Polo del Conocimiento

Pol. Con. (Edición núm. 36) Vol. 4, No 8
Agosto 2019, pp. 165-189
ISSN: 2550 - 682X
DOI: 10.23857/pc.v4i8.1053

Recepción: 16 / 06 / 2019
Aceptación: 20 / 07 / 2019
Publicación: 05 / 08 / 2019

Ciencias económicas y empresariales

Artículo de investigación

Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó

Risk management of the computer area of the Manta y Jaramijó white fishing export companies

Gerenciamento de risco da área de informática das empresas exportadoras de pescado branco Manta y Jaramijó

Walter Alberto Bailón-Lourido [I]
wbailon@hotmail.com

Correspondencia: wbailon@hotmail.com

I. Magíster en Auditoria de Tecnologías de la Información, Magíster en Finanzas y Comercio Internacional, Ingeniero en Sistemas, Tecnólogo en Computación Administrativa, Docente de la Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador.

Resumen

Los constantes avances tecnológicos y un aumento en la cantidad de información generada, han contribuido en un incremento de los riesgos informáticos de las empresas, provocando en determinados casos pérdida o alteración de información. Por esta razón, el objetivo del presente trabajo es proponer una metodología de gestión del riesgo informático para las empresas exportadoras de pesca blanca de las ciudades de Manta y Jaramijó. Para ello, se realizó una encuesta para determinar el nivel de conocimiento y aplicación de la gestión de riesgos en las empresas anteriormente mencionadas. Adicionalmente, se seleccionaron normas y metodologías internacionales de gestión de riesgo informáticos en base a trabajos previos y literatura revisada, que se evaluaron comparativamente por criterios de expertos, obteniendo con ello una nueva metodología de gestión de riesgos informáticos basada en las normas ISO 9001, ISO 31000, ISO 27005 e ISO 27002. La población estuvo constituida por 4 empresas exportadoras de pesca blanca de la ciudad de Manta y Jaramijó. Los resultados que existen tres las razones por las que no se adopta un plan de gestión de riesgos, tales como el desconocimiento del proceso, falta de presupuesto y complejidad de las normativas, en la que predomino el desconocimiento del proceso como principal limitante. Entre las conclusiones derivadas, se pudo afirmar que las empresas del sector exportador de pesca blanca de la ciudad de Manta y Jaramijó, no cuentan con una metodología específica de gestión de riesgos para el área informática.

Palabras clave: Gestión de riesgos informáticos; normas; metodologías; información; PILAR.

Abstract

The constant technological advances and an increase for information generated, have contributed to an increase of computer risks of the companies, in some cases resulting in loss or alteration of information. For this reason, the objective of the present study is to propose a methodology for risk management software for exporting companies of white fish of the cities of Manta and Jaramijó. To this end, a survey was conducted to determine the level of knowledge and application of risk management in the above-mentioned companies. Additionally, selected international risk management methodologies and standards information based on previous work and literature reviewed which were comparatively evaluated by criteria of experts, obtaining with this a new methodology of computer risk management based on the ISO 9001, ISO 31000, ISO 27005 and ISO

27002. The population was made up of 4 white fish in the city of Manta and Jaramijó export companies. The results that there are three reasons why a plan of management of risks, such as lack of knowledge of the process, lack of budget and complexity of regulations, in which dominance ignorance of the process as the main constraint is not adopted. Between the derived conclusions, we could say that companies in the export sector of the city of Manta and Jaramijó white fish do not have a specific methodology of risk management for the computer area.

Key words: Computer risk management; standards; methodologies; information; PILAR

Resumo

Os constantes avanços tecnológicos e o aumento da quantidade de informações geradas contribuíram para o aumento dos riscos computacionais das empresas, causando, em alguns casos, perda ou alteração de informações. Por esta razão, o objetivo do presente trabalho é propor uma metodologia de gerenciamento de risco computacional para as empresas exportadoras de pescado branco das cidades de Manta e Jaramijó. Para isso, foi realizada uma pesquisa para determinar o nível de conhecimento e aplicação do gerenciamento de riscos nas empresas supracitadas. Além disso, foram selecionados padrões e metodologias internacionais para gerenciamento de riscos computacionais com base em trabalhos anteriores e literatura revisada, os quais foram avaliados comparativamente por critérios de especialistas, obtendo uma nova metodologia para gerenciamento de riscos de TI com base nas normas ISO 9001, ISO 31000, ISO 27005 e ISO 27002. A população era composta por 4 empresas exportadoras de pesca de pelo branco na cidade de Manta e Jaramijó. Os resultados são três razões pelas quais um plano de gerenciamento de riscos não é adotado, como o desconhecimento do processo, a falta de orçamento e a complexidade das regulamentações, em que prevaleceu o desconhecimento do processo como principal fator limitante. Dentre as conclusões, foi possível afirmar que as empresas do setor exportador de pescado branco da cidade de Manta e Jaramijó, não possuem uma metodologia específica de gerenciamento de risco para a área de informática.

Palavras-chave: Gerenciamento de risco computacional; normas; metodologias; informação; PILAR

Introducción

Los dinámicos avances tecnológicos en los últimos años, contribuyen en la generación y acceso a gran cantidad de datos, incrementando el riesgo en la información desde su proceso hasta su almacenamiento (Castillo, 2016). Martínez (2016) considera la información un activo invaluable, que debe conservar sus características de confidencialidad, integridad y disponibilidad, siendo necesario aplicar un nivel óptimo de seguridad. Adicionalmente, las empresas están cada vez más conscientes del valor de la información como activo y de lo atractivo que estos activos pueden ser para las partes equivocadas (Yeo, Rolland, Ulmer, & Patterson, 2014).

Por otra parte, las empresas comienzan a relacionar la gestión de riesgo con el desarrollo desmedido de las tecnologías (Hernández, Yelandy y Cuza, 2013); y la dependencia de las mismas para sus operaciones (Yue, Cakanyildirim, Ryu, y Liu, 2007), por lo que la gestión de riesgo ha tomado valor como un medio para prevenir y/o minimizar impactos negativos que pueden generarse en las áreas informáticas de las empresas. A todo nivel, muchas empresas han tenido algún tipo de ataque tales como robo, manipulación de información confidencial, pérdidas por falta de respaldos, por desastres naturales, poca o ninguna gestión de riesgo (Tarazona, 2007). Por esta razón y debido a la importancia que actualmente tiene la información, es necesario conocer cómo se le debe proteger a través de una adecuada Gestión de Riesgo.

Toda infraestructura tecnológica debe ser correctamente analizada y auditada para poder mitigar los riesgos, en caso de recibir algún tipo de delito informático, desastre natural o este sea provocado por el hombre, la empresa no funciona sin sus recursos tecnológicos, lo que conlleva a pérdidas financieras sustanciales, afectando en ciertos casos la credibilidad de sus clientes y proveedores, y perjudicando la imagen corporativa de la empresa (Solarte y Enriquez, 2015).

De acuerdo a encuestas de la industria, realizadas por Information Security Magazine, Information Week y Ernst and Young, un uso adecuado de los recursos de seguridad es importante, pero el presupuesto de seguridad es un obstáculo, por la falta del mismo (Ernst y Young, 2003; Stein, 23 September, 2003; Briney, 2001). A pesar de la extensa investigación llevada a cabo durante más de 30 años en los factores de riesgo del proyecto de TI que resultan en una orientación normativa sobre la gestión del riesgo de proyectos de TI, la adopción de estos métodos de gestión de riesgos en la práctica es inconsistente. La gestión del riesgo en los proyectos de TI sigue siendo un desafío clave para muchas organizaciones (Taylor, Artman, y Woelfer, 2012).

Según Burgos y Campos (2008) cuando no se contemplan y aplican normas y metodologías que permitan mitigar los riesgos, estos pueden provocar que la información sufra alteraciones, sustracción, ataques cibernéticos, pérdidas por desastres naturales. En la actualidad los gerentes tienen más atención a los riesgos, debido al aumento constante de ataques a los sistemas informáticos (Cavusoglu, Raghunathan, y Yue, 2008). Dado el peligro significativo y creciente de estas amenazas, es imperativo que los líderes de todos los niveles de una organización comprendan su responsabilidad para lograr mantener segura la información adecuada y para gestionar los riesgos de seguridad relacionados con el sistema de información (Ross, 2014). Debido a su naturaleza indispensable, la gestión de riesgos también se ha vuelto vital. En todos los dominios, las actividades de gestión de riesgos deben estar bajo control (Barafort, Mesquida, y Mas, 2017). Las empresas deben tratar el riesgo de información como parte de su programa de gestión de riesgos operativos, debido a que están siendo cada vez más presionadas para administrar mejor los riesgos operativos, incluidos los riesgos de información.

Existe una necesidad urgente de metodologías complejas perfectamente refinadas y herramientas instrumentales para la toma de decisiones que faciliten en las organizaciones innovadoras, la gestión de riesgos en proyectos de TI (Chernysheva, 2013).

Internacionalmente existen diversas normas y metodologías para la gestión de riesgo informático, pero no hay un standard único para su aplicación en las empresas u organizaciones, lo que dificulta la implementación de la gestión de riesgo (Burgos y Campos, 2008), por otra parte Crespo (2016), en un estudio realizado en 50 empresas MPYME (Micro,Pequeñas Y Medianas Empresas) del Ecuador, indica que se presenta como dificultad para implementar la gestión de riesgos en las áreas informáticas, la falta de presupuesto, desconocimiento del proceso, complejidad de las normativas. Ante esta evidencia de la falta de aplicación de gestión de riesgos, se hace posible llegar al problema central, que no existe una metodología apropiada para la gestión de riesgo en las áreas informáticas en las empresas objeto de estudio, por lo que se hace necesario utilizar o adaptar una metodología acorde a los requerimientos y necesidades de las empresas del Ecuador, entre las que se encuentran las MPYME, categoría en que se encuentran las empresas donde se desarrolla el presente estudio, siendo estas las exportadoras de pesca blanca de la ciudad de Manta y Jaramijó.

Ante lo expuesto, el objetivo de esta investigación, es proponer una metodología basada en las normas ISO 9001, ISO 31000, ISO 27005 y ISO 27002, apoyada con la metodología MAGERIT y su herramienta PILAR, para la gestión de riesgo en el área informática. La metodología propuesta, se

obtuvo considerando la encuesta realizada en las empresas del sector exportador de pesca blanca de las ciudades de Manta y Jaramijó, revisión de literatura relacionada al tema, y selección de normas y metodologías de gestión de riesgo informáticos en base a juicio de expertos acorde a las necesidades de las empresas objeto de estudio. La metodología de gestión de riesgo desarrollada en el presente trabajo de investigación, servirá como guía para su implementación, además permitirá obtener un diagnóstico de la situación actual de la empresa y administrar la gestión de riesgo en las áreas informáticas, para de esta manera mantener el riesgo en niveles aceptables.

Desarrollo

Coronel (2013), explica que el riesgo es todo evento que pueda ocurrir y afectar negativamente a una organización. Por su parte el Instituto Ecuatoriano de Normalización,(2014), lo señala como la consecución de los objetivos. Así mismo, se considera riesgo a toda amenaza que probablemente se transforme en un desastre. Las amenazas o las vulnerabilidades, por si solas no son un peligro, pero al juntarse se pueden convertir en un riesgo, aumentando la probabilidad que un desastre ocurra (The United Nations Office for Disaster Risk Reduction, 2016).

Gestión de Riesgos

La gestión de riesgos, tiene como objetivo minimizar que un evento negativo o adverso ocurra, realizando la detección, evaluación, corrección, monitoreo y control de los riesgos (Coronel, 2013). La gestión de riesgos de seguridad de TI permite lograr estos objetivos. Las actividades principales consisten en identificar y clasificar los riesgos de seguridad informática de la organización (evaluación de riesgos) e identificar estrategias apropiadas para mitigar los riesgos (mitigación de riesgos). En general, la gestión de riesgos de TI puede considerarse fundamentalmente un requisito previo para tomar decisiones de inversión en seguridad (Yue, Cakanyildirim, Ryu, y Liu, 2007).

Valoración de riesgo

La valoración de riesgos está definida en la ISO 73 como el proceso general de análisis y de evaluación de riesgos. Es el primer proceso en la metodología de gestión de riesgos; las organizaciones la utilizan para determinar el alcance de la amenaza potencial y el riesgo asociado con un sistema de TI a lo largo del ciclo de vida de desarrollo del sistema. La salida de este proceso ayuda a identificar los controles apropiados para reducir o eliminar el proceso de mitigación del riesgo (NIST, 2002).

Análisis de riesgo

De acuerdo a la ISO 73 el análisis de riesgo comprende la identificación, descripción y estimación de riesgos. Del Carpio (2006), indica que el análisis de riesgo es el proceso cuantitativo o cualitativo que faculta la evaluación de riesgos; esto involucra una estimación de incertidumbre del riesgo y su impacto.

Evaluación de riesgos

Los criterios de riesgo pueden incluir costos y beneficios asociados, requisitos legales, factores socioeconómicos y medioambientales, preocupaciones de los interesados, entre otros. Por tanto, se usa la evaluación de riesgos para tomar decisiones acerca de su importancia para la empresa y sobre si se debe aceptar o tratar un conflicto específico (Instituto Ecuatoriano de Normalización, 2014).

Tratamiento de riesgos

El tratamiento de riesgos es el proceso de seleccionar y aplicar medidas para modificar el riesgo; incluye como principal elemento, el control o mitigación del riesgo, pero también se extiende más allá, por ejemplo, a la elusión de riesgos, a la transferencia de riesgos, a la financiación de riesgos, entre otros. (Instituto Ecuatoriano de Normalización, 2014)

Salvaguardas

Dícese de las instrucciones o elementos de tecnología que contribuyen a disminuir el riesgo. Existen riesgos que se pueden eliminar mediante una correcta organización, algunos necesitan instrumentos técnicos de apoyo como software o equipos; otros se reducen con seguridad física y política de personal (Gobierno de España Portal Administración Electrónica, 2016).

Riesgo repercutido

Se refiere al cálculo de un activo tomando en consideración: el impacto de la amenaza; y la probabilidad de la misma. Dicho riesgo se calcula para cada activo, por cada amenaza y en cada dimensión de valoración. Mediante este cálculo se pueden establecer las consecuencias de las incidencias técnicas sobre el objetivo del sistema de información (Gobierno de España Portal Administración Electrónica, 2016).

Riesgo acumulado

Dícese del cálculo de un activo tomando en consideración: el impacto acumulado de la amenaza; y la probabilidad de la misma. Este riesgo se calcula para cada activo, por cada amenaza y en cada dimensión de valoración. A través de este cálculo se reconocen las salvaguardas de que hay que asignar a los medios de trabajo: protección de los equipos, copias de respaldo, entre otros (Gobierno de España Portal Administración Electrónica, 2016).

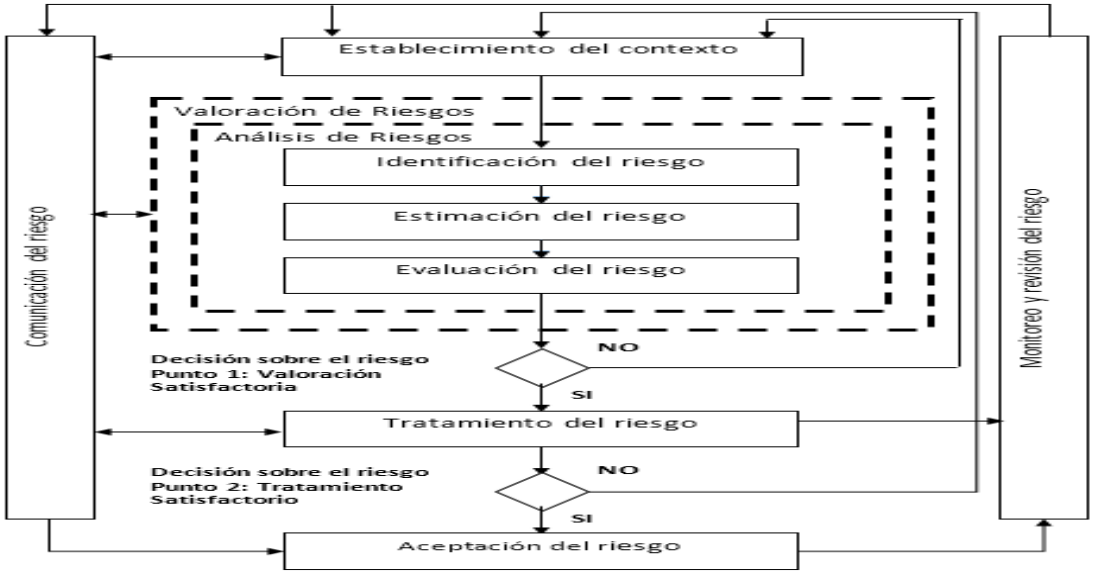
Estándares o Normas de gestión de riesgo

ISO 27001: La norma ISO 27001 fue creada para certificar la selección de las medidas adecuadas de seguridad que salvaguardan los activos referentes a información. Este estándar se puede aplicar en cualquier tipo de organización como: empresas comerciales, gobierno y organizaciones sin fines de lucro; detallando los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI (Sistema de Gestión de la Seguridad de la Información) según la compañía (Molina, 2015).

ISO 27005:2011: La norma ISO 27005, indica las directrices para la gestión de riesgos, pero específicamente no instruye las actividades que se debe realizar, por eso es necesario apoyarse con una metodología para la gestión de riesgos (Espinoza, Martínez, y Siler, 2014).

Considera las pautas a seguir para ejecutar el proceso de gestión del riesgo, se puede implementar en todo tipo de organización (Espinosa y Martínez, 2014).

Figura 1. Proceso para gestión de riesgos en la seguridad de la información ISO 27005.



Fuente: Adaptado de Norma ISO 27005. Proyecto de Norma Técnica Colombiana NTC-ISO 27005 (2009)

ISO 31000: Esta norma tiene como finalidad gestionar el riesgo con efectividad en las empresas. Determina principios que tienen que cumplirse para lograr una gestión óptima de riesgo. Además, recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte (Castro, 2011).

ISO 27002:2013: Esta norma trata sobre los dominios y mecanismos de control, que se pueden aplicar en una empresa, mediante las bases de la norma ISO 27001. Los controles que pertenecen a esta norma tratan de disminuir el impacto o la posibilidad de acontecimiento de los riesgos a los que está expuesto el negocio (Gutiérrez, 2013).

ISO 9001:2015: ISO 9001 es un estándar que establece los requisitos para un sistema de gestión de calidad. Ayuda a las empresas y organizaciones a ser más eficientes y mejorar la satisfacción del cliente (International Organization for Standardization, 2015). Tiene en cuenta aspectos como la flexibilidad dependiendo de las características de la empresa, la gestión del riesgo y oportunidades, un lenguaje más sencillo y aplicable, un enfoque más orientado al cliente, entre otros (Crespo S. , 2017).

Metodologías de gestión de riesgo

COBIT: Control Objectives for Information and related Technology (COBIT), esta metodología se basa principalmente en alcanzar los objetivos de la empresa estableciendo un modelo aprobado a nivel mundial en temas de control y seguridad de la información. Implanta las necesidades de los procesos, recursos y criterios de información para alcanzar los objetivos de la empresa, de esta manera los jefes del área de informática pueden estar al tanto de los requerimientos de control, aspectos técnicos y riesgos de negocio (Carrillo, 2012).

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), es otra metodología que apoya a la norma ISO 27005, detectando las amenazas y la información crítica del sistema (Balseca, 2014) , MAGERIT contribuye a implementar el Proceso de Gestión de riesgos, enmarcado en un trabajo para la toma de decisiones de los directivos, considerando los riesgos al utilizar las tecnologías de la información (Gobierno de España Portal Administración Electrónica, 2016).

ITIL: Information Technology Infrastructure Library (ITIL) o Librería de Infraestructura de Tecnologías de Información , es una metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la Oficina Gubernativa de Comercio Británica (Bravo, 2012).

Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado (Jaramillo D. , 2014).

Herramienta PILAR

Procedimiento Informático Lógico para el Análisis de Riesgos (PILAR), es una herramienta de análisis y gestión de riesgos basada en la metodología MAGERIT e ISO/IEC 31000 (Gobierno de España Portal Administración Electrónica, 2017). Creada por el Centro Nacional de Inteligencia de España. Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. (Molina, 2015).

PILAR posee una biblioteca estándar de propósito general que permite evaluar con puntaje a la seguridad informática (Viteri, Chiriboga, y Páliz, 2013).

Real Decreto 1720/2007

El 21 de diciembre del 2007 se realiza el Real Decreto (RD) 1720, el cuál aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (Gobierno de España Boletín Oficial del Estado, 2017)

Ciclo Deming o Ciclo PHVA (Planear, Hacer, Verificar, Actuar)

El ciclo Deming o PHVA, se utiliza como modelo base, con el fin de establecer un proceso de gestión, enfocado en la mejora continua, está compuesto por cuatro fases, que son Planear, Hacer, Verificar y Actuar (Ramírez y Ortiz, 2011).

P. Planear: Establecer el contexto, identificación y valoración del riesgo, planificación y desarrollo del Plan de tratamiento de riesgos, aceptación de riesgos.

H. Hacer: Implementar el plan de tratamiento de riesgos.

V. Verificar: Ejecutar procedimientos de seguimiento y revisión de los riesgos.

A. Actuar: Implementar y mantener las mejoras en el proceso de gestión de riesgos.

Metodología

Esta investigación tuvo un enfoque mixto cuantitativo – cuantitativo. El enfoque cuantitativo reflejado en la recolección de datos e información que aportó con insumos para determinar el diagnóstico situacional del objeto de estudio. Además, se aplicó el enfoque cualitativo, que permitió recabar información proporcionada por los expertos, quienes seleccionaron las actividades óptimas y pertinentes sobre la base de los procesos de las normas y procedimientos de gestión de riesgos tecnológicos parametrizados según estudios desarrollados por Guerrero y Gómez (2011); Crespo (2016); Ramírez y Ortiz (2011); IT Governance Institute (2008); con los resultados obtenidos se desarrolló la propuesta planteada.

La investigación fue de tipo descriptivo, puesto que se revisó la bibliografía documental sobre la teoría general, sustantiva y de referentes empíricos en relación al tema objeto de estudio, su compilación permitió estructurar información que sirvió para el análisis de la caracterización de los parámetros para diseñar la metodología de gestión de riesgos. Con el enfoque cuantitativo, se recolectó, analizó y vinculó datos, que posteriormente se relacionaron al enfoque cualitativo en un mismo estudio. Este enfoque mixto presentó varias ventajas tales como: logro de una perspectiva más precisa del

fenómeno; ayuda en la clarificación y formulación del planteamiento del problema, así como las formas más apropiadas para estudiar y teorizar los problemas de investigación (Sampieri, 2010).

La población de estudio abordo el área informática de cuatro empresas exportadoras de pesca blanca de la ciudad de Manta y Jaramijó. Para ilustrar la metodología de gestión de riesgo propuesta, se procedió con su implementación y ejecución en una de las empresas del sector antes mencionado, donde se evaluó en dos oportunidades los riesgos informáticos, para así obtener inicialmente el nivel de riesgo y aplicar los correctivos correspondientes, y luego realizar la segunda evaluación, finalmente se compararon los resultados obtenidos de ambas evaluaciones para verificar la eficacia de la metodología de gestión de riesgos desarrollada.

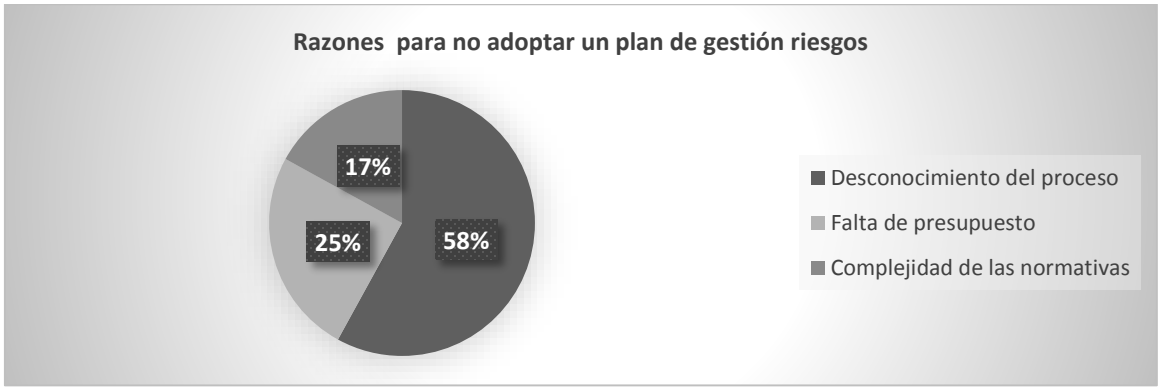
Análisis de resultados

Posterior al análisis hermenéutico de las teorías revisadas y el procesamiento de los datos del instrumento de recolección de información se pudo constatar los siguientes resultados:

Análisis de la Encuesta

En el grafico 1, se presenta la distribución descriptiva frecuencia del indicador conocimiento del entorno realizada por Crespo (2016), en 50 empresas MPYME del Ecuador, quien determinó que son tres las razones por las que no se adopta un plan de gestión de riesgos: desconocimiento del proceso, falta de presupuesto y complejidad de las normativas

Grafico 1. Distribución descriptiva frecuencial del indicador razones para no adoptar un plan de riesgos

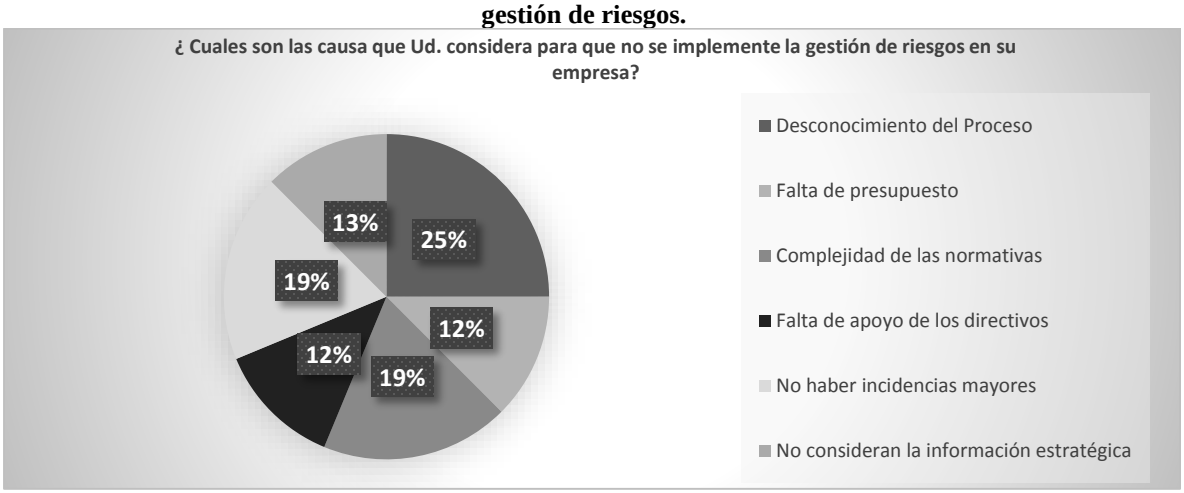


Fuente: Adaptado de Crespo (2016) Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES.

La encuesta contempló la población total, comprendida por cuatro directores del área informática, de las empresas antes mencionadas-

En el grafico 2, se presenta la distribución descriptiva frecuencial del indicador causas que se consideran para no implementar la gestión de riesgos, en la que se pudo corroborar el trabajo realizado por Crespo, ya que se determinó que entre las causas que no permiten que se implementen gestión de riegos en áreas informáticas, está el desconocimiento del proceso como principal limitante, seguido por la complejidad de las normativas y no haber incidencias mayores (mientras no suceda un riesgo de valor considerable, no se realiza ninguna gestión). En menor medida los directivos no consideran la información estratégica, la falta de presupuesto y la falta de apoyo de los directivos.

Grafico 2. Distribución descriptiva frecuencial del indicador causas que se consideran para no implementar la gestión de riesgos.



Fuente: Elaboración propia.

En relación al análisis de la primera evaluación de gestión de riesgo; el programa PILAR en base a la valoración de los activos, de los niveles de madurez registrados en el Real Decreto 1702 y en la norma 27002:2013, procede a calcular en forma automática los niveles de madurez, niveles de amenazas. Por lo que se puede indicar en forma general, que los niveles de madurez en la mayoría de los casos estaban en nivel L2, es decir Reproducible, pero intuitivo, siendo esto un nivel bajo. Los niveles del riesgo de los activos esenciales, estaban con una valoración sobre los niveles objetivo y aún más de los sugeridos por el PILAR. Por lo tanto, se deben aplicar y mejorar las medidas de control para aumentar los niveles de madurez y con ello reducir los riesgos.

Aplicación y Mejoras de medidas de control; posterior a la realización d**e** la primera evaluación, se realizó un análisis de los niveles de madurez de la protección de datos de carácter personal en base al RD 1720, así como también de los controles de seguridad de la información en base a la norma ISO 27002:2013, para verificar los controles que tenían un nivel de madurez bajo, se consideró aplicar y mejorar en algunos casos las normativas existentes y aplicar los controles necesarios, además de considerar las salvaguardas sugeridas por el PILAR (ver anexo 19), de acuerdo a las posibilidades de la empresa. Adicionalmente se consideró la aplicación de las medidas de control en los activos seleccionados de la empresa, entre los correctivos que se aplicaron se pueden mencionar: la aplicación de un mejor control de spam en el firewall, el firewall sugiere el nivel 6 pero se le bajo a nivel 5 (entre menor el número de nivel se incrementa el nivel de seguridad), para aminorar el número de spam que ingrese a los correos de la empresa. Se monitoreo y se alimentó la lista negra (black listing) y se monitoreo el uso de los recursos de los usuarios de la empresa, a través de los reportes de accesos, en el Firewall Endian.

En relación a la segunda evaluación, análisis comparativo de resultados; se utilizó la metodología de gestión de riesgos, desde su ejecución en el programa PILAR, en las valoraciones, en base al Real Decreto 1720, así como también de los controles de la norma ISO 27002:2013, se pudo constatar que los resultados obtenidos con la evaluación con el Real Decreto 1720, se apreció un incremento del nivel de madurez de algunos de los dominios en la segunda evaluación con respecto a la inicial, y en ciertos casos acercándose a los niveles sugeridos por el PILAR y objetivo. Sin embargo otros dominios no variaron su nivel. (Ver tabla 1)

Tabla 1: Evaluación RD 1720 (2007)

Evaluación Real Decreto 1720	Objetivo	PILAR	Actual	
			1	2
Funciones y Obligaciones del personal	90	50	80	80
Gestión de incidencias	80	80	50	80
Control de acceso	83	75	65	67
Gestión de soportes y documentos	80	5	20	55
Indentificación y autenticación	90	90	68	80
Copias de respaldo y recuperación	83	80	70	83
Responsale de seguridad	90	80	50	80
Auditoría	80	50	50	80
Control de acceso físico	80	0	50	80
Registro de incidencias	80	80	80	80
Gestión y distribucion de soportes	80	0	18	35
Registro de accesos	83	65	50	78
Telecomunicaciones	75	75	50	50

Nota: Información tomada del PILAR, Elaboración propia. Comparación del nivel actual, el 1 representa a la primera evaluación, y el 2 a la segunda.

La tabla 2, presenta la evaluación con la norma ISO 27002:2013 Código de prácticas de controles de seguridad de la información, donde se aprecia en la evaluación inicial, que el nivel de madurez actual se encuentra en su mayor parte, por debajo del sugerido por el PILAR. Sin embargo en la segunda evaluación, se puede observar que el nivel de madurez alcanzo en la mayor parte el nivel del PILAR de la evaluación inicial, y en algunos casos superando a los sugeridos por PILAR, pero en la gestión de la seguridad de las comunicaciones y criptografía, el nivel actual están muy por debajo del sugerido por el PILAR.

Tabla 2: Evaluación ISO 27002:2013

	Evaluación ISO 27002:2013	Obj.	PILAR	Actual 1	Actual 2
5	Políticas de seguridad de la información	90	50	78	78
6	Organización de la seguridad de la información	80	70	50	68
7	Seguridad relativa a los recurso humanos	85	0	50	64
8	Gestión de activos	82	70	37	62
9	Control de acceso	80	65	55	70
10	Criptografía	65	65	25	27
11	Seguridad física y del entorno	70	73	34	62
12	Seguridad de las operaciones	85	73	52	73
13	Seguridad de las comunicaciones	58	75	30	50
14	Adq. Des. Y mant. Sistemas de información	85	70	50	72
15	Relación con proveedores	90	60	58	62
16	Gestión de incidentes de Seguridad de información	88	68	50	57
17	Aspectos de Seg. de inf. para gestión continuidad del negocio	85	72	50	57
18	Cumplimiento	80	60	50	62

Nota: Información tomada del PILAR, Elaboración propia, En la columna actual el valor 1 corresponde a la primera evaluación y el 2 a la segunda.

En la tabla 3, se indica el análisis de la Valoración de los riesgos en los activos esenciales que se utilizan para la valoración de los riesgos.

Tabla 3: Valoración de riesgos

[9]	Catástrofe
[8]	Desastre
[7]	Extremadamente crítico
[6]	muy crítico
[5]	Crítico
[4]	Muy alto
[3]	Alto
[2]	Medio
[1]	Bajo
[0]	Despreciable

Fuente: Elaboración propia.

Nota: Información tomada del MAGERIT

En la Tabla 4, se puede apreciar que los activos esenciales tanto en la fase objetivo como actual, han tenido una disminución del riesgo en la segunda evaluación con respecto a la primera. El único activo esencial, con un nivel mínimo inferior a los otros activos, es el antivirus.

Tabla 4: Valoración de activos esenciales

ACTIVOS:Valoración de riesgo	objetivo		Actual	
	1	2	1	2
FIREWALL	5,1	4,6	5,8	5,2
CORREO (ZIMBRA)	5,1	4,6	5,8	5,2
SERVIDOR INTERNET	5,1	4,6	5,8	5,2
SYSTMARD	5,1	4,6	5,8	5,2
OFIMATICA	5,1	4,6	5,8	5,2
ANTIVIRUS	3,9	3,4	4,6	4,0
SISTEMA OPERATIVO	5,1	4,6	5,8	5,2
SERVIDOR DE DATOS	5,1	4,6	5,8	5,2
RED LAN	5,1	4,6	5,8	5,2
UPS	5,1	4,6	5,8	5,2
SERVIDOR BACKUP	5,1	4,6	5,8	5,2
ROUTER	5,1	4,6	5,8	5,2

Nota: Información tomada del PILAR, Elaboración propia, en las columnas objetivo y actual, el valor 1 corresponde a la primera evaluación y el 2 a la segunda.

Informe de Análisis de riesgo.

En el informe de análisis de riesgo, emitido por la herramienta PILAR, se obtienen los siguientes resultados:

El riesgo acumulado, que indica la dimensión, impacto y riesgo de la amenaza sobre los activos, en las distintas fases como son potencial, actual, objetivo y la recomendada por el PILAR (según la selección al momento de generar el informe). En la fase actual de este informe, se puede apreciar una leve reducción del nivel del riesgo de las amenazas, según se puede observar en la Tabla 5.

Tabla 5: ***Riesgo acumulado***

Amenaza	Dim.	Imp.	Riesgo 1	Riesgo 2
Acceso no autorizado	C	7	6,3	5,9
Manipulación de los registros de Actividad (log)	I	7	6,2	5,8
Suplantación de indetidad	A	8	6,1	5,8

Nota: Información tomada del informe de análisis de riesgo del PILAR.

En la Tabla 6, se muestran las amenazas sobre los activos esenciales, lo que representa el riesgo repercutido, se toma como ejemplo el firewall en la fase actual de la evaluación inicial, donde se puede observar una disminución en el valor del riesgo de las amenazas. Es importante acotar que la amenaza Denegación de servicio desaparece en la segunda evaluación.

Tabla 6: ***Riesgo repercutido***

Amenaza (FIREWALL)	Dim.	Imp.	Riesgo 1	Riesgo 2
Acceso no autorizado	C,A	7	6,3	5,9
Manipulación de los registros de Actividad (log)	T	7	6,2	5,8
Suplantación de indetidad	I,C,A ,T	8	6,1	5,8
Denegación de servicio	D	8	5,8	0

Nota: Información tomada del informe de análisis de riesgo del PILAR.

Informe de Cumplimiento ISO/IEC 27002:2013

En este informe, se encuentra la aplicación y los niveles de madurez de los dominios y objetivos de control de la norma ISO/IEC 27002:2013.

En la Tabla 7 se comparó el informe de ambas evaluaciones, donde se puede apreciar un incremento en los valores en algunos de los controles de los dominios, como muestra se puede apreciar los valores de un extracto de la organización de la seguridad de la información.

Tabla 7: Cumplimiento ISO/IEC 27002:2013

	[6] Organización de la seguridad de la información	Evaluación 1	2
[6]	Organización de la seguridad de la información	51	68
[6.1]	Organización interna	52	74
[6.1.1]	Roles y responsabilidades en seguridad de la información	57	72
[6.1.2]	Separación de tareas	50	78
[6.1.3]	Contacto con las autoridades	55	79

Nota: Información tomada del informe de cumplimiento ISO/IEC 27002:2013 del PILAR.

Informe de Declaración de Aplicabilidad –ISO/IEC 27002:2013

Este informe indica si aplican los controles de los dominios de la norma ISO/IEC 27002:2013. En la comparación del informe inicial con el de la segunda evaluación, se observa que en la mayoría de los controles no hay variación (si aplican), a excepción del control requisitos de seguridad en sistemas de información, que en la segunda evaluación cambia de si aplica a no aplica.

Informe de Cumplimiento RD 1720(2007).

En este informe se encuentra la aplicación y las medidas de seguridad del nivel básico, medio y alto de la madurez de los dominios y objetivos de control del Real Decreto 1720 (2007).

En la Tabla 8, se comparó tanto el primer informe como el segundo informe de las evaluaciones realizadas, donde hubo un incremento en los valores en algunos de los controles de los dominios. Como ejemplo, se toma como muestra las medidas de seguridad de nivel básico, donde se aprecia el incremento del valor de las medidas.

Tabla 8: ***Cumplimiento RD 1720(2007)***

		Evaluación	
	Medidas de seguridad de nivel básico	1	2
[8]	Medidas de seguridad de nivel básico	51	68
[89]	Funciones y obligaciones del personal	52	74
[90]	Gestión de incidencias	57	72
[91]	Control de acceso	57	72
[92]	Gestión de soportes y documentos	57	72
[93]	Identificación y autenticación	50	78
[94]	Copias de respaldo y recuperación	55	79

Nota: Información tomada del informe de cumplimiento RD 1720(2007) del PILAR.

Con los resultados obtenidos de las dos evaluaciones en la empresa seleccionada, se puede observar que en la evaluación realizada con el Real Decreto 1720 y con la norma ISO/IEC 27002:2013, se aprecia que se ha dado un aumento en los niveles de madurez en algunos de los dominios, esto se corrobora en los informes de cumplimiento de RD 1720 y la norma anteriormente mencionada. Como consecuencia de lo anterior descrito, los niveles de riesgos han disminuido. En el informe de análisis de riesgo, tanto el riesgo repercutido como acumulado, han tenido una leve reducción en el nivel de riesgo, y por lo tanto una reducción en el nivel de la amenaza.

Conclusiones

La investigación realizada hace posible afirmar que las empresas del sector exportador de pesca blanca de la ciudad de Manta y Jaramijó, no cuentan con una metodología específica de gestión de riesgos para el área informática.

La encuesta permitió determinar que la principal causa para no aplicar la gestión de riesgos en el área informática es el desconocimiento del proceso, luego de ello vienen la complejidad de las normativas y no haber incidencias mayores (mientras no suceda un riesgo de valor considerable, no se realiza ninguna gestión). Otras causas están relacionadas con los directivos, quienes no consideran la información estratégica, la falta de presupuesto y la falta de apoyo por su parte.

La revisión de las diversas normas y metodologías de gestión de riesgo consideradas en el presente estudio, permitió diseñar una metodología de gestión de riesgos informáticos basada en los estándares ISO 9001, ISO 27005, ISO 31000, ISO 27002, apoyados con la metodología MAGERIT y la herramienta PILAR micro 6.3, que servirá como guía para su implementación, además de permitir gestionar los riesgos en las áreas informáticas en las empresas exportadoras de pesca blanca.

La aplicación de la metodología de gestión de riesgo propuesta en el sector de estudio, permitió obtener: la valorización de los activos informáticos, los riesgos, amenazas; el valor del nivel de madurez de los controles en base al Real Decreto 1720(2007) e ISO/IEC 27002:2013 y las salvaguardas a aplicar. La mejora en los controles y aplicación de salvaguardas, que permitieron aumentar los niveles de madurez de las medidas de control tanto del RD 1720 y la norma ISO 27002:2013, logrando reducir los niveles de riesgos, así como también vale mencionar la eliminación de una amenaza encontrada en la primera evaluación. Lo que permite corroborar la funcionabilidad de la metodología diseñada.

La metodología de gestión de riesgo propuesta en el presente trabajo, permitirá realizar un proceso de gestión de riesgos en el área informática a las empresas que no lo han realizado por diversos factores. Entre las limitaciones, se puede indicar que, si bien hay bibliografía y trabajos de investigación sobre la sobre el tema investigado, se encuentra más bien enfocado a determinados sectores o industrias, sin embargo para la empresa o tipo sector estudiado, hay pocos que han escrito que sobre el tema. Otra limitación fue la falta de disponibilidad de tiempo de los directores de TI, así como también de los diversos expertos que colaboraron en este trabajo por sus diversas actividades que desempeñan, y por último la predisposición de las empresas en dar las facilidades para la aplicación de la metodología.

Como trabajo futuro se debe extender la aplicación de la metodología de gestión de riesgos a los otros activos de las áreas informáticas de la empresa. Ampliar la aplicación de la metodología propuesta al sector de MPYME u otras áreas productivas, para probar la efectividad en otro tipo de empresas. Adicionalmente considerar que normas y metodologías se podrían incorporar, para de esta forma mejorar la metodología de gestión de riesgo propuesta.

Referencias Bibliográficas

Balseca, A. S. (01 de 2014). *Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5.* Obtenido de Repositorio Digital ESPE: http://repositorio.espe.edu.ec/bitstream/21000/8152/1/AC-GRT-ESPE-047641.pdf

Barafort, B., Mesquida, A., y Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards and Interfaces,* 176-185.

Bravo, M. E. (2012). *ITIL: Gestión de versiones.* Cuenca: Universidad Católica de Cuenca.

Briney, A. (2001). 2001 industry survey. *Information Security Magazine*, 34–46.

Burgos, J., y Campos, P. G. (2008). Modelo para Seguridad de la Información en TIC. Concepción, Chile: Universidad de Bío-Bío.

Carrillo, J. (2012). *Guía y análisis de gestión de riesgos en la adquisición e implantación de equipamiento y servicios de tecnologías de información y comunicaciones para proyectos de alcance nacional.* Quito: Escuela Politécnica Nacional.

Castillo, C. (2016). *Propuesta metodológica para la identificación de riesgos asociados a la gestión documental.* Recuperado el 20 de Febrero de 2018, de Trabajo de Investigación del Máster en Gestión Documental, Transparencia y Acceso a la Información de la Escuela Superior de Archivística y Gestión de Documentos de la Universidad Autónoma de Barcelona: https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_272839/TrabajoClaudiaCastilloCorrecto.pdf

Castro, M. (2011). *El nuevo estándar ISO para la gestión de riesgo.* Chile: Surlatina Consultores.

Cavusoglu, H., Raghunathan, S., y Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems,* 281-304.

Chernysheva, T. Y. (2013). Preliminary risk assessment in it projects. *Applied Mechanics and Materials Vol. 379,* 220-223.

Coronel, I. K. (08 de 2013). *Metodología de evaluación del gobierno, riesgos y cumplimiento de la tecnología de información en instituciones del sistema financiero ecuatoriano.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/6249/T-PUCE-6429.pdf?sequence=1

Crespo, P. (2016). *Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES.* Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/26105/1/Tesis.pdf

Crespo, S. (2017). *Comparación Norma ISO 9001:2008-2015 y adaptación.* España: Universidad de Valladolid.

Del Carpio, J. (2006). *Análisis del riesgo en la administración de proyectos de tecnología de información.* Peru: Universidad Nacional Mayor de San Marcos.

Ernst, y Young. (2003). *Global information security survey 2003.* Ernst & Young LLP, White Paper.

Espinosa, D., y Martínez, J. (2014). *Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011.* Colombia: Universidad de San Buenaventura.

Gobierno de España Boletín Oficial del Estado. (09 de 2017). Obtenido de http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

Gobierno de España Portal Administración Electrónica. (2016). Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?comentarioContenido=0#.V3XLNvnhA2w

Gobierno de España Portal Administración Electrónica. (09 de 2017). Obtenido de https://administracionelectronica.gob.es/ctt/pilar#.WcQkH7LyjIU

Guerrero, M., y Gómez, L. (2011). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. *Estudios Gerenciales*, 195-215.

Gutiérrez, C. (2013). *ISO/IEC 27002:2013 y los cambios en los dominios de control.* Colombia: Awareness & Research.

Hernández-Díaz, N., Yelandy-Leyva, M., y Cuza-García, B. (2013). *Modelos causales para la Gestión de Riesgos.* Recuperado el 20 de Febrero de 2018, de Revista Cubana de Ciencias

Informáticas: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992013000400005&lng=es&tlng=es

Instituto Ecuatoriano de Normalización. (2014). Guía Práctica Ecuatoriana GPE INEN-ISO 73. En *Gestión de Riesgo - Vocabulario.* Quito: INEN.

International Organization for Standardization. (2015). *ISO 9001:2015 How to use it.* Suiza: ISO.org.

ISO/IEC 27005:2008. (s.f.). *Information technology - Security tecniques - Information security risk management.* Obtenido de http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

IT Governance Institute. (2008). *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio del negocio.* Obtenido de IT Governance Institute / Office of Government Commerce: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

Jaramillo, D. (2014). *Propuesta de una metodología de gestión de incidentes para empresas de microfinanzas.* Quito, Ecuador: Universidad Tecnológica de Israel.

Martínez, D. (2016). *Sistemas de información estratégicos, herramienta para la optimización de gestión en las empresas del sector de la salud.* Recuperado el 22 de Febrero de 2018, de Universidad Militar Nueva Granada: https://hdl.handle.net/10654/14473

Molina, M. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la ESPOL*. Ecuador: Universidad Politécnica de Madrid.

NIST. (Julio de 2002). *NIST*. Recuperado el 5 de Septiembre de 2017, de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

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

Ross, R. S. (2014). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. *Special Publication (NIST SP)-800-37 Rev 1*.

Sampieri, D. R. (2010). *Metodología de la investigación.* México: McGraw-Hill.

Solarte, F., y Enriquez, E. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. Ecuador: Revista Tecnológica ESPOL.

Stein, T. (23 September, 2003). Security gets top-level attention, Optimize. *Information Week*.

Tarazona, C. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*, 137-146. Obtenido de https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

The United Nations Office for Disaster Risk Reduction. (24 de Junio de 2016). *¿Que es el riesgo?* Obtenido de https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf

Viteri, M., Chiriboga, G., y Páliz, V. (2013). *Evaluación técnica de la seguridad informática del Data Center de la Brigada de Fuerzas Especiales No. 9 Patria*. Quito: Escuela Politécnica del Ejército.

Yeo, M. L., Rolland, E., Ulmer, J. R., & Patterson, R. A. (2014). Risk mitigation decisions for it security. ACM Transactions on Management Information Systems.

Yue, W. T., Cakanyildirim, M., Ryu, Y. U., y Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems*, 1-16.