.2.4 Determinación de ventajas y desventajas

- Propone las mejoras de procesos a nivel global, de esta forma toda la organización puede aplicar estos procesos a todos los proyectos.

- CMM describe las prácticas para cada nivel de madurez y plantea como seguirlas. Sin embargo, los avances se miden por nivel y no existen evaluaciones “parciales”. Es decir que para considerar a la empresa “certificable” deben cumplirse sin excepción todos los niveles.

- Aunque menciona la importancia de las métricas no indica claramente cuáles son las métricas mínimas para una correcta implementación.

4.3 Análisis del modelo ISM3

ISM3 no tiene como objetivo conseguir un sistema invulnerable o alcanzar “riesgo cero”, más bien trata de mantener un nivel de riesgo

aceptable y alinear los objetivos de seguridad con los objetivos del negocio, es decir, garantizar la seguridad de los objetivos de la organización sin descuidar la seguridad de la información.

Está alineado con los principios de gestión de calidad ISO 9001, por lo tanto vincula la seguridad a las necesidades del negocio, es decir que, ISM3 no solo se centra en prevenir los ataques a los sistemas de información, sino en cumplir con los objetivos de la organización a pesar de los ataques y errores que se presenten.

El diseño de niveles dentro de los modelos de madurez permite a las organizaciones invertir un 20% y obtener un 80% de los resultados (regla del 80/20); es decir que cada organización puede tomar la mayoría de los niveles como punto de referencia para sus propios sistemas de gestión inicial y utilizar el resto de niveles de acuerdo a cómo evolucione la organización.

Según Vicente Aceituno Canal: “Con los niveles de madurez, las organizaciones pueden priorizar la inversión y medir el progreso” (Aceituno Canal, 2008)

Usa un enfoque orientado a procesos, manejando el principio de: “lo que no se puede medir, no se puede manejar y lo que no se puede manejar, no se puede controlar” (Aceituno Canal, 2008)

La medición de los procesos se realiza a través de métricas, esto permite mostrar resultados, definir como los resultados benefician a la organización y saber cómo influyen las mejoras en los procesos.

4.3.1 Estructura

Su estructura está basada en niveles (Figura 4.2). Aplica un modelo de gestión a través de tareas operativas, estratégicas y tácticas a fin de definir activos, recursos y medidas a implementar.

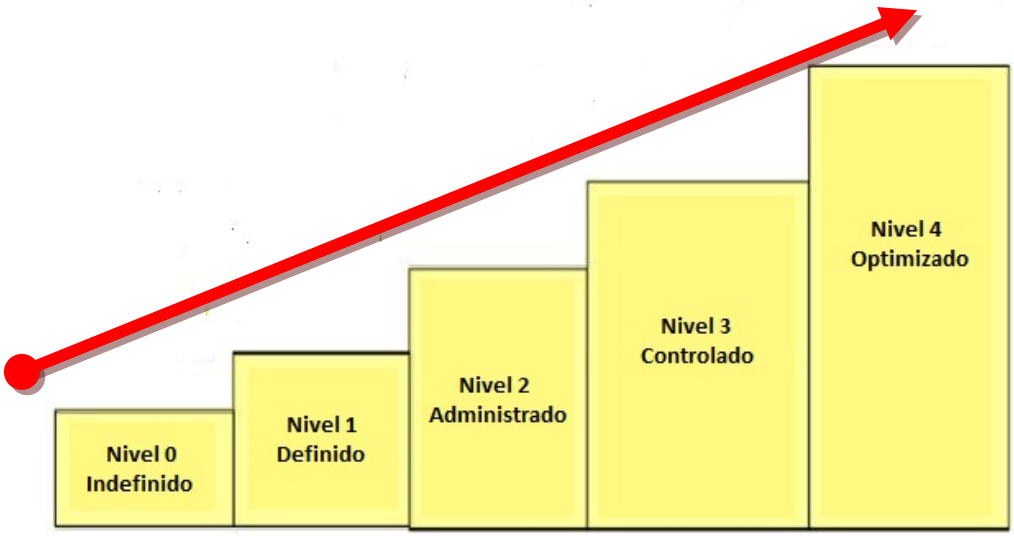


Figura 4.2 Niveles ISM3

4.3.2 Niveles de madurez

Sus 5 niveles de madurez permiten adaptarse a cualquier tipo de empresa grande o pequeña, madura o en proceso; incluso permite reutilizar recursos y objetivos de seguridad existente o en proceso. Cada empresa puede detenerse en el nivel que esté más acorde a su situación e ir mejorándolo para alcanzar el siguiente nivel. Los niveles de madurez de este modelo se indican en la Tabla 4.6

Esta es una de sus principales características, ya que la organización puede avanzar a su propio ritmo y mantenerse en el nivel que considere “seguro”, sin estar obligado a completar todos los niveles del modelo.

Tabla 4.6
Niveles de madurez ISM3

NIVEL	CARACTERISTICAS
0: Indefinido	No reduce significativamente el riesgo. Es mejor no permanecer en este nivel.
1: Definido	Se consigue una reducción aceptable de riesgos técnicos con una mínima inversión. Recomendable para organizaciones con objetivos de seguridad bajos.
2: Administrado	Mayor reducción de riesgos con una inversión modesta. Recomendable para organizaciones en entornos normales de seguridad.
3: Controlado	Mayor reducción de riesgo con una inversión considerable. Se recomienda para organizaciones con objetivos de seguridad ambiciosos en entornos normales o de alto riesgo.
4: Optimizado	Mayor reducción de riesgos con una inversión alta. Recomendado para organizaciones que comparten información sensible.

4.3.3 Métricas

ISM3 aplica métricas de gestión de procesos; esto permite que cada proceso pueda ser mejorado de forma constante y sostenible. Las métricas definidas para este modelo permiten medir: disponibilidad, actividad, cobertura y actualización de cada proceso, tal como lo indica la Tabla 4.7.

La utilización de métricas asegura contar con los criterios cuantitativos suficientes para la toma de decisiones y una eficiente asignación de recursos (materiales, tecnológicos, personal, tiempo, dinero). Esto se traduce en reducción de riesgo y mejor retorno de la inversión (ROI, Return of Investment)

Tabla 4.7
Métricas usadas en ISM3 (Traducción propia)

TIPO DE METRICA	DESCRIPCION
Actividad	Número de salidas producidas. Estadísticas (edad promedio, tiempo entre salidas, tiempo entre entradas/salidas, etc)
Cobertura	Proporción de todas las unidades de entrada cubiertas por el proceso. Proporción de todos los parámetros de muestreo o prueba
No disponibilidad	Número de interrupciones a la operación normal de los procesos. Frecuencias de interrupciones a la operación normal de los procesos.
Eficacia	Número de entradas. Media de tiempo entre entradas. Fracción de entradas que producen una salida.
Eficiencia	Relación entre el número de resultados presentados por este proceso a los recursos disponibles para este proceso en el uso actual. Relación de la proporción de todas las unidades de entrada cubierto por este proceso de los recursos disponibles para este proceso en el uso actual. Relación entre la proporción de unidades de entrada muestreadas o probados de acuerdo con los recursos disponibles para este proceso en uso actual.
Carga	Proporción de los recursos en uso actual.
Calidad	Exactitud, precisión u otras mediciones de la aptitud del propósito de la salida.

Fuente: (OpenGroup, 2011)

4.3.4 Niveles de responsabilidad

Una característica importante de ISM3, es la de definir claramente a los responsables de cada tipo de procesos y que están clasificados en 3 grupos:

- Estratégicos
- Operacionales

- Tácticos

Con esto se consigue que la información siempre esté en conocimiento de los responsables de cada proceso y cada uno reporte al nivel superior.

La figura 4.3 resume la jerarquía de las responsabilidades y el flujo de los reportes:

Figura 4.3 Jerarquía de reportes de la gestión de seguridad de (Traducción propia) Fuente: (OpenGroup, 2011).

4.3.5 Determinación de ventajas y desventajas

- En cada nivel de madurez se hace referencia a otros estándares que pueden ser complementados o trabajar a la par de ISM3.

- Fomenta la colaboración y comunicación entre los diferentes responsables de los procesos (líderes, gestores, técnicos), ya que existe una distribución detallada de las responsabilidades.

- Amplio aporte a las organizaciones con experiencia en ISO27001 e ITIL.

- Cambia la imagen de la seguridad de la información y en general de la tecnología ante los ejecutivos de la empresa, que la pueden visualizar como una inversión necesaria y no sólo como gasto.

- La empresa puede mantenerse en un nivel aceptable que cubra los objetivos del negocio (temporal), sin la obligatoriedad de cubrir todos los niveles en una sola implementación.

Las características de ISM3 se resumen en la Tabla 4.8:

Tabla 4.8
Resumen de características de ISM3

Característica	Descripción
Enfoque	El modelo es Orientado a Procesos.
Medición/Evaluación	Se realiza a través de Métricas básicas definidas
Base de su estructura	Considera los niveles de madurez aplicados a los objetivos del negocio
Alineación con otras normas y estándares	El documento de gestión del ISM3 puede aplicarse como base para ISO 9001 y como herramienta para cumplir con los requerimientos de ISO 27001.

4.4 ANALISIS COMPARATIVO DE CMM E ISM3

Para conocer diferencias y similitudes, se realizó un proceso de comparación o “Benchmarking”. Esto permitió extraer:

- Las características relevantes de cada uno.
- Los procesos comunes.

- Los procesos aplicables para una Pyme.
- Características aplicables a la seguridad de las redes de información.
- Un bosquejo de estructura del modelo propuesto.
- Una definición de estructura del modelo propuesto.

Para la comparación de estos modelos se consideraron las KPA's de CMM versus los procesos requeridos por ISM3, y los niveles de madurez, todo esto en conjunto proporcionó una idea general de las tareas a desarrollarse para la aplicación del modelo y su definición formal.

Las KPA's del modelo CMM abarcan tareas de gestión, organizacionales e ingeniería, por lo que se las clasificó de acuerdo a su ámbito; de esta forma, se logró establecer comparaciones entre grupos similares de tipos de tareas a fin de mantener una correspondencia y analizar el enfoque de cada modelo.

Posteriormente se analizaron los niveles de madurez que aplica cada modelo.

4.4.1 Comparación de Tareas

De acuerdo al ámbito de cada una de las KPA's, se las clasificó de la siguiente forma dentro de los 3 grupos de tareas:

- **Tareas de Gestión**

- Gestión de acuerdos y contratos con proveedores
- Gestión de requisitos
- Gestión integrada del proyecto
- Gestión de la calidad del software
- Gestión cuantitativa de procesos
- Gestión del cambio en los procesos

- **Tareas Organizacionales**

- Planificación, seguimiento y control de proyectos
- Coordinación dentro del grupo de trabajo
- Programa de formación
- Revisión detallada de los procesos
- Definición del proceso organizativo
- Enfoque hacia los procesos organizativos

- **Tareas de Ingeniería**

- Gestión de la configuración de software
- Aseguramiento de la calidad del software
- Ingeniería del producto software
- Prevención de defectos
- Gestión de los cambios tecnológicos

A su vez ISM3 clasifica sus tareas de la siguiente forma (Consortium, 2007) (traducción propia):

- **Tareas Estratégicas**

SSP1.- Informar a los directivos
SSP2.- Coordinación
SSP3.- Alcanzar visión estratégica
SSP4.- Definir reglas para separación de responsabilidades TPSRSR
SSP6.- Asignar recursos para seguridad de la información

- **Tareas Tácticas**

TSP1.- Informar a la administración estratégica

TSP2.- Gestionar los recursos asignados
TSP3.- Definir las metas de seguridad
TSP4.- Gestionar los niveles de servicio
TSP6.- Definir ambientes y ciclos de vida
TSP7.- Investigar antecedentes y referencias
TSP8.- Seleccionar al personal de seguridad
TSP9.- Capacitar al personal de seguridad
TSP10.- Definir procesos disciplinarios
TSP11.- Alcanzar conciencia de seguridad
TSP13. - Gestión de seguros

- **Tareas Operativas**

OSP1.- Informar a la gestión táctica
OSP2.- Seleccionar herramientas para la implementación de medidas de seguridad
OSP3.- Gestión de inventario
OSP4.- Controlar el cambio del ambiente de los sistemas de información
OSP5.- Refaccionar el ambiente
OSP6.- Limpiar el ambiente
OSP7.- Fortalecer el ambiente
OSP8.- Controlar el ciclo de vida de desarrollo del software
OSP9.- Controlar los cambios de las medidas de seguridad
OSP10.- Gestionar los respaldos
OSP11.- Control de acceso
OSP12.- Llevar registro de usuarios
OSP14.- Gestionar la protección del ambiente físico
OSP15.- Gestionar la continuidad de operaciones
OSP16.- Gestionar el filtrado y segmentación
OSP17.- Gestionar la protección contra malware
OSP19.- Auditoría Técnica Interna

OSP20.- Emular incidentes

OSP21.- Comprobar la calidad de la información

OSP22.- Monitorizar alertas

OSP23.- Detectar y analizar eventos

OSP24.- Manejar los incidentes y pseudo-incidentes

OSP25.- Realizar análisis forense

OSP26.- Gestión de la disponibilidad y mejoramiento de la fiabilidad

OSP27.- Gestión de archivo

Comparación de tareas Organizacionales (CMM) con Estratégicas (ISM3)

Tabla 4.9
Tareas organizacionales vs Tareas Estratégicas

CMM TAREAS ORGANIZACIONALES	ISM3 TAREAS ESTRATÉGICAS	ANÁLISIS
- Planificación, seguimiento y control de proyectos - Coordinación dentro del grupo de trabajo - Programa de formación - Revisión detallada de los procesos - Definición del proceso organizativo - Enfoque hacia los procesos organizativos	SSP1.- Informar a los directivos SSP2.- Coordinación SSP3.- Alcanzar visión estratégica SSP4.- Definir reglas para separación de responsabilidades TPSRSR SSP6.- Asignar recursos para seguridad de la información	Las tareas estratégicas de ISM3 se encargan de la definición y coordinación de las actividades y procesos, así como la definición de objetivos estratégicos y la delegación de responsabilidades. La gestión estratégica es el enlace entre los directivos de la organización y el equipo de seguridad, esta etapa requiere el entendimiento del funcionamiento de la organización y de sus objetivos. Además, se asignan los recursos necesarios para las tareas de seguridad. CMM con sus tareas organizacionales define los procesos acordes a los objetivos

CONTINUA ⟶

	organizacionales (enfocado en las tareas de desarrollo), planifica y coordina los proyectos. Un punto importante es que CMM define un proceso de formación para el personal, el mismo que también es controlado.

Comparación de tareas de Gestión (CMM) y Tácticas (ISM3)

Tabla 4.10
Tareas de gestión vs Tareas Tácticas

CMM TAREAS DE GESTIÓN	ISM3 TAREAS TÁCTICAS	ANÁLISIS
- Gestión de acuerdos y contratos con proveedores - Gestión de requisitos - Gestión integrada del proyecto - Gestión de la calidad del software - Gestión cuantitativa de procesos - Gestión del cambio en los procesos	TSP1.- Informar a la administración estratégica TSP2.- Gestionar los recursos asignados TSP3.- Definir las metas de seguridad TSP4.- Gestionar los niveles de servicio TSP6.- Definir ambientes y ciclos de vida TSP7.- Investigar antecedentes y referencias TSP8.- Seleccionar al personal de seguridad TSP9.- Capacitar al personal de seguridad TSP10.- Definir procesos disciplinarios TSP11.- Alcanzar conciencia de seguridad TSP13.- Gestión de seguros	ISM3 a través de las tareas tácticas controla el desempeño del ISM, esto incluye el correcto manejo de los recursos y las tareas asignadas al personal. Además define las metas e indicadores de eficiencia y los ambientes y ciclos de vida. CMM con sus tareas de gestión se encarga de administrar los recursos del proyecto, incluyendo el personal y los proveedores involucrados. Administra los cambios en los procesos y en la evaluación de los resultados de los procesos aplicados.

Comparación de tareas de Ingeniería (CMM) y Operativas (ISM3)

Tabla 4.11
Tareas de ingeniería vs Tareas Operativas

CMM TAREAS DE INGENIERÍA	ISM3 TAREAS OPERATIVAS	ANÁLISIS
- Gestión de la configuración de software - Aseguramiento de la calidad del software - Ingeniería del producto software - Prevención de defectos - Gestión de los cambios tecnológicos	OSP1.- Informar a la gestión táctica OSP2.- Seleccionar herramientas para la implementación de medidas de seguridad OSP3.- Gestión de inventario OSP4.- Controlar el cambio del ambiente de los sistemas de información OSP5.- Refaccionar el ambiente OSP6.- Limpiar el ambiente OSP7.- Fortalecer el ambiente OSP8.- Controlar el ciclo de vida de desarrollo del software OSP9.- Controlar los cambios de las medidas de seguridad OSP10.- Gestionar los respaldos OSP11.- Control de acceso OSP12.- Llevar registro de usuarios OSP14.- Gestionar la protección del ambiente físico OSP15.- Gestionar la continuidad de operaciones OSP16.- Gestionar el filtrado y segmentación OSP17.- Gestionar la protección contra malware OSP19.- Auditoría Técnica Interna OSP20.- Emular incidentes OSP21.- Comprobar la calidad de la información	Las tareas operativas de ISM3 se encargan de aplicar las medidas de seguridad definidas en las etapas anteriores. Con la implementación y seguimiento a cada uno de los procesos necesarios para mantener la seguridad de la información, permite la retroalimentación a los niveles superiores. Este grupo de tareas manejan los incidentes que puedan presentarse y analizan las posibles causas a fin de mitigarlas. CMM a través de las KPA's de ingeniería gestiona y administra todo el ciclo de vida del software, cubriendo la prevención de los defectos en el producto final. Se controla la evaluación y aplicación de los cambios necesarios en la tecnología a fin de aumentar valor a la calidad del producto.

CONTINUA ⟶

	OSP22.- Monitorizar alertas OSP23.- Detectar y analizar eventos OSP24.- Manejar los incidentes y pseudo-incidentes OSP25.- Realizar análisis forense OSP26.- Enhanced Reliability and Availability Management OSP27.- Gestión de archivo

4.4.2 Comparación de Niveles de Madurez

El nivel 0, en realidad no puede considerarse como un “nivel” dentro de la implementación misma del modelo, sino como el “estado inicial lógico” cuando una organización da el primer paso para implementar un modelo de madurez.

El nivel 1 en ISM3, puede adoptarse como un nivel inicial, ya que se aplican regulaciones mínimas de seguridad, en CMM sigue siendo el “estado inicial” de la organización.

Los niveles 2 y 3 en ambos modelos son aceptables, ya que existe inversión, procesos detallados, reducción de riesgo, disciplina. Estos niveles conforman un nivel intermedio de madurez.

Los niveles 4 y 5, conforman los niveles de madurez más altos, en los que ya existe: reducción de riesgo, procesos de mejoramiento, aplicación de métricas a los procesos. En este punto las organizaciones están completamente comprometidas con el modelo y no solo se conforman con mantenerse en este nivel, sino que se implementan mejoras a los procesos documentados.

A continuación se muestra en forma tabular la matriz de comparación de los niveles de cada modelo:

Tabla 4.12
Comparación de los niveles de madurez de CMM e ISM3

NIVEL DE MADUREZ	CMM	ISM3	ANÁLISIS
0	No aplica	No existe reducción de riesgo.	Es el escalón inicial. La mayoría de organizaciones que se inician en la aplicación de normas, estándares, etc., se encuentran en este estado
1	Sin garantía de calidad en el producto.	Mínima inversión, reducción considerable de riesgos.	En esta etapa no existen procesos definidos pero la organización reconoce que existen problemas que deben solucionarse. Si bien en ocasiones pueden desarrollarse proyectos con éxito, ninguno de ellos está planificado ni tiene el control de los recursos. No puede garantizarse calidad.
2	Existen ciertos procesos de planificación y administración.	Inversión modesta, mayor reducción de riesgos.	Existen procesos planificados, por lo tanto se aplica monitoreo y control de las diferentes etapas. El desarrollo de los procesos es disciplinado y los resultados cumplen estándares básicos de calidad.
3	Los procesos son estándar y documentados.	Inversión considerable, mayor reducción de riesgo.	Existe documentación detallada de cada uno de los procesos y toda la organización tiene conocimiento de ello. Los problemas pueden detectarse antes de que ocurran de tal forma que pueden tomarse medidas de mitigación antes de que afecten al resultado final.

CONTINUA ⟶

4	Aplicación de métricas. Se mide calidad y productividad.	Inversión alta, mayor reducción de riesgos.	Además de seguir al pie de la letra los procesos documentados, en este nivel se aplican métricas. Se pueden definir claramente todos los recursos necesarios para obtener el resultado deseado dentro de los tiempos establecidos.
5	Mejoramiento constante. Procesos detallados y definidos.	No aplica.	Una vez que la organización adopta todos los procesos como una práctica diaria y, estos se encuentran completamente controlados y comprendidos, se pueden ir haciendo mejoras.

4.5 Conclusiones parciales

Debido a que CMM es la base de muchos de los modelos de madurez que se han desarrollo desde su aparición, es innegable que existe relación entre CMM e ISM3, a pesar de que por el objetivo al que cada uno de ellos se aplica, no todos los temas en uno u otro son abordados por completo.

No es fácil determinar exactamente el nivel de similitud o diferencia de estos modelos, ya que el ámbito de aplicación de cada uno es diferente, sin embargo, se puede apreciar que ISM3 es mucho más específico y detallado en las tareas a ejecutarse, lo que facilita su implementación y la consecución de los objetivos; mientras que CMM es más general en los procesos que deben cubrirse para cada nivel, dejando un mayor rango de posibilidades a elegir, lo que puede convertir a los procesos en un conjunto de tareas que no finalicen dentro de un tiempo definido, dilatando el tiempo de implementación. Es decir los procesos se volverían eventualmente problemáticos.

Un aspecto relevante en ambos modelos, es la necesidad de documentar y revisar los procesos y aplicarlos tal como están definidos. Esto permite

que toda la organización tenga conocimiento de la correcta aplicación de los procesos y que se pueda obtener retroalimentación de cada una de las áreas involucradas en las evaluaciones para aplicar las mejoras necesarias y actualizar la documentación respectiva.

Respecto a las métricas que utilizan los modelos, las pocas que se describen para CMM son bastante generales, lo que puede originar que cada organización aplique más o menos número de métricas, y entre ellas se pueden olvidar las realmente determinantes para el incremento en la calidad del producto. Esto a diferencia de ISM3 que determina pocas métricas sencillas, que pueden ser comprendidas y evaluadas de mejor forma, tanto por personal técnico como por directivos de otras áreas.

CMM no define claramente las métricas a aplicarse, y se basa en métodos de análisis de riesgos como proceso inicial. Define prácticas de ingeniería en cada nivel de madurez, hasta lograr el desarrollo de un producto de calidad en el nivel 5.

CMM hace énfasis en la calidad del producto final e ISM3 en los objetivos del negocio.

También es importante recalcar, que en ningún caso es necesario aplicar estrictamente todo lo que indica la teoría, ya que cada empresa debe adoptar las métricas más eficientes para su realidad e inclusive añadir otras. Al aplicar correctamente cualquiera de los modelos se obtienen varios beneficios tanto a nivel de ingeniería como a nivel económico y organizacional.

CAPITULO V

FORMALIZACIÓN DEL MODELO PROPUESTO

5.1 Lineamientos generales

Considerando las características de las Pymes ecuatorianas, es necesario definir los lineamientos que se aplicarán al modelo propuesto, ya que la realidad de este tipo de organizaciones indica que:

- No facilita la obtención de certificaciones.
- No se prioriza la aplicación de normas internacionales de forma continua.
- No existe un sólido compromiso de los directivos.
- Es deficiente la asignación de recursos humanos y económicos en áreas que no corresponden al core del negocio.

Después de analizar cada uno de los enfoques de los modelos estudiados, se determina que ISM3 es el que mejor se adapta a los objetivos de este trabajo pues mantiene su enfoque en los objetivos del negocio, lo que es atractivo para los ejecutivos de la empresa además de que su ámbito de aplicación es la seguridad tecnológica.

Al estar alineado con los objetivos de negocio, ISM3 no depende de procesos de análisis de riesgo y esto genera una ventaja adicional para su implementación, ya que los métodos de análisis de riesgos generalmente son costosos, a esto debemos sumar el tiempo adicional y la experiencia necesarios para su aplicación.

Finalmente, ISM3 busca un nivel de seguridad aceptable, equilibrando los objetivos de negocio con los objetivos de seguridad sin convertirse en una camisa de fuerza para la empresa, por lo tanto se convierte en una base que abarca tareas relacionadas con seguridad tecnológica y mantiene la herencia de CMM.

Respecto a la gestión de tareas, ISM3 plantea 3 niveles de gestión que se traducen en 3 grandes grupos de tareas, sin embargo para el caso de las Pymes dado su tamaño y recursos, se fusionaran las tareas Estratégicas y Tácticas, por lo tanto también sus responsabilidades.

El proceso de documentación, mencionado en ambos modelos base, permite garantizar la definición de las tareas y el control de las versiones aprobadas que deberán ser puestas en conocimiento del personal responsable en cada etapa; en consecuencia debe mantenerse.

5.1.1 Niveles

De la comparación de los modelos anteriormente estudiados, se ha determinado que la evaluación por niveles permite obtener una visión rápida de la situación de la empresa e indica las tareas que se deben realizar para escalar en los niveles del modelo.

El modelo propuesto estará formado por 5 niveles:

- Nivel cero “0”, para definir el estado inicial de una empresa que decide acoger el modelo de madurez. Este será el nivel en el que ubicará la empresa cuando inicia la aplicación del modelo.

- Niveles 1 y 2, o niveles básicos en los que la empresa realizará un levantamiento de información inicial para conocer su situación y a continuación, decidir qué y a qué necesita

aplicar las políticas de seguridad definidas en relación con los objetivos del negocio. Muchas empresas pueden alcanzar estos niveles y mantenerse en ellos, sin embargo, a pesar de que pueden parecer niveles bastantes estables, no son los niveles finales y, dependiendo de las necesidades del negocio y recursos disponibles se puede avanzar.

- Nivel 3, es uno de los niveles avanzados, en los que toda la empresa tiene conciencia de seguridad y todos los procesos del negocio están alineados con ella. En este nivel, se realizarán constantes revisiones y correcciones a los procesos definidos inicialmente; obviamente la inversión de recursos es mayor.

- Nivel 4, este nivel es dedicado al cumplimiento de objetivos y aplicación de métricas para la evaluación. La retroalimentación debe ser constante.

5.1.2 Gestión Estratégica y Táctica

Los responsables de esta gestión serán los encargados de reportar a los ejecutivos/gerentes del negocio a fin de obtener y mantener su compromiso.

Los objetivos a cumplir en esta gestión son:

- Coordinar y liderar el proceso de implementación del modelo, definiendo objetivos de seguridad consistentes con los objetivos del negocio.
- Analizar las revisiones de las versiones del modelo.
- Gestionar la delegación de recursos.
- Definir los responsables de cada rol y sus funciones.

A continuación se detallan las tareas propuestas para el nuevo modelo, fusionando las tareas de la gestión estratégica con las de la gestión táctica:

Tabla 5.1
Propuesta de tareas para la gestión estratégica

TAREA ESTRATÉGICA MODELO ORIGINAL	TAREA ESTRATÉGICA PROPUESTA	ANÁLISIS
SSP1-Informar a los accionistas	STSP1-Informar a los ejecutivos	La documentación e información a los niveles superiores se mantiene, debido a su importancia para la correcta toma de decisiones.
SSP2-Coordinar **SSP6-Asignar recursos para seguridad de la información**	STSP2-Coordinación, asignación y gestión de recursos	Se integran las actividades de coordinación y asignación de recursos. La coordinación de personal y recursos es fundamental para asegurar el cumplimiento de las actividades y alcanzar los objetivos de la organización.
SSP3-Alcanzar visión estratégica	STSP3-Definir objetivos organizacionales y de seguridad de las redes de información, así como metas e indicadores para los procesos.	Es necesario entender el ambiente estratégico de la organización (objetivos) para definir correctamente las políticas de seguridad.
SSP4-Definir las reglas para la separación de responsabilidades: transparencia, particionado, supervisión, rotación y separación de responsabilidades (TPSRSR) **SSP5-Comprobar el cumplimiento con las reglas TPSRSR**		Debido a la cantidad de personal en el área de IT, las responsabilidades no serán divididas, por tanto SSP4 y SSP5 no aplican como tareas específicas, sin embargo se debe establecer una auto-comprobación para la correcta aplicación del modelo.

Tabla 5.2
Propuesta de tareas para la gestión táctica

TAREA TÁCTICA MODELO ORIGINAL	TAREA TÁCTICA PROPUESTA	ANÁLISIS
TSP1-Informar a la gestión estratégica	STSP1-Informar a los ejecutivos	La documentación e información a los niveles superiores se mantiene, debido a su importancia para la correcta toma de decisiones. Como el mismo personal se encargará de la gestión estratégica y táctica, se fusionaran las tareas SSP1 y TSP1 del modelo original, con este procedimiento se formalizaran los informes presentados a los ejecutivos.
TSP2-Gestionar los recursos asignados	STSP2-Coordinación, asignación y gestión de recursos	Se integran las actividades de coordinación y asignación de recursos. La coordinación de personal y recursos es fundamental para asegurar el cumplimiento de las actividades y alcanzar los objetivos de la organización. Se fusionan las tareas SSP2, SSP6 y TSP2.
TSP3-Definir las Metas de seguridad **TSP4-Definir los indicadores para los procesos de seguridad**	STSP3-Definir objetivos, metas e indicadores para los procesos.	Es necesario entender el ambiente estratégico de la organización (objetivos) para definir correctamente las políticas de seguridad. Debido a la cantidad de personal en el área de IT, las responsabilidades no serán divididas, por tanto SSP4 y SSP5 no aplican como tareas específicas, sin embargo se debe establecer una auto-comprobación para la correcta aplicación del modelo. Se agrupan TSP3, TSP4 y SSP4.
TSP5-Definir grupos de propiedades	No se propone en el nuevo modelo.	No se consideran repositorios de información, ya que su alcance está fuera de esta investigación.
TSP6-Arquitectura de seguridad	No se propone en el nuevo modelo.	No se consideran ambientes y ciclos de vida lógicos dentro del alcance de esta investigación.

CONTINUA ⟶

TSP7-Investigar antecedentes y referencias	STSP4- Selección, capacitación y control del personal asignado	Es necesario definir roles del personal de seguridad y lineamientos para el control de sus funciones.
TSP8-Seleccionar el personal de seguridad		
TSP9-Capacitar al personal de seguridad		
TSP10-Definir procesos disciplinarios		
TSP11-Alcanzar conciencia en seguridad	No se propone en el nuevo modelo.	Las Pymes cuentan con recursos limitados para campañas internas de concientización en Seguridad de Redes de Información. La socialización de la seguridad no se desarrollará como un proceso independiente, sino que se pondrá en conocimiento del personal involucrado utilizando reuniones informativos generales y específicas como parte del proceso STSP2 en la coordinación y asignación de recursos.
TSP12-Seleccionar procesos específicos	No se propone en el nuevo modelo.	Esta tarea se basa en la aplicación de procesos de evaluación y análisis, sin embargo ISM3 no condiciona el uso de este tipo de procesos que generalmente suelen ser costosos. Las Pymes pueden alcanzar y mantenerse en el nivel de madurez más alto que sus recursos le permitan llegar. La aplicación del modelo está encaminado a pequeña empresas, en las que la áreas de tecnología no cuentan con presupuestos propios y la inversión en estos aspectos es reducida, por lo que éste proceso no será incluido.
TSP13-Insurance Management	No se propone en el nuevo modelo.	Administración de garantías y seguros de equipos, no se contempla dentro de las funciones del área de IT. Se contempla tareas de actualización de inventario y reporte de fallas, incluidas en las tareas OSP3 y OSP4.

5.1.3 Gestión Operativa

Reportará directamente a la Gestión Estratégica/Táctica.
Sus objetivos son:

- Retroalimentar al nivel de gestión superior.
- Dar soporte a las redes de información.
- Manejar eficientemente los recursos asignados.
- Aplicar los procesos para obtener un nivel de seguridad aceptable.

A continuación se presenta la propuesta de tareas operativas para el nuevo modelo:

Tabla 5.3
Propuesta de tareas para la gestión operativa

TAREA OPERATIVA (MODELO ORIGINAL)	PROPUESTA	JUSTIFICACIÓN
OSP1-Informar a la gestión táctica	OSP1- Informa a la gestión estratégica/táctica	La documentación e información a los niveles superiores se mantiene, debido a su importancia para la correcta toma de decisiones. Con este procedimiento se formalizaran los informes presentados al nivel superior.
OSP2-Seleccionar las herramientas para implementar las medidas de seguridad	OSP2-Selección de herramientas	
OSP3-Gestionar el inventario	OSP3- Gestión de inventario	Es de suma importancia mantener un inventario actualizado y controlado.
OSP4-Controlar el cambio de los ambientes de los sistemas de información	OSP4- Control de cambios de los ambientes de las redes de comunicaciones.	Mantener una bitácora de los cambios que afectan a las redes de comunicaciones.
OSP5-Refaccionar el ambiente	OSP5- Actualización y limpieza del ambiente	Normas mínimas para mantener el orden y el correcto funcionamiento de las redes de información.
OSP6-Limpiar el ambiente		
OSP7-Fortalecer el ambiente	No se propone en el nuevo modelo.	Esta tarea estará incluida en OSP4.
OSP8-Controlar el ciclo de vida de desarrollo del software	No se propone en el nuevo modelo.	El software no está considerado en el alcance del modelo.

CONTINUA →

OSP9-Controlar los cambios en las medidas de seguridad	OSP7- Control de cambios de las medidas de seguridad	Las políticas de seguridad deben mantenerse actualizadas.
OSP10-Gestionar el respaldo y redundancia	OSP8- Gestión de backups	Necesidad de mantener respaldo de configuraciones y cambios realizados.
OSP11-Controlar el acceso sobre servicios, repositorios, canales e interfaces	OSP9- Control de accesos a las redes de comunicaciones por parte de usuarios	Mantener un control usuarios, perfiles y permisos otorgados a los usuarios de la red, así como quien. Desde donde, cuando y hacia donde accedieron los usuarios internos y externos.
OSP12-Llevar el registro de usuarios		
OSP13-Gestionar el cifrado		
OSP14-Gestionar la protección del ambiente físico	OSP10- Gestionar la protección del ambiente físico	Control de los medios físicos, coordinación con proveedores para evitar o solucionar problemas detectados.
OSP15-Gestionar la continuidad de operaciones		
OSP16-Gestionar el filtrado y segmentación	OSP11- Gestionar la protección del ambiente lógico	Control de configuraciones de equipos y aplicaciones de protección instaladas.
OSP17-Gestionar la protección contra malware		
OSP18-Gestionar el aseguramiento	No se propone en el nuevo modelo.	La función de aseguramiento no se considera dentro de las funciones del área de IT.
OSP19-Emular ataques, errores y accidentes	OSP12- Emulación de ataques, errores e incidentes	Realizar pruebas coordinadas de posibles ataques e incidentes.
OSP20-Emular incidentes		
OSP21-Comprobar la calidad de la información	OSP13- Comprobación de la calidad de la información.	Tarea integrada en OSP9.
OSP22-Monitorizar alertas		
OSP23-Detectar y analizar eventos	OSP14- Monitoreo y análisis de eventos e incidentes	Mantener un monitoreo constante de las redes de información y analizar los eventos presentados para tomar correctivos.
OSP24-Manejar incidentes y pseudo-incidentes		
OSP25-Realizar el análisis forense	No se propone en el nuevo modelo.	La tarea de análisis forense requiere de personal especializado y alta asignación de tiempo, por lo que no se considera dentro de las tareas de IT para una Pyme.

La tabla 5.4 muestra de forma resumida las tareas propuestas y su relación con las tareas del modelo original (las tareas se relacionan mediante colores):

Tabla 5.4

Matriz resumen de tareas propuestas para el nuevo modelo basado en ISM3

TAREA ESTRATÉGICA (MODELO ORIGINAL)	TAREA TÁCTICA (MODELO ORIGINAL)	TAREA OPERATIVA (MODELO ORIGINAL)	PROPUESTA
SSP1-Informar a los accionistas	TSP1-Informar a la gestión estratégica	OSP1-Informar a la gestión táctica	STSP1-Informar a los directivos
SSP2-Coordinar	TSP2-Gestionar los recursos asignados	OSP2-Seleccionar las herramientas para implementar las medidas de seguridad	STSP2-Coordinar, asignar y gestionar los recursos.
SSP6-Asignar recursos para seguridad de la información	TSP3-Definir las Metas de seguridad	OSP3-Gestionar el inventario	STSP3-Definir objetivos, metas e indicadores para los procesos.
SSP3-Alcanzar visión estratégica	TSP4-Definir los indicadores para los procesos de seguridad	OSP4-Controlar el cambio de los ambientes de los sistemas de información	STSP4- Seleccionar, capacitar y dirigir al personal asignado.
SSP4-Definir las reglas para la separación de responsabilidades: transparencia, particionado, supervisión, rotación y separación de responsabilidades (TPSRSR)	TSP5-Definir grupos de propiedades	OSP5-Refaccionar el ambiente	OSP1- Informar a la gestión estratégica/táctica
	TSP6-Arquitectura de seguridad	OSP6-Limpiar el ambiente	OSP2-Seleccionar las herramientas necesarias.
SSP5-Comprobar el cumplimiento con las reglas TPSRSR	TSP7-Investigar antecedentes y referencias	OSP7-Fortalecer el ambiente	OSP3- Gestionar el inventario.

CONTINUA →

	TSP8-Seleccionar el personal de seguridad	OSP8-Controlar el ciclo de vida de desarrollo del software	OSP4- Controlar los cambios de los ambientes de las redes de información.
	TSP9-Capacitar al personal de seguridad	OSP9-Controlar los cambios en las medidas de seguridad	OSP5- Limpiar y actualizar el ambiente.
	TSP10-Definir procesos disciplinarios	OSP10-Gestionar el respaldo y redundancia	OSP6- Fortalecer el ambiente.
	TSP11-Alcanzar conciencia en seguridad	OSP11-Controlar el acceso sobre servicios, repositorios, canales e interfaces	OSP7- Controlar los cambios de las medidas de seguridad
	TSP12-Seleccionar procesos específicos	OSP12-Llevar el registro de usuarios	OSP8- Gestionar los backups.
	TSP13-Insurance Management	OSP13-Gestionar el cifrado	OSP9- Controlar el acceso de los usuarios.
		OSP14-Gestionar la protección del ambiente físico	OSP10- Gestionar la protección del ambiente físico.
		OSP15-Gestionar la continuidad de operaciones	OSP11- Gestionar la protección del ambiente lógico.
		OSP16-Gestionar el filtrado y segmentación	OSP12- Ejecutar emulaciones de ataques, errores e incidentes
		OSP17-Gestionar la protección contra malware	OSP13- Comprobar la calidad de la información
		OSP18-Gestionar el aseguramiento	OSP14- Monitorear y analizar eventos e incidentes
		OSP19-Emular ataques, errores y accidentes	
		OSP20-Emular incidentes	
		OSP21-Comprobar la calidad de la información	
		OSP22-Monitorizar alertas	
		OSP23-Detectar y analizar eventos	
		OSP24-Manejar incidentes y pseudo-incidentes	
		OSP25-Realizar el análisis forense	

5.1.4 Componentes de la red de información en las Pymes

Las redes de información son un concepto complejo que a veces se confunde o se utiliza a la par con el de “sistemas de información”, es necesario delimitar el alcance de las tareas a ejecutarse en el modelo propuesto, definiendo de forma particular a las “redes de información”.

Por tanto para claridad de la propuesta, las Redes de Información se definirán como el medio físico, con sus respectivas configuraciones y controles, por el que fluye la información dentro de una empresa, sin considerar repositorios, ni quien la genera o a quien va dirigida.

Mientras que los Sistemas de información, serán los recursos o repositorios de información en los cuales se origina, reúne, almacena y procesa la información a través de procesos determinados.

5.2 Definición del modelo propuesto

5.2.1 Estructura

El modelo propuesto basa su estructura en 5 niveles de madurez, los mismos que dependen de que se cumpla con ciertas características para cada uno de los procesos estratégicos/tácticos y operacionales.

A su vez cada tarea/proceso depende del cumplimento de un conjunto de actividades que cada organización determinará de acuerdo su realidad.

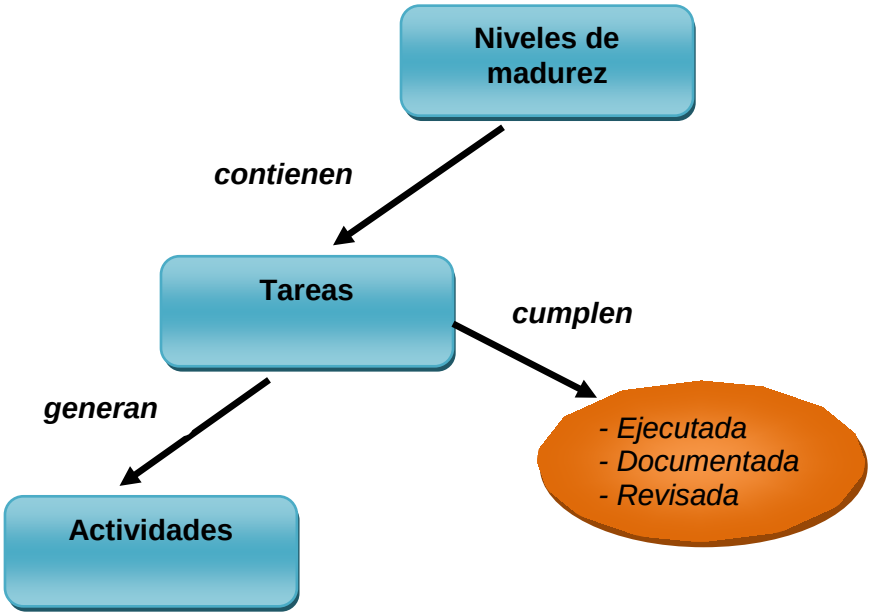


Figura 5. 1 Estructura del modelo propuesto

5.2.2 Responsables

Se realizaran 2 tipos de gestión: Estratégica/Táctica y Operativa.

La primera deberá estar a cargo de Jefes o Directores de área y reportará al nivel directivo o gerencial.

La segunda estará a cargo del personal operativo, siempre que los recursos lo permitan, caso contrario los roles pueden manejarse a la par.

La gestión operativa reportará a la gestión estratégica/táctica. Tal como se muestra en la figura 5.2.

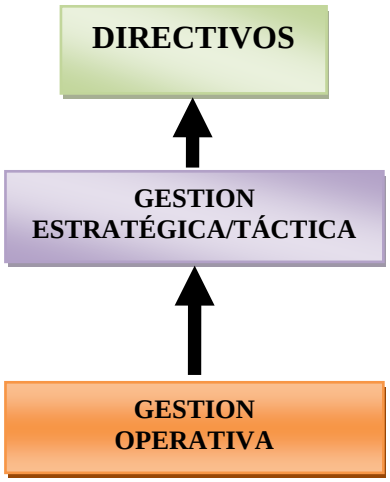


Figura 5. 2 Flujo de responsabilidades

5.2.3 Niveles de madurez

Se propone un Modelo de Madures de 5 niveles, considerando un estado inicial como nivel “cero”.

Nivel 0

En realidad es el estado inicial de la empresa, los procesos del negocio se encuentran en marcha, sin embargo, no existen manuales, procedimientos o políticas de seguridad definidas.

Nivel 1

La empresa está comprometida con la seguridad e inicia la definición de políticas de seguridad y procedimientos asociados a ella.

Se determinan los primeros permisos, accesos y responsables, para “arrancar” con el proceso de gestionar la seguridad. La empresa toma conciencia de que existe mucho por hacer y así avanzar al siguiente nivel.

Nivel 2

Los procedimientos y políticas deben ser socializados con todo el personal.

Todos los procesos y tareas diarias en la empresa se encaminan a la seguridad. Se definen los perfiles de acceso a la información.
Se aplican o mejoran las medidas de seguridad internas y externas.

Nivel 3

Los costos que genera la gestión de seguridad se analizan desde otro perfil y ya no se consideran como un gasto, inclusive algunos pueden disminuir. La seguridad en términos generales ha mejorado, el acceso a la información está correctamente definido.

Se realizan o actualizan inventarios, registros de eventos y soluciones aplicadas, tiempos de respuesta de proveedores internos y externos, es decir se cuenta con información del estado de la seguridad de las redes de forma centralizada.

Los procesos de actualización y mantenimiento son claramente definidos y coordinados.

Este nivel es bastante competitivo, pero no debe considerarse el máximo nivel, los procesos de seguridad deben estar en constante actualización.

Nivel 4

Se realizan pruebas periódicas para determinar que las medidas de seguridad y controles son suficientes y están funcionando correctamente. Se aplican correctivos de ser necesario.

Si es posible para la organización, es recomendable la aplicación de auditorías internas o externas al menos 1 vez al año. Debe capacitarse constantemente al personal para mantenerlos actualizados en los temas de

seguridad e incluir al personal nuevo en los procesos normales de la empresa.

5.2.4 Tareas

Las tareas a cumplirse de acuerdo al tipo de gestión se resumen en la tabla 5.5

Tabla 5.5
Tareas del modelo de madurez propuesto

TIPO DE GESTIÓN	TAREAS
ESTRATÉGICA/TÁCTICA	STSP1-Informar a los niveles gerenciales
	STSP2-Coordinar, asignar y gestionar los recursos
	STSP3-Definir objetivos, metas e indicadores para los procesos.
	STSP4- Selección, capacitación y control del personal asignado
OPERATIVA	OSP1- Informa a la gestión estratégica/táctica
	OSP2-Selección de herramientas
	OSP3- Gestión de inventario
	OSP4- Control de cambios de los ambientes de las redes de información
	OSP5- Actualización y limpieza del ambiente
	OSP6- Fortalecimiento del ambiente
	OSP7- Control de cambios de las medidas de seguridad
	OSP8- Gestión de backups
	OSP9- Control de accesos por parte de usuarios
	OSP10- Gestionar la protección del ambiente físico
	OSP11- Gestionar la protección del ambiente lógico
	OSP12- Emulación de ataques, errores e incidentes
	OSP13- Comprobación de la calidad de la información - Monitoreo
	OSP14- Analizar eventos e incidentes

5.2.5 Formato general para la documentación de las tareas

Todo proceso deberá ser documentado, de tal forma que se asegure que pueda ser revisado, repetido, socializado y esté correctamente definido.

Para ello se utilizará el siguiente formato (Tabla 5.6):

Tabla 5.6
Formato para documentación de las tareas

Tipo de tarea	Código y Nombre
Descripción	Detalle de la tarea realizada
Pre-requisitos	Pueden ser documentos o tareas necesarios para llegar a la nueva tarea.
Resultados	Pueden ser documentos o tareas, son las salidas de la ejecución de la tarea
Responsable	Responsable del proceso (ejecución y/o actualización)
Tareas relacionadas	Otros procesos del modelo que estén correlacionados
Actualizaciones	Fecha de actualización
Observaciones	Datos adicionales relevantes

5.2.6 Tablas de validación y evaluación

Para validar que una tarea ha sido “aprobada” debe cumplir con 3 características fundamentales, similares a las características comunes del modelo CMM, y éstas son:

- Ejecutado.- Deben existir evidencias de que las tareas son llevadas a cabo, a tiempo y que están generando resultados.

- Documentado.- Se requiere una descripción completa de la tarea. Todas las actualizaciones y nuevas versiones deben estar claramente documentadas. Así también los resultados obtenidos.

- Revisado.- Los resultados de la tarea realizada deben ser verificados y transmitidos al nivel superior. Sobre esta información se procede con la toma de decisiones.

Por tanto para poder dar por finalizada una tarea se debe asignar un valor a cada opción posible, para éstas características:

Si= 1
No= 0
En proceso= 0.5
Se desconoce= -1
No aplica= 0

Es decir, que para dar por aprobada una tarea/proceso, debe obtener un puntaje de 3, a menos que la tarea deba omitirse por razones documentadas. En este caso se deberá revisar la valoración global del nivel y excluir los puntos omitidos.

Para la tabulación de estos resultados se utilizarán las plantillas indicadas en las Tabla 5.7 y 5.8.

Tabla 5.7
Validación Tareas Estratégica/Tácticas

TAREAS O PROCESOS	Ejecutado	Documentado	Revisado	Sumatoria
ESTRATÉGICA/TACTICA				
STSP1-Informar a los niveles gerenciales				
STSP2-Coordinar, asignar y gestionar los recursos				
STSP3-Definir objetivos, metas e indicadores para los procesos.				
STSP4- Selección, capacitación y control del personal asignado				

Tabla 5.8
Validación Tareas Operacionales

TAREAS O PROCESOS	Ejecutado	Documentado	Revisado	Sumatoria
OPERACIONAL				
OSP1- Informa a la gestión estratégica/táctica				
OSP2-Selección de herramientas				
OSP3- Gestión de inventario				
OSP4- Control de cambios de los ambientes de las redes de información				
OSP5- Actualización y limpieza del ambiente				
OSP6- Fortalecimiento del ambiente				
OSP7- Control de cambios de las medidas de seguridad				
OSP8- Gestión de backups				
OSP9- Control de accesos por parte de usuarios				
OSP10- Gestionar la protección del ambiente físico				
OSP11- Gestionar la protección del ambiente lógico				

CONTINUA ⟶

OSP12- Emulación de ataques, errores e incidentes
OSP13- Comprobación de la calidad de la información - Monitoreo
OSP14- Analizar eventos e incidentes

Luego de la valoración y validación de las tareas realizadas, es necesario determinar en qué nivel de madurez se encuentra la organización.

Cada estándar y normativa define diferentes objetivos de control, por lo que el modelo propuesto intenta definir “tareas” o “procesos” en una estructura más práctica, que permita facilitar su aplicación. Sin embargo ésta estructura debe acoplarse a la realidad de la organización.

Para ello y, considerando que el modelo propuesto se fundamente en los lineamientos ISM3 se propone la plantilla detallada en la Tabla 5.9, esto provee como valor agregado el que se mantengan estándares básicos en la aplicación de seguridad y de esta forma se obtengan los mejores resultados, permitiendo a futuro poder ajustarse a estándares internacionales.

Dependiendo de las tareas que han sido completadas tanto estratégicas/tácticas como operacionales, la organización irá avanzando en los niveles hasta encontrar el nivel en el que satisfaga sus objetivos o finalmente alcance el máximo nivel.

Tabla 5.9
Plantilla para evaluación de niveles de madurez

TAREAS O PROCESOS	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ESTRATÉGICA/TÁCTICA					
STSP1-Informar a los niveles gerenciales	X	X	X	X	X
STSP2-Coordinar, asignar y gestionar los recursos	X	X	X	X	X
STSP3-Definir objetivos, metas e indicadores para los procesos.				X	X
STSP4- Selección, capacitación y control del personal asignado			X	X	X
OPERACIONALES					
OSP1- Informa a la gestión estratégica/táctica	X	X	X	X	X
OSP2-Selección de herramientas		X	X	X	X
OSP3- Gestión de inventario				X	X
OSP4- Control de cambios de los ambientes de las redes de información				X	X
OSP5- Actualización y limpieza del ambiente				X	X
OSP6- Fortalecimiento del ambiente				X	X
OSP7- Control de cambios de las medidas de seguridad				X	X
OSP8- Gestión de backups	X	X	X	X	X
OSP9- Control de accesos por parte de usuarios	X	X	X	X	X
OSP10- Gestionar la protección del ambiente físico		X	X	X	X
OSP11- Gestionar la protección del ambiente lógico		X	X	X	X
OSP12- Emulación de ataques, errores e incidentes					X
OSP13- Comprobación de la calidad de la información - Monitoreo		X	X	X	X
OSP14- Analizar eventos e incidentes					X

En el caso de las Pymes, el “core” del negocio se encuentra definido, pero para las redes de información no se pretende un nivel de confianza tan alto, si se compara con grandes multinacionales o instituciones financieras,

en las cuales la información es el corazón de sus actividades, sin embargo este aspecto puede ser un diferenciador en una negociación.

Cualquier esfuerzo por mejorar la seguridad tecnológica permitirá disponer de la información y comunicaciones en el momento que se requiera, además que incrementará la confianza de directivos, empleados, clientes y proveedores, lo cual al largo plazo, permite crear un mejor ambiente de trabajo.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Las encuestas aplicadas permitieron conocer que mayoritariamente en las Pymes las redes se evalúan en base a los comentarios del cliente, llamadas a help desk o reportes de terceros, el término “modelo de madurez” es nuevo en nuestro medio, muy poco conocido en lo que respecta a su aplicación en tecnología.

- Definidas las mejores características de los modelos se formalizó una nueva propuesta para ser aplicada en las Pymes, este tipo de modelos están tomando mucha importancia dadas las nuevas necesidades organizacionales, el crecimiento económico globalizado y la evolución de IT en las organizaciones. Sin embargo, no puede adoptarse como un “estándar”, ya que se debe analizar la naturaleza de la organización, las personas, los objetivos, la tecnología existente, factores que también van cambiando a lo largo del “período de madurez”, por lo que sería mejor considerarlo como un conjunto de “lineamientos” que permitan manejar y adecuarse al cambio y evolución.

- La aplicación de una guía, normativa o estándar para la evaluación de la seguridad en las redes de información como ayuda en la gestión de la seguridad, es necesaria ya que permite la optimización del uso de los recursos y mejora el desempeño del personal y de los equipos, lo que a la larga se traduce en beneficios económicos para la organización.

- El modelo propuesto es el resultado del análisis de modelos existentes aplicados a nivel internacional y de la experiencia personal de administración de IT en Pymes. Este modelo se constituye en una herramienta de diagnóstico inicial de seguridad de redes de información en las Pymes que permitirá adoptar políticas que mejoren los procesos de gestión de IT en dichas organizaciones, utilizando los recursos ya existentes

- Del desarrollo de esta investigación se concluye que, para la correcta implementación de un modelo como el propuesto se deben cumplir condiciones básicas para el éxito de esta iniciativa: compromiso, evaluación, definición de objetivos, socialización y mejora.

6.2 Recomendaciones

- Es importante conocer las características de los modelos base para adoptar el que más se adapta a las necesidades y objetivos del negocio.

- ISM3 no se constituye en una camisa de fuerza para el negocio, sino que permite logros parciales, hasta llegar al nivel más adecuado para cada tipo de empresa. CMM fue adoptado como base de variantes de modelos de madurez que cada vez son aplicados en áreas diversas del conocimiento y los negocios.

- Realizar la validación del modelo propuesto a través de su aplicación en un caso real, con el objetivo de obtener la retroalimentación y refinamiento del modelo.

- Para la implementación de cualquier normativa o modelo es absolutamente necesario alcanzar el compromiso de los ejecutivos de la empresa, esta es la única forma de contar con la colaboración de toda la organización y obtener los resultados esperados.

- Diseñar una metodología para la aplicación de modelos de madurez en las Pymes, trabajando a la par con otras áreas como dirección de proyectos, finanzas, planificación, con el objetivo de definir el momento oportuno para la aplicación de este tipo de herramientas en la organización.

BIBLIOGRAFIA

Aceituno Canal, V. (2004). *ISM3 1.0.* Obtenido de iit.edu: http://trygstad.rice.iit.edu:8000/Policies%20&%20Tools/ISM3_1.0_InformationSecurityManagementMaturityModel.pdf

Aceituno Canal, V. (2008). Obtenido de http://www.isaca.org/Journal/archives/2008/Volume-2/Pages/Usefulness-of-an-Information-Security-Management-Maturity-Model1.aspx

Aceituno, V. (2014). vaceituno@inovement.es.

ACIS. (2013). *V Encuesta de Seguridad*. Obtenido de http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/XIII_JornadaSeguridad/ELSI2013.pdf

Arbeláez Cortez, R. C. (2008). Obtenido de acis.org.co: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_Jornada Seguridad/05-ModelosMadurezSeguridadInformatica.pdf

Belgrado, U. d. (s.f.). Obtenido de http://www.ub.edu.ar/catedras/ingenieria/auditoria/cmm/cmm-2.htm

Carnegie Mellon University. (2013). *Carnegie Mellon University*. Obtenido de http://www.cmu.edu

Claros Liendo, A. (2012). Obtenido de projectools.wordpress.com: http://projectools.wordpress.com/modelos-de-madurez-en-gestion-de-proyectos/

CMMI en Mexico y el mundo. (2012). Obtenido de everac99.wordpress.com: https://everac99.wordpress.com/2012/07/20/cmmi-en-mexico-y-el-mundo-2012/

Consortium, I. (2007). Obtenido de lean.org: http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf

Deloitte. (2010). *nouvelstrategies.com*. Obtenido de http://nouvelstrategies.com/E/Management-Awareness/Entries/2010/7/1_Deloitte_2010_Financial_Services_Global_Security_Study.html

Ecuapymes. (s.f.). Obtenido de ecupymes.ec: http://www.ecuapymes.ec/que es PYME.mht/

ESET. (2012). *Security Report Latinoamerica 2012.* Obtenido de http://www.welivesecurity.com/wp-content/uploads/2014/01/eset-security-report-latam-2012.pdf

ESET. (2014). *Security Report Latinoamerica 2014.* Obtenido de http://www.welivesecurity.com/wp-content/uploads/2014/06/informe_esr14.pdf

Fau, C. (2006). Obtenido de carlosfau.com.ar: http://carlosfau.com.ar/nqi/nqifiles/CMM-Informe.pdf

INEC. (2013). Obtenido de ecuadorencifras: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/140210%20DirEmpresas%20final3.pdf

ISACA. (2007). *COBIT 4.1*. Obtenido de isaca.org: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx

Kaspersky, L. (2012). Obtenido de http://www.viruslist.com/sp/analysis?pubid=207271158

Kaspersky, L. (2013). Obtenido de http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-68-de-empresas-en-am%C3%A9rica-latin

Kaspersky, L. (2014). Obtenido de http://latam.kaspersky.com/analisis2014pronosticos2015LatAm

Mas Pichaco, A., & Amengual Alcover, E. (2007). CMM. En V. Autores, *Técnicas cuantitativas para la Gestión en la Ingeniería de Software* (págs. 7-15). Netbiblo.

OpenGroup. (2011). Obtenido de opengroup.org: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12238

Ramirez, J. M. (2009). Obtenido de slideshare.net: http://es.slideshare.net/jmramireza/los-modelos-de-madurez-organizacionales-y-los-factores-crticos-de-xito-en-la-implantacin-de-sistemas-de-informacin?qid=17c1a38c-0ba3-421d-99a7-cd5fe5ea102c&v=qf1&b=&from_search=1

rickymartinfoundation. (2008). *rickymartinfoundation*. Obtenido de http://www.rickymartinfoundation.org/es/lo-ultimo/noticias/248-ante-el-aumento-en-el-software-de-seguridad-falso-microsoft-y-la-fundacion-ricky-martin-hacen-un-llamado-por-la-seguridad-en-internet

SRI. (2014). Obtenido de sri.gob.ec: www.sri.gob.ec/de/32

Superintendencia, d. C. (2011). Obtenido de blog.smsecuador.ec: http://blog.smsecuador.ec/2011/11/superintendencia-de-companias-resolucion-sc-ici-cpaifrs-g-11-010/

Symantec. (2011). *SMB Threat Awareness Pool*. Obtenido de http://www.symantec.com/content/en/us/about/media/pdfs/symc-smb-threat-awareness-poll.pdf

Universia. (2008). *universia.net.co*. Obtenido de http://noticias.universia.net.co/movilidad-academica/noticia/2008/06/24/242106/multiples-retos-pymes-america-latina.html

Wikipedia. (2013). *Wikipedia: la enciclopedia libre*. Obtenido de http://es.wikipedia.org

GLOSARIO

Benchmarking: Comparación sistemática y continua de productos, servicios o procesos de una organización.

CAPEIPI: Cámara de Pequeña y Mediana Empresa de Pichincha.

CMM: Capability Maturity Model. Modelo de maduez aplicado al Desarrollo de Software.

CMMI: Capability Maturity Model Integration. Modelo de madurez de capacidad aplicado para la mejora de la calidad del software.

Estándar: Ver norma.

Estratégico: Relativo a la estrategia. Conjunto de acciones planificadas sistemáticamente en el tiempo que se llevan a cabo para lograr un determinado fin o misión.

Help desk: Mesa de ayuda, es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles relacionados a las Tecnologías de la Información y la Comunicación (TIC).

ISMS: (Information Security Manager System). Sistema de gestión de la seguridad de la información (SGSI). Conjunto de políticas de administración de la información.

ISM3: Information Security Management Maturity Model. Modelo de madurez aplicado a Seguridad de la Información.

ISO 27001: Estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional por International Organization for Standardization.

ISO 9000: Conjunto de normas sobre calidad y gestión de calidad, establecidas por la Organización Internacional de Normalización (ISO).

IT: (Information Technology) Tecnologías de la Información. Término que se refiere a la agrupación de elementos y técnicas utilizadas en el tratamiento y transmisión de la información.

ITIL: (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de Información

KPA: (Key Process Area). Areas Claves de Proceso, término utilizado en el modelo CMM.

Métricas: Medida o conjunto de medidas que permiten caracterizar un software o sistema de información.

Norma: O estándar, es una especificación que reglamenta procesos y productos para garantizar la interoperabilidad.

Operacional: Relativo a operaciones.

Outsourcing: subcontratación o tercerización, es el proceso económico en el cual una empresa destina los recursos orientados a cumplir ciertas tareas hacia una empresa externa por medio de un contrato.

Phising: O suplantación de identidad. Es un término informático que denomina al intento de adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

PYMES: Acrónimo de pequeña y mediana empresa.

ROI: (Return of Investment) Retorno de la inversion.

Spam: Correo basura o mensaje basura. Se denomina así a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo).

Táctico: Método empleado con el fin de tener un objetivo.

TPSRSR: Transparencia, particionado, supervisión, rotación y separación de responsabilidades.

Virus: Malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

ANEXO A:

FORMATO DE ENCUESTA ONLINE

ANEXO B:

ISM3 HANDBOOK

ANEXO C:

BENCHMARKING CMM vs ISM3