MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

GESTIÓN DE RIESGOS DEL ÁREA INFORMÁTICA DE LAS EMPRESAS EXPORTADORAS DE PESCA BLANCA DE MANTA Y JARAMIJÓ, COMO APORTE A LA CONTINUIDAD DEL NEGOCIO

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Ing. Sist. Walter Alberto Bailón Lourido

Bajo la dirección de:
Ing. Marco Vinicio Sotomayor Sánchez, MSC

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Abril del 2018

Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó, como aporte a la continuidad del negocio.

Management of risks in the IT area of the white fish exporting companies of Manta and Jaramijó, as a contribution to the business continuity.

Walter Alberto BAILÓN LOURIDO[1]
Marco Vinicio Sotomayor Sánchez [2]

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 lo que es necesario protegerla a través de una gestión del riesgo adecuada por medio de una norma o metodología que permita mitigar o minimizar el impacto que éste provocaría en la organización. Por esta razón, el objetivo del presente trabajo es obtener una metodología de gestión del riesgo informático para las empresas exportadoras de pesca blanca de las ciudades de Manta y Jaramijó. Para ello, primeramente 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, apoyadas en la metodología MAGERIT y su herramienta PILAR, que permitirá conservar la confidencialidad, integridad y disponibilidad de la información. La metodología resultante fue evaluada en una de las empresas objeto de estudio, que permitió; gestionar los riesgos, valorar activos, valorar amenazas, determinar las salvaguardas. Los resultados de la evaluación permitieron comprobar la reducción de los niveles de riesgos y eliminación de amenazas.

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

Abstract

The constant technological advances and an increase in the amount of information generated, have contributed to an increase in the computer risks of the companies, causing in certain cases loss or alteration of information; therefore, it is necessary to protect it through adequate risk management through a standard or methodology that mitigates or minimizes the impact that this would have on the organization. For this reason, the objective of this paper is to obtain a computer risk management methodology for white fishing exporting companies in the cities of Manta and Jaramijó. For this, a survey was first conducted to determine the level of knowledge and application of risk management in the aforementioned companies. Additionally, international standards and methodologies for computerized risk management were selected based on previous works and a revised literature, which were evaluated comparatively by expert criteria, thus obtaining a new methodology for managing computer risks based on ISO 9001, ISO standards. 31000, ISO 27005 and ISO 27002, supported by the MAGERIT methodology and its PILAR tool, which will preserve the confidentiality, integrity and availability of information. The resulting methodology was evaluated in one of the companies under study, which allowed; manage risks, value assets, assess threats, determine safeguards.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. Docente de la Universidad Laica Eloy Alfaro de Manabí. E-mail wbailon@uees.edu.ec.
[2] Master en TI. Tutor de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador.

The results of the evaluation allowed to verify the reduction of risk levels and elimination of threats.

Key words	Computer risk management, standards, methodologies, information, PILAR.

INTRODUCCIÓN

Los dinámicos avances tecnológicos en los últimos años, contribuyen en la generación y acceso a gran cantidad de información, incrementando el riesgo en la información desde su proceso hasta su almacenamiento (Castillo, 2016). Por otro lado, al tratar sobre la gestión de riesgos, las empresas comienzan a relacionar la gestión de riesgo con el desarrollo desmedido de las tecnologías (Hernández-Díaz, Yelandy-Leyva, & Cuza-García, 2013); y la dependencia de las mismas para sus operaciones (Yue, Cakanyildirim, Ryu, & Liu, 2007), por lo que la gestión de riesgos 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 riesgos (Tarazona, 2007). Por esta razón y debido a la importancia que actualmente tiene la información, es necesario conocer cómo se la debe proteger a través de una adecuada Gestión de Riesgos.

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).

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 provocado por el hombre, la empresa no podría funcionar sin sus recursos tecnológicos, lo que conllevaría a pérdidas financieras sustanciales, afectando en ciertos casos la credibilidad de sus clientes y proveedores, y perjudicando la imagen corporativa de la empresa (Solarte & Enriquez, 2015).

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 ataque a los sistemas informáticos (Cavusoglu, Raghunathan, & Yue, 2008). Dado el peligro significativo y creciente de estas amenazas, es imperativo que los líderes de todos los niveles de una organización comprendan sus responsabilidades para lograr una seguridad de 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, & Mas, 2017) . Las empresas deben gestionar su riesgo de información como parte de su programa de gestión de riesgos operativos, debido a que están siendo cada vez más presionadas para gestionar mejor los riesgos operativos, incluidos los riesgos de información.

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).

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).

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, & Woelfer, 2012).

Internacionalmente existen diversas normas y metodologías para gestionar los riesgos informáticos, pero no hay un standard único para su aplicación en las empresas u organizaciones, lo que dificulta la implementación de la gestión de riesgos (Burgos & 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, 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 obtener una nueva 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 riesgos en las áreas informáticas. La metodología anteriormente descrita 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 riesgos informáticos en base a juicio de expertos y que están acorde a las necesidades de las empresas objeto de estudio. La metodología de gestión de riesgos desarrollada en el presente trabajo de investigación, servirá como guía para su implementación, realizar un diagnóstico de la situación actual de la empresa, gestionar los riesgos en las áreas informáticas para que estén en niveles aceptables.

MARCO TEÓRICO

En la presente sección se hará una revisión literaria de trabajos relacionados y conceptos relevantes con el tema de estudio.

TRABAJOS RELACIONADOS

Ramírez, A., Ortiz, Z. (2011), presentan una propuesta de una metodología para la gestión de riesgos, basadas en los estándares ISO 31000 e ISO 27005, pero considerando que estos solo indican los requerimientos, más no como poder realizar la gestión, adoptan e incorporan de otras guías y metodologías, recomendaciones y buenas prácticas para la gestión de riesgos, tales como MAGERIT, NIST SP 800-30, NTC 5254, ISO 27001 y el ITIL para la seguridad de servicios.

En la práctica, la gestión del riesgo empresarial y la gestión del riesgo de TI también se tratan como temas separados. Con ISO 31000: 2009 e ISO / IEC 27005: 2008 la Organización Internacional de Normalización trata el ERM y la gestión de riesgos de seguridad de la información como dos estándares distintos. La alineación de la TI con los negocios en la práctica se realiza principalmente a través de los marcos de gestión de TI, como COBIT e ITIL (Racz, Weippl, & Seufert, 2010)

Gaona (2013) expone un trabajo utilizando la metodología MAGERIT, basado en una serie de pasos estructurados para el análisis y gestión de riesgo, utilizando la herramienta PILAR 5.2 como soporte en la valoración de los riesgos en diferentes etapas, obteniendo los mecanismos de seguridad a implementar en el proyecto.

Burgos y Campos (2008) indican que existen internacionalmente diversas organizaciones que han desarrollado estándares y normas para la gestión de riesgos, por esto, proponen un modelo para asegurar la información, en donde se gestionan los riesgos, este modelo está basado en estándares y normas internacionales, en los que se consideran la ISO 17779, COBIT, ITIL, LEY SOX, COSO e ISO Serie 27000 (27001, 27002, 27003, 27004, 27005, 27006, 27007, 27011, 27031, 27032, 27033, 27034 y 27799), además de esto expresan que en Chile hay un 90% de empresas que ignoran sobre sistemas de seguridad de la información.

Según Macedo (2012), en la gestión de TI, usualmente se utilizan metodologías estándares, como Cobit o ITIL, sin embargo son desarrollados para un contexto diferente para Latinoamérica, en este caso México, por lo que propone una metodología hibrida entre Cobit e ITIL. Por otra parte, Eterovic y Pagliari (2012) realizan una propuesta de una metodología para el análisis de riesgos informáticos, en la cual toman como base las metodologías Magerit, Octave y Mehari para su desarrollo.

El IT Governance Institute (2008) expresa en su informe “Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio del negocio” que las empresas adoptan mejores prácticas de TI en pro de la mejora en calidad y la confiabilidad de tecnología y para afrontar un aumento de número de requerimientos regulatorios y contractuales”.

En el año 2012, en Lima, Perú; en la empresa Card Perú S.A. se utilizó la metodología de Magerit para minimizar los riesgos de la implantación y uso de TI en dicha Institución, brindándoles una visión clara de cómo sus labores cotidianas aportan en la mejora del sistema de gestión (Barrantes & Hugo, 2012)

El modelo MAGERIT se ha utilizado frecuentemente en Ecuador, con la asistencia de la herramienta PILAR, buscando mejorar la gestión de riesgo de la empresa, se exponen los siguientes casos:

- En el año 2012, en Cuenca, Ecuador; en la Cooperativa de Ahorro y Crédito Jardín Azuayo, se recurrió a Magerit con la finalidad de mitigar los riesgos, mediante perfiles de seguridad y salvaguardas adecuados recomendados por PILAR basic, con el objetivo de proteger el activo en todo tiempo (Lucero & Valverde, 2012).

- En el 2014, en Quito, Ecuador, se realizó un análisis de riesgos de la seguridad de la red de área local LAN de la matriz de la contraloría general del Estado, aplicando Magerit basada en PILAR, determinando los activos con mayor nivel de riesgo por la falta de implementación de salvaguardas como recomiendan los estándares para la gestión de Seguridad de la Información (Rosero, 2014).

Si bien es cierto, que se han encontrado diversos estudios en que se aplican metodologías de gestión de riesgos informáticos, luego de lo analizado, se puede observar que no hay una metodología estándar que aplique a todo tipo de organización, por esta razón debido a que no hay una metodología especifica que pueda ser aplicada para las empresas exportadoras de pesca Blanca, la presente investigación abordara ese problema, donde se hace necesario realizar un estudio para seleccionar normas y metodologías de gestión de riesgos informáticos, para poder crear una metodología que esté acorde a las empresas objeto de estudio.

A continuación se exponen algunos conceptos relacionados con la Gestión de Riesgos, que son necesarios conocer, para de esta forma tener un mejor fundamento, referente a la gestión de riesgos.

Definición de Riesgo

Riesgo es todo evento que pueda ocurrir y afectar negativamente a una organización (Coronel, 2013); es el efecto de la incertidumbre sobre la consecución de los objetivos (ISO 73, 2014). 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, & 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 la importancia de los riesgos para la empresa y sobre si se debe aceptar o tratar un riesgo específico. (ISO 73, 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. (ISO 73, 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 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, & Siler, 2014).

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

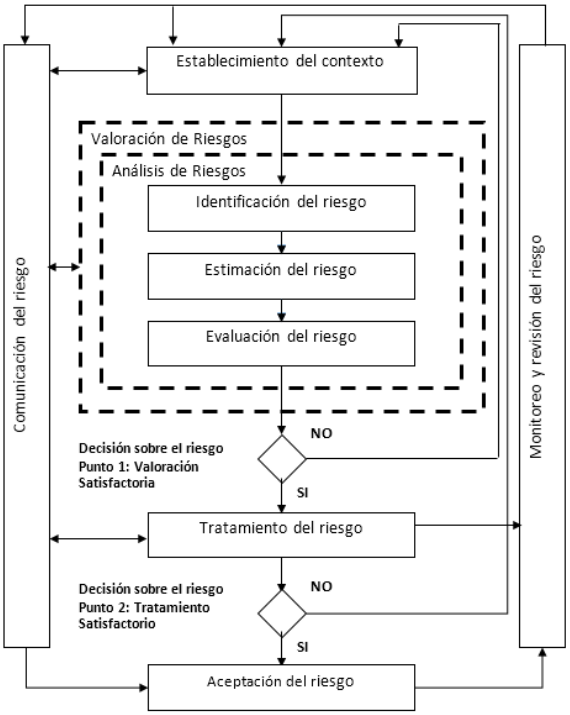


Figura 1. Proceso para gestión de riesgos en la seguridad de la información ISO 27005. Adaptado de Norma ISO 27005.

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, 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, & Páliz, 2013).

Real Decreto 1720/2007

El 21 de diciembre del 2017 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 & Ortiz, Gestión de riesgos tecnológicos basada en ISO

31000 e ISO 27005 y su aporte a la continuidad de negocios, 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.

La metodología utilizada en el presente trabajo de investigación es de tipo exploratoria, debido a que se va a desarrollar una nueva metodología de gestión de riesgos informáticos, que se aplique a las empresas exportadoras de pesca blanca. Adicionalmente, se basó en un enfoque cualitativo, ya que se recolectó, analizó y vinculó datos considerados relevantes, entre los que se pueden mencionar las normas y metodologías de gestión de riesgos que contribuirán al desarrollo del objetivo propuesto.

A continuación se describirá el proceso metodológico que consiste en las siguientes etapas:

Diagnóstico del sector.

Como primer paso, con asesoría y validación por dos expertos se elaboró una encuesta, y esta se aplicó en las empresas consideradas en este estudio. Con la información recabada, se procedió a tabularla en una hoja electrónica y obtener resultados en forma gráfica para su respectivo análisis. Esto permitió obtener el nivel de conocimiento sobre gestión de riesgos de los jefes o encargados del área informática, así como también la situación actual y las razones porque no se aplican la gestión de riesgos en las áreas de informática de las empresas exportadoras de pesca blanca de las ciudades de Manta y Jaramijó.

Revisión bibliográfica.

En base a revisión de literatura se procedió a recopilar información acerca de la gestión de riesgos y conocer trabajos relacionados al tema de investigación.

Breve descripción del desarrollo de la propuesta.

En esta etapa, se elaboró una matriz en base a un cuadro comparativo de las normas y metodologías del trabajo realizado por Guerrero y Gómez (2011), que se complementó con los trabajos de Crespo (2016), Ramírez y Ortiz (2011), IT Governance Institute (2008) y literatura revisada. Luego de esto, se procedió a analizar y seleccionar por parte de expertos, las normas o metodologías de gestión de riesgos que estén acorde a las necesidades de las empresas exportadoras de pesca blanca de las ciudades de Manta y Jaramijó, y como resultado de ello se obtuvo una nueva metodología de Gestión de Riesgos informáticos,

Ejecución y validación.

Finalmente se desarrolló una prueba de la metodología de gestión de riesgos propuesta, que se validó en una de las cuatro empresas objeto de estudio. Para su ejecución se consideró la aplicación de las actividades estándar de la nueva metodología de gestión de riesgos, que sirvió para obtener una evaluación preliminar de la empresa, a continuación se aplicaron las medidas de control necesarias para minimizar los riesgos en base a los resultados iniciales, y seguidamente se realizó una segunda evaluación para verificar la disminución de riesgos y con ello confirmar la funcionabilidad de la metodología de gestión de riesgos desarrollada en el presente trabajo.

Alcance de la investigación.

El presente estudio se realizó en áreas informáticas 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 comparó los resultados obtenidos de ambas evaluaciones para verificar la eficacia de la nueva metodología de gestión de riesgos.

Desarrollo de la propuesta.

En esta sección se describirá en detalle las fases del proceso metodológico.

Análisis de la Encuesta: conocimiento del entorno

En el estudio realizado por Crespo (2016), en 50 empresas MPYME del Ecuador, se 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 como se aprecia en la Figura 2.

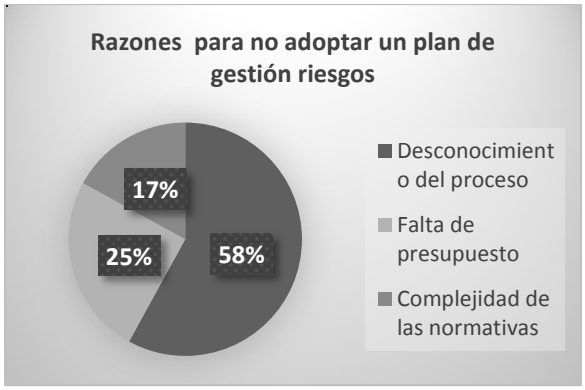


Figura 2 Razones para no adoptar un plan de riesgos. Adaptado de Crespo 2016.

Para la elaboración de la encuesta, se desarrolló un banco de preguntas, aplicando la escala de Likert, con la asesoría y validación de dos expertos, y se consideró para la elaboración de una de las preguntas el trabajo realizado por Crespo (2016).

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

De acuerdo al resultado de la encuesta realizado en las empresas de la presente investigación, 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, como se aprecia en la Figura 3.

Figura 3 Análisis de las causas que se consideran para no implementar la gestión de riesgos.

Diseño de metodología de gestión de riesgos informáticos.

Para diseñar la metodología de gestión de riesgo propuesta en el presente trabajo, se realizó una revisión bibliográfica de trabajos relacionados, luego de ello se consideró el trabajo elaborado por Guerrero y Gómez (2011) como base, ya que realizó un cuadro comparativo, donde analizó diversas normas y metodologías de gestión de riesgo y las alineó con las actividades de gestión de riesgos y controles en sistemas de información (GRCSI) , este cuadro se complementó con el análisis realizado por Crespo (2016) sobre las normas ISO 27001, 27002, 27005 y 31000; el de Ramírez y Ortiz (2011) donde desarrolla una metodología para la gestión del riesgo informático basados en la norma ISO 27005 y 31000, en la que alinea los procesos o

actividades de las normas ISO 27005 y 31000 con el ciclo PHVA y el de IT Governance Institute (2008) donde alinean COBIT, ITIL y ISO 27002 en beneficio del negocio. Adicionalmente, se considera incluir la norma ISO 9001, porque las empresas objeto de estudio se basan en esta norma para gestionar la calidad de sus procesos

.

El cuadro comparativo resultante se presenta en la Tabla 1. La alineación de las actividades o procesos con las normas y metodologías de gestión de riesgo tecnológico, están marcadas con una X.

Tabla1: *Cuadro comparativo de normas y metodologías de gestión de riesgos.*

	Guerrero & Gómez (2011)									Crespo (2016), Ramírez y Ortiz (2011) y IT Governance Institute(2008)					Autor
Actividad Estándar	ISO 27005	OCTAVE	ISM3	AS/NZS	SP800-30	SOMAP	MAGUERIT	MEHARI	SP800-39	ISO 31000	ISO 27001	ISO 27002	COBIT	ITIL	ISO 9001
A1. Establecer el contexto. Medir y caracterizar el estado actual de la seguridad de los sistemas y la organización. Evaluar la exposición inherente.	x		x	x	x			x	x	x	x	x	x	x	x
A2. Identificar y valorar los activos críticos.		x					x			x	x	x	x	x	
A3. Identificar las amenazas y las vulnerabilidades de la organización.		x	x		x		x			x	x	x	x	x	
A4. Identificar los componentes claves y las vulnerabilidades técnicas que ocasionan los riesgos.	x	x		x	x		x				x	x	x	x	
A5. Evaluar el riesgo. Identificar el riesgo. Estimar el riesgo. Valorar el riesgo.	x	x		x	x	x	x		x	x	x		x		x
A6. Determinar y evaluar el impacto.							x	x		x		x	x	x	
A7. Tratar el riesgo. Identificar las exigencias de seguridad y las normas existentes. Desarrollar estrategias de protección basadas en buenas prácticas. Implementar proteociones.	x	x	x	x	x	x	x		x	x		x	x		x
A8. Aceptar el riesgo. Dar prioridad a la inversión de los procesos de seguridad.	x		x					x	x					x	
A9. Comunicar el riesgo.	x							x		x	x		x		x
A10. Realizar seguimiento al riesgo. Establecer un plan de reducción de los riesgos. Monitorear y revisar.	x	x	x	x	x	x	x	x	x	x	x		x	x	x
A11. Documentar resultados.					x				x	x	x		x	x	

Nota. Compendio de los trabajos previos realizados por Guerrero y Gómez (2011); Crespo (2016), Ramírez y Ortiz (2011); IT Governance Institute (2008) y literatura revisada.

Para escoger las normas y metodologías de gestión de riesgo, que estén acordes con las necesidades de las empresas objeto de estudio, se utilizó la Tabla 1, donde la selección fue realizada por expertos, conformada por dos de los directores de TI con mayor experiencia, un auditor de las empresas donde se realizó el estudio y un docente con experiencia en el tema tratado en el presente trabajo. Donde escogieron las normas y metodologías de acuerdo a su alineación con las actividades de gestión de riesgo.

Metodología modelo.

Una vez realizada la selección por los expertos, se obtuvo una nueva metodología para la gestión de riesgos en el área informática, basada en los estándares ISO 9001, ISO 31000, ISO 27005 e ISO 27002; Junto con la metodología MAGERIT y la herramienta PILAR micro versión 6.3, las que se pueden apreciar en la Tabla 2.

Para complementar la nueva metodología de gestión de riesgos, se aplica el ciclo PHVA, con el fin de establecer un proceso de gestión, enfocado en la mejora continua.

Tabla 2: *Metodología de gestión de riesgos informáticos obtenida.*

Actividad Estándar	Metodología Propuesta
A1. Establecer el contexto. Medir y caracterizar el estado actual de la seguridad de los sistemas y la organización. Evaluar la exposición inherente.	ISO 9001:2015
A2. Identificar y valorar los activos críticos.	MAGERIT/ PILAR
A3. Identificar las amenazas y las vulnerabilidades de la organización.	MAGERIT/ PILAR
A4. Identificar los componentes claves y las vulnerabilidades técnicas que ocasionan los riesgos.	MAGERIT/ PILAR
A5. Evaluar el riesgo. Identificar el riesgo. Estimar el riesgo. Valorar el riesgo.	MAGERIT/ PILAR
A6. Determinar y evaluar el impacto.	MAGERIT/ PILAR
A7. Tratar el riesgo. Identificar las exigencias de seguridad y las normas existentes. Desarrollar estrategias de protección basadas en buenas prácticas. Implementar protecciones.	MAGERIT/ PILAR ISO 27002
A8. Aceptar el riesgo. Dar prioridad a la inversión de los procesos de seguridad.	ISO 27005
A9. Comunicar el riesgo.	ISO 27005
A10. Realizar seguimiento al riesgo. Establecer un plan de reducción de los riesgos. Monitorear y revisar.	ISO 27005 MAGERIT
A11. Documentar resultados.	ISO 31000

Aplicación de la metodología

El presente trabajo, no comprende una auditoría integral del área de informática y se aplicó en una las empresas exportadoras de pesca blanca de Manta y Jaramijó, donde se realizó una evaluación inicial, utilizando la metodología de gestión de riesgo resultante en este estudio, seguidamente se aplicó las medidas de control que estaban acordes a los recursos, disponibilidad y predisposición de la empresa, a continuación se procedió a realizar una segunda valoración de la gestión de riesgos, para finalmente proceder a analizar los resultados de ambas evaluaciones.

Fase de implementación

La implementación de la metodología de gestión de riesgos informático obtenida en este estudio, se la realizo en una empresa del sector estudiado, el cual fue definido en el alcance de la investigación, para esto se procedió a la instalación de la herramienta PILAR, y se ejecutaron las actividades estándar de la metodología de gestión de riesgos informáticos obtenida, las mismas que se detalla a continuación:

En la actividad inicial (A1) del proceso de gestión de riesgos, para establecer el contexto de la empresa, se realizó un análisis del organigrama y los procesos de todas las áreas de la empresa.

Continuando con la siguiente actividad, para identificar los activos críticos, se procedió conjuntamente con el director de TI, a escoger una muestra de los activos informáticos más relevantes, los mismos que se detallan en la Tabla 4.

Tabla 4: *Selección de activos informáticos más relevantes de la empresa.*

NUM	Activo
	Servicios Internos
1	Firewall
2	Correos (ZIMBRA)
3	Internet
	Equipamiento
	Aplicaciones
4	SYSTEMARDEX
5	Ofimática
6	Antivirus
7	Sistema Operativo
	Equipos
8	Servidor de Base de Datos
9	Servidor : Backup
10	Router
	Comunicaciones
11	Red LAN
	Elementos Auxiliares
12	Sistema de Alimentación Ininterrumpida

Una vez determinados los activos informáticos, se procede a su ingreso en la Herramienta de análisis de riesgo PILAR micro 6.3, seguidamente se valoran cualitativamente los activos críticos, como se indica en la Figura 4, a continuación se ingresa la clase de activo, cumpliendo de esta forma con la actividad de identificar y valorar los activos críticos (A2).

dimensión	[D]	[I]	[C]	[A]	[T]
AETES] ASOEXPEBLA	[10]	[10]	[10]	[10]	[10]
Activos esenciales					
is [FIRE] FIREWALL	[10]	[10]	[10]	[10]	[10]
is [[HW][SW]CORREO] CORREC	[10]	[10]	[10]	[8]	[8]
is [INTER] SERVIDOR INTERNET	[10]	[10]	[8]	[8]	[8]
is [[SW]SYSMAR] SYSTMARD	[10]	[10]	[8]	[8]	[8]
is [[SW]OFIM] OFIMATICA	[8]	[8]	[6]	[7]	[6]
is [[SW]ANTIVIR]	[10]	[10]	[8]	[6]	[6]
is [[SW]SO] SISTEMA OPERATI	[10]	[10]	[8]	[10]	[8]
is [[HW][SW]SERVDAT] SERVID	[10]	[10]	[10]	[10]	[10]
is [[RED]REDLAN] RED LAN	[10]				
is [[AUX]UPS] UPS SISTEMA DE	[10]				
is [[HW]BACK] SERVIDOR BACK	[10]	[10]	[10]	[10]	[10]
sistema de protección de frontera ló					
sistema de protección física del peri					
contratado a terceros					
[[HW]] ROUTER	[10]	[10]	[10]	[10]	[10]

Figura 4 Identificación y valoración de activos. Información tomada del programa PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Para cumplir con las actividades desde la A3 hasta la A7, con el programa PILAR, se valoriza el nivel de madurez actual 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 . Cabe indicar que se valorizan de acuerdo a la tabla de nivel de madurez de eficacia de salvaguardas mostrada en la Tabla 5.

Tabla 5: *Niveles de madurez*.

Niveles de madurez	
L0	Inexistente
L1	Inicial / ad hoc
L2	Reproducible, pero intuitivo
L3	Proceso definido
L4	Gestionado y medible
L5	Optimizado

Nota: Información tomada de MAGERIT.

En base a la información ingresada, el PILAR calcula los niveles de amenazas potencial, objetivo, actual y el sugerido por esta herramienta. También indica las amenazas sobre los activos, en la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad. Con la información generada, se procedió a tabularla en una hoja electrónica, y generar en forma gráfica el valor de las amenazas sobre los activos.

El programa PILAR genera el resumen del impacto (actividad A6) y riesgo, en donde indica los activos con sus respectivas amenazas potenciales, actuales, objetivos y sugeridas por el PILAR.

La herramienta de análisis PILAR genera los informes de análisis de riesgo, declaración de aplicabilidad – ISO/IEC 27000(2013), cumplimiento ISO/IEC 27000(2013), cumplimiento Real Decreto 1720(2007), que se utilizaron para la actividad de aceptación del riesgo.

Para comunicar el riesgo, se elaboró un formato, que se utilizó para el registro del riesgo, las causas y sus consecuencias, las acciones a realizar y conclusiones y recomendaciones, entre otros apuntes, que servirán para registrar las comunicaciones generadas durante el proceso. También para comunicar el riesgo se pueden utilizar circulares, presentaciones o charlas, entre otros.

Para realizar el seguimiento al riesgo y controlar el monitoreo y la revisión de los controles implementados, se elaboró y utilizó un formato, para asegurar su constante funcionamiento y correcta aplicación.

Para documentar los resultados (actividad A11), se considera toda la documentación generada durante el proceso.

Análisis de resultados

Análisis de primera evaluación

Luego de aplicar la primera evaluación de la metodología de gestión de riesgo, 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.

Una vez realizada 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 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.

Segunda evaluación, análisis comparativo de resultados.

A continuación, se aplicó una segunda evaluación, utilizando 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, donde se obtuvieron los siguientes resultados:

Evaluación con el Real Decreto 1720(2007)

De acuerdo a los resultados obtenidos con la evaluación con el Real Decreto 1720, se puede apreciar en la Tabla 6 el 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.

Tabla 6: 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.

Evaluación con la norma ISO 27002:2013 Código de prácticas de controles de seguridad de la información.

Aplicando la norma ISO 27002:2013, en la Tabla 7, se puede apreciar 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 7: Evaluación ISO 27002:2013

		Obj.	PILAR	Actual	
	Evaluación ISO 27002:2013			1	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.

Análisis de la Valoración de los riesgos en los activos esenciales.

Los valores indicados en la Tabla 8, se utilizan para la valoración de los riesgos.

Tabla 8: 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

Nota : Información tomada del MAGERIT, Elaboración propia.

En la Tabla 9, 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 9: Valoración de activos esenciales

ACTIVOS:Valoración	objetivo		Actual	
de riesgo	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 10.

Tabla 10: *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 11, 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 11: *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 12 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 12: *Cumplimiento ISO/IEC 27002:2013*

	[6] Organización de la seguridad de la información	Evaluación 1	Evaluación 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 14.1 requisitos de seguridad en sistemas de información, que en la segunda evaluación cambia de si aplica a no aplica (n.a.).

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 13, 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 13: *Cumplimiento RD 1720(2007)*

	Medidas de seguridad de nivel básico	Evaluación 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 puede apreciar que ha habido 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, que permita gestionar los riesgos en caso de producirse un hecho de este tipo.

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). Y por último los directivos no consideran la información estratégica, la falta de presupuesto y la falta de apoyo de los directivos

La revisión de las diversas normas y metodologías de gestión de riesgo consideradas en el presente estudio, permitió obtener una nueva 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 para gestionar los riesgos en las áreas informáticas y como guía para su implementación en las empresas exportadoras de pesca blanca.

La aplicación de la metodología de gestión de riesgo propuesta en una de las empresas del sector de estudio, permitió obtener los siguientes resultados: 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. Se logró alcanzar, en algunos casos los objetivos planteados en la evaluación inicial, que permitieron aumentar los niveles de madurez de las medidas de control tanto del RD 1720 y la norma anteriormente mencionada, 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.

Es importante la intervención de los directivos de las empresas, debido a que es necesario su compromiso para la implementación de la metodología de gestión de riesgo propuesta, y consecuentemente la aceptación y tratamiento de riesgos tecnológicos.

La utilización de la metodología de gestión de riesgo obtenida en el presente trabajo, permitirá a las empresas que no han realizado un análisis de riesgos debido a: la complejidad de las normas y metodologías, factor económico entre otros, a realizar un proceso de gestión de riesgos en el área informática.

Entre las limitaciones de la aplicación de la metodología de la gestión de riesgo en la empresa donde se realizó su implementación y ejecución, se pueden indicar: la falta de recurso humano, por ejemplo la disponibilidad de tiempo del director de TI; la empresa no cuenta con un presupuesto para la gestión de riesgo en el área informática. Adicionalmente, la empresa se encuentra en un proceso de certificación, por lo que parte de los recursos con que cuenta la empresa están destinados a mejoras en la infraestructura y también el sector está atravesando por una situación económica adversa.

Como trabajo futuro se debe ampliar 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, 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 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., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards and Interfaces*, 176-185.

Barrantes, C., & Hugo, J. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos.* Lima, Perú: Universidad de San Martín de Porres.

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., & 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.* Barcelona, España: Universidad Autónoma de Barcelona.

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

Cavusoglu, H., Raghunathan, S., & 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, & Young. (2003). *Global information security survey 2003.* Ernst & Young LLP, White Paper.

Espinosa, D., & 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.

Espinoza, T., Martínez, J., & Siler, A. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control. *USBMed*.

Eterovic, J., & Pagliari, G. (2012). *Metodología de Análisis de Riesgos Informáticos.* Buenos Aires, Argentina: EAE.

Gaona, K. (2013). *Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera Bravito S.A. en la ciudad de Machala.* Cuenca: Universidad Politécnica Salesiana.

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., & 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., & Cuza-García, B. (2013). Modelos causales para la Gestión de Riesgos. *Revista Cubana de Ciencias Informáticas*, 58-74.

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

ISO 73. (2014). *Gestión de Riesgo - Vocabulario.* Quito: Instituto Ecuatoriano de Normalización.

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.* Office of Government Commerce.

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

Lucero, A., & Valverde, J. (2012). *Análisis y Gestión de Riesgos de los Sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología Magerit.* Cuenca: Universidad de Cuenca.

Macedo, L. (2012). *Desarrollo de una nueva metodología de administración informática para empresas u organizaciones mexicanas.* México: Instituto Politécnico Nacional.

Martínez, D. (2016). *Sistemas de información estratégicos, herramienta para la optimización de gestión en las empresas.* Bogotá; Colombia: Universidad Militar Nueva Granada.

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

Quesada, G. (25 de 11 de 2005). *Gestiopolis*. Obtenido de Mejoramiento continuo principio de gestión de la calidad: http://www.gestiopolis.com/mejoramiento-continuo-principio-de-gestion-de-la-calidad/

Racz, N., Weippl, E., & Seufert, A. (2010). Questioning the need for separate IT risk management frameworks. Paper presented at the INFORMATIK 2010 - Service Science - Neue Perspektiven Fur Die Informatik, Beitrage Der 40. Jahrestagung Der Gesellschaft Fur Die Informatik, Beitrage Der 40. Jahrestag. 245-252. Retrieved from www.scopus.com.

Ramírez, A., & 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.

Rosero, E. (2014). *Análisis de riesgos de la seguridad de la red de área local LAN de la matriz de la Contraloría General del*

Estado. Quito: Universidad Central del Ecuador.

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., & 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.* España: Etek Internacional.

Taylor, H., Artman, E., & Woelfer, J. P. (2012). Information technology project risk management: Bridging the gap between research and practice. *Journal of Information Technology*, 17-34.

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., & 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.

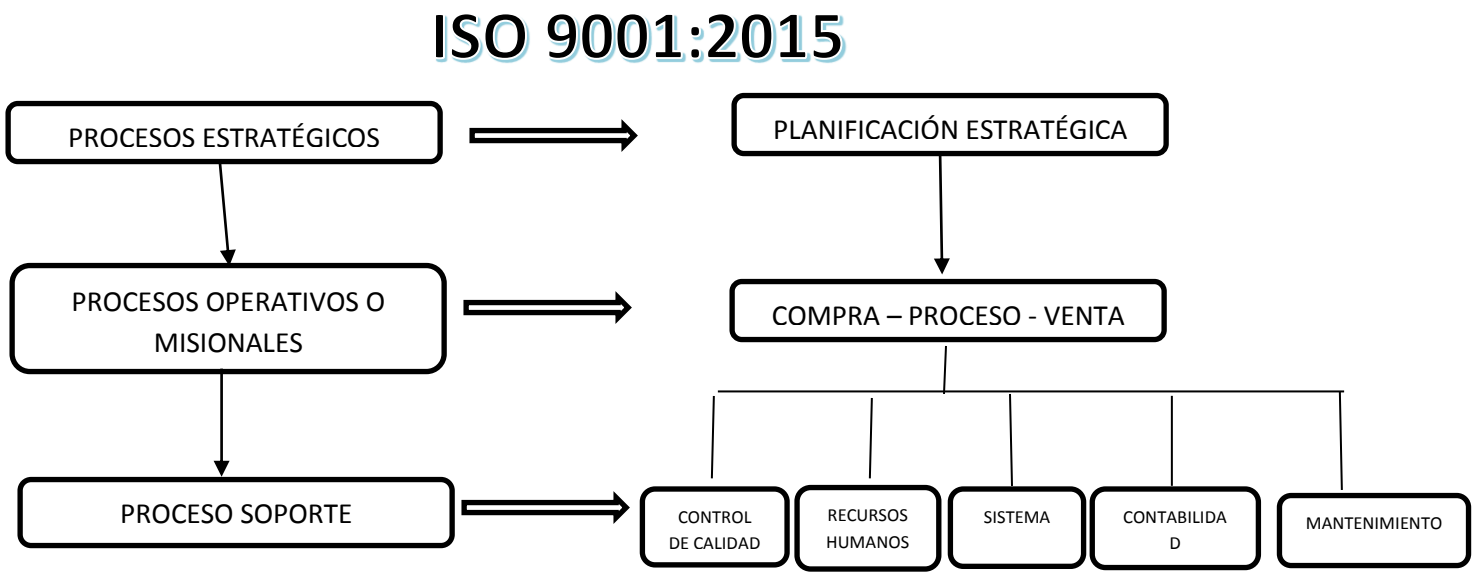
Yeo, M. L., Rolland, E., Ulmer, J. R., & Patterson, R. A. (2014). Risk mitigation decisions for it security. ACM Transactions on Management Information Systems.

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

ANEXOS

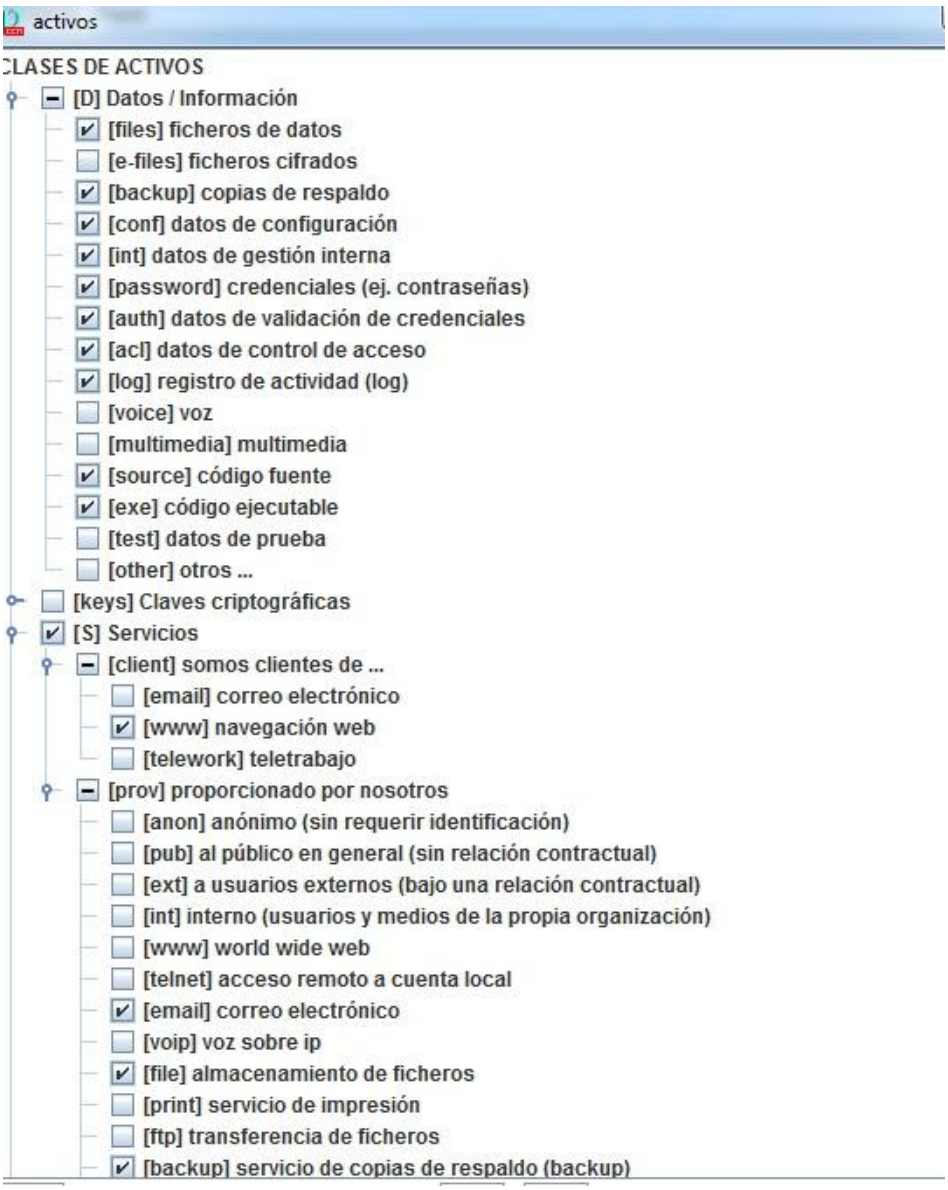
ANEXO 1

A1 Establecer el contexto



ANEXO 2

A2 Clase de Activos



Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

ANEXO 3

[RD 1720] Protección de datos de carácter personal

Expandir operación madurez Exportar

	reco...		control	dudas	aplica	com...	current	target	PILAR
☐			[RD 1720] Protección de datos de carácter personal				_-L4 (L0-L4)	L3-L5 (L3-L4)	L2-L5
☐	9		[B] Medidas de seguridad de nivel básico				_-L3 (L1-L4)	L3-L5 (L3-L4)	L2-L5
☐	3		[89] Funciones y obligaciones del personal				L3	L4	L2-L3
☐	3		[90] Gestión de las incidencias				(L3)	L3	L3
☐	7		[91] Control de acceso				L2-L3 (L2-L4)	L3-L5 (L3-L4)	L3-L4 (L2-L4)
☐			[92] Gestión de soportes y documentos				L2 (L1-L3)	L3-L5 (L3)	n.a.
☐	9		[93] Identificación y autenticación				L3	L4	L3-L5
☐	6		[94] Copias de respaldo y recuperación				L3 (L3-L4)	L3-L5 (L3-L4)	L3-L4 (L2-L4)
☐	5		[M] Medidas de seguridad de nivel medio				L1-L3 (L0-L4)	L3-L4 (L3)	L2-L3
☐	5		[95] Responsable de seguridad				L3	L4	L3
☐	5		[96] Auditoría				L1-L3 (L3)	L3	L2-L3 (L2)
☐			[97] Gestión de soportes y documentos				L2 (L2-L3)	L3	n.a.
☐	4		[98] Identificación y autenticación				L1 (L2)	L4 (L3)	L3 (L2-L3)
☐			[99] Control de acceso físico				L2 (L0-L4)	L3	n.a.
☐	5		[100] Registro de incidencias				L2-L3 (L3)	L3	L3
☐	6		[A] Medidas de seguridad de nivel alto				L2-L4 (L1-L4)	L3-L5 (L3-L4)	L2-L4
☐			[101] Gestión y distribución de soportes				L2 (L1-L3)	L3	n.a.
☐	6		[102] Copias de respaldo y recuperación				L3 (L3-L4)	L3	L4 (L3-L4)
☐	5		[103] Registro de accesos				L2-L4	L3-L4	L2-L3
☐	5		[104] Telecomunicaciones				L2	L5 (L3)	L3

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

ANEXO 4

Norma ISO 27002:2013: Valoración de madurez actual y objetivo

[27002:2013] Código de prácticas para los controles de seguridad de la información

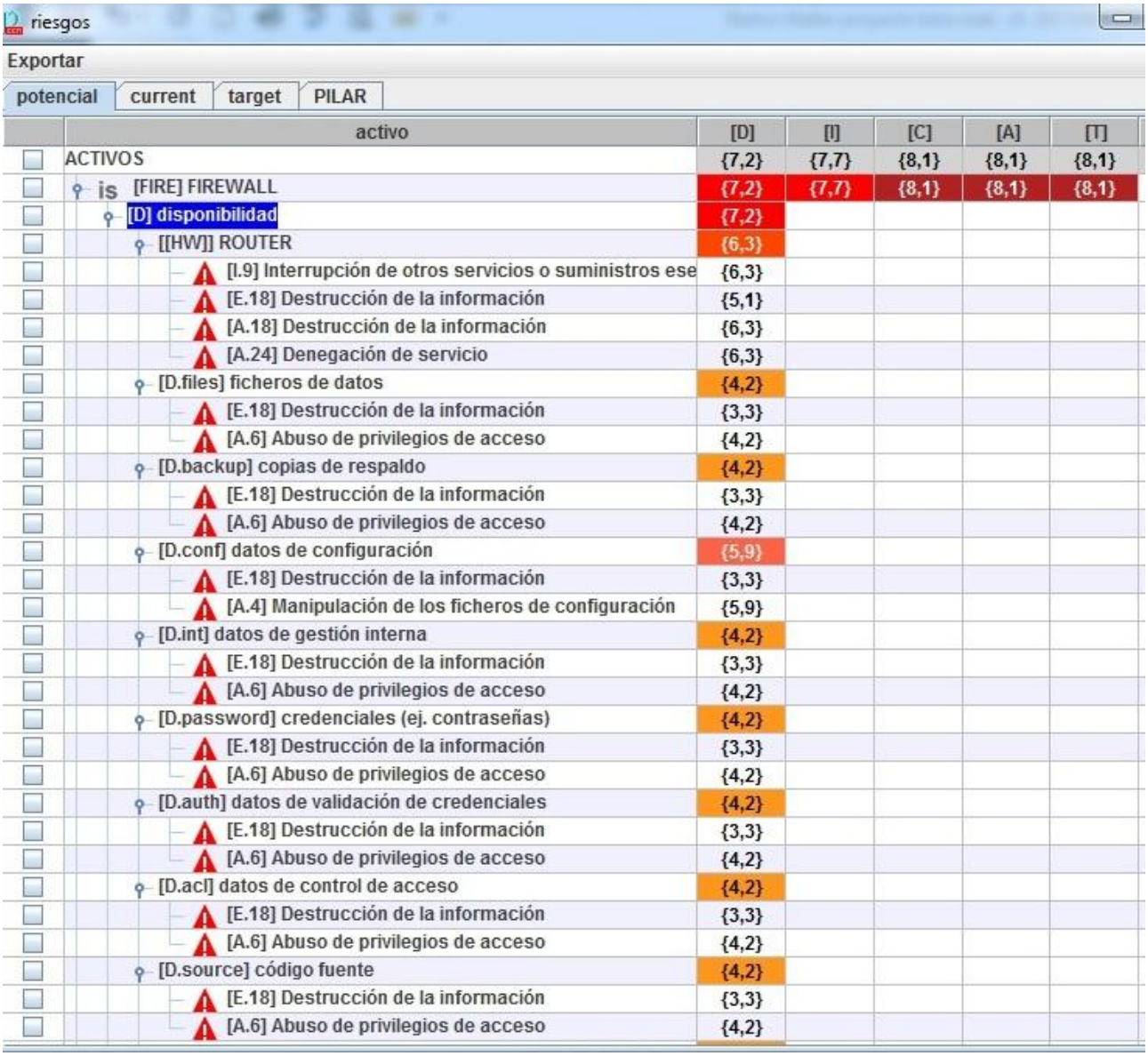
Expandir operación madurez Exportar

	reco...		control	dudas	aplica	com...	current	target	PILAR
			[27002:2013] Código de prácticas para los controles de seguridad de la información				_-L3	_-L4	L2-L5
	2		[5] Políticas de seguridad de la información				L3	L4	L2
	2		[5.1] Directrices de gestión de la seguridad de la información				L3	L4	L2
	2		[5.1.1] Políticas para la seguridad de la información				L3	L4	L2
	2		[G.3.3] Normas de seguridad				L3	L4	L2
	2		[G.3.3.1] Emanan y están aprobadas por el responsable de seguridad				L3	L4	L2
	2		[G.3.3.2] Se precisa lo que es uso adecuado y uso indebido				L3	L4	L2
	2		[G.3.3.3] Se precisa la responsabilidad de las personas respecto de su cumplimiento y violación				L3	L4	L2
	2		[G.3.3.4] Todo el personal de la organización tiene acceso a los documentos				L3	L4	L2
	2		[G.3.3.5] Son conocidas y aceptadas por los afectados				L3	L4	L2
	2		[G.3.3.6] Se revisan regularmente				L3	L4	L2
	2		[5.1.2] Revisión de las políticas para la seguridad de la información				L3	L4	L2
	2		[G.3.3.6] Se revisan regularmente				L3	L4	L2
	7		[6] Organización de la seguridad de la información				L2 (L2-L3)	L3 (L3-L4)	L2-L4
	7		[6.1] Organización interna				L2 (L2-L3)	L3 (L3-L4)	L2-L4
	3		[6.1.1] Roles y responsabilidades en seguridad de la información				L2 (L2-L3)	L3 (L3-L4)	L2-L3
	2		[G.1.1] Comité de seguridad de la información				L2	L3	L2
	2		[G.1.1] Comité de seguridad de la información				L2	L3	L2
	2		[G.1.1.1] Está respaldado por la dirección				L2	L3	L2
	2		[G.1.1.2] Define claramente las funciones de seguridad				L2	L3	L2
	2		[G.1.1.3] Aprueba las designaciones de responsables de seguridad				L2	L3	L2
	2		[G.1.1.4] Identifica los objetivos de seguridad				L2	L3	L2
	2		[G.1.1.5] Revisa, evalúa y aprueba la normativa de seguridad				L2	L3	L2
	2		[G.1.1.6] Asegura la coordinación en materia de seguridad dentro de la organización				L2	L3	L2
	3		[G.1.3] Roles identificados				L2	L3	L3 (L2-L3)
	2		[G.1.4] Asignación de responsabilidades para la seguridad de la información				L2 (L3)	L3 (L4)	L2
	2		[G.1.2] Coordinación interna				L2	L3	L2

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

ANEXO 5

Riesgos: Identificación de amenazas por activo


riesgos

Exportar

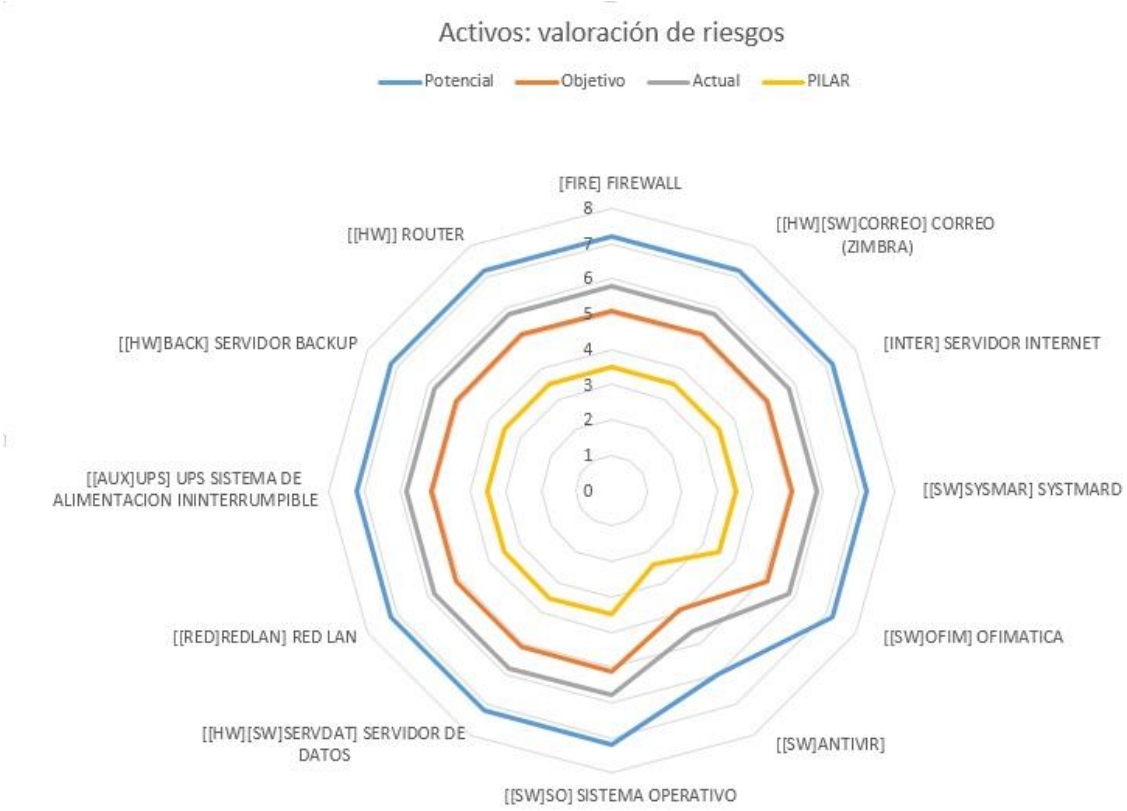
potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{7,2}	{7,7}	{8,1}	{8,1}	{8,1}
is [FIRE] FIREWALL	{7,2}	{7,7}	{8,1}	{8,1}	{8,1}
[D] disponibilidad	{7,2}				
[[HW]] ROUTER	{6,3}				
[I.9] Interrupción de otros servicios o suministros ese	{6,3}				
[E.18] Destrucción de la información	{5,1}				
[A.18] Destrucción de la información	{6,3}				
[A.24] Denegación de servicio	{6,3}				
[D.files] ficheros de datos	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				
[D.backup] copias de respaldo	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				
[D.conf] datos de configuración	{5,9}				
[E.18] Destrucción de la información	{3,3}				
[A.4] Manipulación de los ficheros de configuración	{5,9}				
[D.int] datos de gestión interna	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				
[D.password] credenciales (ej. contraseñas)	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				
[D.auth] datos de validación de credenciales	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				
[D.acl] datos de control de acceso	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				
[D.source] código fuente	{4,2}				
[E.18] Destrucción de la información	{3,3}				
[A.6] Abuso de privilegios de acceso	{4,2}				

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

ANEXO 6

Valoración de riesgos en los activos esenciales



Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Elaboración: Autor

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

Anexo 7

Resumen de Impacto

potencial | current | target | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	impacto	current	target	PILAR
[D.source] código fuente	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.exe] código ejecutable	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.acl] datos de control de acceso	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.int] datos de gestión interna	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[D.auth] datos de validación de credenciales	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[7]	[6]
[S.prov.email] correo electrónico	[A.13] Repudio (negación de actuaciones)	[T]	[10]	[8]	[7]	[6]
[S.prov.file] almacenamiento de ficheros	[A.13] Repudio (negación de actuaciones)	[T]	[10]	[8]	[7]	[6]
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de activ...	[I]	[9]	[7]	[6]	[5]
[D.source] código fuente	[A.11] Acceso no autorizado	[C]	[9]	[7]	[7]	[5]
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]	[9]	[7]	[7]	[5]
[D.exe] código ejecutable	[A.11] Acceso no autorizado	[C]	[9]	[7]	[7]	[5]
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]	[9]	[7]	[7]	[5]
[D.password] credenciales (ej. contraseñas)	[A.11] Acceso no autorizado	[C]	[9]	[7]	[7]	[5]
[HW.backup] equipamiento de respaldo	[E.24] Caída del sistema por agotamiento d...	[D]	[9]	[7]	[6]	[5]
[HW.mid] equipos medios	[E.24] Caída del sistema por agotamiento d...	[D]	[9]	[7]	[6]	[5]
[HW.pc] informática personal	[E.24] Caída del sistema por agotamiento d...	[D]	[9]	[7]	[6]	[5]
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[6]	[5]
[D.exe] código ejecutable	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[6]	[5]
[D.source] código fuente	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[6]	[5]
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[6]	[5]
[D.password] credenciales (ej. contraseñas)	[A.6] Abuso de privilegios de acceso	[C]	[9]	[6]	[5]	[5]
[COM.Internet] Internet	[A.24] Denegación de servicio	[D]	[9]	[7]	[7]	[5]
[S.prov.email] correo electrónico	[A.24] Denegación de servicio	[D]	[9]	[7]	[6]	[5]
[S.prov.email] correo electrónico	[E.24] Caída del sistema por agotamiento d...	[D]	[9]	[7]	[6]	[5]
[S.prov.file] almacenamiento de ficheros	[A.24] Denegación de servicio	[D]	[9]	[7]	[6]	[5]
[S.prov.file] almacenamiento de ficheros	[E.24] Caída del sistema por agotamiento d...	[D]	[9]	[7]	[6]	[5]
[COM.LAN] red local	[A.24] Denegación de servicio	[D]	[9]	[8]	[7]	[5]
[S.prov.ipm] gestión de privilegios	[A.24] Denegación de servicio	[D]	[9]	[7]	[6]	[5]

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Anexo 8

Resumen de riesgo

potencial | current | target | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	riesgo	current	target	PILAR
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de activ...	[I]	{8,1}	{6,2}	{5,1}	{4,3}
[D.source] código fuente	[A.11] Acceso no autorizado	[C]	{8,1}	{6,3}	{5,6}	{4,2}
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]	{8,1}	{6,3}	{5,6}	{4,2}
[D.exe] código ejecutable	[A.11] Acceso no autorizado	[C]	{8,1}	{6,3}	{5,6}	{4,2}
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]	{8,1}	{6,3}	{5,6}	{4,2}
[D.password] credenciales (ej. contraseñas)	[A.11] Acceso no autorizado	[C]	{8,1}	{6,3}	{5,6}	{4,1}
[D.source] código fuente	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,9}
[D.exe] código ejecutable	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,9}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,9}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,9}
[D.acl] datos de control de acceso	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,8}
[D.int] datos de gestión interna	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,8}
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,8}
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,8}
[D.auth] datos de validación de credenciales	[A.5] Suplantación de la identidad	[A]	{7,7}	{6,1}	{5,4}	{3,8}
[S.prov.email] correo electrónico	[A.13] Repudio (negación de actuaciones)	[T]	{7,4}	{5,3}	{4,3}	{3,6}
[S.prov.file] almacenamiento de ficheros	[A.13] Repudio (negación de actuaciones)	[T]	{7,4}	{5,3}	{4,4}	{3,6}
[HW.backup] equipamiento de respaldo	[E.24] Caída del sistema por agotamiento d...	[D]	{7,2}	{5,3}	{4,3}	{3,5}
[HW.mid] equipos medios	[E.24] Caída del sistema por agotamiento d...	[D]	{7,2}	{5,3}	{4,3}	{3,5}
[HW.pc] informática personal	[E.24] Caída del sistema por agotamiento d...	[D]	{7,2}	{5,3}	{4,3}	{3,5}
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]	{7,2}	{5,0}	{4,0}	{3,4}
[D.exe] código ejecutable	[A.6] Abuso de privilegios de acceso	[C]	{7,2}	{5,0}	{4,0}	{3,4}
[D.source] código fuente	[A.6] Abuso de privilegios de acceso	[C]	{7,2}	{5,0}	{4,0}	{3,4}
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]	{7,2}	{5,0}	{4,0}	{3,4}
[D.password] credenciales (ej. contraseñas)	[A.6] Abuso de privilegios de acceso	[C]	{7,2}	{4,8}	{3,9}	{3,4}
[COM.Internet] Internet	[A.24] Denegación de servicio	[D]	{7,2}	{5,6}	{4,8}	{3,4}
[S.prov.email] correo electrónico	[A.24] Denegación de servicio	[D]	{7,2}	{5,1}	{4,1}	{3,3}
[S.prov.email] correo electrónico	[E.24] Caída del sistema por agotamiento d...	[D]	{7,2}	{5,1}	{4,1}	{3,3}
[S.prov.file] almacenamiento de ficheros	[A.24] Denegación de servicio	[D]	{7,2}	{5,1}	{4,2}	{3,3}
[S.prov.file] almacenamiento de ficheros	[E.24] Caída del sistema por agotamiento d...	[D]	{7,2}	{5,1}	{4,2}	{3,3}
[COM.LAN] red local	[A.24] Denegación de servicio	[D]	{7,2}	{5,8}	{5,1}	{3,3}
[S.prov.ipm] gestión de privilegios	[A.24] Denegación de servicio	[D]	{7,2}	{4,9}	{4,0}	{3,3}

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

ANEXO 9

A9 Formato para comunicar el riesgo

Empresa Exportadora de Pesca Blanca

COMUNICACIÓN	Código:	R1
	Versión:	
	Fecha Elaboración:	18/12/2017
	Página:	

Comunicación		
COMUNICANTE	Fecha:	Área:
	Director de TI	Endian Firewall(Reporte de acesos)

COMUNICADO	**Riesgo:** Virus , rasomware
	Causas: Navegación en paginas indeseadas
	Consecuencias: Pérdidas de información y ataques

ACCIONES O DECISIONES	FECHA	RESPONSABLE
Alimentar el listado de paginas prohibidas	17/01/2018	Javier
Aumentar el servicio de control d	22/01/2018	Javier
Conclusiones: al implementar esta medidad, no se permitira el uso indebido del internet		
Recomendaciones: Monitorear el reporte de acceso a paginas (pornografía, juegos, páginas de compras) Politicas de acceso paginas que se bloquean		

Firma responsable

ANEXO 10

A10 Formato para monitoreo y revisión

EMPRESA EXPORTADORA DE PESCA BLANCA

MONITOREO Y REVISIÓN DE RIESGOS	Código:	R91
	Versión:	
	Elaborado:	28/01/2018
	Página:	1 de 1

Riesgo	Fecha	Logros	Justificación	Indicador	Reportado A	Existe Riesgo Emergente		Observaciones
						Si	No	
Ingreso de Correo excesivo spam (Zimbra)	25/01/2018	Disminución de correo no deseado spam	Se debe controlar y minimizar el ingreso de correos spam	Disminución de correo no deseado spam	Jefe de Sistema		X	El monitoreo de los riesgos es realizado
Ralentización y saturación de recursos, por envío de archivos de gran tamaño.	26/01/2018	Controlar el ingreso de correo de gran tamaño	La optimización de recursos, necesita de controlar el ingreso de archivos de gran tamaño.	Disminución de consumo de recursos	Jefe de Sistema		X	El monitoreo de los riesgos es realizado

Elaborado por: W	Fecha: 25/01/2018
Revisado por: J.A	Fecha: 28/01 /2018
Aprobado por: J.A.	Fecha: 28/01/2018

ANEXO 11

Análisis de Riesgos
[MAETES] ASOEXPEBLA

1.10.2017

Introducción

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

Datos del sistema sujeto a análisis:

Código: MAETES
Nombre: ASOEXPEBLA
Descripción:
Datos administrativos:

- responsable: Walter Bailón Lourido
- fecha: 2017

Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [V] Valor

Agravantes y atenuantes

[base] Base

Valoración de los activos

capa: [essential] Activos esenciales

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]
[FIRE] FIREWALL	[10]	[10]	[10]	[10]	[10]	
[[HW][SW]CORREO] CORREO (ZIMBRA)	[10]	[10](1)	[10]	[8]	[8]	
[INTER] SERVIDOR INTERNET	[10]	[10]	[8]	[8]	[8]	

[[SW]SYSMAR] SYSTMARD	[10]	[10]	[8]	[8]	[8]	
[[SW]OFIM] OFIMATICA	[8]	[8]	[6]	[7]	[6]	
[[SW]ANTIVIR]	[10]	[10]	[8]	[6]	[6]	
[[SW]SO] SISTEMA OPERATIVO	[10]	[10]	[8]	[10]	[8]	
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[10]	[10]	[10]	[10]	[10]	
[[RED]REDLAN] RED LAN	[10]					
[[AUX]UPS] UPS SISTEMA DE ALIMENTACION ININTERRUMPIBLE	[10]					
[[HW]BACK] SERVIDOR BACKUP	[10]	[10]	[10]	[10]	[10]	

(1) [crm] Persecución de Delitos:

Valoración de los dominios

dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]
[base] Base	[10]	[10]	[10]	[10]	[10]	

Riesgo acumulado

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

amenaza
presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella
D – dimensión
se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza
I – impacto
se muestra el máximo impacto causado por esta amenaza en algún activo del sistema
R – riesgo
se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

Phase: [potencial]

Amenaza	D	I	R
[A.11] Acceso no autorizado	C	[9]	{8,1}
[A.3] Manipulación de los registros de actividad (log)	I	[9]	{8,1}
[A.5] Suplantación de la identidad	A	[10]	{7,7}

Phase: [current] situación actual

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[7]	{6,3}
[A.3] Manipulación de los registros de actividad (log)	I	[7]	{6,2}
[A.5] Suplantación de la identidad	A	[8]	{6,1}

Phase: [target] situación objetivo

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[7]	{5,6}
[A.5] Suplantación de la identidad	A	[7]	{5,4}

Phase: [PILAR] recomendación

amenaza	D	I	R
[A.3] Manipulación de los registros de actividad (log)	I	[5]	{4,3}
[A.11] Acceso no autorizado	C	[5]	{4,2}
[A.5] Suplantación de la identidad	A	[6]	{3,9}

Riesgo repercutido
Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

activo
presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza
amenaza
presenta la amenaza dentro del catálogo de PILAR.
D – dimensión
se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza
I – impacto
se muestra el máximo impacto causado por esta amenaza sobre el activo esencial
R – riesgo
se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

Phase: [potencial]

activo	amenaza	D	I	R
[FIRE] FIREWALL	[A.11] Acceso no autorizado	C, A	[9]	{8,1}
[FIRE] FIREWALL	[A.3] Manipulación de los registros de actividad (log)	T	[9]	{8,1}

[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.11] Acceso no autorizado	C	[9]	{8,1}
[[SW]SO] SISTEMA OPERATIVO	[A.11] Acceso no autorizado	A	[9]	{8,1}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.11] Acceso no autorizado	C, A	[9]	{8,1}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.3] Manipulación de los registros de actividad (log)	T	[9]	{8,1}
[[HW]BACK] SERVIDOR BACKUP	[A.11] Acceso no autorizado	C, A	[9]	{8,1}
[[HW]BACK] SERVIDOR BACKUP	[A.3] Manipulación de los registros de actividad (log)	T	[9]	{8,1}
[FIRE] FIREWALL	[A.5] Suplantación de la identidad	I, C, A, T	[10]	{7,7}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.5] Suplantación de la identidad	I, C	[10]	{7,7}
[INTER] SERVIDOR INTERNET	[A.5] Suplantación de la identidad	I	[10]	{7,7}
[[SW]SYSMAR] SYSTMARD	[A.5] Suplantación de la identidad	I	[10]	{7,7}
[[SW]ANTIVIR]	[A.5] Suplantación de la identidad	I	[10]	{7,7}
[[SW]SO] SISTEMA OPERATIVO	[A.5] Suplantación de la identidad	I, A	[10]	{7,7}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.5] Suplantación de la identidad	I, C, A, T	[10]	{7,7}
[[HW]BACK] SERVIDOR BACKUP	[A.5] Suplantación de la identidad	I, C, A, T	[10]	{7,7}
[FIRE] FIREWALL	[A.13] Repudio (negación de actuaciones)	T	[10]	{7,4}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.13] Repudio (negación de actuaciones)	T	[10]	{7,4}
[[HW]BACK] SERVIDOR BACKUP	[A.13] Repudio (negación de actuaciones)	T	[10]	{7,4}

Phase: [current] situación actual

activo	amenaza	D	I	R
[FIRE] FIREWALL	[A.11] Acceso no autorizado	C, A	[7]	{6,3}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.11] Acceso no autorizado	C	[7]	{6,3}
[[SW]SO] SISTEMA OPERATIVO	[A.11] Acceso no autorizado	A	[7]	{6,3}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.11] Acceso no autorizado	C, A	[7]	{6,3}
[[HW]BACK] SERVIDOR BACKUP	[A.11] Acceso no autorizado	C, A	[7]	{6,3}
[FIRE] FIREWALL	[A.3] Manipulación de los registros de actividad (log)	T	[7]	{6,2}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.3] Manipulación de los registros de actividad (log)	T	[7]	{6,2}

[[HW]BACK] SERVIDOR BACKUP	[A.3] Manipulación de los registros de actividad (log)	T	[7]	{6,2}
[FIRE] FIREWALL	[A.5] Suplantación de la identidad	I, C, A, T	[8]	{6,1}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.5] Suplantación de la identidad	I, C	[8]	{6,1}
[INTER] SERVIDOR INTERNET	[A.5] Suplantación de la identidad	I	[8]	{6,1}
[[SW]SYSMAR] SYSTMARD	[A.5] Suplantación de la identidad	I	[8]	{6,1}
[[SW]ANTIVIR]	[A.5] Suplantación de la identidad	I	[8]	{6,1}
[[SW]SO] SISTEMA OPERATIVO	[A.5] Suplantación de la identidad	I, A	[8]	{6,1}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.5] Suplantación de la identidad	I, C, A, T	[8]	{6,1}
[[HW]BACK] SERVIDOR BACKUP	[A.5] Suplantación de la identidad	I, C, A, T	[8]	{6,1}
[FIRE] FIREWALL	[A.24] Denegación de servicio	D	[8]	{5,8}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.24] Denegación de servicio	D	[8]	{5,8}
[INTER] SERVIDOR INTERNET	[A.24] Denegación de servicio	D	[8]	{5,8}
[[SW]SYSMAR] SYSTMARD	[A.24] Denegación de servicio	D	[8]	{5,8}
[[SW]ANTIVIR]	[A.24] Denegación de servicio	D	[8]	{5,8}
[[SW]SO] SISTEMA OPERATIVO	[A.24] Denegación de servicio	D	[8]	{5,8}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.24] Denegación de servicio	D	[8]	{5,8}
[[RED]REDLAN] RED LAN	[A.24] Denegación de servicio	D	[8]	{5,8}
[[AUX]UPS] UPS SISTEMA DE ALIMENTACION ININTERRUMPIBLE	[A.24] Denegación de servicio	D	[8]	{5,8}
[[HW]BACK] SERVIDOR BACKUP	[A.24] Denegación de servicio	D	[8]	{5,8}

Phase: [target] situación objetivo

activo	amenaza	D	I	R
[FIRE] FIREWALL	[A.11] Acceso no autorizado	C, A	[7]	{5,6}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.11] Acceso no autorizado	C	[7]	{5,6}
[[SW]SO] SISTEMA OPERATIVO	[A.11] Acceso no autorizado	A	[7]	{5,6}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.11] Acceso no autorizado	C, A	[7]	{5,6}
[[HW]BACK] SERVIDOR BACKUP	[A.11] Acceso no autorizado	C, A	[7]	{5,6}
[FIRE] FIREWALL	[A.5] Suplantación de la identidad	I, C, A, T	[7]	{5,4}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.5] Suplantación de la	I, C	[7]	{5,4}

	identidad			
[INTER] SERVIDOR INTERNET	[A.5] Suplantación de la identidad	I	[7]	{5,4}
[[SW]SYSMAR] SYSTMARD	[A.5] Suplantación de la identidad	I	[7]	{5,4}
[[SW]ANTIVIR]	[A.5] Suplantación de la identidad	I	[7]	{5,4}
[[SW]SO] SISTEMA OPERATIVO	[A.5] Suplantación de la identidad	I, A	[7]	{5,4}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.5] Suplantación de la identidad	I, C, A, T	[7]	{5,4}
[[HW]BACK] SERVIDOR BACKUP	[A.5] Suplantación de la identidad	I, C, A, T	[7]	{5,4}
[FIRE] FIREWALL	[A.24] Denegación de servicio	D	[7]	{5,1}
[FIRE] FIREWALL	[A.3] Manipulación de los registros de actividad (log)	T	[6]	{5,1}
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.24] Denegación de servicio	D	[7]	{5,1}
[INTER] SERVIDOR INTERNET	[A.24] Denegación de servicio	D	[7]	{5,1}
[[SW]SYSMAR] SYSTMARD	[A.24] Denegación de servicio	D	[7]	{5,1}
[[SW]ANTIVIR]	[A.24] Denegación de servicio	D	[7]	{5,1}
[[SW]SO] SISTEMA OPERATIVO	[A.24] Denegación de servicio	D	[7]	{5,1}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.24] Denegación de servicio	D	[7]	{5,1}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.3] Manipulación de los registros de actividad (log)	T	[6]	{5,1}
[[RED]REDLAN] RED LAN	[A.24] Denegación de servicio	D	[7]	{5,1}
[[AUX]UPS] UPS SISTEMA DE ALIMENTACION ININTERRUMPIBLE	[A.24] Denegación de servicio	D	[7]	{5,1}
[[HW]BACK] SERVIDOR BACKUP	[A.24] Denegación de servicio	D	[7]	{5,1}
[[HW]BACK] SERVIDOR BACKUP	[A.3] Manipulación de los registros de actividad (log)	T	[6]	{5,1}

Phase: [PILAR] recomendación

activo	amenaza	D	I	R
[FIRE] FIREWALL	[A.3] Manipulación de los registros de actividad (log)	T	[5]	{4,3}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.3] Manipulación de los registros de actividad (log)	T	[5]	{4,3}
[[HW]BACK] SERVIDOR BACKUP	[A.3] Manipulación de los registros de actividad (log)	T	[5]	{4,3}
[FIRE] FIREWALL	[A.11] Acceso no autorizado	C,	[5]	{4,2}

		A		
[[HW][SW]CORREO] CORREO (ZIMBRA)	[A.11] Acceso no autorizado	C	[5]	{4,2}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.11] Acceso no autorizado	C, A	[5]	{4,2}
[[HW]BACK] SERVIDOR BACKUP	[A.11] Acceso no autorizado	C, A	[5]	{4,2}
[[SW]SO] SISTEMA OPERATIVO	[A.11] Acceso no autorizado	A	[5]	{4,1}
[FIRE] FIREWALL	[A.5] Suplantación de la identidad	A	[6]	{3,9}
[[SW]SO] SISTEMA OPERATIVO	[A.5] Suplantación de la identidad	A	[6]	{3,9}
[[HW][SW]SERVDAT] SERVIDOR DE DATOS	[A.5] Suplantación de la identidad	A	[6]	{3,9}
[[HW]BACK] SERVIDOR BACKUP	[A.5] Suplantación de la identidad	A	[6]	{3,9}

Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] Base

- **Activos esenciales**
- [essential] Activos esenciales
- [FIRE] FIREWALL
- [[HW][SW]CORREO] CORREO (ZIMBRA)
- [INTER] SERVIDOR INTERNET
- [[SW]SYSMAR] SYSTMARD
- [[SW]OFIM] OFIMATICA
- [[SW]ANTIVIR]
- [[SW]SO] SISTEMA OPERATIVO
- [[HW][SW]SERVDAT] SERVIDOR DE DATOS
- [[RED]REDLAN] RED LAN
- [[AUX]UPS] UPS SISTEMA DE ALIMENTACION ININTERRUMPIBLE
- [[HW]BACK] SERVIDOR BACKUP
- **activos**
- [S.3rd] contratado a terceros
- [[HW]] ROUTER
- [D] Datos / Información
- [D.files] ficheros de datos
- [D.backup] copias de respaldo
- [D.conf] datos de configuración
- [D.int] datos de gestión interna

- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [D.acl] datos de control de acceso
- [D.log] registro de actividad (log)
- [D.source] código fuente
- [D.exe] código ejecutable
- **[S] Servicios**
- [S.client.www] navegación web
- [S.prov.email] correo electrónico
- [S.prov.file] almacenamiento de ficheros
- [S.prov.backup] servicio de copias de respaldo (backup)
- [S.prov.ipm] gestión de privilegios
- [**SW] Aplicaciones (software)**
- [SW.prp] desarrollo propio (in house)
- [SW.std.office] ofimática
- [SW.std.os.windows] windows
- [SW.std.os.linux] linux
- [SW.sec.av] anti virus
- [SW.sec.ids] IDS / IPS (deteción / prevención de intrusion)
- [SW.sec.traf] análisis de tráfico
- **[HW] Equipamiento informático (hardware)**
- [HW.mid] equipos medios
- [HW.pc] informática personal
- [HW.backup] equipamiento de respaldo
- **[COM] Redes de comunicaciones**
- [COM.LAN] red local
- [COM.Internet] Internet
- **[AUX] Equipamiento auxiliar**
- [AUX.ups] sai - sistemas de alimentación ininterrumpida

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Anexo 12

Informe de cumplimiento ISO/IEC 27002:2013

Cumplimiento ISO/IEC 27002:2013

[MAETES] ASOEXPEBLA

1.10.2017

Introducción

Código: MAETES

Nombre: ASOEXPEBLA

Descripción:

Datos administrativos:

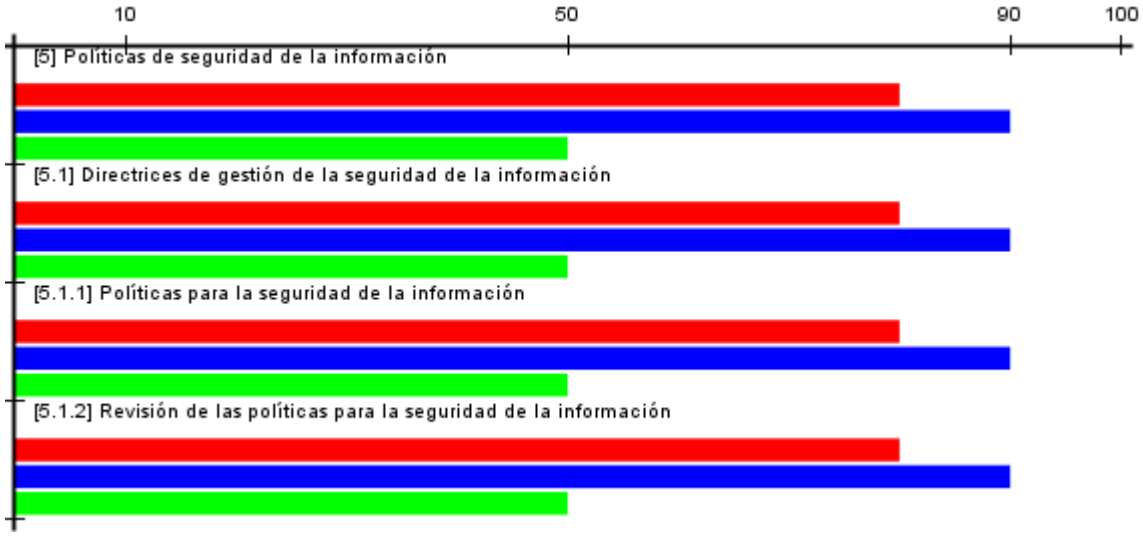
- responsable: Walter Bailón Lourido
- fecha: 2017

Controles

Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

[5] Políticas de seguridad



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio de seguridad: [base] Base

Control	aplica	current	target	PILAR
[5] Políticas de seguridad de la información	sí	L3	L4	L2
[5.1] Directrices de gestión de la seguridad de la información	sí	L3	L4	L2
[5.1.1] Políticas para la seguridad de la información	sí	L3	L4	L2
[5.1.2] Revisión de las políticas para la seguridad de la información	sí	L3	L4	L2

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Anexo 13

Declaración de Aplicabilidad - ISO/IEC 27002:2013
[MAETES] ASOEXPEBLA

1.10.2017

Introducción

Código: MAETES

Nombre: ASOEXPEBLA

Descripción:

Datos administrativos:

- responsable: Walter Bailón Lourido
- fecha: 2017

Dominios de seguridad

[base] Base

Valoración de los activos

capa: [essential] Activos esenciales

Activos esenciales

Controles

[5] Políticas de seguridad

dominio de seguridad: [base] Base

Control	aplica
[5] Políticas de seguridad de la información	sí
[5.1] Directrices de gestión de la seguridad de la información	sí
[5.1.1] Políticas para la seguridad de la información	sí
[5.1.2] Revisión de las políticas para la seguridad de la información	sí

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Anexo 14

Cumplimiento RD 1720 (2007)
[MAETES] ASOEXPEBLA

27.3.2018

Introducción

Código: MAETES

Nombre: ASOEXPEBLA

Descripción:

Datos administrativos:

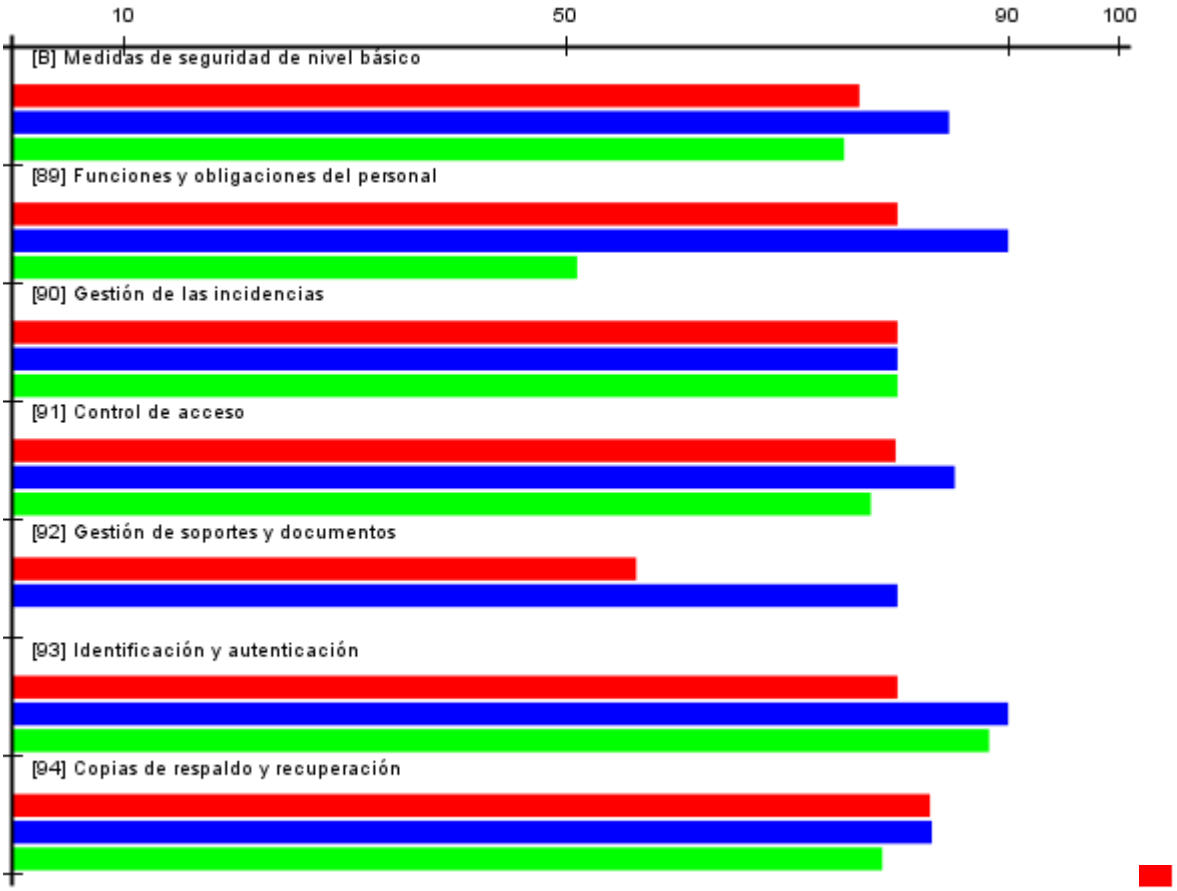
- responsable: Walter Bailón Lourido
- versión: 2
- fecha: 2018

Controles

Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

Medidas de seguridad de nivel básico



[current] situación actual

[target] situación objetivo

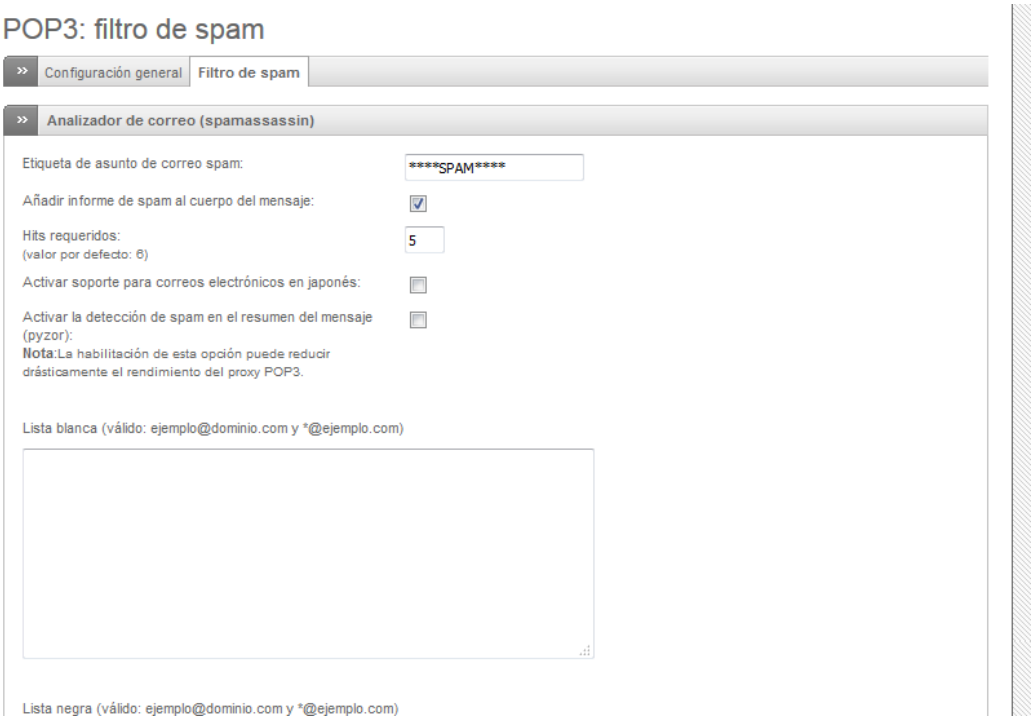
[PILAR] recomendación

dominio de seguridad: [base] Base

control	aplica	current	target	PILAR
[B] Medidas de seguridad de nivel básico	sí	_-L3	L3-L5	L2-L5
[89] Funciones y obligaciones del personal	sí	L3	L4	L2-L3
[90] Gestión de las incidencias	sí		L3	L3
[91] Control de acceso	sí	L2-L3	L3-L5	L3-L4
[92] Gestión de soportes y documentos	sí	L2	L3-L5	n.a.
[93] Identificación y autenticación	sí	L3	L4	L3-L5
[94] Copias de respaldo y recuperación	sí	L3	L3-L5	L3-L4

Fuente: PILAR MICRO (6.3) Herramienta de Análisis de riesgos

Anexo 15



Fuente : empresa auditada

Anexo 16

Lista Negra (Black listing)

		192.168.1.230				
6	acceso denegado	GREEN BLUE	.cangrejas.com .porno.com .poringa.net .lapetardas.com .prialepaste.com .facebook.com .youtube.com .hi5.com .badoo.com .pegateya.com .myspace.com .bravotube.net .redtube.com .tusecreto.com.ar .morbocornudos.com .plus.google.com .play.google.com .googleusercontent.com .windowsupdate.com .skype.com .mixcloud.com .hulkshare.com .dailymotion.com .musicascristianas.net .musicascristianas.online .twimg.com .pornovideosx.xxx .foxmusicagratis.com .foxmusica.net .foxmusica.online .mus7.foxmusica.net .yasuena.com .mus1.foxmusica.net .musicaideal.net .estabulla.com .fullvicio.com .goomusica.com .fbcdn.net .es.bravesporno.com .thm.bravesporno.com .vercomicporno.net .vercomicsporno.com .googlevideo.com .verpornocomic.com .comicspornox.com .comicporno.org .pedofilia.net .comicspornohentai.com	no necesario	Siempre	CUALQUIERA
		192.168.1.2				

Fuente: empresa auditada

Anexo 17

Endian Firewall HTTP Proxy Access Reports

Period: 2018Jan16-2018Jan16
Sort: BYTES, reverse
Topuser

Topsites
Sites & Users
Downloads
Denied

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	exportacion. ex.com.ec	4.52K	229.67M	18.60%	0.52%	99.48%	01:11:59	4.31M	4.06%
2	ex.com.ec	6.70K	157.60M	12.76%	3.35%	96.65%	02:03:00	7.38M	6.93%
3	ana-hp .com.ec	10.45K	153.07M	12.39%	0.21%	99.79%	01:33:45	5.62M	5.28%
4	ex.com.ec	10.53K	88.85M	7.19%	5.10%	94.90%	03:11:07	11.46M	10.77%
5	.com.ec	6.76K	70.42M	5.70%	2.53%	97.47%	01:22:45	4.96M	4.66%
6	.com.ec	4.13K	61.58M	4.99%	2.90%	97.10%	00:44:00	2.64M	2.48%
7	.com.ec	3.51K	57.51M	4.66%	1.79%	98.21%	00:31:54	1.91M	1.80%
8	alexander com.ec	5.79K	48.81M	3.95%	2.22%	97.78%	05:40:43	20.44M	19.20%
9	x.com.ec	4.57K	42.55M	3.45%	4.52%	95.48%	00:35:00	2.10M	1.97%
10	x.com.ec	3.98K	37.43M	3.03%	0.96%	99.04%	00:36:40	2.20M	2.07%
11	192.168.2.100	234	33.10M	2.68%	0.30%	99.70%	02:27:12	8.83M	8.29%
12	om.ec	1.73K	22.91M	1.86%	3.43%	96.57%	00:10:20	620.77K	0.58%
13	jfrio. .com.ec	3.64K	21.69M	1.76%	1.92%	98.08%	00:15:41	941.76K	0.88%
14	jmantenimiento. .com.ec	4.78K	20.71M	1.68%	4.50%	95.50%	00:39:22	2.36M	2.22%
15	.com.ec	2.18K	20.10M	1.63%	1.58%	98.42%	00:11:39	699.30K	0.66%
16	lap-compaq. x.com.ec	205	19.15M	1.55%	0.21%	99.79%	00:05:57	357.94K	0.34%
17	auxconta5. .com.ec	2.89K	18.62M	1.51%	26.80%	73.20%	00:14:49	889.40K	0.84%
18	dmedico. .com.ec	1.65K	16.03M	1.30%	2.15%	97.85%	00:21:07	1.26M	1.19%
19	gme x.com.ec	1.58K	14.77M	1.20%	0.50%	99.50%	00:06:36	396.05K	0.37%
20	x.com.ec	484	13.14M	1.06%	1.00%	99.00%	00:03:56	236.49K	0.22%
21	auxiliar2TH.mardex.com.ec	1.59K	12.67M	1.03%	3.14%	96.86%	00:12:11	731.57K	0.69%
22	ssa x.com.ec	1.02K	11.98M	0.97%	4.70%	95.30%	00:09:43	583.53K	0.55%

Fuente: empresa auditada

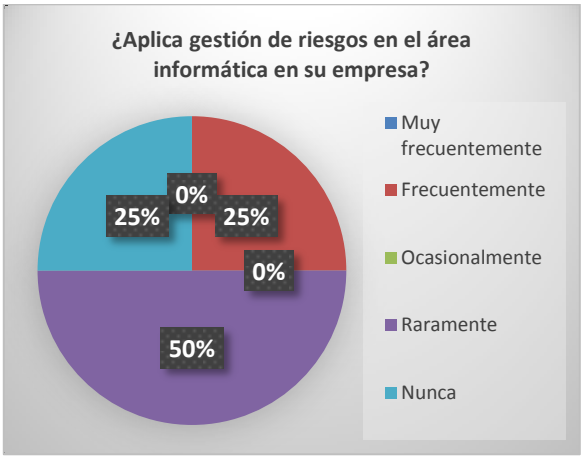
Anexo 18

Encuesta dirigida a los jefes o administradores del área informática sobre la gestión de riesgos, en las empresas exportadoras de pesca blanca de las ciudades de Manta y Jaramijó.

¿Aplica gestión de riesgos en el área informática en su empresa?

Muy Frecuentemente ☐ Frecuentemente ☐ ocasionalmente ☐ raramente nunca ☐

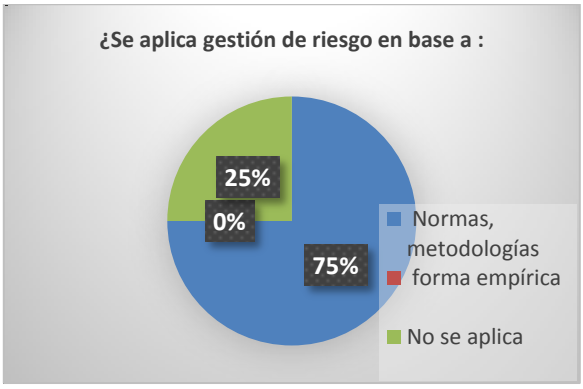
Como se puede observar , el 50% de las empresas raramente aplican gestión riesgos, un 25% no ha aplicado y el restante 25% frecuentemente.



¿Se aplica gestión de riesgo en base a :

Normas, metodologías ☐ forma empírica ☐ no se aplica ☐

S se aprecia, que el 75% de las empresas aplican la gestión de riesgos en base a normas o metodologías, y un 25% no aplica.



¿Conoce Ud. las normas, métodos, herramientas que se pueden aplicar en la gestión de riesgos, en su empresa? Marque las que conoce

ISO 27001 ☐ ISO 27005 ☐ ISO 31000 ☐

MAGERIT ☐ OCTAVE ☐ NIST SP 800-30 ☐

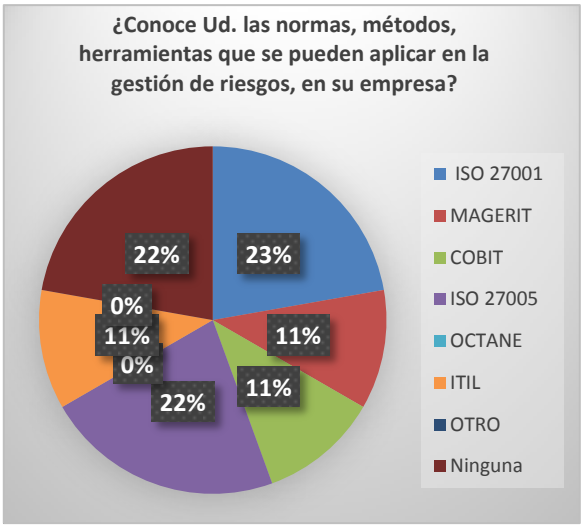
COBIT ☐ ITIL ☐

OTRO ☐

Mencione_____

Ninguna ☐

Entre las normas y metodologías conocidas por los directores de TI, se puede apreciar que; ISO 27001, ISO 27005 ocupan entre un 23% y 22% de ser conocidas; un 22% no tiene conocimiento de metodologías, y en el rango del 11%.

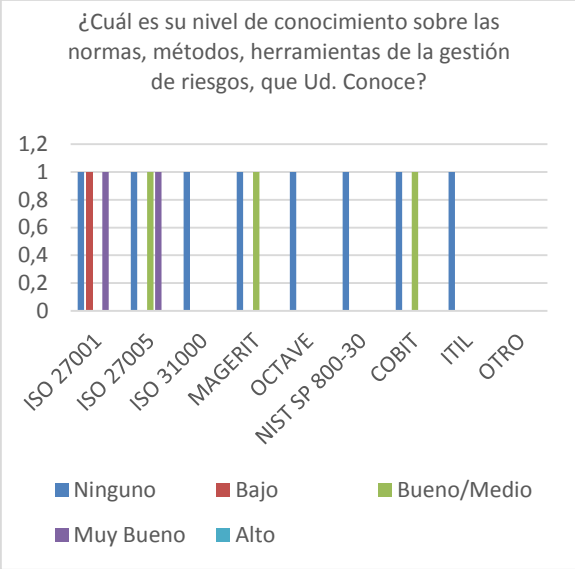


¿Cuál es su nivel de conocimiento sobre las normas, métodos, herramientas de la gestión de riesgos, que Ud. conoce? (siempre y cuando haya escogido o mencionado por lo menos una)

	Ninguno	Bajo	Bueno/Medio	Muy Bueno	Alto
ISO 27001	☐	☐	☐	☐	☐
ISO 27005	☐	☐	☐	☐	☐
ISO 31000	☐	☐	☐	☐	☐
MAGERIT	☐	☐	☐	☐	☐
OCTAVE	☐	☐	☐	☐	☐
NIST SP 800-30	☐	☐	☐	☐	☐
COBIT	☐	☐	☐	☐	☐
ITIL	☐	☐	☐	☐	☐

OTRO ☐ ☐ ☐ ☐ ☐

Los resultados se explican de la siguiente manera, que del total de encuestados, uno tiene conocimientos muy buenos de las normas ISO 27001 e ISO 27005, Bueno/Medio de MAGERIT y COBIT, otro tiene un conocimiento Bueno/Medio de ISO 27005 y bajo de ISO 27001. Los dos restantes no tienen ningún conocimiento de las normas, metodologías o herramientas de gestión de riesgo.



¿De las normas, métodos, herramientas anteriormente descritas, cual(es) aplica en la gestión de riesgo de su empresa? Marque la(s) que utiliza

ISO 27001 ☐ ISO 27005 ☐ ISO 31000 ☐

MAGERIT ☐ OCTAVE ☐ NIST SP 800-30 ☐

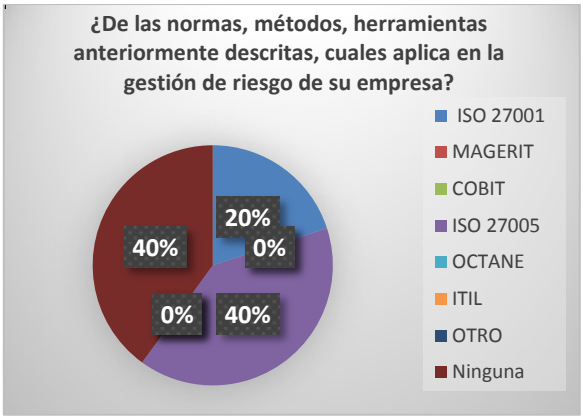
COBIT ☐ ITIL ☐

OTRO ☐

Mencione_____

Ninguna ☐

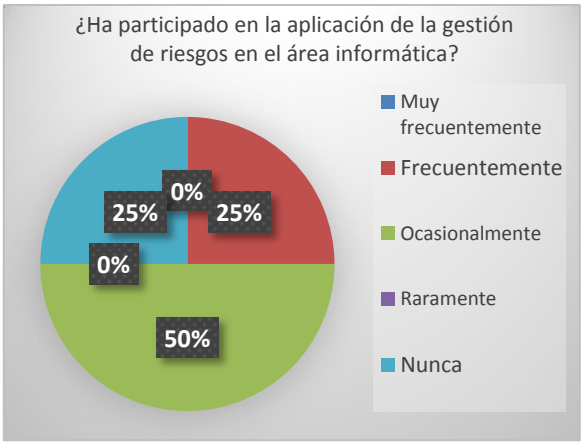
En un 40% de las empresas se aplica la norma ISO 27005, un 20% en conjunto con la norma anterior aplica la norma ISO 27001 y un 40% no aplica ninguna norma o metodología, como en puede en el siguiente gráfico.



¿Ha participado en la aplicación de la gestión de riesgos en el área informática?

Muy frecuentemente☐ Frecuentemente☐ Ocasionalmente☐ Raramente☐ Nunca☐

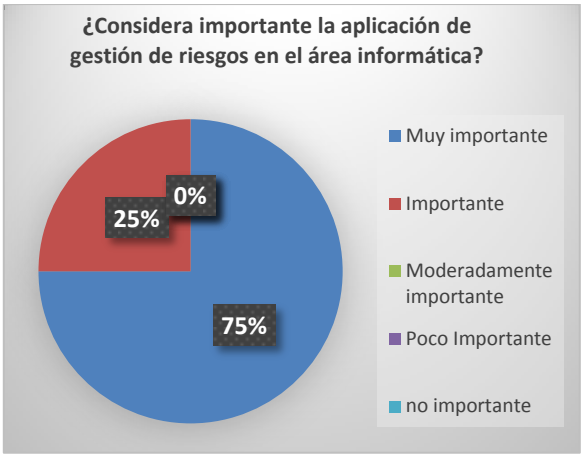
Se aprecia que un 50% de los directores de TI han trabajado ocasionalmente en la gestión de riesgos, un 25% frecuentemente y un 25% nunca ha trabajado.



¿Considera importante la aplicación de gestión de riesgos en el área informática?

Muy importante☐ importante☐ moderadamente importante☐ poco importante☐ no importante☐

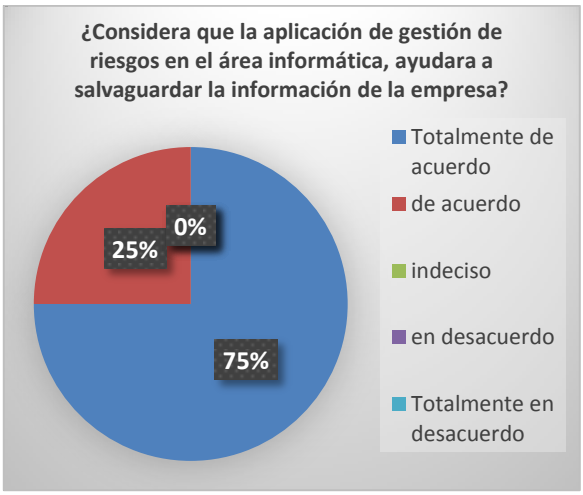
En 75% consideran importante la aplicación de la gestión de riesgos, y el 25% importante, ver Figura 9.



¿Considera que la aplicación de gestión de riesgos en el área informática, ayudara a salvaguardar la información y demás activos de la empresa?

Totalmente de acuerdo☐ de acuerdo☐ indec☐ en desacuerdo☐ totalmente en ☐ desacuerdo

Se puede apreciar que un 75% de los directores de los departamentos de TI, están totalmente de acuerdo en que la gestión de riesgos ayuda a salvaguardar la información; un 25% está de acuerdo.



¿Los directivos de la empresa consideran la gestión de riesgos en el área informática, dentro de sus planes de dirección ?

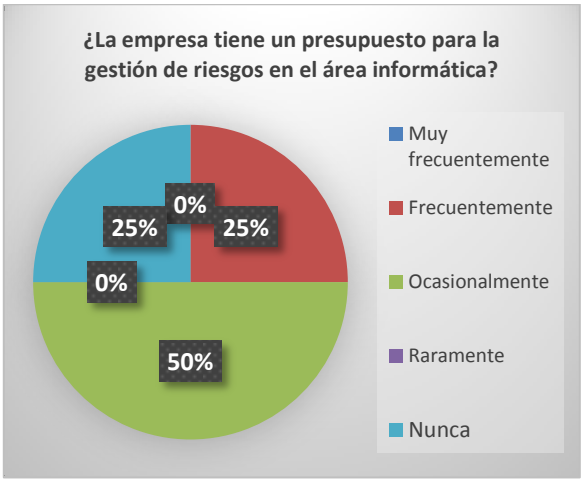
Muy frecuentemente☐ Frecuentemente☐ Ocasionalmente☐ Raramente☐ Nunca☐

Se observa, que solo un 25%, de los encuestados consideran frecuentemente la gestión de riesgos en el área informática de la empresa, otro 25% raramente, y el 50% restante ocasionalmente.

¿La empresa cuenta con un presupuesto para la gestión de riesgos en el área informática?

Muy frecuentemente ☐ Frecuentemente ☐ Ocasionalmente ☐ Raramente ☐ Nunca ☐

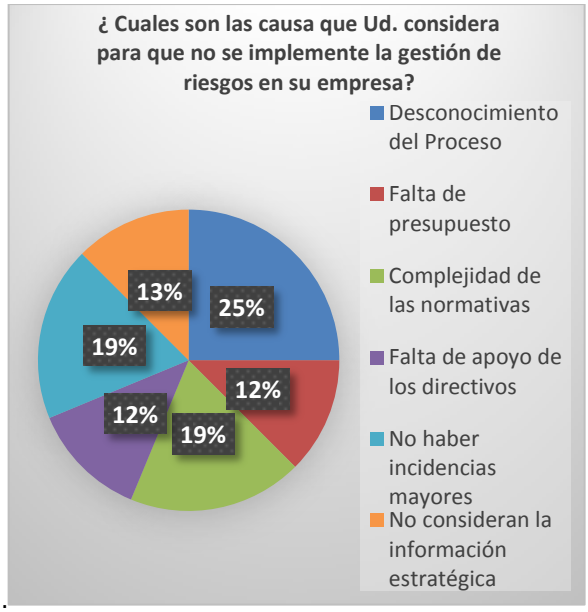
Se puede apreciar que del 100% de las empresas evaluadas, solo un 25% designa frecuentemente presupuesto para la gestión de riesgos, un 50% ocasionalmente y el restante 25% nunca.



¿ Cuales son las causas que Ud. considera para que no se implemente la gestión de riesgos en una empresa?

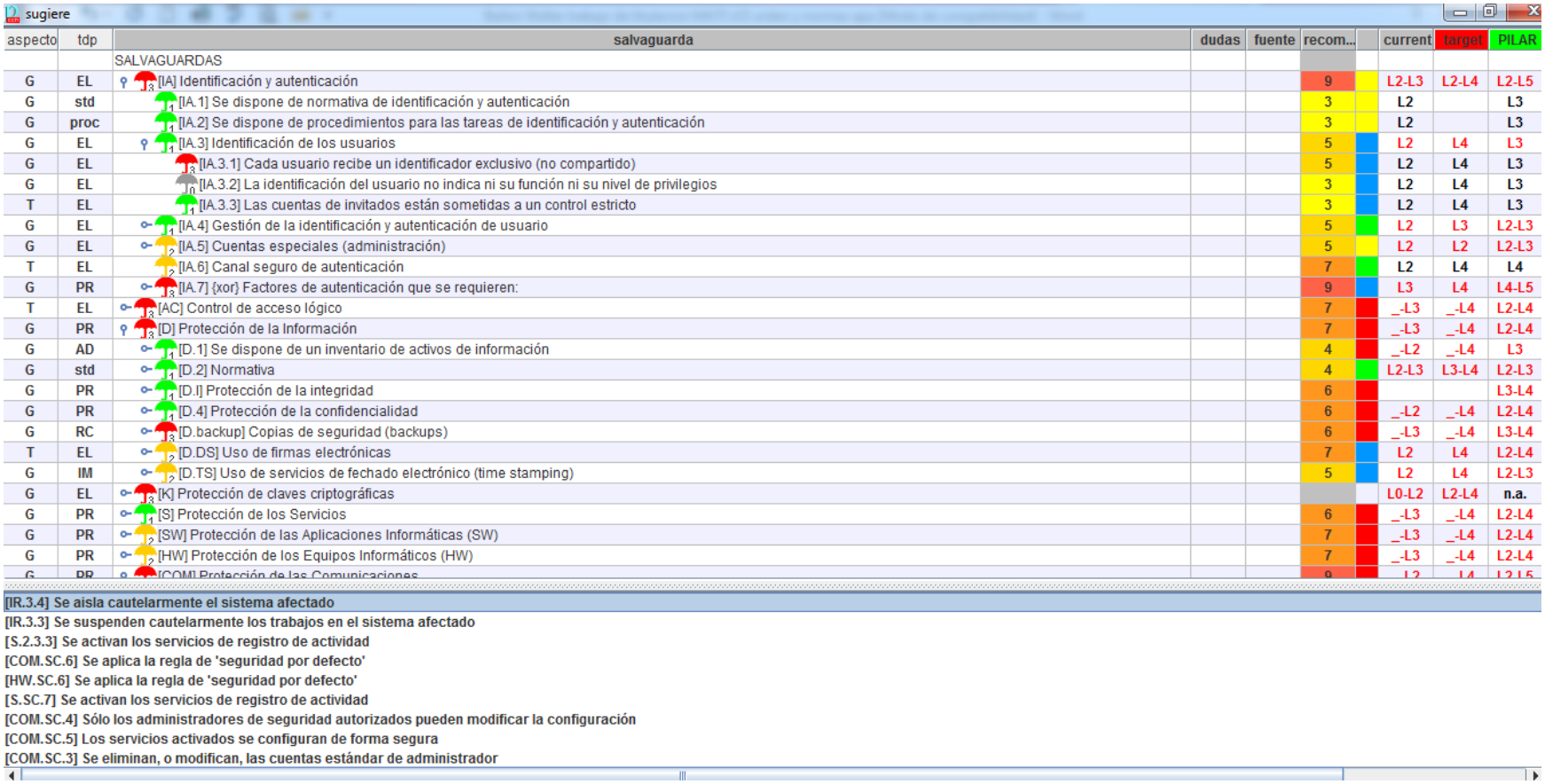
☐ Desconocimiento del proceso
☐ Falta de apoyo de los directivos
☐ Falta de presupuesto
☐ No haber incidencias mayores
☐ Complejidad de las normativas
☐ No consideran la información estratégica

Entre las causas que se consideran que no se implementen gestión de riegos en las empresas objetos de este estudio, se aprecia, que el desconocimiento del proceso es la principal limitante, seguida por la complejidad de las normativas y no haber incidencias mayores, en menor medida los directivos no consideran la información estratégica, la falta de presupuesto y considera la falta de apoyo de los directivos.


¿ Cuales son las causa que Ud. considera para que no se implemente la gestión de riesgos en su empresa?
Desconocimiento del Proceso
Falta de presupuesto
Complejidad de las normativas
Falta de apoyo de los directivos
No haber incidencias mayores
No consideran la información estratégica
25%
12%
19%
12%
19%
13%

.

Anexo 19
Salvaguardas sugeridas por el PILAR



sugiere

aspecto	tdp	salvaguarda	dudas	fuente	recom...		current	target	PILAR
		SALVAGUARDAS							
G	EL	[IA] Identificación y autenticación			9		L2-L3	L2-L4	L2-L5
G	std	[IA.1] Se dispone de normativa de identificación y autenticación			3		L2		L3
G	proc	[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación			3		L2		L3
G	EL	[IA.3] Identificación de los usuarios			5		L2	L4	L3
G	EL	[IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)			5		L2	L4	L3
G	EL	[IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios			3		L2	L4	L3
T	EL	[IA.3.3] Las cuentas de invitados están sometidas a un control estricto			3		L2	L4	L3
G	EL	[IA.4] Gestión de la identificación y autenticación de usuario			5		L2	L3	L2-L3
G	EL	[IA.5] Cuentas especiales (administración)			5		L2	L2	L2-L3
T	EL	[IA.6] Canal seguro de autenticación			7		L2	L4	L4
G	PR	[IA.7] {xor} Factores de autenticación que se requieren:			9		L3	L4	L4-L5
T	EL	[AC] Control de acceso lógico			7		_-L3	_-L4	L2-L4
G	PR	[D] Protección de la Información			7		_-L3	_-L4	L2-L4
G	AD	[D.1] Se dispone de un inventario de activos de información			4		_-L2	_-L4	L3
G	std	[D.2] Normativa			4		L2-L3	L3-L4	L2-L3
G	PR	[D.I] Protección de la integridad			6				L3-L4
G	PR	[D.4] Protección de la confidencialidad			6		_-L2	_-L4	L2-L4
G	RC	[D.backup] Copias de seguridad (backups)			6		_-L3	_-L4	L3-L4
T	EL	[D.DS] Uso de firmas electrónicas			7		L2	L4	L2-L4
G	IM	[D.TS] Uso de servicios de fechado electrónico (time stamping)			5		L2	L4	L2-L3
G	EL	[K] Protección de claves criptográficas					L0-L2	L2-L4	n.a.
G	PR	[S] Protección de los Servicios			6		_-L3	_-L4	L2-L4
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)			7		_-L3	_-L4	L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)			7		_-L3	_-L4	L2-L4
G	PR	[COM] Protección de las Comunicaciones			9		L2	L4	L2-L5

[IR.3.4] Se aisla cautelarmente el sistema afectado
[IR.3.3] Se suspenden cautelarmente los trabajos en el sistema afectado
[S.2.3.3] Se activan los servicios de registro de actividad
[COM.SC.6] Se aplica la regla de 'seguridad por defecto'
[HW.SC.6] Se aplica la regla de 'seguridad por defecto'
[S.SC.7] Se activan los servicios de registro de actividad
[COM.SC.4] Sólo los administradores de seguridad autorizados pueden modificar la configuración
[COM.SC.5] Los servicios activados se configuran de forma segura
[COM.SC.3] Se eliminan, o modifican, las cuentas estándar de administrador