CENTRO DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

DEPARTAMENTO DE FINANZAS

TRABAJO PRÁCTICO:

"ESTUDIO DE VIABILIDAD SOBRE LA INVERSIÓN EN SEGURIDAD INFORMÁTICA PARA LAS PYMES"

PRESENTA:

Jonathan Balderrama López

Para obtener el grado de MAESTRO EN CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

TUTOR

M.B.A. Ricardo Garcia Ramírez

COMITÉ TUTORAL

Dr. Felipe de Jesús Salvador Leal Medina

M.F.I. Juan Manuel Arriaga Rivera

AGUASCALIENTES, AGS., 30 de Noviembre del 2012

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

CENTRO DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

Oficio No. / CCEA / D / 068 / 2012

C.P. MARIA ESTHER RANGEL JIMENEZ,
JEFA DEL DEPTO. DE CONTROL ESCOLAR,
P R E S E N T E .

Me es grato comunicarle que el alumno(a) **JONATHAN BALDERRAMA LOPEZ** con Id 136762, ha concluido satisfactoriamente su trabajo práctico para obtener el grado de MAESTRÍA EN CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS (AREA FINANZAS), con el titulo ***"ESTUDIO DE VIABILIDAD SOBRE LA INVERSIÓN EN SEGURIDAD INFORMÁTICA PARA LAS PYMES",*** este proyecto se realizó bajo la dirección de su Comité Tutoral:

Director de Tesis	M.B.A. RICARDO GARCIA RAMIREZ
Lector 1	DR. FELIPE DE JESUS SALVADOR LEAL MEDINA
Lector 2	M.F.N. JUAN MANUEL ARRIAGA RIVERA

El cual se concluyó satisfactoriamente con ***VOTO APROBATORIO*** de acuerdo a lo señalado por el Art. 175 apartado II del Reglamento General de Docencia, anexando copia de la citada aprobación.

Sin otro particular por el momento quedamos a sus atentas órdenes para cualquier aclaración al respecto.

A t e n t a m e n t e
Aguascalientes, Ags., 30 de noviembre de 2012
" SE LUMEN PROFERRE "

DRA. MARIA DEL CARMEN MARTINEZ SERNA
DECANA DEL CENTRO

c.c.p.- Secretaría de Investigación y Posgrado del CCEA
c.c.p.- Depto. de Apoyo al Posgrado
c.c.p.- Minuta de Sec. Inv. y Posgrado
c.c.p.- Archivo Maestría

'mchn

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

CENTRO DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

DRA. MARIA DEL CARMEN MARTINEZ SERNA
DECANA DEL CENTRO DE CIENCIAS
ECONÓMICAS Y ADMINISTRATIVAS
P R E S E N T E

Por medio del presente como Comité Tutoral designado del alumno: **JONATHAN BALDERRAMA LÓPEZ** con ID 136762 quien realizó la tesis titulada: **"ESTUDIO DE VIABILIDAD SOBRE LA INVERSIÓN EN SEGURIDAD INFORMÁTICA PARA LAS PYMES"** y con fundamento en el artículo 175, apartado II, del Reglamento General de Docencia, nos permitimos emitir el **VOTO APROBATORIO,** para que pueda proceder a imprimirla, así como continuar con el procedimiento administrativo para la obtención del grado correspondiente de la Maestría en Ciencias Económicas y Administrativas, área Finanzas.

Ponemos lo anterior a su consideración y sin otro particular por el momento, le enviamos un cordial saludo.

ATENTAMENTE
Aguascalientes, Ags., 30 de Noviembre del 2012
"SE LUMEN PROFERRE"

M.B.A. RICARDO GARCÍA RAMÍREZ
DIRECTOR

DR. FELIPE DE JESUS SALVADOR LEAL MEDINA
Lector 1

M.F.N. JUAN MANUEL ARRIAGA.
Lector 2

c.c.p. Alumno
c.c.p. Secretaría de Investigación y Posgrado del CCEA
c.c.p. Secretaría Técnica de la MCEA
c.c.p. Jefatura Depto. Finanzas

UNIVERSIDAD AUTÓNOMA DE AGUASCALIENTES

POSGRADOS UAA

DICTAMEN DE REVISIÓN DE LA TESIS / TRABAJO PRÁCTICO

DATOS DEL ESTUDIANTE	
NOMBRE: JONATHAN BALDERRAMA LOPEZ	ID (No. de Registro): 136762
PROGRAMA: MAESTRIA EN CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS	ÁREA: FINANZAS
TUTOR/TUTORES: M.B.A. RICARDO GARCÍA RAMÍREZ (Tutor) DR. FELIPE DE JESÚS SALVADOR LEAL MEDINA (Lector 1) M.F.N. JUAN MANUEL ARRIAGA RIVERA (Lector 2)	
TESIS ( ) TRABAJO PRÁCTICO (x)	
TITULO: "ESTUDIO DE VIABILIDAD SOBRE LA INVERSIÓN EN SEGURIDAD INFORMÁTICA PARA LAS PYMES" OBJETIVO: REALIZAR UN ESTUDIO DE FACTIBILIDAD SOBRE INVERTIR EN SEGURIDAD INFORMÁTICA EN LAS PYMES.	

DICTAMEN	
CUMPLE CON CRÉDITOS ACADÉMICOS:	(x)
CONGRUENCIAS CON LAS LGAC DEL PROGRAMA:	(x)
CONGRUENCIA CON LOS CUERPOS ACADÉMICOS:	(x)
CUMPLE CON LAS NORMAS OPERATIVAS:	(x)
CONINCIDENCIA DEL OBJETIVO CON EL REGISTRO:	(x)

Aguascalientes, Ags. A 30 Noviembre de 2012

FIRMAS

DR. FELIPE DE JESÚS SALVADOR LEAL MEDINA
CONSEJERO ACADÉMICO DEL ÁREA

MA. ALBERTO PONTON CASTRO
SECRETARIO TÉCNICO DEL POSGRADO

DRA. LAURA ROMO ROJAS
SECRETARIO DE INVESTIGACIÓN Y POSGRADO

Código: FO-040200-23
Revisión: 00
Emisión: 21/02/11

AGRADECIMIENTOS

A Dios: Por haberme dado el privilegio y la oportunidad de estudiar este posgrado en la Universidad Autónoma de Aguascalientes, recuerdo muy bien que después de 3 años de haber estado en oración y de haber tenido la intención de comenzar un posgrado en finanzas, El respondió mis oraciones y las de mi esposa. Sin duda este trabajo y toda la maestría es un gesto de gratitud de parte de Dios y todo lo que he logrado es para su honor y gloria. Sin la voluntad de Dios Padre definitivamente que nada de lo que soy y nada de lo que he logrado hubiera sido posible. Gracias Padre.

A mi Esposa Elizabeth y a mis Hijos Joel y Jacob: Gracias por el amor, animo y gran alegría que me han brindado estos últimos cinco años de mi vida, en especial gracias por apoyarme con paciencia en el tiempo los fines de semana que no estuve presente por dedicarme al estudio de esta maestría durante estos últimos dos años y medio. Esposa mía: te agradezco por guiarme y ser mi ayuda idónea en nuestro matrimonio, tú y nuestros hijos significan para mí un gesto del gran regalo y bendición que Dios ha dispuesto en mi vida.

A mi Madre y a mi Padre: Raquel Lopez y Xavier Balderrama (+), por ser ambos un gran ejemplo e inspiración en mi vida, sin su amor y sin su educación no hubiese podido llegar aquí, Dios definitivamente me ha bendecido por haberme dado un gran padre carnal que durante su vida se esforzó y lucho con amor por dar lo mejor de sí mismo a su familia, siempre guiándonos con sabiduría. Gratamente Dios me ha bendecido también con una madre excepcional, una madre que hasta la fecha admiro enormemente por darme el ejemplo de cómo superar tantas prueba en la vida y seguir adelante, a ella en especial le agradezco por su apoyo y animo en lograr este estudio, Madre simplemente no tengo palabras para describir lo que siento por todo lo que has hecho por nosotros, te agradezco por tu amor y por siempre estar presente en mi vida.

Al Dr. Felipe de Jesús Leal Medina: Por su constante apoyo durante la maestría y por darnos ánimo de concluir este posgrado; así también quiero agradecer el gran apoyo que me ha brindado durante estas últimas semanas de revisión del presente trabajo práctico.

A la Dra. Laura Romo Rojas: Por haber transmitido sus conocimientos durante el curso de Dirección Estratégica, materia que hasta la fecha ha sido de gran apoyo en mi vida profesional. Así también por siempre dar lo mejor de sí misma para los tres grupos de especialidad en la maestría Ciencias Económicas y Administrativas. Gracias Doctora por su apoyo y por habernos escuchado a los alumnos de la especialidad en finanzas durante estos últimos dos años y medio, usted es muy valiosa para todos nosotros (sus alumnos) y sin duda para la Universidad Autónoma de Aguascalientes.

A mis tutores de tesis: M.B.A. Ricardo Garcia y el M.F.I. Juan Manuel Arriaga que me apoyaron con su invaluable aportación, recomendaciones y retroalimentación para este trabajo.

A mis compañeros de maestría: Por su amistad durante estos últimos años y por compartir sus experiencias profesionales y personales mismas que nos han alimentado a todos y nos han hecho crecer en el transcurso de este posgrado.

Jonathan Balderrama López

MOTIVOS PERSONALES PARA LA REALIZACIÓN DEL TRABAJO

- Obtener el grado de Maestría de Ciencias Económicas y Administrativas.

- Dar una aportación de tal forma que esta investigación soporte la profesionalización de las PYMES en México.

- Utilizar los conocimientos y fundamentos financieros adquiridos durante la maestría y aplicarlos al área de seguridad informática, mi área profesional de especialización.

- Contar con una base solida para llevar a cabo un estudio de viabilidad financiera en mi empresa (PYME) y aplicarla a la hora de tener una oportunidad de proyecto de inversión en seguridad informática.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS Y GRÁFICOS

ACRÓNIMOS

ALE: (del inglés Annual Loss Expectancy) expectativa de pérdida anual.

ARO: (del inglés Annual Rate of Occurrence) tasa anual de eventos.

AV: (del inglés Asset Value) valor del activo.

B2C: (del inglés Business to Customer) de la empresa al consumidor.

CIA: (del inglés Confidentiality, Integrity and Availability) confidencialidad, integridad y disponibilidad.

EF: (del inglés Exposure Factor) factor de exposición.

PR: Período de recuperación.

ROI: Retorno sobre la inversión.

SLE: (del inglés Single Loss Expectancy) expectativa de pérdida por evento.

TIR: Tasa interna de retorno.

TREMA: Tasa de rendimiento mínima aceptada.

VAN: Valor actual neto, también llamado valor presente neto.

VPN: Valor presente neto, también llamado valor actual neto.

RESUMEN

Directores de finanzas, dueños de empresa o socios de algún negocio antes de invertir dinero en cualquier control de seguridad informática como: software, dispositivos de hardware o cualquier solución de seguridad informática en general, buscarían comprobar que la inversión esté financieramente justificada o por lo menos se estarían cerciorando de que, al hacer una inversión de este tipo aportará beneficios para la empresa.

En ese sentido, las inversiones en seguridad informática no son diferentes a cualquier otro tipo de inversión dentro de una empresa, estas tienen que estar alineadas a las necesidades de la compañía. Un elemento importante para quienes toman decisiones financieras son las métricas de seguridad que muestren cómo las brechas de seguridad informática impactan financieramente a una empresa. No hay razón ni justificación de implementar una solución en seguridad si su costo verdadero es mayor que costo de exposición del riesgo.

Este trabajo tratará dos modelos financieros y tres modelos no financieros para el análisis de viabilidad financiera de proyectos de inversión en seguridad informática, de tal forma que pueda ser sustentada alguna inversión de esta clase. A lo largo de este trabajo práctico así mismo se definen y enmarcan conceptos necesarios en el ámbito de seguridad informática y de finanzas para poder llevar a cabo un análisis de viabilidad que sea sustentable.

Palabras Clave: *Proyecto de inversión, seguridad informática, viabilidad financiera, PYMES.*

ABSTRACT

A Chief Finance Officer, a small business owner or any shareholder of a company before investing money on any information security control like: software, hardware devices or any other information security solution in general, he or she would seek the financial benefits obtained from investing on information security.

On this sense, information security investments are not different from any other type of investments in a company; these investments would need to be aligned to the business needs. An important element for the financial decision-making process is the: security metrics that would proof how security breaches have direct financial impact on a business. There is no reason or justification on implementing any security solution if its cost is higher than the exposed cost of risk.

This present work will introduce the reader two financial models and three non financial models for making a financial viability analysis against an information security investment project, in such way that an investment decision of this class could be backed up. In addition this work defines and bounds concepts related to: information security and finance in order to perform a reliable finance viability analysis.

Keywords: *Investment projects, information security, financial sustainability, small businesses.*

INTRODUCCIÓN

Alguna vez se ha preguntado lo siguiente: ¿Cuál es nivel de seguridad de protección de los datos que se encuentran almacenados en las computadoras de su empresa?, ¿Cuál el nivel de seguridad con el que otras empresas resguardan su información: personal, financiera, medica, etc.? – o al menos ¿alguno de estos últimos dos aspectos le han preocupado?

Todos los días, individuos y empresas son víctimas de *brechas de seguridad en la información*, mismas que tienen implicaciones financieras significativas. Naturalmente la constante evolución de las redes (p. ej. internet a través de *tecnologías inalámbricas*) y los medios computacionales para acceder dichas redes (p. ej.: dispositivos electrónicos móviles tales como: *netbooks*, *tabletas*, *teléfonos inteligentes*, *lectores de libros electrónicos*), dan paso a la generación de nuevas oportunidades para criminales astutos de infiltrar sistemas computacionales.

Esas infiltraciones son a las comúnmente se les refiere como brechas en el tema de *seguridad informática*. Para poder obtener tranquilidad y prevenir brechas futuras, existen empresas que toman algunos pasos para implantar algún nivel de seguridad informática. Sin embargo, debido a la naturaleza impredecible de estas brechas de seguridad en la información, la toma de decisiones de inversión en el ámbito de seguridad informática es intuitiva en lugar de ser analítica.

El presente trabajo describe una guía para soportar la toma de decisiones de inversión en seguridad informática a través de un análisis de viabilidad financiera.

A lo largo del primer capítulo se presenta descripción de la problemática, su justificación, los objetivos y las preguntas de investigación del presente trabajo práctico.

El segundo capítulo habla de teoría acerca de conceptos de seguridad en la información y seguridad informática además de incorporar modelos que sirven para el análisis de viabilidad financiera, esto con el objetivo de contar con bases solidas para el desarrollo de la metodología a tratar en el trabajo práctico.

El tercer capítulo es la metodología con la cual se ataca el caso práctico, objeto de estudio de esta tesis.

Por último, en el cuarto capítulo enumera las conclusiones del trabajo práctico seguida de recomendaciones que servirán para otras líneas de investigación relacionadas con el tema de este trabajo práctico.

CAPÍTULO I

Planteamiento Del Problema

“En la actualidad existen dos tipos de empresas: las que han sido hackeadas y las que serán hackeadas”

FBI: Rober Mueller, 2012 (Cowley, 2012), (Pullicino, 2011)

1.1 DESCRIPCIÓN DE LA PROBLEMÁTICA

En la última década ha sido notorio el avance de las tecnologías de información que se abrió paso gracias a la revolución del internet. Esta interconectividad cambio la manera de hacer negocios. En estos días el uso del internet tiene diversas aplicaciones: comunicación con otras personas, comercio en línea, investigación y entretenimiento.

Básicamente internet ha cambiado la manera en como las empresas operan. Por ejemplo: el internet ahora permite que empleados trabajen prácticamente desde cualquier ubicación. Además, permite que las empresas efectúen compras directas de vendedores y ventas a clientes desde cualquier parte del mundo en tiempo real.

En la figura 1 podemos apreciar la tendencia del 2012 al 2015 que se tendrá en México de hacer comercio electrónico por internet por parte de empresas al consumidor (*B2C*):

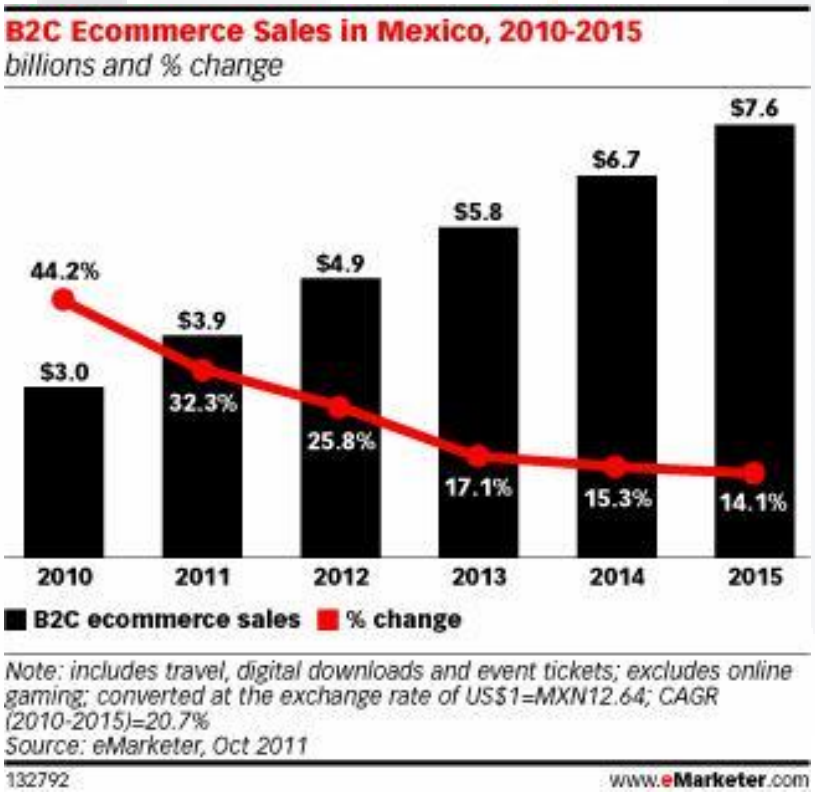

FIGURA 1 – TENDENCIA DE *COMERCIO ELECTRÓNICO* B2C EN MÉXICO (eMarketer, 2011)

Sin duda para cualquier empresa o individuo en particular, los beneficios de utilizar el internet son enormes, sin embargo esto trae consigo costos significativos. Uno de estos costos, que ha causado pérdidas a incontables individuos y empresas, son los relacionados con brechas de seguridad en la información. *Malware computacional*,

robo de identidad y espionaje corporativo están dentro de las brechas de seguridad en la información más conocidas.

Una de las razones de la proliferación de las brechas de seguridad en la información es de que e internet no fue diseñado tomando en cuenta la seguridad de la información. Encuestas recientes muestran que los ataques vía internet son el método más común de crimen computacional.

FIGURA 2 – CRÍMENES COMPUTACIONALES

La información provee valor a la empresa de numerosas maneras p. ej.: ayudando a los administradores a tomar mejores decisiones: operacionales, mercadológicas y financieras; apoyando a los administradores a controlar actividades y procesos; y ayudando a la administración del capital humano. En la presente economía basada en la información, los activos de información remplazan los activos físicos como un medio para dar a una empresa una ventaja competitiva con respecto a otras en el mercado. Debido a la naturaleza estratégica de la información, las empresas deben salvaguardar sus activos intangibles de tal manera como harían con sus activos físicos. Los tipos de información que significan activos estratégicos en las empresas de hoy incluyen: transacciones electrónicas de día a día, formulas secretas, productos en desarrollo, planes de mercado, fusiones y adquisiciones, etc. El valor de la información para una empresa es intrínsecamente ligada a su nivel de privacidad y seguridad.

Como se muestra en la Figura 3, la asignación del valor de empresa entre activos tangibles, intangibles y fondo de comercio, varía en gran medida en función del sector de actividad en que opere la compañía adquirida. Los sectores que muestran un mayor nivel de activos intangibles son el farmacéutico y el biotecnológico, puesto que la mayor parte de su valor se debe a los activos intangibles vinculados a las patentes y a la tecnología utilizada (Ramos, 2009).

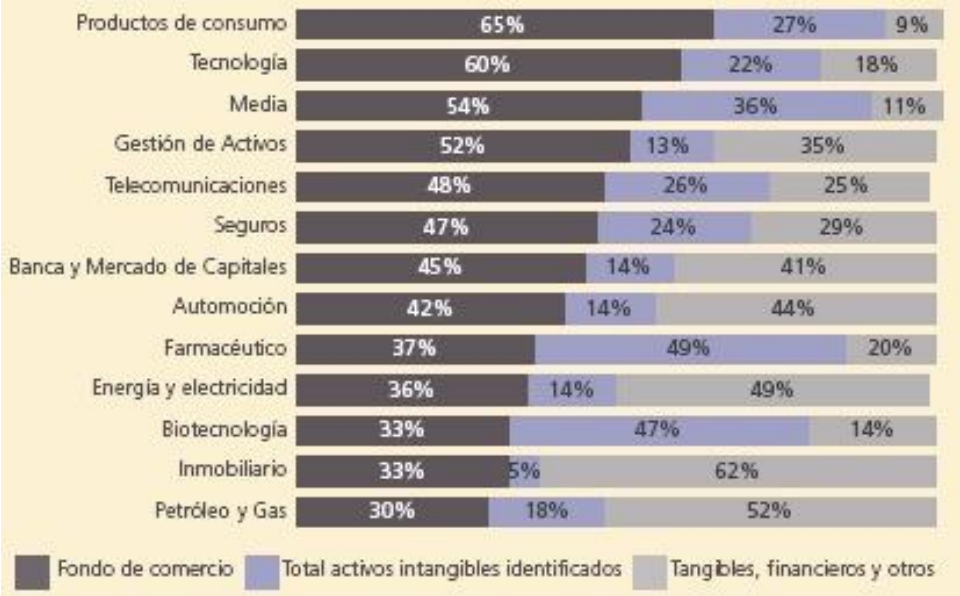

FIGURA 3 – ASIGNACIÓN DEL VALOR DE EMPRESA (%) (LAS CIFRAS QUE NO SUMEN 100% ES DEBIDO A LOS REDONDEOS) (Ramos, 2009)

Las empresas típicamente acumulan información de otras partes basadas en el entendimiento de que la empresa misma protegerá la confidencialidad de la información. Esto es particularmente cierto para información financiera y medica. Responsabilidad legal y cumplimiento con lineamientos y regulaciones son suficientes alicientes para proteger la información. El riesgo de una demanda crece cuando un fallo en el sistema de seguridad informático afecta a una tercera parte. En conjunto con el daño causado por comprometer la confidencialidad de la información (p. ej.: fuga de records médicos o financieros).

Invertir en seguridad informática para estar en cumplimiento con las prácticas de la industria y con el sistema legal y regulatorio, proporciona a una empresa con un nivel de protección. Sin embargo, la parte complicada del proceso de toma de decisión para un proyecto de inversión en seguridad informática es el estudio de viabilidad financiera,

esto cuando existen diversas alternativas de inversión en soluciones de seguridad informática. Esta problemática ha sido atacada a través de diferentes modelos financieros y será tema de estudio del presente trabajo práctico, de tal manera que pueda ser adaptado a las PYMES en México.

JUSTIFICACIÓN

En un estudio realizado por la división Cloud de Symantec (Symantec es una corporación internacional dedicada al desarrollo y comercialización de software en el dominio de la seguridad informática, con sede central en Mountain View, California), que se llevo a cabo alrededor del mundo a 1900 empresas, 50% de estas PYMES, PYMES según la definición del U.S. Small Business Administration (SBA, 2012), algunas con base en Latinoamérica (25 en Argentina, 14 en México, 10 en Colombia y 11 en Brasil) reveló lo siguiente (Symantec, 2011):

a) El 40% del grueso de hackeos realizados de enero 2011 hasta finales del 2011 se enfocaron a empresas con menos de 500 empleados.

b) Asimismo las empresas están familiarizadas con amenazas de seguridad tales como: los *ataques dirigidos*, *programas de captura de teclado* y riesgos que provienen por el uso de teléfonos inteligentes. Así también más de la mitad de las empresas declaró que el malware podría causar pérdida de productividad y 36% reconoció que los *hackers* podrían acceder a información confidencial de las empresas. Los encuestados además dijeron que los ataques dirigidos afectan a las empresas y 46% de ellos afirmó que éstos pueden ocasionar pérdida de ingresos y un 20% dijo que pueden generar pérdida de clientes.

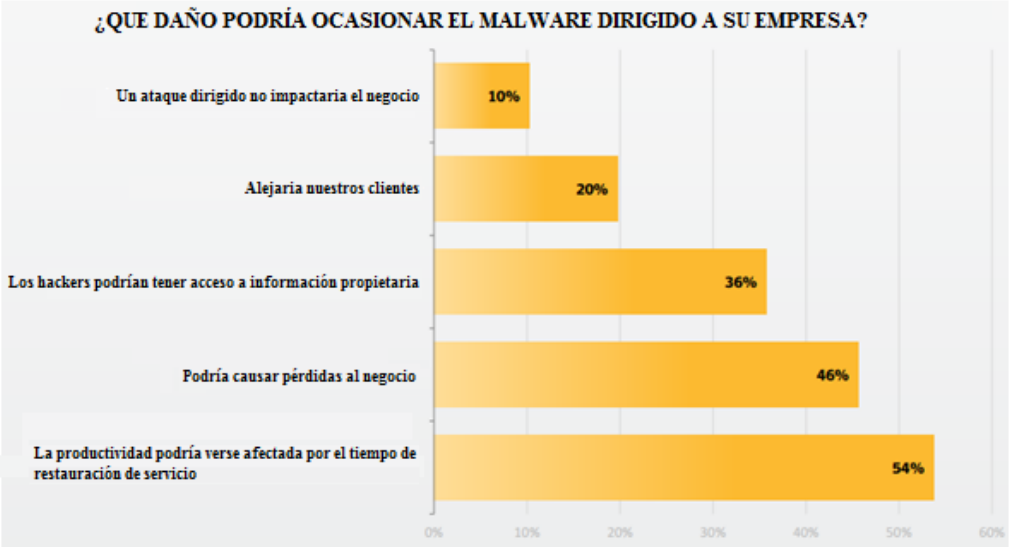

FIGURA 4 – ¿QUE DAÑO PODRÍA OCASIONAR EL MALWARE DIRIGIDO A SU EMPRESA? (Symantec, 2011)

c) Las empresas no se consideran objeto de ataque, sorprendentemente, aunque las empresas que participaron en la encuesta conocen los peligros de las brechas de seguridad informática, no creen que corran riesgo. La mitad de ellas consideran que al ser empresas pequeñas no están en peligro y que son las grandes empresas las que tienen que preocuparse por los ataques.

d) Las empresas no toman medidas, puesto que las empresas no se consideran objeto de ataques, muchas de ellas no toman precauciones básicas para proteger su información. mientras que dos tercios de las empresas restringen el acceso a los que tienen información de ingreso, un 63% no protege los equipos utilizados para la banca en línea y 9% no toma precauciones adicionales.

Lo anterior muestra un gran desinterés de las empresas en destinar un presupuesto eficiente para crear un ambiente más seguro en términos informáticos (Moreno, 2009).

Considerando lo descrito con anterioridad y consciente de las oportunidades de seguridad informática dentro de las PYMES, además de que México el 99% de las empresas son MIPYMES (Hernández, 2012) esta investigación dará pauta a el desarrollo de otras investigaciones y trabajos posteriores de estudiantes de licenciatura o postgrado además de comprobar la necesidad de las inversiones en seguridad informática, esto a través de un mecanismo formal de análisis que sea coherente y convincente para socios y dueños de las PYMES en México.

OBJETIVOS

1.2 OBJETIVO GENERAL

El objetivo del presente es realizar un estudio de factibilidad sobre invertir en seguridad informática en las PYMES.

1.3 OBJETIVOS ESPECÍFICOS

1. Llevar a cabo una investigación y contextualización de los siguientes temas y conceptos: seguridad de la información, servicios de seguridad en la información, seguridad informática, necesidad de seguridad informática en la empresa, amenazas, administración de riesgos, inversiones en seguridad informática, modelos para el análisis de viabilidad financiera en proyectos de seguridad informática y los costos de inversiones en seguridad informática.

2. Contrastar las ventajas y desventajas sobre los modelos de análisis financiero de proyectos de inversión para inversiones en seguridad informática.

3. Demostrar que hay ocasiones en las que es mayor el beneficio para una PYME de invertir en seguridad informática sobre los costos que conlleva afrontar una brecha de seguridad informática.

PREGUNTAS DE INVESTIGACIÓN

1. ¿Qué modelos financieros apoyan el análisis de viabilidad financiera para el cálculo de retorno de la inversión en proyectos de seguridad informática?

2. ¿Qué modelo se puede utilizar para calcular el tiempo de recuperación de la inversión en seguridad informática?

3. ¿Qué ventajas y desventajas llevan implícitos cada modelo para el cálculo de retorno de inversión en seguridad informática?

4. ¿Cómo se pueden integrar los anteriores modelos en un estudio de viabilidad financiera que soporte la inversión de seguridad informática en una PYME?

5. ¿Es posible demostrar que hay mayor beneficio en invertir en seguridad informática sobre, no invertir en seguridad informática en las PYMES en base a un estudio de viabilidad financiera?

CAPÍTULO II

Marco Teórico

“Conócete a ti mismo y conoce a tu enemigo y en cien batallas no correrás peligro” (Sun Tzu).

2 SEGURIDAD DE LA INFORMACIÓN

La seguridad se define como la calidad o estado que permite estar libre de cualquier peligro o le permite minimizar cualquier riesgo a un nivel aceptable, una empresa exitosa deberá contar con múltiples capas de seguridad implantadas para proteger sus operaciones (Whitman & Mattord, 2012):

- **Seguridad física**, para proteger objetos físicos, de acceso no autorizado o mal uso.
- **Seguridad de personal**, para proteger un individuo o grupo de individuos que tienen acceso a la empresas y sus operaciones.
- **Seguridad operacional**, que protege los detalles de una operación en particular o serie de actividades.
- **Seguridad de comunicaciones**, para proteger los medios de comunicación, tecnología y contenido.
- **Seguridad de redes**, para proteger dispositivos de red, conexiones de red y contenidos.
- **Seguridad de la información**, para proteger la confidencialidad, integridad y disponibilidad de los activos de información, ya sea en medios de almacenamiento, procesamiento o transmisión. Es lograda a través la implantación de una política, educación, entrenamiento, concientización y tecnología.

2.1 ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

Es la protección de información y sus elementos críticos, incluyendo sistemas de hardware que usan, almacenan y transmiten la información (Whitman & Mattord, 2012), incluye la definición y posterior implementación de protecciones, políticas y procedimientos, en búsqueda de la preservación de la integridad, disponibilidad y confidencialidad de la información, los recursos que la soportan (hardware, software, firmware, dispositivos de comunicación) y los individuos que la utilizan o conocen. El modelo más conocido para explicar la seguridad informática es el triangulo *CIA* mostrado en la figura 4. Durante 20 años, ha sido utilizado como el estándar de seguridad de la información basado en el uso de la información, que consiste en: confidencialidad, integridad y disponibilidad, conceptos ya antes mencionados.

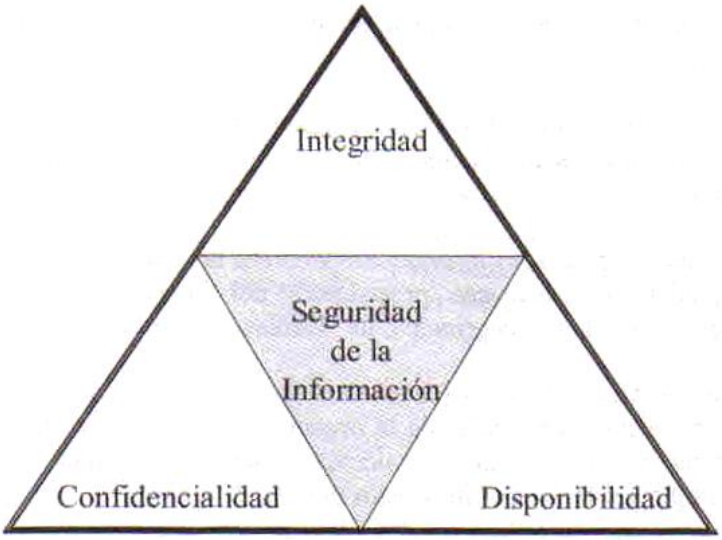

FIGURA 5 – EL TRIANGULO DE CIA

2.2 CARACTERÍSTICAS IMPORTANTES DE LA INFORMACIÓN

La información posee un valor intrínseco derivado de sus características. Si alguna característica de la información es alterada, el valor tendera a crecer o decrecer. Por otra parte el valor de la información basada en sus características también depende de la situación y el entorno, las siguientes son características importantes de la información (Whitman & Mattord, 2012):

2.2.1 CONFIDENCIALIDAD

Se define como asegurar que solo las personas que están autorizadas a tener acceso a cierta información sean las únicas en tener acceso (BS_7799, 1999). En otras palabras, la confidencialidad es la prevención de divulgación de información a individuos o sistemas sin privilegios (Whitman & Mattord, 2012). La confidencialidad en la información asegura que solo los individuos o sistemas autorizados puedan acceder información. Si algún individuo o sistema no autorizado llega acceder información protegida, en ese momento se dice que la confidencialidad de dicha información ha sido violada. Como resultado el valor de la información decrece. La confidencialidad se vuelve muy importante cuando se lleva al contexto de información personal. Para prevenir una brecha de confidencialidad en la información, se puede implementar alguna medida de seguridad como la clasificación de información, aseguramiento de

los dispositivos de almacenamiento de información, aplicación de políticas de seguridad, educación en seguridad informática a los usuarios de la información.

En México la información pública se clasifica en dos niveles de confidencialidad, según la Ley Federal De Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG, 2006):

1. **Reservada**: se considera información reservada aquella cuya publicación comprometa la seguridad nacional, la seguridad pública y la defensa nacional; menoscabe la conducción de las negociaciones y las relaciones internacionales; ponga en riesgo la estabilidad financiera, económica o monetaria del país; ponga en peligro la vida, la seguridad o la salud de cualquier persona; y cause un serio perjuicio a las actividades de verificación del cumplimiento de las leyes las actividades de prevención y persecución de los delitos, las atribuciones que ejerce el Ministerio Público durante la averiguación previa y ante los tribunales del Poder Judicial de la Federación, la impartición de justicia, la recaudación de las contribuciones y las operaciones de control migratorio.

   Igualmente se considera información reservada la contenida en los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto éstos no hayan causado estado; y la información relativa a las actuaciones y constancias administrativas de los procedimientos de responsabilidades de los servidores públicos previstos en la legislación aplicable, hasta en tanto no se haya dictado resolución administrativa o jurisdiccional definitiva.

2. **Confidencial**: La información confidencial se refiere a los datos personales tales como domicilio, número telefónico, patrimonio, ideas religiosas o políticas, estado de salud, entre otros, que se entregan al gobierno. También es considerada confidencial aquella información que entregan con ese carácter los particulares a dependencias o entidades, y para que ésta pueda ser difundida se requiere del consentimiento del titular de la información.

2.2.2 INTEGRIDAD

Esta característica se encarga de salvaguardar la precisión y la longitud de la información y los métodos de procesamiento (BS_7799, 1999), dicho en otras palabras, la integridad es el estado de incorruptibilidad y totalidad en la información (Whitman & Mattord, 2012). Si la información es corrompida, dañada o alterada de su estado original, de dice que la integridad ha sido comprometida. Esto puede pasar al momento que la información es recopilada, almacenada o transmitida. El propósito de la mayoría de los virus es corromper la información. Dos algoritmos para detectar corrupción en datos son: sondeando algún cambio de tamaños en archivos o a través de *funciones hash* para archivos.

2.2.3 DISPONIBILIDAD

Es definida como asegurar que usuarios o sistemas autorizados tengan acceso a la información protegida en el momento requerido (BS_7799, 1999). En otras palabras, la disponibilidad es el estado de un usuario o sistema computacional que permite acceder a información protegida sin interferencia u obstrucción en el formato requerido (Whitman & Mattord, 2012). La disponibilidad parece ser la característica más sencilla, sin embargo es muy importante.

2.2.4 CONFIABILIDAD

Es la característica que permite rastrear alguna acción de manera irrefutable de una entidad en el sistema de forma exclusiva a esa entidad (NIST, 2002). Es usualmente cerciorada a través de mecanismos de registro de acciones. En general es preciso que alguna especie de identificación al usuario o sistema computacional se realice antes de ejecutar alguna acción (lectura, modificación y transmisión) sobre la información protegida.

2.3 SERVICIOS DE SEGURIDAD EN LA INFORMACIÓN

Para lograr la preservación de las características de la información: confidencialidad, integridad, disponibilidad y confiabilidad, se definen una serie de servicios que pueden ser implantados. A continuación se presentan cuatro clasificaciones de los servicios principales que son la base para una infraestructura de seguridad de tecnologías de información:

2.3.1 AUTENTICACIÓN

Busca asegurar la validez de una identidad proporcionada para tener acceso a un sistema, esto se logra proporcionando cualquiera de estas tres formas de identidad del usuario: algo que el usuario conoce (p. ej.: usuarios, contraseñas), algo que el usuario tiene (p. ej.: una tarjeta con banda magnética, un chip) o por algo que el usuario es (p. ej.: huellas digitales).

2.3.2 AUTORIZACIÓN

Permite la especificación y administración de las acciones permisibles a ciertos usuarios, para acceso, modificación, o inserción de información a un sistema mediante permisos a los mismos.

2.3.3 NO REPUDIO

Provee los mecanismos para identificar quien ha llevado a cabo una o varias acciones en un sistema, de tal forma que usuarios no puedan objetar responsabilidades de las acciones ejercidas sobre un sistema. En otras palabras este mecanismo ofrece protección a un usuario frente a que otro usuario que niegue alguna acción efectuada en algún sistema de información. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

2.3.4 AUDITABILIDAD

Proporciona y facilita el mecanismo para detección y recuperación ante posibles fallas o incidentes de seguridad, mediante el registro de eventos y acciones en un sistema. Dicho de otra forma permite la reconstrucción, revisión y análisis de una secuencia de eventos

2.4 SEGURIDAD INFORMÁTICA

Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable, se considera seguro un sistema que cumple con las propiedades de integridad, confidencialidad y disponibilidad de la información (Aguilera, 2010).

El concepto de seguridad informática se confunde con el concepto de seguridad de la información (definido anteriormente en este marco teórico), este último concepto es más amplio y se refiere a la protección de la información encontrada en cualquier forma o medio no solo en medios informáticos (software, bases de datos y archivos), he ahí el nacimiento de una rama de la seguridad de la información llamada seguridad informática.

Un sistema informático, no obstante las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo. Para afrontar el establecimiento de un sistema de seguridad es necesario conocer: los elementos que componen un sistema informático, los peligros o riesgos que afectan el sistema informático y las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales (Aguilera, 2010).

Todos los elementos que participan en un sistema informático puede verse afectados por fallos de seguridad, si bien se suele considerar la información como el factor más vulnerable. El hardware y otros elementos físicos se pueden a volver a comprar y restaurar, el software puede volver a ser reinstalado, pero la información dañada no siempre es recuperable, lo que puede ocasionar daños de diversa índole sobre la economía y la imagen de la empresa y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es la mayoría de los fallos de seguridad se deben al factor humano (Aguilera, 2010).

Un sistema informático se divide en seis componentes: software, hardware, datos, usuarios, procedimientos y redes los cuales hacen posible el uso de recursos de información dentro de la empresa. Estos seis elementos críticos del sistema informático permiten que la información sea ingresada, procesada, extraída o almacenada (Whitman & Mattord, 2012):

2.4.1 SOFTWARE

Comprende aplicaciones y sistemas operativos, cabe mencionar que este componente en particular es el más difícil de asegurar, la prueba está en el numero de errores de programación que son explotados día a día y que representan una parte substancial del total de los ataques a información almacenada en sistemas informáticos. La industria de tecnologías de la información está repleta de reportes de advertencias de agujeros, *bichos*, debilidades y otros problemas relacionados al software. En estos

tiempos muchas facetas de nuestra vida son afectadas por errores en software, desde fallos en teléfonos inteligentes hasta computadores de control automotriz con fallas que lleva a la retirada del mercado de dichas piezas.

La causa raíz de los defectos encontrados en el software desafortunadamente es debido a que es creado bajo restricciones por parte de la administración de proyectos, que limitan tiempo, costo y capital humano. La seguridad en el *desarrollo de software* es muy pocas veces tomada en cuenta y en la mayoría de los casos es una ocurrencia tardía, en lugar de ser desarrollada como una parte integral del software desde la primer *fase de desarrollo de software*. De este modo, el software es el componente que se vuelve el blanco de ataques intencionales o accidentales más común.

2.4.2 HARDWARE

El propósito principal del hardware debe ser la posibilidad de instalar Software, almacenar y trasmitir datos, proporcionando interfaces para ingresar o remover datos del sistema. Los métodos que aplican para proteger el hardware son llaves y candados (físicos) y controles de acceso a componentes físicos. Sin embargo el porcentaje de robos de teléfonos inteligentes y laptops sigue siendo alto. En varios casos, el valor de la información contenida en el hardware es mayor al hardware en sí.

2.4.3 DATOS

Es lo que se ingresa, procesa, almacena, transmite y remueve del sistema informático. Los datos o información es el objetivo principal del ataque a un sistema informático.

2.4.4 USUARIOS

Tienen tres tipos de impacto al sistema informático: positivo, neutral y negativo. Los usuarios pueden ser entrenados de tal forma que el sistema informático sea más seguro. Por ejemplo, pueden ser entrenados para fijar una contraseña difícil de ser adivinada y por ejemplo terminar la sesión del sistema informático al momento de dejar la computadora desatendida. Es importante notar que los usuarios son una amenaza al sistema informático. De acuerdo al CSI Computer Crime and Security Survey en el 2010 (Richardson, 2011), el quinto incidente de seguridad más frecuente es el abuso del uso de la red y correo electrónico por parte de empleados internos:

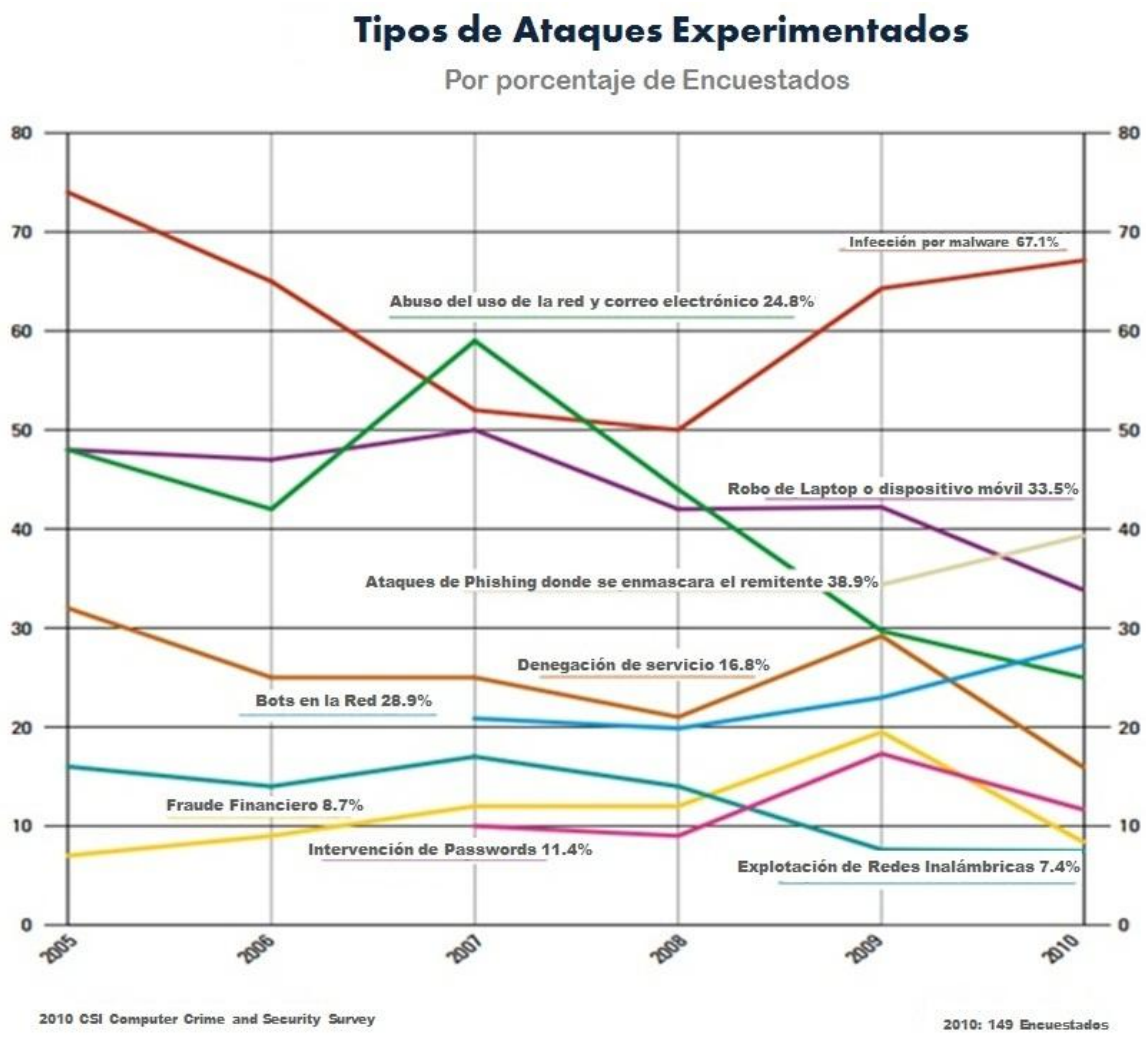

FIGURA 6 – INCIDENTES DE SEGURIDAD MAS FRECUENTES (COMPUTER CRIME AND SECURITY SURVEY)

Además de usuarios maliciosos, existen usuarios sin intención maliciosa que de manera no intencionalmente causan daños en cualquier componente(s) del sistema informático. Cabe recalcar que los usuarios siguen siendo el componente más débil debido al error humano, a menos que medidas de seguridad como políticas, educación y entrenamiento sean propiamente implantadas.

2.4.5 PROCEDIMIENTOS

Son instrucciones que especifican la manera de completar una tarea. Los procedimientos son tan importantes como los otros componentes porque procedimiento inconsistente puede ocasionar que todo el sistema informático no esté asegurado. Por ejemplo la falta de autenticación al sistema. Por otra parte el entrenamiento del

procedimiento a usuarios del sistema informático es crucial. Esto es porque los procedimientos pueden ayudar a reducir el error humano cuando los usuarios son entrenados adecuadamente a seguir apropiadamente dichos procedimientos.

2.4.6 REDES

Este componente da soporte al sistema informático para poder tener accesible dicho sistema ya sea en una red de área local o globalmente mediante el internet. La seguridad informática enfrenta varios retos que han incrementado la importancia de proveer seguridad de redes para asegurar la información en transmisión.

2.5 NECESIDAD DE SEGURIDAD INFORMÁTICA EN LA EMPRESA

Para un negocio la seguridad tiene varias funciones como proteger la información, permitir al negocio operar normalmente, proveer una plataforma de resguardo a aplicaciones y salvaguardar activos tecnológicos (Whitman & Mattord, 2012). Especialmente en negocios basados en tecnologías de información, las siguientes funcionalidades desempeñadas dentro de la seguridad informática son clave para asegurar el éxito de un negocio:

2.5.1 PROTEGER LA INFORMACIÓN

El valor de la información depende de sus características y de las circunstancias en que se presentan. Proteger la información en este caso significa mantener la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, no solo datos o información almacenada necesita ser protegida, sino también la información transmitida a través de la red o la que es ejecutada a través de cualquier aplicación.

2.5.2 HABILITAR LA OPERACIÓN DEL NEGOCIO

La seguridad informática es implementada para asegurar que el negocio opere de manera eficaz y eficiente. Es un hecho que la implementación de la seguridad informática tiene que ver con administración, la cual se traduce en la definición de políticas y la puesta en marcha de estas, más que un asunto de tecnología en sí. Para definir la necesidad del nivel de seguridad, es necesario concentrase más en la evaluación de el aseguramiento en términos de impacto en el negocio más que en el problema tecnológico.

2.5.3 PROVEER DE UNA PLATAFORMA SEGURA PARA LAS APLICACIONES

Las empresas de hoy están bajo una enorme presión de adquirir y operar eficientes y capaces aplicaciones. Una empresa necesita crear un ambiente que proteja estas aplicaciones, particularmente esas que sean pieza elemental para la infraestructura de la empresa como sistemas operativos, correo electrónico y mensajeros instantáneos.

2.5.4 RESGUARDAR LOS ACTIVOS TECNOLÓGICOS

Servicios de seguridad informática deben ser implantados para proteger activos tecnológicos en la empresa. Estos servicios deben ser basados en el tamaño, alcance e intereses de la empresa. Además es recomendable que cuando la empresa crezca y la solución tecnológica existente no pueda soportar la necesidad de cambio, una solución tecnológica más robusta debe remplazar los programas de seguridad que la empresa ha sobrepasado.

2.6 AMENAZAS

Es un objeto, persona u otro ente que representa un peligro potencial a un activo (Whitman & Mattord, 2012), siendo capaz de explotar una vulnerabilidad intencionalmente o accidentalmente, y de esta manera obtener, dañar o destruir información. Para proteger de amenazas una empresa u organización es necesario estar familiarizado con la información que se quiere proteger y los sistemas informáticos que la almacenaran, transportaran y procesaran; y conocer las amenazas a las que se puede enfrentar el negocio. La siguiente tabla muestra a continuación diferentes categorías de amenazas acompañadas de ejemplos:

	Categoría de amenaza	Ejemplos
1.	Violaciones a la propiedad intelectual	Piratería, violación a derechos de autor
2.	Ataques a través de software	Virus, gusanos, macros, denegación de servicio
3.	Degradación en el suministro de servicio	Proveedor de servicios de internet, energía eléctrica
4.	Espionaje o transgresión	Acceso no autorizado o robo de datos
5.	Fuerzas naturales	Incendios, inundaciones, terremotos, tormentas eléctricas
6.	Errores y fallas humanas	Accidentes, errores de empleados
7.	Extorsiones	Chantaje, divulgación de información
8.	Controles de seguridad incompletos, inadecuados y faltantes	Red comprometida por que no existía un cortafuegos
9.	Sabotaje y vandalismo	Destrucción de sistemas o información
10.	Robo	Confiscación ilegal de información o equipos
11.	Errores o fallas técnicas en el hardware	Falla en equipos
12.	Errores o fallas técnicas en el software	Bichos de programación, problemas de codificación, vulnerabilidades desconocidas
13.	Tecnología obsoleta	Tecnologías anticuadas o desactualizadas

TABLA 1 – AMENAZAS DE SEGURIDAD INFORMÁTICA (Whitman & Mattord, 2012)

2.7 ADMINISTRACIÓN DE RIESGOS

Es el proceso que permite a los administradores de tecnologías de información balancear costos económicos y operacionales de medidas de protección y de esta manera proteger los sistemas de información y datos que soportan la misión de una empresa (NIST, 2002).

De esta forma la administración de riesgos es el proceso para identificar, controlar y reducir la probabilidad y el impacto de incidentes de seguridad a un nivel aceptable.

2.7.1 PROCESO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD

De la definición anterior la formula más común para el cálculo del riesgo es la siguiente (NIST, 2002):

$$\boldsymbol{Riesgo = Impacto \times Probabilidad}$$

Existen diversas metodologías para el proceso de administración de riesgos, varias de estas metodologías se encuentran en documentos de investigación científica y otras metodologías se encuentran en estándares y lineamientos como en publicaciones del ISO 27000 y en publicaciones del NIST (National Institute of Standards and Technology).

Generalmente el proceso de administración de riesgos se compone de varios pasos, entre estos:

I. Análisis de riesgos.
II. Evaluación de riesgos.
III. Selección de estrategias.
IV. Análisis costo beneficio.
V. Implantación.

FIGURA 7 – PROCESO DE ADMINISTRACIÓN DE RIESGOS

Cabe señalar que el proceso de administración de riesgos es un proceso continuo, esto quiere decir que incluso después de la fase de implantación, existe un ciclo que lleva a la primera fase del proceso donde se evalúa el último ciclo implementado y compararlo con el nivel deseado en la siguiente iteración de administración de riesgos.

2.7.2 ANÁLISIS DE RIESGOS

El objetivo de este análisis es identificar y medir el riesgo para poder tomar decisiones. Para este análisis se necesita información acerca de los activos a proteger dentro de la empresa, las amenazas a las que estos activos están expuestos y vulnerabilidades que se podrían explotar en los sistemas (ver Figura 8).

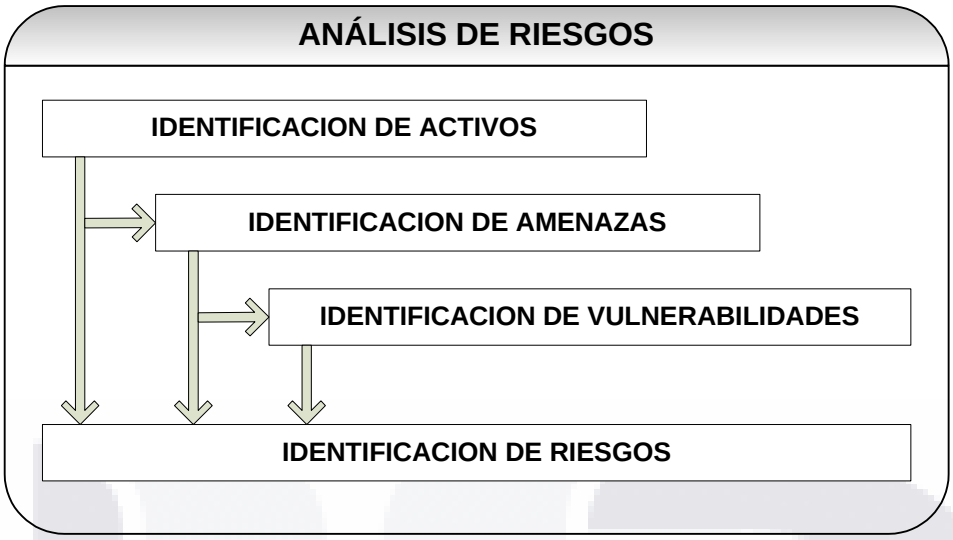

FIGURA 8 – ANÁLISIS DE RIESGOS

Identificación de activos: en la actualidad las empresas dependen fuertemente de activos informáticos. Antes de identificar los activos de una empresa, los límites del sistema de tecnologías de información deben ser identificados, luego debe ser clasificado como sigue (NIST, 2002):

- Equipos Informáticos - Hardware
- Aplicaciones - Software
- Redes de comunicaciones – internas y externas
- Datos / información
- Personal – Usuarios y personal de soporte de las tecnologías de información

Después de especificar el alcance del análisis, de identificar los activos, clasificarlos y valorarlos. Hay que recalcar que activos tangibles tales como: servidores, terminales y dispositivos de red, son más fácil de calcular su valor que activos intangibles tales como: datos de negocio, conocimiento de la empresa y propiedad intelectual almacenada.

Para la valuación de activos se pueden tomar dos criterios:

I. Nivel de criticidad para el éxito de la compañía: este criterio se refiere a la importancia del activo para la empresa y para el objetivo y misión de la misma siendo que los procesos de negocio dependen de información. Ejemplos son: impacto a los ingresos, rentabilidad e imagen pública.

II. Valor para los adversarios: Este criterio estima el valor que tiene un activo para algún competidor o algún adversario.

Esta valuación de activos puede llevarse a cabo a través de un proceso cuantitativo (como el que se muestra en la siguiente tabla) o puede ser a través de un proceso cualitativo (critico, alto, mediano, bajo e insignificante). El puntaje recomendado varía entre: 0.01 y 1.0 (recomendado por el NIST SP800-30). Entre más criterios se tengan, lo más preciso pero al mismo tiempo lo mas tardado será para determinar la valuación.

Activo (Información)	Criterio 1: Impacto en los ingresos	Criterio 2: Impacto en la rentabilidad	Criterio 3: Impacto en imagen pública	Peso Puntaje
Peso del criterio	30	40	30	
Informacion A	0.8	0.9	0.5	75
Informacion B	0.4	0.5	0.3	41
Informacion C	0.4	0.4	0.9	55

TABLA 2 – EJEMPLO DE VALUACIÓN DE ACTIVOS CUANTITATIVA SEGÚN SU IMPORTANCIA

La tabla 2 muestra un ejemplo de un formato para valuación de activos; el resultado de esta tabla soporta el análisis para hacer priorizar los activos. Después de esto, los activos son priorizados en un orden que permite a la empresa enfocarse en los activos más críticos. Estos activos pueden priorizarse según el peso o puntaje de la tabla. Como resultado en este ejemplo de valuación, la información A es la más importante para la empresa seguida de la información C y la información B.

Identificación de amenazas: El segundo paso en el análisis de riesgos es la identificación de amenazas, que a su vez deben ser priorizadas. Las amenazas por lo regular afectan a diferentes tipos de activos. Existen dos grandes clases de amenazas: los desastres naturales y actos humanos (pueden ser malintencionados y no malintencionados).

Para identificar amenazas, existen diversos métodos, como: crear listas, examinar datos históricos internos/externos y lluvia de ideas (Whitman & Mattord, 2012). Las amenazas deben de ser valoradas según su capacidad de comprometer la empresa y se deben priorizar según su peligro y/o desembolso necesario para cubrir dichas amenazas.

Identificación de vulnerabilidades: Una vulnerabilidad es una debilidad en un activo de información, procedimiento de seguridad, diseño técnico o control que una amenaza

puede explotar. Muchos de los incidentes hoy en día ocurren por vulnerabilidades presentes en aplicaciones (software). Sin embargo no todo tipo de vulnerabilidades caen en la clasificación de errores técnicos, también son consecuencia de errores humanos (p. ej.: cuando usuarios comparten su contraseña, cuando un usuario configura una contraseña fácil de adivinar, cuando un usuario descarga programas maliciosos). Para identificar vulnerabilidades, se pueden utilizar métodos similares a la identificación de amenazas, sin embargo el proceso es subjetivo, debido a que se basa en el conocimiento y experiencia de los expertos (Whitman & Mattord, 2012). Una vez que se analizaron riesgos, se listaron activos, amenazas y vulnerabilidades, se procede a la evaluación de riesgos.

2.7.3 EVALUACIÓN DE RIESGOS

El objetivo de la valoración de riesgos es apoyar a la empresa en la toma de decisiones de la estrategia que hará frente a los riesgos de seguridad informática y con la inversión en controles de seguridad. La valoración de riesgos por lo regular necesita datos de la situación actual sobre el impacto de los riesgos o la pérdida potencial para la empresa y la probabilidad de ocurrencia (ver figura 9).

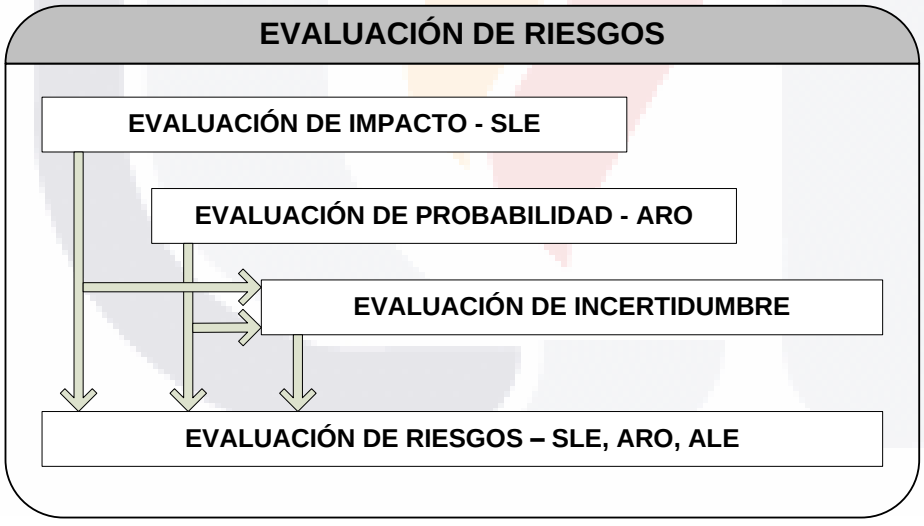

FIGURA 9 – EVALUACIÓN DE RIESGOS

Adicionalmente se puede agregar la evaluación de incertidumbre para compensar la falta de conocimiento preciso del experto y la incertidumbre en el entorno de seguridad informática.

Uno de los métodos analíticos cuantitativos más comunes para exponer un riesgo es: expectativa de pérdida anual (*ALE*). Este método es recomendado por: International Information Systems Security Certification Consortium (ISC)^2. El cálculo de la expectativa de pérdida anual o ALE requiere de la determinación cuantitativa de la pérdida según el impacto, el cual es llamada: expectativa de pérdida por evento (*SLE*). Por otra parte la determinación de la probabilidad de la ocurrencia de un riesgo, la cual es llamada: Tasa anual de eventos (*ARO*) es requerida también para el cálculo.

Evaluación de impacto: puede ser considerada como la parte más problemática de la evaluación de riesgos por que existen múltiples maneras de evaluar el impacto de riesgos informáticos. La evaluación de impacto determina la consecuencia de un riesgo, estas consecuencias abarcan: muertes, daños, pérdidas financieras, suministro de servicio, etc. Después una calificación apropiada es definida, en general se aplica la medida: SLE (expectativa de perdida por evento, descrita anteriormente).

Expectativa de pérdida por evento (SLE):

El SLE representa el "monto total" de pérdida en los ingresos de una empresa, consecuencia de una sola ocurrencia de un riesgo. Una medida monetaria es asignada para representar la perdida potencial de una empresa si una amenaza explota una vulnerabilidad de un sistema informático soporta activos intangibles de la empresa. El SLE en veces se obtiene de multiplicar el valor del activo (*AV*) con el factor de exposición (*EF*) como se muestra a continuación:

$$\boldsymbol{SLE = AV \times EF}$$

El factor AV representa la creación, desarrollo, soporte, remplazo y valor intrínseco de un activo y es expresado como el valor monetario del activo (Ronald & Vines, 2004). El factor EF representa la magnitud de la pérdida o impacto en el valor del activo resultado de una amenaza y es expresado como porcentaje.

Evaluación de probabilidad: es la probabilidad de que una vulnerabilidad será explotada (NIST, 2002), para esto existen diversos sistemas de clasificación, en general se puede aplicar la medida ARO (tasa anual de eventos).

Tasa anual de eventos (ARO):

La medida de SLE (expectativa de perdida por evento) se obtiene para estimar el nivel de impacto potencial de un riesgo, el ARO se requiere para determinar la frecuencia de ocurrencia del riesgo. Básicamente el ARO representa el número de veces que ocurra un riesgo determinado en la compañía anualmente.

Evaluación de incertidumbre: Para entender un poco más la incertidumbre, es bueno recordar la interpretación de la probabilidad según el punto de vista frecuentista y bayesiano, donde el punto de vista frecuentista considera la probabilidad de un evento como la frecuencia relativa de ocurrencia de un experimento, cuando el experimento es completamente aleatorio y bien definido. Dicho de otras palabras la estadística frecuentista tiene como objetivo determinar una determinar una conclusión, sea en base a significación estadística o aceptación y rechazo de hipótesis, siempre dentro del marco del estudio que se esté realizando. No existen subjetividades referentes a parámetros, puesto que se han fijado los criterios de decisión a priori y estos permanecen estáticos durante todo el estudio.

En contraste del punto de vista bayesiano que considera que la probabilidad de que ocurra un suceso varía de acuerdo a información externa al estudio que se realiza, Así pues, las fuentes de información “apriori” se ven trasformadas en probabilidad “a posteriori” y se utilizan a continuación para realizar la inferencia.

Teniendo esto en cuenta, existen dos tipos de incertidumbre:

- Incertidumbre debido a la variabilidad en la población: este tipo de incertidumbre no puede ser reducida agregando más información.
- Incertidumbre debido a la falta de conocimiento: Este tipo de incertidumbre puede ser reducida por medio de información adicional.

Después de todas las determinaciones anteriores se procede a obtener la expectativa de pérdida anual (ALE), que se obtiene de multiplicar la tasa anual de eventos (ARO) por la expectativa de perdida por evento (SLE) como se muestra a continuación:

$$\boldsymbol{ALE = ARO \times SLE}$$

El ALE representa la pérdida financiera anual resultado de no mitigar un riesgo en particular. Después de obtener los valores de SLE, ARO y ALE, una escala de

calificación puede ser generada para priorizar riesgos en una empresa utilizando el valor ALE.

Métricas de Riesgo:

En general el riesgo se refiere a la incertidumbre de que un evento ocurra. En el contexto de seguridad informática, el riesgo usualmente se refiere a la incertidumbre asociada con la ocurrencia de eventos perjudiciales (Gordon & Loeb, 2006).

La medida de riesgo mejor conocida entre los profesionistas de seguridad informática es la perdida esperada (monetaria) por brechas de seguridad, la cual es la medida que provee el concepto base para el desarrollo y uso de la expectativa de pérdida anual (ALE). La pérdida esperada (o, de forma más precisa, el valor esperado de las pérdidas) combina dos elementos asociados con el riesgo: la probabilidad de las pérdidas y la magnitud de las pérdidas. De esta forma el producto de estos dos factores mencionados dan lugar a la perdida esperada por una brecha de seguridad. En la literatura de seguridad informática, la perdida esperada esta usualmente asociada con el riesgo de no tener suficientes medidas de seguridad implantadas (Gordon & Loeb, 2006).

Para mostrar que la pérdida esperada no captura todo el cuadro de riesgo, tomaremos el siguiente ejemplo que muestra información de tres inversiones en seguridad informática denominadas: A, B y C. Cada inversión representa una combinación diferente de actividades y tecnologías de seguridad informática, sin embargo se asume que cuestan el mismo monto. Así también por simplicidad se asume que todo (perdidas por brechas de seguridad y gastos/inversiones en seguridad informática) toma lugar en un mismo período. Además, se asume que existen cuatro posibilidades referente a perdidas: (1) no habrá brechas de seguridad, por tanto las pérdidas son cero, (2) brechas resultaran en pérdidas de $1,000,000, (3) brechas de seguridad que representaran $2,000,000 en perdidas y (4) brechas de seguridad que resultaran en pérdidas de $3,000,000. Estas posibilidades se muestran en la columna 1 de la tabla 3. Las probabilidades para cada nivel de pérdida de cada una de las inversiones (A, B y C) se muestran en las columnas 2, 4 y 6 respectivamente (Gordon & Loeb, 2006).

Como se puede apreciar de las tres líneas de la tabla 3, las inversiones en seguridad informática A, B y C resultan en la misma perdida esperada por brechas de seguridad,

esta pérdida esperada es exactamente: $1,200,000. Sin embargo aunque todas estas inversiones muestran la misma perdida esperada, difieren con respecto a otras medidas de riesgo. Esto será demostrado considerando tres métricas adicionales de seguridad.

(1)	(2)	(3) = (1) x (2)	(4)	(5) = (1) x (4)	(6)	(7) = (1) x (6)
Pérdidas esperadas	Probabilidad de pérdidas con inversión A	Valor esperado de la pérdida con la inversión A	Probabilidad de pérdidas con inversión B	Valor esperado de la pérdida con la inversión B	Probabilidad de pérdidas con inversión C	Valor esperado de la pérdida con la inversión C
$ -	0.4	$ -	0.6	$ -	0.15	$ -
$ 1,000,000.00	0	$ -	0	$ -	0.6	$ 600,000.00
$ 2,000,000.00	0.6	$ 1,200,000.00	0	$ -	0.15	$ 300,000.00
$ 3,000,000.00	0	$ -	0.4	$ 1,200,000.00	0.1	$ 300,000.00
Valor esperado de las pérdidas con Inversión A=suma de columna (3)	$ 1,200,000.00					
Valor esperado de las pérdidas inversión B = suma de columna (5)	$ 1,200,000.00					
Valor esperado de las pérdidas inversión C = suma de columna (6)	$ 1,200,000.00					

TABLA 3 – TRES INVERSIONES EN SEGURIDAD INFORMÁTICA CON MISMAS PÉRDIDAS ESPERADAS (Gordon & Loeb, 2006)

La primer métrica adicional para considerar en el contexto de seguridad informática es la probabilidad que cualquier pérdida ocurrirá (equivalentemente, para esta ilustración, la probabilidad que la empresa sufrirá una pérdida de por lo menos $1,000,000). Examinando las columnas 2, 4 y 6 de la tabla 3, podemos apreciar que usando esta métrica, la inversión B será la menos riesgosa con una probabilidad de pérdida de solo 40% (habiendo un 60% de probabilidad de que no haya pérdidas), seguido de la inversión A con un 60% de probabilidad de pérdidas (existiendo un 40% de probabilidad de que no existan pérdidas) y por último la inversión C será llamada la mas riesgosa, teniendo un 85% de pérdidas (teniendo 15% de probabilidad de que no existan pérdidas) (Gordon & Loeb, 2006).

En lugar de enfocarse en la probabilidad de que cualquier pérdida ocurra, la segunda métrica adicional para riesgo se enfoca en la probabilidad más grande de que una pérdida mayor ocurra (p. ej.: la probabilidad de que la empresa sufra una pérdida de $3,000,000) . Examinando la tabla 3, podemos apreciar que usando esta métrica, la inversión A será la menos riesgosa, siendo que no hay probabilidad de que exista alguna perdida de $3,000,000, seguida de la inversión C con un 10% de probabilidad de tener una pérdida de $3,000,000 y la inversión B será la más riesgosa, teniendo un 40% de sufrir una pérdida de $3,000,000.

En economía y finanzas, la varianza es la métrica más utilizada de riesgo. De este modo, una tercera métrica adicional de riesgo para considerar en el contexto de seguridad informática es la varianza de las perdidas. La varianza (o la desviación estándar, que es igual a la raíz cuadrada de la varianza) es una medida de dispersión que está asociada a la distribución probabilidad de pérdidas. Para calcular la varianza, primero se toma la suma del producto de la probabilidad de cada perdida y el cuadrado de la diferencia entre cada perdida esperada y el valor de la pérdida por inversión. La varianza de las pérdidas para la inversión A es igual a 0.96M (donde M es millones), la varianza de pérdidas para B es igual a 2.16 y la varianza de pérdidas para la inversión C es 0.66 M. Por tanto, usando la varianza como una medida de riesgo, la inversión C es la menos riesgosa, seguida de la inversión A y considerándose la inversión B como la más riesgosa (Gordon & Loeb, 2006).

Como este ejemplo lo demuestra, no hay una sola métrica de riesgo que capture todos los elementos del riesgo asociados con un conjunto de actividades de seguridad informática e inversiones. Mientras que la métrica de pérdida esperada calcula el riesgo de las inversiones A, B y C como iguales, el cálculo de riesgo de las tres métricas de riesgo adicionales no fue consistente a través de las tres métricas examinadas (Gordon & Loeb, 2006).

Con respecto a la primer métrica de riesgo adicional (probabilidad de que ocurra cualquier pérdida), se observo que las inversiones, de menor a mayor riesgo fueron: B, A y luego C. Con respecto a la segunda métrica de riesgo adicional (probabilidad más grande de que una pérdida mayor ocurra) se observo de menor a mayor riesgo el siguiente orden: A, C y B. Finalmente la ponderación del riesgo basado en la tercer métrica de seguridad (varianza de las pérdidas) arrojo: C, A y luego B. La tabla 4 concentra todos los resultados. Siendo que no se puede capturar todas las caras del riesgo, la decisión sobre una inversión en seguridad se tiene que realizar considerando todo el cuadro de riesgo (en lenguaje técnico, toda la distribución probabilidad de pérdidas), así como la preferencia al riesgo, al momento de seleccionar entre diferentes arreglos de actividades e inversiones (Gordon & Loeb, 2006).

Métrica de riesgo	Inversiones		
	A	B	C
Valor esperado de pérdidas	Igual	Igual	Igual
Probabilidad de que ocurra cualquier pérdida	Mediano	Peor	Mejor
Probabilidad más grande de que una pérdida mayor ocurra	Peor	Mejor	Mediano
Varianza de pérdidas	Mediano	Mejor	Peor

TABLA 4 – PONDERACIONES DE RIESGO DE LAS TRES INVERSIONES EN SEGURIDAD INFORMÁTICA (Gordon & Loeb, 2006)

El riesgo y la seguridad informática son conceptos intrínsecamente relacionados. Atrás de esta relación esta la noción de que el riesgo está directamente conectado a la exposición y tamaño de una pérdida potencial causada por una brecha de seguridad, como se describió anteriormente la medida más conocida por los administradores de seguridad se deriva de la noción de perdidas esperadas (ALE). A pesar de ser importante, esta medida representa solo una métrica de riesgo, por tanto los profesionistas en seguridad informática deben estar familiarizados con otras medidas de riesgo de tal modo que puedan ejercer decisiones racionales de asignación de recursos que conciernen a actividades de seguridad informática. La realidad es que muchos profesionistas de seguridad informática carecen de entendimiento total de la administración de riesgos de seguridad informática (Gordon & Loeb, 2006).

El proceso de administración de riesgos es un proceso que involucra identificar el riesgo y reducirlo a un nivel aceptable. Por supuesto, el proceso de administración de riesgos también debe ser considerado dentro del contexto de análisis costo-beneficio. Es decir, no hace sentido derrochar (p. ej.: gastar más de los beneficios monetarios esperados) en cualquier etapa del proceso de administración de riesgos (Gordon & Loeb, 2006).

2.7.4 SELECCIÓN DE ESTRATEGIAS

Después que se han analizado y evaluado los riesgos de seguridad, la compañía continúa con el siguiente paso en la administración de riesgos, seleccionando la estrategia más apropiada para reducir sus riesgos (NIST, 2002):

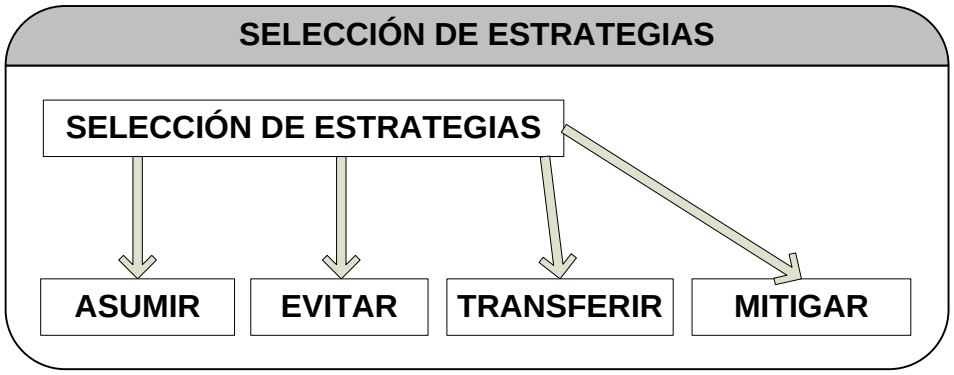

FIGURA 10 – SELECCIÓN DE ESTRATEGIA

Asumir: Es la opción de no hacer nada contra tener el riesgo de una amenaza explotando una vulnerabilidad en la compañía y asume los daños como costos de hacer negocio. Es razonable esta opción cuando el ARO es pequeño o cuando el costo de mitigar un riesgo es mucho mayor que el beneficio.

Evitar: Es la alternativa que considera remover la fuente de riesgo y/o consecuencias. Esta estrategia se toma por lo regular cuando el impacto del riesgo es mucho mayor al beneficio de tener un activo.

Transferir: Contempla el pasar riesgos a otros activos, procesos u empresas a través de coberturas (usualmente esto se visualiza como compañías de servicios de seguridad de información y aseguradoras).

Mitigar: Es la opción de mitigar el impacto de una vulnerabilidad implementando sistemas o herramientas de seguridad de información o a través de mecanismos de control como políticas y controles de accesos. Esta es considerada la estrategia primaria de la administración de riesgos.

En realidad no existe un procedimiento estandarizado para escoger la estrategia de mitigación más adecuada. En general una empresa debe seleccionar la estrategia que más se apegue a la situación en la que se encuentra.

Controles de Seguridad: Las compañías utilizan contramedidas para manejar amenazas, estas contramedidas pueden ser divididas en dos clasificaciones:

I. La primera clasificación consiste en:

a. **Controles Físicos**: Estas medidas son para proteger equipos de tecnologías de información de amenazas físicas como malfuncionamiento, acceso no autorizado, daño físico y robo (p. ej.: candados, cajas fuertes).

b. **Controles Lógicos**: Estas medidas son diseñadas para proteger aplicaciones de tecnologías de información o datos para prevenir acceso no autorizado, errores y fraudes (p. ej.: controles de acceso, encriptación y protección de virus).

c. **Controles Organizacionales**: Estas medidas complementan los sistemas de controles físicos y lógicos, dentro de esta clasificación se encuentran las políticas y lineamientos.

II. La segunda clasificación se compone de:

a. **Controles de prevención**: Este tipo de controles previenen amenazas de tecnologías de información de materializarse en incidentes de seguridad (p. ej.: control de accesos, encriptación y autenticación).

b. **Controles de detención**: El objetivo es detectar incidentes para prevenir las consecuencias devastadoras de incidentes de seguridad (p. ej. registros de auditoría, mecanismos de detección de intrusos).

c. **Controles de regresión**: Estos tienen la meta de reducir los daños y consecuencias de daños cuando estos no pueden ser prevenidos.

d. **Controles de corrección**: El propósito de estas medidas de corrección es reparar daños causados por incidentes de seguridad, es un subtipo de controles de regresión en términos que reducen las consecuencias después de algún daño ocasionado.

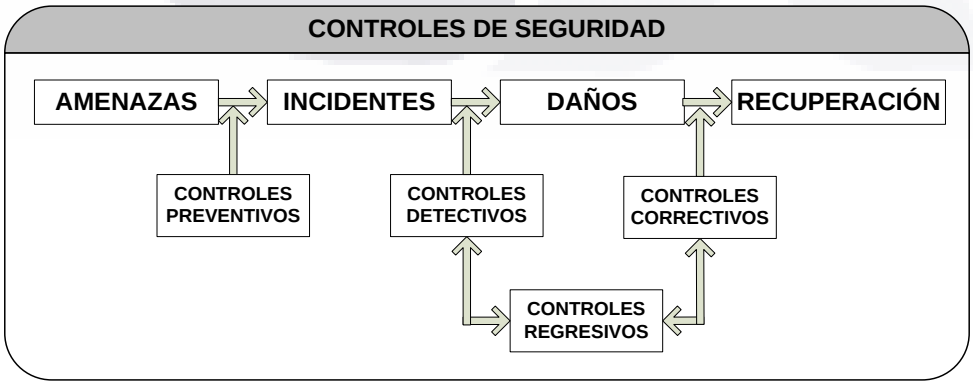

FIGURA 11 – EL IMPACTO DE CONTROLES DE SEGURIDAD

2.8 INVERSIONES EN SEGURIDAD INFORMÁTICA – ANÁLISIS COSTO BENEFICIO

El análisis costo beneficio es un principio económico ampliamente aceptado para administrar todos los recursos de una empresa. Este principio requiere que el costo de una actividad sea comparado con los beneficios de la misma, de tal modo que cuando los beneficios exceden los costos, es redituable el involucramiento en dicha actividad. Cuando los costos superan los beneficios, no es conveniente el involucramiento en dicha actividad y cuando los costos y los beneficios de la actividad son los mismos, el responsable en tomar una decisión debe mostrarse indiferente a dicha actividad (Gordon & Loeb, 2006).

Cuando los responsables en tomar decisiones seleccionan una estrategia de mitigación para manejar riesgos, una inversión en seguridad para implementar las contramedidas contra esos riesgos debe ser evaluada. La intención de estas inversiones es minimizar los impactos o severas consecuencias y la probabilidad de brechas de seguridad.

Los riesgos podrán ser óptimamente mitigados mediante el uso de un análisis costo-beneficio. Existen varios enfoques que incorporan el análisis costo beneficio como el análisis de retorno de la inversión (*ROI*), valor presente neto (*VPN*) y la tasa interna de retorno (*TIR*). Estos anteriores son utilizados como métricas financieras para cuantificar el costo y beneficio de las inversiones en tecnologías de información.

Las empresas deben considerar la viabilidad financiera al momento de implantar medidas de seguridad en la información. En general las organizaciones deben invertir en seguridad informática cuando los beneficios rebasen sus costos.

El beneficio es el valor monetario que la empresa ahorra a través de medidas que reducen perdidas de alguna vulnerabilidad, puede ser visto en términos de que tanto impacto y probabilidad de incidentes en tecnologías de información se pueden reducir, en otras palabras es una reducción en la expectativa de pérdida anual (ALE).

Los costos deben ir en términos de costos de implantación (hardware y software), costo de mantenimiento, costo de entrenamiento y personal a contratar.

2.9 MODELOS PARA EL ANÁLISIS DE VIABILIDAD FINANCIERA EN PROYECTOS DE SEGURIDAD DE INFORMÁTICA

La primera acción que debe realizarse para soportar una buena toma de decisiones con respecto a la viabilidad financiera de una inversión en seguridad informática, es la que se refiere a evaluación financiera o estudio de rentabilidad de dicho proyecto de inversión.

"El estudio de la rentabilidad de un proyecto de inversión, busca determinar con mayor precisión posible, la cuantía de las inversiones, costos y beneficios de un proyecto, para posteriormente compararlos y determinar la conveniencia de emprenderlo" (SAPAG C., 2001).

La evaluación financiera consiste en analizar un proyecto, a la luz de un conjunto de criterios. Un proyecto de inversión es económicamente factible cuando sus ingresos son capaces de cubrir los gastos y generar un excedente adecuado para las condiciones de riesgo del proyecto.

La viabilidad financiera de le la inversión se determina a través de la estimación de varios modelos financieros como el valor presente neto (VPN) y la tasa interna de retorno (TIR). También existen otros modelos no financieros (aquellos que no conceden al dinero valor en el tiempo) tales como: período de recuperación, retorno sobre la inversión (ROI) y retorno sobre la inversión en seguridad informática (ROISI).

MODELOS FINANCIEROS

2.9.1 VALOR PRESENTE NETO (VPN)

Es una herramienta financiera para comparar costos y beneficios anticipados en un período de tiempo, por tanto es una herramienta adecuada para inversiones a largo plazo. El principal enfoque de la herramienta es descontar todos los costos y beneficios de la inversión a su valor presente, de esta forma se considera también el valor del dinero a través del tiempo. El VPN se calcula restando todos los flujos de efectivo asociados al valor total de los beneficios y costos para cada año futuro en n períodos del costo inicial de la inversión. Es común asumir que los costos y beneficios futuros, con excepción de los costos para la inversión inicial, se dan al final del período (anual) correspondiente, como se muestra en la formula a continuación:

$$\text{VPN} = -\text{C}_0 + \sum_{t=1}^{n} \frac{B_t - C_t}{(1+k)^t}$$

Suponga que B_t son los beneficios del período t, C_t son todos los costos del período t, C_0 el costo de la inversión inicial y k es la tasa de descuento, la cual se asume por lo regular es el costo de capital promedio de la empresa (p. ej.: la tasa mínima aceptable para que un proyecto necesita cobrar para que el valor de la empresa no sea reducido) *n* es el número de años. La estimación racional de la tasa de descuento y los flujos de efectivo son críticos debido a que el método de VPN es muy sensible a esos parámetros.

Reglas de decisión del VPN para proyectos de inversión en seguridad independientes:

- **VPN > 0** Se elige el proyecto.
- **VPN > 0** No se acepta el proyecto.
- **VPN = 0** Financieramente no se elige, pero estratégicamente puede ser escogido.

Para mostrar un ejemplo tomaremos la siguiente tabla de flujos de efectivo:

Período	Flujos de efectivo	Flujos de efectivo Acumulados
0	$ (1,115,000.00)	$ (1,115,000.00)
1	$ 146,745.00	$ (968,255.00)
2	$ 384,393.00	$ (583,862.00)
3	$ 396,613.00	$ (187,249.00)
4	$ 397,113.00	$ 209,864.00
5	$ 309,148.00	$ 519,012.00
6	$ 221,861.00	$ 740,873.00
7	$ 208,698.00	$ 949,571.00
8	$ 428,180.00	$ 1,377,751.00

TABLA 5 – TABLA DE FLUJOS DE EFECTIVO PARA CALCULO DE PERIODO DE VPN

$$\text{VPN} = -1{,}115{,}000 + \sum_{t=1}^{8} \frac{Flujo\ de\ Efectivo_t}{(1+20\%)^t} = 51{,}622.68$$

CALCULO DE COSTO DE CAPITAL (k)

El valor de K que se utiliza para el cálculo del VPN representa el rendimiento mínimo necesario para cubrir los costos financieros de todas las fuentes de financiamiento, independientemente de su origen (Fernández Espinoza, 2007).

Ejemplo:

Si una empresa requiere hacer un proyecto de inversión y tiene las siguientes fuentes de capital, determine el costo de capital:

Fuente	I%	Peso	% de (K)
Aporte de capital socios	50%	30%	15%
Banco estatal	32%	50%	16%
Banco privado	45%	20%	9%
		Total del costo de capital	**40%**

TABLA 6 – CALCULO DE COSTO DE CAPITAL (Fernández Espinoza, 2007)

Una vez evaluado el proyecto de inversión en seguridad informática a través del modelo del VPN a una tasa de descuento (k) del 40%, si el resultado del VPN es mayor a cero, nos indica que es capaz de cubrir el costo de la deuda y generar una un beneficio para la empresa.

Así también cabe mencionar que no es inusual que empresas ajusten una prima adicional a proyectos de inversión en seguridad informática con mayor riesgo. Es decir, si se ha determinado como 15% el costo de capital de una empresa, no hay razón por la cual dicha empresa decida usar un 20% para ciertas inversiones en seguridad donde los ahorros en costos sean altamente inciertos.

2.9.2 TASA INTERNA DE RETORNO (TIR)

Como el VPN, la TIR es frecuentemente utilizada para evaluar y comparar inversiones a largo plazo. La TIR es la tasa de retorno que hace el valor presente valer cero. En otras palabras la TIR es la tasa a la cual el total del valor presente de los flujos de efectivo anticipados habrán de recuperar la inversión más el interés correspondiente a la TIR, en el periodo de evaluación considerado:

$$C_0 = \sum_{t=1}^{n} \frac{B_t - C_t}{(1 + TIR)^t}$$

Suponga que B_t son los beneficios del período t, C_t son todos los costos del período t, C_0 el costo de la inversión inicial, n es el periodo económico de evaluación y se establece en función a la vida útil del activo más importante de la empresa en términos económicos y la TIR es la tasa de retorno.

Una regla general para los responsables de tomar decisiones de oportunidades de inversión es aceptar las oportunidades de inversión en seguridad informática cuando su TIR sea mayor que su *k* (donde su k es fijada como el costo de capital o la tasa mínima aceptable de rendimiento o *TREMA*, de la empresa). La TIR es utilizada especialmente en proyectos de inversión a largo plazo en los cuales los costos cambian radicalmente año con año.

Para proyectos de inversión independientes se tiene la siguiente regla de decisión:

- Si la TIR > k y VAN > 0, se elije el proyecto.
- Si la TIR < k y VAN < 0, no se elije el proyecto.
- Si la TIR = k y VAN = 0, no se elije el proyecto.

Para mostrar un ejemplo tomaremos la siguiente tabla de flujos de efectivo:

Período	Flujos de efectivo	Flujos de efectivo Acumulados
0	$ (1,115,000.00)	$ (1,115,000.00)
1	$ 146,745.00	$ (968,255.00)
2	$ 384,393.00	$ (583,862.00)
3	$ 396,613.00	$ (187,249.00)
4	$ 397,113.00	$ 209,864.00
5	$ 309,148.00	$ 519,012.00
6	$ 221,861.00	$ 740,873.00
7	$ 208,698.00	$ 949,571.00
8	$ 428,180.00	$ 1,377,751.00

TABLA 7 – TABLA DE FLUJOS DE EFECTIVO PARA CALCULO DE PERIODO DE LA TIR

$$1{,}115{,}000 = \sum_{t=1}^{8} \frac{Flujos\ de\ efectivo}{(1+TIR)^t} \mid \text{TIR} \approx 21.46\%$$

ANALOGÍAS Y DIFERENCIAS ENTRE EL VPN Y TIR

Los dos métodos de evaluación de proyectos, VPN y TIR, proporcionan, alternativamente, en algunas situaciones recomendaciones concordantes y, en otras, recomendaciones contradictorias (Fernández Espinoza, 2007).

El primer caso de ambigüedad es magnitudes diferentes de flujos y de la inversión inicial:

	Proyecto A	Proyecto B
Io	100 000	1 000 000
Flujo 1	60 000	500 000
Flujo 2	50 000	450 000
Flujo 3	80 000	600 000
K	20%	20%
VAN	31 082	76 389
TIR	38,13%	24,70%

TABLA 8 – PRIMER CASO DE AMBIGÜEDAD DE VPN (O *VAN*) Y TIR (Fernández Espinoza, 2007)

Depende de si los 900,000 restantes del proyecto A (que no fueron invertidos en A pero si son invertidos en el proyecto B, que tiene una inversión inicial de 1,000,000), pueden invertirse en otro proyecto que genere una ganancia superior a al proyecto B; entonces, se escoge el proyecto A. Si no es así, se elige el proyecto B.

El segundo caso de ambigüedad se produce por la distribución de los flujos en el tiempo:

	Proyecto A	Proyecto B	K%	VAN A	VAN B
Io	4 500	4 500	5%	2 755	1 878
Flujo 1	500	3 000	10%	1 751	1 349
Flujo 2	1 250	2 000	15%	932	893
Flujo 3	2 250	1 500	20%	256	498
Flujo 4	4 500	500	25%	-305	153
			30%	-775	-151
TIR	**22,18%**	**27,40%**			

TABLA 9 – SEGUNDO CASO DE AMBIGÜEDAD DE VPN (O VAN) Y TIR (Fernández Espinoza, 2007)

Al analizar el VPN del proyecto A y el VPN del proyecto B con respecto al incremento de K se nota lo siguiente:

- El VPN de A disminuye en una mayor proporción que el VPN de B ante el aumento de la tasa de descuento k.
- El VPN del proyecto A que ante un valor K del 5% inició con un valor más alto, alcanza más rápidamente un valor por debajo de cero que el VPN del proyecto B.
- La TIR es congruente con el resultado del VPN a partir de un valor k común para ambos proyectos. Por debajo de esa tasa, ambos resultados son incoherentes.

Si construimos un grafico en donde se muestre el valor VAN (o VAN) vs. El valor de k de ambos proyectos, obtenemos el siguiente grafico, el cual muestra el comportamiento descrito anteriormente; pero además, se puede observar que hay un punto en que los VPNs de ambos proyectos alcanzan el mismo valor a un mismo valor de k. A ese punto se le denomina tasa de Fisher (Fernández Espinoza, 2007).

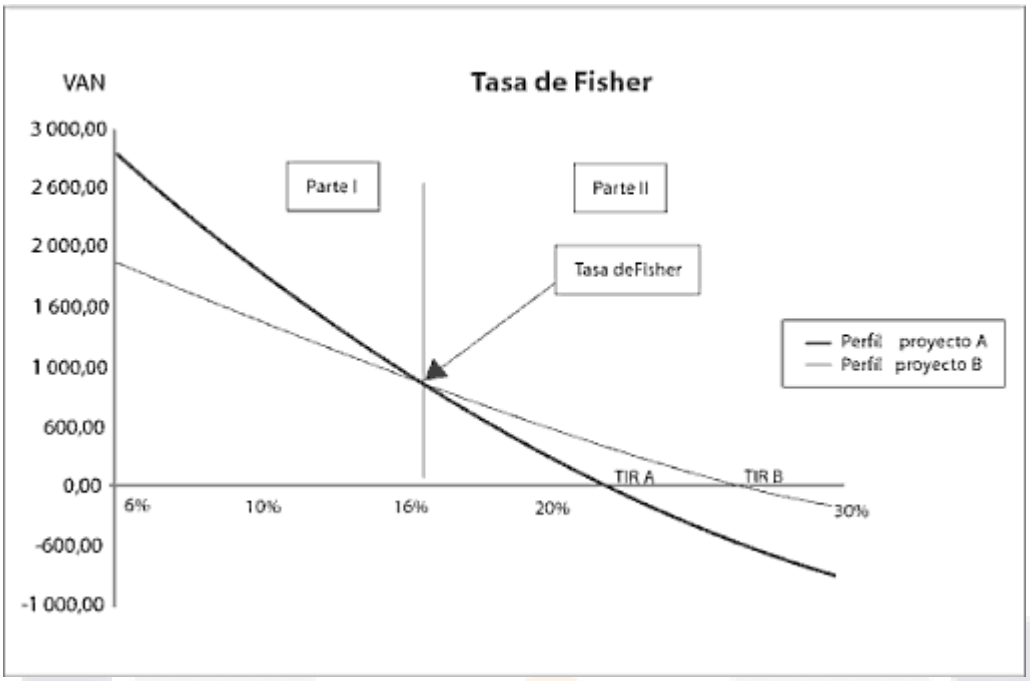

FIGURA 12 – TASA DE FISHER (Fernández Espinoza, 2007)

La tasa de Fisher es aquella tasa de descuento que hace que el VPN de dos proyectos sea igual. VPN A = VPN B.

La regla de decisión de la tasa de Fisher es el siguiente (Fernández Espinoza, 2007):

- Si RF > k, hay ambigüedad; entonces se elige por criterio de VPN.
- Si RF < k, no hay ambigüedad; y por lo tanto, se elige por criterio VPN o TIR.
- Si RF = k, no hay ambigüedad; entonces se elige por criterio TIR.

2.9.3 PERÍODO DE RECUPERACIÓN (PR)

Se define como el tiempo en años que tarda en recuperarse el monto de la inversión en seguridad informática (Fernández Espinoza, 2007).

Para el cálculo de este si los flujos de efectivo son iguales en cada período, entonces:

$$\mathrm{PR} = \frac{\mathrm{Io}}{\mathrm{Fn}}$$

Donde: Io = Inversión inicial y Fn = Flujo neto de efectivo actual

Si los flujos netos de efectivo no son iguales, el PR se calcula acumulando los flujos de efectivo sucesivos (positivos o negativos), hasta que su suma sea igual a la inversión.

$$\mathrm{PR} = \mathrm{N.^{\circ}\ de\ años\ antes\ de\ cubrir\ Io} + \frac{\text{Monto no cubierto de Io}}{\text{Flujo del año en que se cubre Io}}$$

Según este método las mejores inversiones son aquellas que tienen un plazo de recuperación más corto. La importancia de este método es que basa la escogencia de los proyectos considerando el criterio de liquidez, más que de rendimiento (Fernández Espinoza, 2007).

Para mostrar un ejemplo tomaremos la siguiente tabla de flujos de efectivo:

Período	Flujos de efectivo	Flujos de efectivo Acumulados
0	$ (1,115,000.00)	$ (1,115,000.00)
1	$ 146,745.00	$ (968,255.00)
2	$ 384,393.00	$ (583,862.00)
3	$ 396,613.00	$ (187,249.00)
4	$ 397,113.00	$ 209,864.00
5	$ 309,148.00	$ 519,012.00
6	$ 221,861.00	$ 740,873.00
7	$ 208,698.00	$ 949,571.00
8	$ 428,180.00	$ 1,377,751.00

TABLA 10 – TABLA DE FLUJOS DE EFECTIVO PARA CALCULO DE PERIODO DE RECUPERACIÓN

$$\mathrm{PR} = 3 + \frac{187{,}249}{397{,}113} \approx 3.4715$$

2.9.4 RETORNO SOBRE LA INVERSIÓN (ROI)

La noción de retorno de inversión es un concepto que administradores en seguridad informática utilizan frecuentemente y confunden con la TIR. El retorno sobre la inversión es esencialmente un concepto de contabilidad que se deriva de dividir las utilidades del último período (derivadas de los ingresos y costos) por el costo de la inversión requeridas para generar las utilidades. Por tanto, el ROI es normalmente visto como una medida de desempeño histórica utilizada para evaluar inversiones en el pasado. En contraste el VPN y la TIR son medidas de desempeño utilizadas para hacer decisiones de nuevas inversiones. A pesar de esto, algunos responsables de tomar decisiones sobre inversiones en seguridad informática estimaran el ROI anticipadamente sobre nuevas inversiones y utilizaran la medida del ROI como si fuera equivalente a la TIR. Sin embargo, al contrario de la TIR, el ROI técnicamente no considera el valor del dinero en el tiempo, el ROI podría ser equivalente a la TIR solo bajo condiciones muy extrañas de encontrar en la práctica, una condición crítica es que la inversión deba producir un retorno constante cada año a perpetuidad. Siendo que esta condición es raramente encontrada en la práctica, es erróneo asumir que el ROI esperado en inversiones de seguridad informática es una buena representación para la TIR esperada de dichas inversiones (Gordon & Loeb, 2006).

La fórmula para el cálculo del ROI es:

$$\text{ROI} = \frac{Beneficio - Costo}{Costo}$$

Un ejemplo simple, si un servidor web cuesta $10,000 y se estima genere $50,000 de ingresos durante en el año, entonces el ROI esperado es 400%:

$$\text{ROI} = \frac{50{,}000-10{,}000}{10{,}000} = 400\%$$

Como se ilustra anteriormente, el ROI no es el mismo concepto que la TIR. Sin embargo, basado en una encuesta de literatura profesional en el campo de seguridad informática y entrevistas con administradores de seguridad informática, claramente muchos administradores utilizan el acrónimo de ROI para representar la TIR. En otras palabras, están llamando a la TIR: ROI o ROSI (retorno sobre la inversión en seguridad informática) (Gordon & Loeb, 2006). Por tanto no es recomendable confundir estas

técnicas porque solo conducirá a problemas a la hora de querer justificar la inversión en seguridad informática.

En la figura 13 muestra que las organizaciones en Estados Unidos utilizan para el cálculo de costo beneficio utilizando modelos financieros y no financieros mostrados anteriormente. Los modelos más utilizados para el cálculo de retorno de la inversión en seguridad informática según la encuesta de CSI (Computer Crime and Security Survey) son los siguientes:

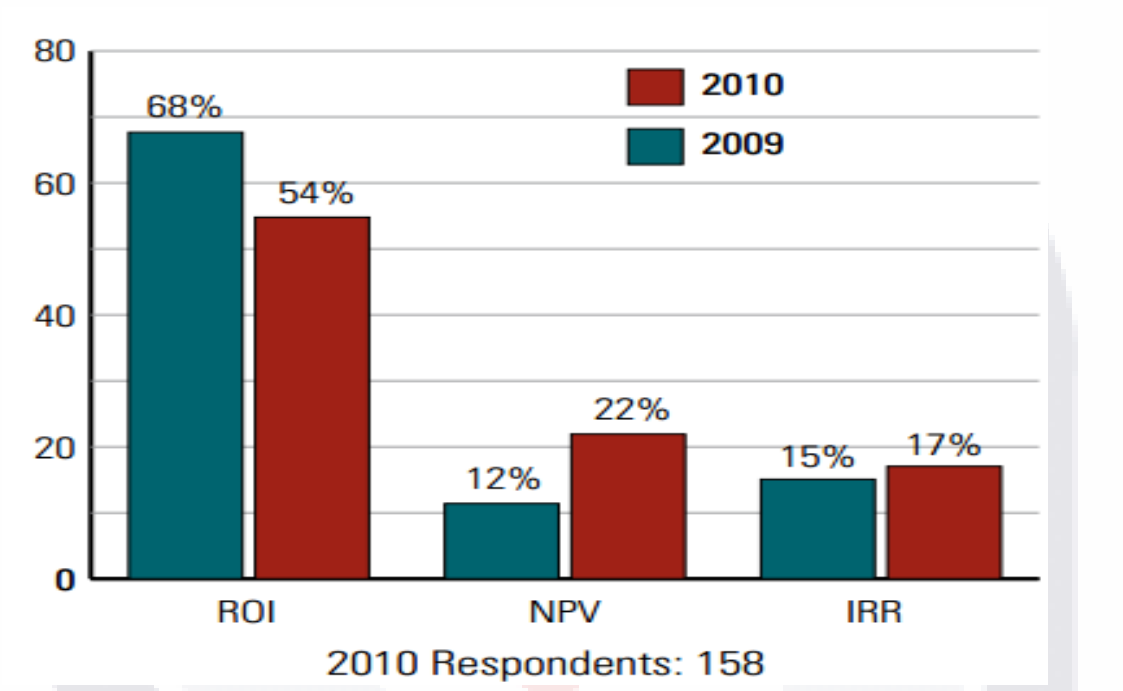

FIGURA 13 – 2010/2011 CSI COMPUTER CRIME AND SECURITY SURVEY (Richardson, 2011)

2.9.5 RETORNO SOBRE LA INVERSIÓN EN SEGURIDAD INFORMÁTICA (ROISI)

Es una medida derivada del ROI que introduce el concepto de ALE (expectativa de pérdida anual) para obtener el beneficio de una inversión de la siguiente manera:

Beneficios = $ALE_{SinProtección} - ALE_{ConProtección}$

El costo de la inversión en seguridad incluye costos de implantación y costos de operación. Los costos de implantación son normalmente costos que se desembolsan solo una ocasión, mientras que los costos operativos (mantenimiento, entrenamiento y empleados de seguridad) son costos anuales.

La fórmula para calcular el ROISI es la siguiente:

$$\text{ROISI} = \frac{ALE_{SinProtección} - ALE_{ConProtección} - COSTO_{Protección}}{COSTO_{Protección}}$$

Para aterrizar este modelo con el ejemplo anterior, la expectativa de pérdida anual (ALE) por una infección de virus informático en un servidor web es de $8,750. Si una compañía instala un software de antivirus, la expectativa de pérdida anual se reduciría a $3,400. La configuración de la herramienta de antivirus cuesta $1,600, mientras que los costos operativos anuales de la protección son $450, entonces el ROISI en el primer año es 160% como se muestra a continuación:

$$\text{ROISI} = \frac{8750 - 3400 - (1600 + 450)}{(1600 + 450)} \approx 160.97\%$$

2.10 COSTOS DE INVERSIONES EN SEGURIDAD INFORMÁTICA

Se dividen en dos costos: los costos de implantación y costos recurrentes. El costo de implantación es aquel que la compañía necesita erogar para diseñar, establecer y empezar a utilizar un sistema de seguridad de información. Este costo es cubierto por lo regular en una sola ocasión, mientras que los costos recurrentes son gastos anuales que se erogan para mantener el sistema en funcionamiento.

Algunos costos de implantación son los siguientes:

- Aplicaciones (software)
- Licencias de aplicaciones
- Hardware
- Servicios de consultoría para implantación de un sistema de seguridad de información
- Entrenamiento

Algunos ejemplos de costos recurrentes son los siguientes:

- Cuota de soporte y mantenimiento
- Sueldos de encargados del monitoreo de sistemas de seguridad de información.

CAPÍTULO III

Metodología

“Es difícil hacer predicciones, especialmente sobre el futuro” (Yogi Berra).

3 CASO PRÁCTICO DE ANÁLISIS DE VIABILIDAD FINANCIERA DE UN PROYECTO DE INVERSIÓN EN SEGURIDAD INFORMÁTICA PARA UNA PYME

En este capítulo, se llevara a cabo un caso práctico para el análisis de viabilidad financiera de la empresa X (por razones de confidencialidad no se revelara el nombre de la empresa), para esto se seguirán lo siguientes pasos para llevar a cabo este análisis (basado en el marco teórico del capítulo anterior):

I. Situación de la empresa X.
II. Análisis de riesgos, que implica:
    a. Identificación de activos.
    b. Identificación de vulnerabilidades y amenazas.
III. Cuantificación de riesgos, que se obtiene a partir de:
    a. Análisis de impactos.
    b. Valoración de probabilidades.
IV. Costo de controles de seguridad a implementar, se definirán en base a:
    a. Costos de implantación.
    b. Costos recurrentes.
V. Cuantificación de riesgo después de aplicar controles de seguridad a través del:
    a. Análisis de impactos.
    b. Valoración de probabilidades.
VI. Análisis de viabilidad financiera que consta de:
    a. Utilizar modelos financieros y modelos no financieros.
VII. Análisis y discusión de resultados.

3.1 CARACTERIZACIÓN DE LA EMPRESA X

La empresa X es una empresa PYME (de 90 empleados) con base en la ciudad de Aguascalientes, México que opera en el sector de servicios dentro del ramo de servicios profesionales en tecnologías de la información, con antigüedad de tres años en el estado de Aguascalientes.

En los últimos 2 años la empresa ha tenido un crecimiento de 200% en el número de trabajadores, consecuente con esto se ha dado la necesidad de implantación de controles de seguridad de tal forma que sea posible mantener la confidencialidad, integridad y disponibilidad de la información.

3.2 ANÁLISIS DE RIESGOS

3.2.1 IDENTIFICACIÓN DE ACTIVOS

Este paso considera la identificación de activos críticos para el negocio, de tal manera que sea posible tomar decisiones apropiadas respecto el nivel de seguridad que debe ser provisto para proteger los activos.

La clasificación de activos que se seguirá es la siguiente:

- Datos / información, cualquier información manejada en la empresa cae dentro de esta categoría. Puede ser colectada, clasificada, organizada y almacenada de muchas maneras. Como ejemplos se pueden describir los siguientes:
    - Bases de datos: información de los clientes, personal, ventas, producción, marketing, finanzas. Esta información es crítica para el negocio.
    - Archivos de datos.
    - Procedimientos operacionales.
    - Información archivada.
    - Estrategias de negocio.
- Activos físicos – Hardware, son activos visibles y tangibles dentro de la empresa, pueden comprender los siguientes:
    - Equipos computacionales.
    - Equipos de comunicación.
    - Medios de almacenamiento.
- Aplicaciones – Software, se pueden dividir en dos sub clasificaciones:
    - Software de Aplicaciones (desarrollados a la medida del negocio para una tarea específica).
    - Software de sistemas: puede ser cualquier software empaquetado como sistemas operativos, herramientas de desarrollo y paquetería de

software como las suites de productividad para la oficina (hojas de cálculo, procesadores de textos, etc.).

- Redes de comunicaciones – internas y externas, como ejemplo:
  - Comunicación por voz.
  - Comunicación de datos.
  - Redes locales**.**

Selección y valuación de activos:

La valuación de activos cuantitativa realizada, tomando en cuenta los siguientes criterios: impacto en los ingresos, impacto en la percepción del cliente y costo de reposición del activo arroja la siguiente tabla:

ID	Clasificación	Activo	Criterio 1: Impacto en los ingresos	Criterio 2: Impacto en la percepción del cliente	Criterio 3: Costo de reposición del activo	Peso Puntaje
		Peso del criterio	30	40	30	
A1	Datos/Información	Estrategias y planes de negocio*	0.9	0.3	0.9	27
A2	Datos/Información	Información del cliente*	0.8	0.9	0.9	24
A3	Datos/Información	Documentación de procesos*	0.6	0.3	0.9	18
A4	Activos físicos	Discos duros de las laptops*	0.3	0.9	0.2	9
A5	Activos físicos	Teléfonos inteligentes	0.3	0.8	0.01	9
A6	Activos físicos	Tabletas	0.3	0.9	0.2	9
A7	Activos físicos	Servidor de archivos del área de pruebas	0.1	0.1	0.2	3

TABLA 11 – ACTIVOS A CONSIDERAR PARA EL ANÁLISIS DE RIESGOS (*)

En base la valuación de activos anterior los activos a considerar para este caso serán los siguientes (según sus puntajes):

1. Estrategias y planes de negocio
2. Información del cliente
3. Documentación de procesos
4. Discos duros de las laptops

3.2.2 IDENTIFICACIÓN DE VULNERABILIDADES Y AMENAZAS

Para la identificación de vulnerabilidades es necesario hacer un análisis de debilidades que el activo posee, de tal forma que esto pueda conducir a la identificación de amenazas de los activos. Las posibles amenazas detectadas que ponen en riesgo a la empresa X son:

Activo	Vulnerabilidad	Amenaza
Estrategias y planes de negocio	Documentos en medios de almacenamiento sin encriptación	Robo de datos
Estrategias y planes de negocio	Los documentos no se encuentran respaldados	Borrado accidental de datos
Estrategias y planes de negocio	Los documentos no se encuentran respaldados	Falla en equipos
Estrategias y planes de negocio	Los documentos no se encuentran respaldados	Ataque por malware
Información del cliente	Dicha información no se encuentra encriptada en los medios de almacenamiento (como discos duros de laptops)	Robo de datos
Documentación de procesos	Dicha información no se encuentra encriptada en los medios de almacenamiento (como discos duros de laptops)	Robo de datos
Documentación de procesos	La informacion no se encuentra respaldada	Borrado accidental de datos
Documentación de procesos	La informacion no se encuentra respaldada	Falla en equipos
Documentación de procesos	La informacion no se encuentra respaldada	Ataque por malware
Discos duros de laptops	No se encuentran encriptados	Robo de datos
Discos duros de laptops	Las laptops no cuentan con una protección física contra robo (p. ej.: un candado)	Robo de equipo

TABLA 12 – VULNERABILIDADES Y AMENAZAS IDENTIFICADAS DURANTE EL ANÁLISIS

3.3 CUANTIFICACIÓN DE RIESGOS

Es necesario para la cuantificación de riesgos tener en cuenta la siguiente tabla para la frecuencia de brechas de seguridad informática:

Frecuencia Cualitativa	Descripción	Frecuencia Cuantitativa
Improbable	Difícil que ocurra una brecha de seguridad	0.005
Muy baja	Probable que ocurra una brecha de seguridad 2-3 veces en 5 años	0.5
Baja	Probable que ocurra una brecha de seguridad cada año	1
Mediana	Probable que ocurra una brecha de seguridad cada seis meses	2
Alta	Probable que ocurra una brecha de seguridad una vez al mes	12
Muy alta	Probable que ocurra una brecha de seguridad varias veces al mes	50
Extrema	Probable que ocurra una brecha de seguridad varias veces al día	500

TABLA 13 – FRECUENCIAS CUALITATIVAS Y FRECUENCIAS CUANTITATIVAS

Para la evaluación de un riesgo se requiere una tabla de intervalos que muestre el nivel de riesgo por cada uno de las posibles brechas de seguridad que se puedan dar en la empresa, la siguiente tabla muestra una propuesta de escala de riesgos:

Escala de Riesgo ($)			Nivel de Riesgo
0	-	5,000	Improbable
5,001	-	100,000	Bajo
100,001	-	200,000	Mediano
200,001	-	1,000,000	Alto
1,000,001	-	10,000,000	Critico

TABLA 14 – NIVELES DE RIESGO SEGÚN LA EXPECTATIVA DE PÉRDIDA ANUAL (ALE)

A continuación, en las tablas siguientes se muestra la cuantificación de riesgos para cada uno de los activos, sin contar con alguna implantación de controles de seguridad:

Activo:	Estrategias y planes de negocio	ID Activo:	A1	Sin controles de seguridad									
Aspecto de seguridad	Amenaza potencial	Probabilidad (ARO)		Impacto (SLE)								Impacto total (SLE)	Riesgo (ALE)
				Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros		
						Software	Hardware	Empleado Interno	Consultor Externo				
Confidencialidad	Robo de datos	1		-	216,000.00	-	-	3,000.00	-	-	-	219,000.00	219,000.00
Disponibilidad	Borrado accidental de datos	2		1,500.00	-	54,000.00	-	1,500.00	-	-	-	57,000.00	114,000.00
	Falla en equipos	2		1,500.00	-	54,000.00	500.00	1,500.00	-	-	-	57,500.00	115,000.00
Integridad	Ataque por malware	2		3,000.00	-	54,000.00	-	1,500.00	-	-	-	58,500.00	117,000.00
Total				6,000.00	216,000.00	162,000.00	500.00	7,500.00	-	-	-	392,000.00	565,000.00

TABLA 15 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A1 (INFORMACIÓN DE ESTRATEGIAS Y PLANES DE NEGOCIO)

Activo:	Información del cliente	ID Activo:	A2	Sin controles de seguridad									
Aspecto de seguridad	Amenaza potencial	Probabilidad (ARO)		Impacto (SLE)								Impacto total (SLE)	Riesgo (ALE)
				Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros		
						Software	Hardware	Empleado Interno	Consultor Externo				
Confidencialidad	Robo de datos	2		1,500.00	-	-	-	-	-	500,000.00	200,000.00	701,500.00	1,403,000.00
Total				1,500.00	-	-	-	-	-	500,000.00	200,000.00	701,500.00	1,403,000.00

TABLA 16 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A2 (INFORMACIÓN DEL CLIENTE)

Activo:	Documentación de procesos	ID Activo:	A3	Sin controles de seguridad									
Aspecto de seguridad	Amenaza potencial	Probabilidad (ARO)		Impacto (SLE)								Impacto total (SLE)	Riesgo (ALE)
				Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros		
						Software	Hardware	Empleado Interno	Consultor Externo				
Confidencialidad	Robo de datos	1		-	54,000.00	-	-	3,000.00	-	-	-	57,000.00	57,000.00
Disponibilidad	Borrado accidental de datos	2		-	54,000.00	-	-	6,000.00	-	-	-	60,000.00	120,000.00
	Falla en equipos	2		-	54,000.00	-	500.00	6,000.00	-	-	-	60,500.00	121,000.00
Integridad	Ataque por malware	2		-	54,000.00	-	-	6,000.00	-	-	-	60,000.00	120,000.00
Total				-	216,000.00	-	500.00	21,000.00	-	-	-	237,500.00	418,000.00

TABLA 17 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A3 (DOCUMENTACIÓN DE PROCESOS)

Activo:	Discos duros de laptops	ID Activo:	*A4*	Sin controles de seguridad									
Aspecto de seguridad	Amenaza potencial	Probabilidad (ARO)		Impacto (SLE)								Impacto total (SLE)	Riesgo (ALE)
				Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros		
						Software	Hardware	Empleado Interno	Consultor Externo				
Confidencialidad	Robo de datos	1		-	54,000.00	-	-	-	-	500,000.00	200,000.00	754,000.00	754,000.00
Disponibilidad	Robo de equipo	2		-	54,000.00	-	20,000.00	6,000.00	-	-	-	80,000.00	160,000.00
Total				-	108,000.00	-	20,000.00	6,000.00	-	500,000.00	200,000.00	834,000.00	914,000.00
Activo A1				6,000.00	216,000.00	162,000.00	500.00	7,500.00	-	-	-	392,000.00	565,000.00
Activo A2				1,500.00	-	-	-	-	-	500,000.00	200,000.00	701,500.00	1,403,000.00
Activo A3				-	216,000.00	-	500.00	21,000.00	-	-	-	237,500.00	418,000.00
Activo A4				-	108,000.00	-	20,000.00	6,000.00	-	500,000.00	200,000.00	834,000.00	914,000.00
Total				7,500.00	540,000.00	162,000.00	21,000.00	34,500.00	-	1,000,000.00	400,000.00	2,165,000.00	3,300,000.00

TABLA 18 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A4 (DISCOS DUROS DE LAPTOPS) Y TOTALES POR ACTIVO

3.4 COSTO DE CONTROLES DE SEGURIDAD A IMPLEMENTAR

Para poder evaluar los costos de seguridad a implementar para mitigar los riesgos existentes en cada uno de los activos analizados, se tienen que desglosar los costos de instalación y los costos recurrentes, la siguiente tabla muestra el detalle de cada uno de los controles propuestos.

Control		Costos de Instalación					Costos Recurrentes			
Nombre del control	ID de control	Software (Licencia)	Hardware	Consultoría	Entrenamiento	Total	Cuota por soporte y mantenimiento	Costo de monitoreo	Total	Total
Software de encriptación de discos duros	C1	-	-	-	-	-	3,900	7,800	11,700	11,700
Servidor de respaldos	C2	-	30,000	-	-	30,000	5,850	11,700	17,550	47,550
Candados para laptops	C3	-	11,900	-	-	11,900	1,190	1,950	3,140	15,040
Solución Antivirus	C4	56,000	15,000	-	-	71,000	-	7,800	7,800	78,800
Total		56,000	56,900	-	-	112,900	10,940	29,250	40,190	153,090

TABLA 19 – CONTROLES DE SEGURIDAD A IMPLEMENTAR

3.5 CUANTIFICACIÓN DE RIESGO DESPUÉS DE APLICAR CONTROLES DE SEGURIDAD

Las siguientes tablas muestran la cuantificación de los riesgos para cada activo, después de la implantación de los controles de seguridad propuestos anteriormente:

Activo: Estrategias y planes de negocio	ID Activo: A1	Con controles de seguridad										
Aspecto de seguridad	Control a Implementar	Probabilidad residual (resARO)	Impacto residual (resSLE)								Impacto total residual (SLE)	Riesgo Residual (resAle)	Beneficio (ALE - resALE)
			Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros			
					Software	Hardware	Empleado Interno	Consultor Externo					
Confidencialidad	Software de encriptación de discos duros	0.5	-	216,000.00	-	-	3,000.00	-	-	-	219,000.00	109,500.00	109,500.00
Disponibilidad	Servidor de respaldos	0.5	1,500.00	-	54,000.00	-	1,500.00	-	-	-	57,000.00	28,500.00	85,500.00
	Servidor de respaldos	0.5	1,500.00	-	54,000.00	500.00	1,500.00	-	-	-	57,500.00	28,750.00	86,250.00
Integridad	Solución Antivirus	1	3,000.00	-	54,000.00	-	1,500.00	-	-	-	58,500.00	58,500.00	58,500.00
Total			6,000.00	216,000.00	162,000.00	500.00	7,500.00	-	-	-	392,000.00	225,250.00	339,750.00

TABLA 20 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A1 (INFORMACIÓN DE ESTRATEGIAS Y PLANES DE NEGOCIO) DESPUÉS DE APLICAR CONTROLES DE SEGURIDAD

Activo: Información del cliente	ID Activo: A2	Con controles de seguridad										
Aspecto de seguridad	Control a Implementar	Probabilidad residual (resARO)	Impacto residual (resSLE)								Impacto total residual (SLE)	Riesgo Residual (resAle)	Beneficio (ALE - resALE)
			Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros			
					Software	Hardware	Empleado Interno	Consultor Externo					
Confidencialidad	Software de encriptación de discos duros	0.5	1,500.00	-	-	-	-	-	500,000.00	200,000.00	701,500.00	350,750.00	1,052,250.00
Total			1,500.00	-	-	-	-	-	500,000.00	200,000.00	701,500.00	350,750.00	1,052,250.00

TABLA 21 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A2 (INFORMACIÓN DEL CLIENTE) DESPUÉS DE APLICAR CONTROLES DE SEGURIDAD

Activo: Documentación de procesos	ID Activo: A3	Con controles de seguridad										
Aspecto de seguridad	Control a Implementar	Probabilidad residual (resARO)	Impacto residual (resSLE)								Impacto total residual (SLE)	Riesgo Residual (resAle)	Beneficio (ALE - resALE)
			Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros			
					Software	Hardware	Empleado Interno	Consultor Externo					
Confidencialidad	Software de encriptación de discos duros	0.5	-	54,000.00	-	-	3,000.00	-	-	-	57,000.00	28,500.00	28,500.00
Disponibilidad	Servidor de respaldos	0.5	-	54,000.00	-	-	6,000.00	-	-	-	60,000.00	30,000.00	90,000.00
	Servidor de respaldos	0.5	-	54,000.00	-	500.00	6,000.00	-	-	-	60,500.00	30,250.00	90,750.00
Integridad	Solución Antivirus	1	-	54,000.00	-	-	6,000.00	-	-	-	60,000.00	60,000.00	60,000.00
Total			-	216,000.00	-	500.00	21,000.00	-	-	-	237,500.00	148,750.00	269,250.00

TABLA 22 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A3 (DOCUMENTACIÓN DE PROCESOS) DESPUÉS DE APLICAR CONTROLES DE SEGURIDAD

Activo:	Discos duros de laptops	ID Activo:	A4	Con controles de seguridad										
Aspecto de seguridad	Control a Implementar	Probabilidad residual (resARO)		Impacto residual (resSLE)								Impacto total residual (SLE)	Riesgo Residual (resAle)	Beneficio (ALE - resALE)
				Baja en la productividad	Daño al activo	Costo de recuperación				Penalización	Otros			
						Software	Hardware	Empleado Interno	Consultor Externo					
Confidencialidad	Software de encriptación de discos duros	0.5		-	54,000.00	-	-	-	-	500,000.00	200,000.00	754,000.00	377,000.00	377,000.00
Disponibilidad	Candados para laptops	1		-	54,000.00	-	20,000.00	6,000.00	-	-	-	80,000.00	80,000.00	80,000.00
Total				-	108,000.00	-	20,000.00	6,000.00	-	500,000.00	200,000.00	834,000.00	457,000.00	457,000.00
	Activo A1			6,000.00	216,000.00	162,000.00	500.00	7,500.00	-	-	-	392,000.00	225,250.00	339,750.00
	Activo A2			1,500.00	-	-	-	-	-	500,000.00	200,000.00	701,500.00	350,750.00	1,052,250.00
	Activo A3			-	216,000.00	-	500.00	21,000.00	-	-	-	237,500.00	148,750.00	269,250.00
	Activo A4			-	108,000.00	-	20,000.00	6,000.00	-	500,000.00	200,000.00	834,000.00	457,000.00	457,000.00
	Total			7,500.00	540,000.00	162,000.00	21,000.00	34,500.00	-	1,000,000.00	400,000.00	2,165,000.00	1,181,750.00	2,118,250.00

TABLA 23 – CUANTIFICACIÓN DE RIESGOS PARA EL ACTIVO A4 (DISCOS DUROS DE LAPTOPS) DESPUÉS DE APLICAR CONTROLES DE SEGURIDAD

3.6 ANÁLISIS DE VIABILIDAD FINANCIERA PARA EL PROYECTO DE INVERSIÓN EN SEGURIDAD INFORMÁTICA

El análisis de viabilidad financiera, se determinara para un horizonte de tres años en base a la información recabada de los costos y beneficios que se concentran en la siguiente tabla:

	Año 0	Año 1	Año 2	Año 3	Total
Beneficios	-	2,118,250	2,118,250	2,118,250	6,354,750
Costos Totales	209,090	96,190	96,190	96,190	497,660
Costos instalación	112,900	-	-	-	112,900
Costos recurrentes	96,190	96,190	96,190	96,190	384,760
Flujos de efectivo	(209,090)	2,022,060	2,022,060	2,022,060	5,857,090
Tasa de descuento (k)	30%				

TABLA 24 – DATOS DE COSTO-BENEFICIO DEL PROYECTO DE INVERSIÓN EN SEGURIDAD INFORMÁTICA

De la tabla anterior, se toman los siguientes flujos de efectivo para el análisis de viabilidad financiera:

Periodo	Flujos de Efectivo	Flujos de Efectivo Acumulados
Año 0	(209,090)	(209,090)
Año 1	2,022,060	1,812,970
Año 2	2,022,060	3,835,030
Año 3	2,022,060	5,857,090

Modelos Financieros	
VPN =	3,463,199.21
TIR =	966%
Modelos No Financieros	
PR (años) =	0.10
ROISI =	1177%

TABLA 25 – ANÁLISIS DE VIABILIDAD FINANCIERA UTILIZANDO UNA TASA DE DESCUENTO (K=30%)

3.7 ANÁLISIS Y RESULTADOS

Los modelos de análisis de viabilidad financiera utilizados para el caso anterior indican que es preciso invertir en seguridad informática para la empresa X. Estos resultados han sido presentados al director de la empresa X y al encargado del departamento de sistemas de tal forma, que estos resultados pudieran soportar la decisión sobre invertir en los controles de seguridad descritos anteriormente. Basándonos en la investigación del marco teórico y el análisis del caso anterior es posible dar respuesta a las preguntas de investigación planteadas inicialmente en el primer capítulo de este trabajo, a continuación enumeramos las preguntas de investigación y damos respuesta a cada una:

1. ¿Qué modelos financieros apoyan el análisis de viabilidad financiera para el cálculo de retorno de la inversión en proyectos de seguridad informática?

Los modelos financieros que apoyan el análisis de viabilidad financiera son los mismos que se utilizan para cualquier proyecto de inversión, los modelos pueden ser

financieros como el valor presente neto (VPN) y la Tasa interna de retorno (TIR); así también los modelos que pueden utilizarse para complementar este análisis son modelos no financieros como el periodo de recuperación (PR) y el retorno sobre la inversión (ROI).

2. ¿Qué modelo se puede utilizar para calcular el tiempo de recuperación de la inversión en seguridad informática?

Se puede utilizar el modelo no financiero llamado periodo de recuperación (PR).

3. ¿Qué ventajas y desventajas llevan implícitos cada modelo para el cálculo de retorno de inversión en seguridad informática?

MODELO	TIPO	VENTAJAS	DESVENTAJAS
Valor presente neto (VPN)	Financiero	1. Considera todos los flujos y el valor del dinero en el tiempo	1. No pondera la importancia de la inversión inicial en su resultado
			2. Conduce a decisiones erróneas ante proyectos con vidas desiguales
			3. Supone la reinversión de los flujos a la tasa de descuento
			4. No permite comparar entre proyectos independientes pues es una medida absoluta que no indica relación entre los beneficios y la inversión inicial
Tasa interna de retorno (TIR)	Financiero	1. Toma en cuenta todos los flujos y su distribución en el tiempo	1. No maximiza la ganancia, que es el objetivo de la empresa
		2. Si pondera intrínsecamente la importancia de la inversión inicial	2. No conduce a decisiones optimas ante proyectos con vidas económicamente desiguales
		3. Si el TIR es mayor que la tasa K, se garantiza cubrir la inversión, el costo financiero y generar un excedente que incrementa la riqueza de la empresa	
Período de recuperación (PR)	No Financiero	1. Distingue la conveniencia de los proyectos de inversión en base a el criterio de liquidez	1. No toma en cuenta el valor del dinero en el tiempo
		2. Es un modelo fácil de aplicar	2. No considera los flujos obtenidos después del plazo de recuperación
Retorno sobre la inversión (ROI)	No Financiero	1. Es un modelo fácil de aplicar	1. Utiliza parámetros contables y no los flujos de efectivo del proyecto
			2. No considera el valor de los beneficios en el tiempo

TABLA 26 – VENTAJAS Y DESVENTAJAS DE MODELOS FINANCIEROS Y MODELOS NO FINANCIEROS PARA EL ANÁLISIS DE VIABILIDAD FINANCIERA

4. ¿Cómo se pueden integrar los anteriores modelos en un estudio de viabilidad financiera que soporte la inversión de seguridad informática en una PYME?

Se pueden integrar después de hacer la evaluación económica de los riesgos y el análisis costo-beneficio obteniendo así los flujos de efectivo para el proyecto de inversión en seguridad informática.

5. ¿Es posible demostrar que hay mayor beneficio en invertir en seguridad informática sobre, no invertir en seguridad informática en las PYMES en base a un estudio de viabilidad financiera?

Si, es posible demostrarlo contundentemente a través de los modelos que se utilizaron para llevar a cabo este estudio, en este caso no invertir en seguridad le costaría a la empresa X un total de: $3,300,000.00 de pérdidas potenciales anualmente por no invertir en seguridad, contra una pérdida potencial de $ 1,181,750.00 mitigando el riesgo e invirtiendo en controles de seguridad para la empresa.

CAPÍTULO IV

Conclusiones

"Al Hombre Superior, cuando descansa en la seguridad, no se le olvida que puede llegar el peligro. Cuando se encuentra en un estado de seguridad no se le olvida la posibilidad de la desgracia. Cuando todo está en orden, no se le olvida que puede venir el desorden. De ese modo, su persona no corre peligro y sus estados y todos sus clanes están a salvo". Confucio (551 A.C. – 479 A.C.)

4 CONCLUSIONES

Para concluir este trabajo, en este capítulo se enlistan las conclusiones del trabajo en el párrafo siguiente. Al final se presentan recomendaciones con el fin de dar continuidad a la investigación respecto al tema de análisis de viabilidad financiera en proyectos de inversión de seguridad informática.

4.1 CONCLUSIONES

La seguridad informática asegura la protección a la información así como al sistema informático o computacional, que a su vez da lugar al aseguramiento de la: confidencialidad, integridad, y disponibilidad. Se demostró que existe una clara necesidad de contar con un nivel de seguridad informática para proteger la información de una empresa (activos intangibles).

Sin embargo cuando una inversión en seguridad y otra oportunidad de inversión se encuentran en el horizonte de una empresa, es sumamente necesario hacer un análisis de viabilidad financiera de la inversión en seguridad como se haría para cualquier otro tipo de inversión, de tal manera que esta pueda ser aceptada por los socios, directores y dueños de empresas.

Mediante este trabajo práctico se logró cumplir el objetivo general que fue: realizar un estudio de factibilidad sobre invertir en proyectos en seguridad informática las PYMES.

El desarrollo de la metodología no hubiera sido posible sin el apoyo del marco teórico, que fue una guía para crear la metodología de acuerdo a las necesidades de la empresa X y factores que deben tomarse en cuenta.

A través del análisis de viabilidad financiera se logró determinar que es conveniente invertir en controles de seguridad sobre no invertir en estos, de tal forma que se puedan mitigar las amenazas que dejan vulnerable los activos descritos para el caso de estudio de la empresa X.

Se observó que los modelos financieros para el análisis de viabilidad financiera (VPN y TIR) mostraban consistencia en sus resultados e indicaban que el proyecto de inversión en seguridad informática era conveniente para la empresa X, siendo que el valor presente neto fue mayor a 0 y la TIR fue mucho mayor a la tasa de descuento k.

También se logro demostrar a través de los modelos no financieros que el proyecto de inversión es viable en términos financieros dado que el retorno de la inversión es de poco más de un mes y el retorno sobre la inversión en seguridad informática es muy superior al 100%.

Con este trabajo práctico fue posible argumentar al dueño de la empresa X la necesidad de asignación de presupuesto para esta inversión en seguridad, ya que en otras ocasiones anteriores se había intentado sin éxito, esto debido a la dificultad que existía en traducir todos los beneficios de un proyecto de inversión en seguridad informática en términos monetarios.

4.2 RECOMENDACIONES

La sección anterior concluye este trabajo práctico; sin embargo existe bastante información para mejorar y confirmar el conocimiento y práctica de este trabajo practico.

Como futuras líneas de investigación se recomendarían las siguientes:

1. Explorar la manera en como una empresa debería seleccionar una estrategia que pueda hacer frente a los riesgos como parte de la metodología de administración de riesgos.

2. En este trabajo práctico la aplicación de la tasa anual de eventos (ARO) fue constante durante los tres años del proyecto; sin embargo, sería interesante encontrar maneras de incorporar la variación del ARO a través de los años en un análisis de viabilidad financiera de proyectos de este tipo.

3. Debido al tiempo limitado en la parte de la evaluación, no se hizo validación de los resultados o no pudieron ser críticamente evaluados. Para investigaciones futuras se puede agregar la validación de los modelos financieros y no financieros utilizados para saber si la aplicación los modelos es válida o no.

4. Así también para seguir con este trabajo práctico se recomienda buscar otras alternativas de inversión en seguridad informática, que mitiguen los riesgos encontrados en este caso, de tal forma que se pueda hacer un análisis de riesgos

más extenso donde sea posible seleccionar más alternativas de inversión en seguridad informática y comparar unas con otras.

5. Por último, un análisis de sensibilidad puede ser incluido como parte del enfoque de evaluación de riesgos para manejar la incertidumbre, se puede investigar cómo integrar un análisis de sensibilidad a los modelos financieros y no financieros, analizando que parámetros del modelo deben ser tomados como entradas para el análisis de sensibilidad.

GLOSARIO

Ataques dirigidos: es cuando un grupo o un individuo atacan a un sistema informático o infraestructura critica, con el objetivo de ganar acceso y boicotear dicho sistema o infraestructura critica.

Bicho: (del inglés bug) es un error o falla en un programa de computador o sistema de software que desencadena un resultado indeseado.

Botnet: es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet (llamado pastor) puede controlar todos los ordenadores/servidores infectados de forma remota.

Brechas de seguridad en la información: es un incidente de seguridad en el cual información sensitiva, protegida o confidencial es: copiada, transmitida, vista, robada o utilizada por un individuo no autorizado.

Comercio electrónico: también conocido como e-commerce, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos, sin embargo con el advenimiento de la Internet y la World Wide Web a mediados de los años 90 comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

Cortafuegos: (del inglés firewall) se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico sobre un conjunto de normas y criterios. Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos, se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet (intranets). Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Denegación de servicio: en seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (del inglés: Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Desarrollo de software: (llamada en la actualidad ingeniería de software) es la aplicación de un enfoque sistemático, disciplinado y cuantificable al desarrollo, operación y mantenimiento de software, y el estudio de estos enfoques, es decir, la aplicación de la ingeniería al software. En esta aplicación se integra matemáticas, ciencias de la computación y prácticas cuyos orígenes se encuentran en la ingeniería.

Fases de desarrollo de software: A pesar de la variedad de propuestas de proceso de software, existe un conjunto de actividades o fases fundamentales que se encuentran presentes en todos ellos: especificación de software (se define la funcionalidad y restricciones operacionales que debe cumplir el software); diseño e implementación (se diseña y construye el software de acuerdo a la especificación); validación (el software debe validarse, para asegurar que cumpla con lo que quiere el cliente); evolución (el software debe evolucionar, para adaptarse a las necesidades del cliente).

Funciones hash: es una función criptográfica que toma un mensaje como entrada y produce una salida que llamamos código hash, o valor hash, o simplemente hash. La idea básica de las funciones criptográficas hash es que los valores hash obtenidos con ellas sirven como una imagen representativa y compactada de una cadena de entrada, y pueden usarse como un posible identificador único de esa cadena de entrada: ese valor hash obtenido del mensaje de entrada suele llamarse resumen del mensaje o huella digital del mensaje. Las funciones hash se emplean en criptografía junto con los sistemas de firma digital para otorgar integridad a los datos. Es necesario que un hash sea deterministas (un mensaje siempre tiene el mismo valor hash) además normalmente se suele requerir que sean uniformes (siempre de la misma longitud) y con efecto avalancha con el objetivo de que sea imposible predecir cualquier valor hash a partir del mensaje de entrada.

Hacker: es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío.

Inversión: es todo activo financiado con pasivos onerosos, cualquiera que sea la clase y plazo de estos recursos. Generalmente también es definida como la renuncia de una satisfacción inmediata con la esperanza de obtener en el futuro una satisfacción mayor.

Lector de libros electrónicos: es un dispositivo electrónico que reproduce los contenidos de libros electrónicos (e-books), con una calidad de lectura como en papel gracias a la tecnología de tinta electrónica.

Malware: (del inglés malicious software), también llamado código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. El término malware incluye: los virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.

Netbook: es una categoría de computadora portátil de bajo costo y generalmente reducidas dimensiones, lo cual aporta una mayor movilidad y autonomía.

Phishing: es el término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Programas de captura de teclado: (del inglés keylogger) es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet. Suele usarse como malware, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

Seguridad informática: es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Tableta: (del inglés: tablet o tablet computer) es un tipo de computadora portátil, de mayor tamaño que un teléfono inteligente o una PDA, integrado en una pantalla táctil con la que se interactúa primariamente con los dedos o una pluma stylus, sin necesidad de teclado físico ni ratón.

Tecnologías inalámbricas: son aquellas que permiten una comunicación en la cual el emisor y el receptor no están unidos por cables, los elementos físicos que emiten y reciben el mensaje se encuentran solamente en el lugar de emisión y recepción, respectivamente. Los dispositivos que cuentan con alguna de las tecnologías inalámbricas hoy en día son usualmente antenas, computadoras portátiles, teléfonos móviles, reproductores multimedia y otros.

Teléfono inteligente: (del inglés smartphone) es un teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de computación y conectividad que un teléfono móvil convencional. El término «inteligente» hace referencia a la capacidad de usarse como un computador de bolsillo, llegando incluso a remplazar a un computador personal en algunos casos.

BIBLIOGRAFÍA

Aguilera, P. (2010). *Seguridad Informática.* Madrid: Editex.

BS_7799. (1999). Information Security Management. Londres, Inglaterra: British Standard Institute. Retrieved Junio 1, 2012, from British Standard Institution: British Standard Institute

Cowley, S. (02 de Marzo de 2012). *FBI Director: Cybercrime will eclipse terrorism*. Recuperado el 06 de Marzo de 2012, de CNNMoney: http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm

eMarketer. (2011, Octubre 1). *Mexican e-commerce boosted by new payment methods*. Retrieved Noviembre 2012, 6, from E-CommerceFacts: http://www.e-commercefacts.com/background/2012/03/e-commerce-mexico/

Fernández Espinoza, S. (2007). *Los Proyectos de Inversión: Evaluación.* Costa Rica: Editorial Tecnológica de Costa Rica.

Gordon, L. A., & Loeb, M. P. (2006). *Managing CyberSecurity Resources A Cost Benefit Analysis.* New York: McGraw Hill.

Hernández, I. V. (28 de Marzo de 2012). *Pymes, el eje de la economía mexicana*. Recuperado el 6 de Noviembre de 2012, de CNN Expansión: http://www.cnnexpansion.com/emprendedores/2012/03/12/pymes-el-eje-de-la-economia-mexicana

LFTAIPG. (6 de 6 de 2006). Ley Federal De Transparencia Y Acceso A La Información Pública Gubernamental. Mexico, Mexico, Mexico.

Moreno, T. M. (12 de Junio de 2009). *Pymes olvidan seguridad en presupuesto*. Recuperado el 7 de Marzo de 2012, de CNNExpansion: http://www.cnnexpansion.com/emprendedores/2009/06/12/pymes-olvidan-seguridad-en-presupuesto

NIST. (2002). Risk Management Guide for Information Technology Systems.

Pullicino, J. (2011, 07 04). *90% of US Companies Hacked!* Retrieved 12 5, 2012, from Acunetix Web Application Security: http://www.acunetix.com/blog/news/90-percent-of-us-companies-hacked/

Ramos, J. S. (1 de Septiembre de 2009). *Activos intangibles, transacciones y crisis económica.* Recuperado el 6 de Noviembre de 2012, de Ernst & Young: http://www.edirectivos.com/articulos/1000023363-activos-intangibles-transacciones-y-crisis-economica

Richardson, R. (2011). *Computer Crime & Security Survey.* New York: Computer Security Institute.

Ronald, K., & Vines, R. D. (2004). *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams.* Wiley.

SAPAG C., N. (2001). *Evaluación de Proyectos de Inversión en la Empresa.* Argentina: Prentice Hall.

SBA. (24 de 10 de 2012). *Table of Small Business Size Standards Matched to North American Industry Classification System Codes.* Recuperado el 30 de 11 de 2012, de SBA: http://www.sba.gov/sites/default/files/files/Size_Standards_Table(1).pdf

Symantec. (2011, Diciembre 27). *SMB Threat Awareness Poll.* Retrieved Marzo 7, 2012, from Symantec: http://www.symantec.com/content/en/us/about/media/pdfs/symc-smb-threat-awareness-poll.pdf

Whitman, M., & Mattord, H. (2012). *Principles of Information Security.* Boston: Cengage Learning