Revista Peruana de Computación y Sistemas 2018 1(1):47-56
http://dx.doi.org/10.15381/rpcs.v1i1.14856

ISSN Online: 2617-2003
Facultad de Ingeniería de Sistemas e Informática
Universidad Nacional Mayor de San Marcos

Artículo de Contribución

Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas

Information security risk management model for Peruvian PYMES

Johari C. García Porras[1]*, Sarita C. Huamani Pastor[2], Rómulo F. Lomparte Alvarado[3]

Facultad de Ingeniería de Sistemas de Información, Universidad Peruana de Ciencias Aplicadas.

[1] u201221820@upc.edu.pe, [2] u201416049@upc.edu.pe, [3] pcsirlom@upc.edu.pe

* Autor para correspondnecia

Resumen

Hoy en día, las empresas tratan de proteger su activo muy valioso, la información, para lo que recurren a la gestión de sus riesgos, tratando de evitar situaciones negativas tales como pérdidas financieras significativas, violación de la confidencialidad de información sensible, pérdida de integridad o disponibilidad de datos confidenciales. En organizaciones como las PYMES no se implementan modelos de gestión de riesgos debido a que estas organizaciones no consideran relevante la seguridad de la información, ya que no se encuentra dentro de lo presupuestado. Existen diferentes enfoques de riesgos, pero, generalmente dirigidos a grandes empresas; para las PYMES es más adecuado emplear un enfoque cualitativo. Este trabajo presenta un modelo de gestión de riesgos basado en la metodología OCTAVE-S y la norma ISO/IEC 27005, consta de las 3 fases de OCTAVE al que se le añade la lista de vulnerabilidades y escenarios en la fase 1, además el cálculo y tratamiento del riesgo de la ISO/IEC 27005 en la última fase. Asimismo, el modelo adopta un enfoque cuantitativo que permite calcular el riesgo residual con base en la efectividad de los controles otorgados, de este modo se logra brindar un modelo adecuado para las organizaciones. El modelo propuesto fue implementado en el proceso de ventas de una PYME peruana del sector cerámicos, demostrando un fácil uso, y logrando identificar los controles necesarios para reducir el riesgo, cuya implementación podría reducir el riesgo en un 53%.

Palabras clave: Gestión de riesgos; Seguridad de la Información; Pymes; OCTAVE; ISO/IEC 27005.

Abstract

Nowadays, companies seek to protect their information because it is a very valuable asset. In order to protect it, it is necessary to manage the risks, which will prevent scenarios that generate a negative impact such as significant financial losses, violation of the confidentiality of sensitive information, loss of integrity, or the availability of confidential information. Organizations such as SMEs do not implement risk management models because they do not care about allocating a budget for information security. There are different approaches that are used to manage the risks, but, in general, these focus on big companies. However, those that target SMEs have a qualitative approach. This paper presents a suitable risk management model, based on the OCTAVE-S methodology and the standard ISO/IEC 27005, it consists of the 3 phases of OCTAVE to which is added the list of vulnerabilities and scenarios in phase 1, as well as the calculation and treatment of the risk of ISO/IEC 27005 in the last phase. Likewise, the model takes a quantitative approach that allows to calculate the residual risk based on the effectiveness of the controls given, creating a suitable model for the organizations, in order to and, therefore, to facilitate decision making. This model has been applied in a Peruvian clay-ceramic industry SME in its sales process, showing its easy use and managing to identify the necessary controls to reduce the risk, whose implementation could reduce the risk by 53%.

Keywords: Risk Management; Security Information; SMES; OCTAVE; ISO/IEC 27005.

Correspondencia:
Nombre: Johari C. García Porras
Dirección: Facultad de Ingeniería de Sistemas de Información, Universidad Peruana de Ciencias Aplicadas, Av. Salaverry 2255, Lima, Perú.

Recibido 28/02/2018 - aceptado 09/03/2018

Citar como:
García J, Huamani S, Lomparte R. Modelo de Gestión de Riesgos de Seguridad de la Información para PYMES peruanas.
Revista Peruana de Computación y Sistemas 2018 1(1):47-56. http://dx.doi.org/10.15381/xxxxxxs

1. Introdución

A medida que los sistemas de información se están incrementando en los negocios, el impacto del riesgo cada vez se ha vuelto más costoso, ya que no se realiza una adecuada gestión de riesgos [1]. Por ejemplo, un estudio realizado por la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) indican que, en el 2016, alrededor del mundo se estimó una pérdida de $575 mil millones por incidencias de seguridad de la información. Mientras que, en el Caribe y Sudamérica, se estimó una perdida entre $90 y 180 mil millones [2]. En otro estudio realizado por Digiware estimó que en Perú el impacto económico fue alto, de $ 4 mil millones, por lo que la gestión de riesgos debería ser considerado un tema más serio dentro de las empresas [3]. En un estudio de Ernst & Young del 2015, el 100% de los encuestados indican que su actual esquema de seguridad de información no cubre plenamente las necesidades de su organización, de este mismo estudio el 41% de empresas consideran que poseen probabilidades mínimas para detectar un ataque sofisticado. Admitieron que el motivo principal que dificulta la efectividad de la seguridad de la información se debe en un 100% a restricciones presupuestarias y en un 89% a la falta de recursos especializados, respectivamente [4].

La protección adecuada de la información exige que las empresas primero determinen los riesgos a los cuales están expuestas, para ello lo recomendable es adoptar un enfoque de gestión de riesgos, metodología, marcos de referencia o estándares de análisis de riesgo para la seguridad de la información, tal como la norma ISO/IEC 27005 “Gestión de Riesgos de Seguridad de la Información” [2].

Desde hace una década, las empresas que tienen muchos intercambios de datos con otras empresas (nacionales o internacionales) o con muchos socios y clientes, han experimentado la necesidad de acordar normas para asegurar la información y los procesos de intercambio. Es precisamente establecer una marca de confianza para la seguridad general de la información dentro de las empresas lo que condujo a la creación de la norma ISO / IEC 27005 [5].

Hoffman, Kiedrowicz, & Stanik señalan que la gestión de riesgos se convierte en un elemento importante de la gestión estratégica de las empresas y, en muchos casos, son cruciales para racionalizar las actividades comerciales y continuar las operaciones. Además, indican que para gestionar correctamente el riesgo de la organización es necesario conocer el papel de la gestión de riesgos [6].

La ISO/IEC 27005 es una norma Internacional que proporciona directrices para la gestión del riesgo de seguridad de la información en una organización, apoyando en particular los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001 [7]. Dado que la norma ISO/IEC 27005 no proporciona una metodología para desarrollar la gestión de los riesgos, la organización debe adaptar el mejor enfoque de análisis de riesgos. El propósito de cualquier análisis de riesgos es proporcionar la mejor información posible sobre la probabilidad de pérdida a los que toman las decisiones [8]. Asimismo, Pacheco indica que la seguridad de la información es un aspecto clave en el funcionamiento de toda organización y es por ello que se requiere profesionales capacitados a la altura de las exigencias del mercado corporativo [9].

Se sugiere el empleo de la metodología OCTAVE, ya que proporciona un análisis de riesgo y evaluación más detallados [10], involucrando todos los aspectos necesarios para una gestión de riesgos, incluyendo a las personas, lo que ninguna metodología actualmente realiza. Específicamente, se sugiere usar el método OCTAVE-S, el cual es implementado dentro de pequeñas o medianas empresas tal como lo es la empresa del caso de estudio.

El presente artículo presenta la integración de la metodología OCTAVE-S con la norma ISO/IEC 27005, para desarrollar un modelo de gestión de riesgos que permita realizar un análisis de gestión de riesgos de seguridad de la información conforme a lo requerido por la norma ISO, el cual ha sido aplicado al proceso de ventas de una empresa de producto de arcilla cerámica. Dicho modelo no solo tiene un enfoque cualitativo sino también cuantitativo, ya que permite calcular el riesgo residual en base a la efectividad de los controles otorgados, es importante tener un modelo completo que indique cual es el valor del riesgo residual luego de aplicar los controles. Para este caso, el nombre de la empresa donde se validó el modelo no será revelado por motivos de seguridad. En la sección 2 se detalla el estado del arte, en la sección 3 se explica el modelo basado en la metodología OCTAVE-S y la norma ISO/IEC 27005, en la sección 4 se explica la validación del modelo. Finalmente, en la sección 5 se detallan las conclusiones.

2. Revisión Literaria

Los enfoques existentes para el análisis de riesgos pueden agruparse en tres categorías principales: los enfoques cuantitativos, los enfoques cualitativos y la combinación de enfoques cuantitativos y cualitativos [1].

Los enfoques cuantitativos se basan en modelos matemáticos y estadísticos para representar el riesgo. En un estudio realizado por Mouna, Latifa & Ridha proponen un modelo sistemático, extensible y modular con el objetivo de ayudar a los gerentes a evaluar con precisión las amenazas de seguridad. Dicho modelo cuantifica el costo de la pérdida que resulta de las amenazas y vulnerabilidades teniendo de esta manera los gerentes una visión más detallada de los costos [11]. En otro estudio realizado por Feng, Harry & Li proponen un modelo de análisis de riesgo de seguridad integrado con Redes Bayesianas (BNs) y optimización de colonia de hormigas, para poder desarrollar la red bayesiana se tiene que integrar las bases de datos de casos observados con expe-

riencia y conocimiento de expertos con la finalidad de representar los factores relacionados al riesgo y mecanismos causales [1].

Mientras que el enfoque cualitativo clasifica al riesgo como alto, medio o bajo. El enfoque cualitativo puede representar mejor el riesgo a diferencia de los enfoques cuantitativos. En un estudio realizado por Shedden y otros proponen un modelo de enfoque cualitativo llamado método de descripción rica (RDM) el cual adopta una visión menos formal y más integrada de los activos de información y conocimiento que existen en los ambientes de trabajo modernos. Este método propuesto utiliza técnicas de análisis y recopilación de datos más relevantes de metodologías cualitativas; y se basa en la distinción entre los aspectos formales e informales de las organizaciones y como se estos se relacionan [12].

Hakemi, y otros plantean un modelo cualitativo llamado EVAO que resulta ser la mejora de la metodología VECTOR mediante la adaptación de OCTAVE para en análisis de proceso de migración de software. Dicho modelo permite a los usuarios cuantificar y representar visualmente todos los aspectos posibles del riesgo para el sistema empresarial [10]. Shamala, Ahmad & Yusoff plantean un modelo basado en la combinación de 6 metodologías con enfoque cualitativo identificando las características mutuas, su modelo propuesto es para cualquier organización, independiente de su tamaño, indican también que los involucrados en realizar el análisis del riesgo deben tener la habilidad, calificación, experiencia y formación requerida [13]. Beranek sugiere un modelo cualitativo basado en la integración de dos metodologías FRAPP y BITS, teniendo como metodología base a BITS. En esta integración, el autor utiliza la evaluación de los activos de FRAPP y para el resto del proceso de análisis se basa en BITS [14].

Debido a las fortalezas y debilidades tanto de las evaluaciones cuantitativas como cualitativas, existe un enfoque híbrido. De esta manera, la organización puede beneficiarse de la sencillez y rapidez de las evaluaciones cualitativas, aprovechando al mismo tiempo la valoración cuantitativa de sus activos más críticos [15]. Un estudio indica que los métodos cuantitativos pueden no ser capaces de modelar escenarios de riesgo complejos en la actualidad [16].

Los métodos de análisis de riesgos basados en medidas cualitativas son más adecuados para el complicado entorno de riesgo de los sistemas de información actuales. Sin embargo, una debilidad significativa del método de análisis cualitativo es el criterio de riesgo de aquellos que crean resultados inestables [16]. En otro estudio se menciona que las métricas de seguridad son más comúnmente cualitativas que cuantitativas [17]. Por su parte, Chanchala y Umesh plantean un modelo para el entorno de red de una Universidad basado en OCTAVE, con el fin de reducir el riesgo de incumplimiento de la seguridad mediante el apoyo a actividades. La primera fase evalúa las amenazas y vulnerabilidades con el fin de identificar el punto débil, la segunda fase se centra en el riesgo más alto y crear un plan de mitigación y la tercera fase reconoce el requisito de cumplimiento de la gestión de la vulnerabilidad para mejorar la seguridad de la Universidad. Su objetivo es medir cuantitativamente el nivel de riesgo que permitirá a los institutos de educación superior entender los riesgos de seguridad de la información [18].

Montenegro y Moncayo proponen un modelo hibrido conformado por la ISO 27005, OCTAVE-S y MAGERIT que tienen el enfoque cualitativo y para el enfoque cuantitativo se basa en el modelo IFRS (International Financial Reporting Standard). Dicho modelo fue aplicado a dos PYMES ecuatorianas, con el objetivo de generar una solución práctica de un problema de gestión de TI para lo cual se necesita el diseño formal y un proceso de evaluación que asegure la calidad de la solución [19]. En otro estudio realizado por Faris, Ghazouani, Medroni & Sayouti desarrollan un modelo con enfoque hibrido que propone una formulación matemática del riesgo utilizando un menor nivel de granularidad de sus elementos tales como amenaza, probabilidad, criterios para determinar el valor de un activo, la exposición, la frecuencia y la medida de protección. Para el enfoque cualitativo hicieron uso de encuestas y cuestionarios internos para lograr la recolección de datos [20].

3. Propuesta de Modelo de Gestión de Riesgos de Seguridad de la Información

3.1. Modelo de Gestión de Riesgos de Seguridad de la Información

El modelo permite a la organización conocer más sobre sus activos y sobre los riesgos que estos tienen, ya que son los expertos del proceso quienes participan. Además, permite a las PYMES cuantificar el valor del riesgo de sus activos y entender la causa de las vulnerabilidades, asimismo brindar controles necesarios para poder contrarrestar posibles riesgos. Dicho modelo cuenta con las 3 fases de OCTAVE-S (Construcción de perfil de amenazas, identificar vulnerabilidades de infraestructura y planes y estrategias de seguridad) y los procesos de la norma ISO/IEC 27005 (Identificación del riesgo, estimación del riesgo, evaluación del riesgo, tratamiento y aceptación del riesgo), para esto se realizó un análisis de ambas resaltando sus bondades y características en común para poder contar con todos los componentes necesarios de una gestión de riesgos (activos, amenazas, vulnerabilidades, riesgos y controles). En la Figura 1, se observa el modelo propuesto con las fases de OCTAVE-S y los procesos de la ISO/IEC 27005.

Como se puede observar en la Fig. 1, el modelo muestra la relación de OCTAVE-S y la ISO/IEC 27005. La fase 1 indica que se debe realizar la generación de perfil de amenazas basados en los activos de la empresa, añadiéndose la lista de vulnerabilidades y escenarios de la ISO/IEC 27005, la fase 2 indica que se debe identificar las vulnerabilidades de infraestructura y finalmente la fase 3 indica que se debe desarrollar estrategias y planes de seguridad. Es dentro de esta fase, donde se añade

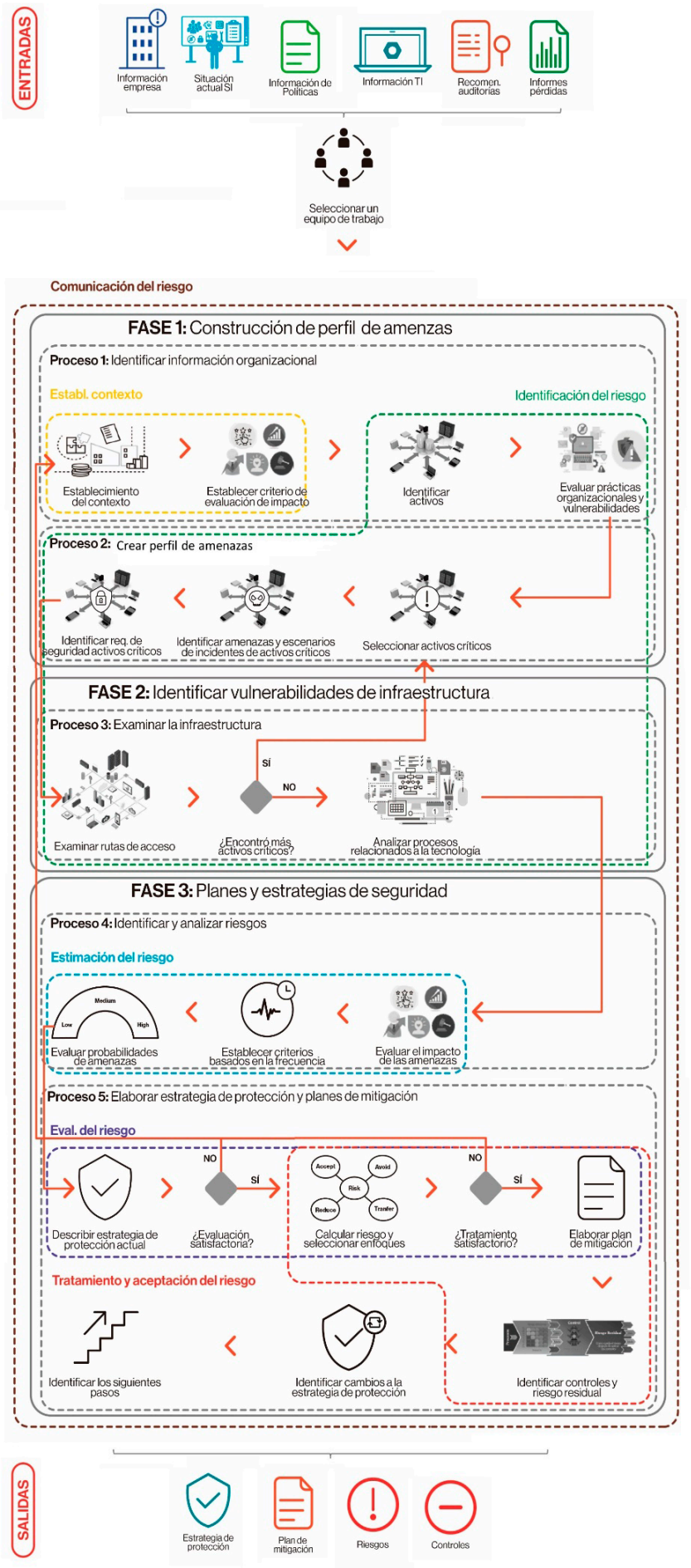

Fig. 1: Modelo de Gestión de Riesgos de Seguridad de Información

el tratamiento y aceptación del riesgo de la norma ISO/IEC 27005 y también donde se calcula el riesgo residual logrando un modelo adecuado para las organizaciones.

La propuesta del modelo incluye el cálculo del riesgo, riesgo residual ayudando a las organizaciones tener una visión global sobre sus riesgos, otros autores tales como Chanchala & Umesh (2017), Montenegro & Moncayo (2016) y Faris, Ghazouani, Medromi, & Sayouti (2014) en sus modelos planteados no calculan el riesgo ni el valor del riesgo residual.

3.2. Fases del Modelo de Gestión de Riesgos de Seguridad de la Información

Antes de iniciar con las fases del modelo, se debe seleccionar un equipo de trabajo que participe en el análisis de riesgo, para poder ejecutar cada proceso, ya que es importante que se cuente con las habilidades y conocimientos suficientes.

El equipo de trabajo debe conformarse entre tres a cinco personas, dentro de las cuales al menos uno de ellos debe ser personal relacionado directamente con el proceso, asimismo deberá tener conocimientos sobre los sistemas relacionados, la información que se maneja, las políticas de la empresa, conocimiento de gestión de riesgos y buenas habilidades blandas.

En este punto, el equipo de trabajo deberá decidir si ejecutará las siguientes fases a toda la empresa, a un área o a un solo proceso crítico.

3.2.1 Fase 1: Construcción de perfil de amenazas

La fase 1 se encarga de construir el perfil de las amenazas, esta fase se compone de dos procesos. El primero es la identificación de información organizacional que se relaciona con el proceso de establecimiento de contexto de la ISO/IEC 27005, este proceso trata de saber cuál es el estado actual de la empresa, asimismo recopilar la información de la empresa para poder entender los procesos que ejecuta, así como su entorno en el que se desarrolla.

En esta fase se define los criterios de impacto, los cuales son finanzas, productividad, vida/salud, multas y reputación teniendo cada uno valores entre 1 al 3. Estos criterios serán usados más adelante en la Fase 3 para calcular el valor cuantitativo del riesgo. Dentro de este proceso, también se realiza la identificación de los activos y si la empresa realiza prácticas de seguridad el cual fue relacionado con el proceso de Identificación del Riesgo de la ISO/IEC 27005.

El segundo proceso que es la creación del perfil de amenaza se ve relacionado con la Identificación del Riesgo, en el cual, de acuerdo a la valoración del activo referente a disponibilidad, integridad y confidencialidad cada uno con valores del 1 al 3, se escogen los activos críticos, los cuales serán usados en las siguientes fases.

Por último, en esta fase se añade la lista de vulnerabilidades y escenarios de la ISO/IEC 27005 que podrían presentarse, es decir se identifican las vulnerabilidades relacionadas a las prácticas de seguridad de la información.

3.2.2 Fase 2: Identificar vulnerabilidades de Infraestructura:

La fase 2 se encarga de identificar los componentes de infraestructura de los activos críticos identificados en la fase 1 de construcción de perfil de amenazas.

Asimismo, también se identifican las vulnerabilidades de estos componentes. Estos deberán colocarse en la lista de vulnerabilidades que brinda la ISO/IEC 27005.

Como se puede apreciar, esta fase solo se compone de un proceso el cual se relaciona con la norma ISO/IEC 27005 con la identificación del riesgo. Si en esta fase se descubren más activos críticos, se deberá regresar al proceso de "Crear perfil de amenaza" de la fase 1.

3.2.3 Fase 3: Planes y estrategias de seguridad:

La fase 3 está compuesta por 2 procesos los cuales son Identificación y Análisis del Riesgo y Elaborar estrategia de protección y planes de mitigación. La identificación y análisis del riesgo considera el proceso de estimación del riesgo de la norma ISO/IEC 27005, es decir, que se evalúa el impacto de las amenazas, la frecuencia con las que ocurren y la probabilidad.

El proceso de Elaborar estrategia de protección y planes de mitigación considera la evaluación del riesgo de la ISO/IEC 27005, se describe la estrategia de protección actual de la empresa y se calcula el valor del riesgo de cada activo. Para ello, primero tenemos que calcular el valor máximo y mínimo de riesgo como menciona la ISO/IEC 27005, según los criterios de impactos ya definidos en la fase 1 (finanzas, productividad, vida/salud, multas y reputación) y las amenazas identificadas durante la evaluación dentro del perfil de riesgos.

Con la información obtenida se logra una matriz donde el mínimo valor del impacto es 5, si todos los impactos son bajos, y máximo de 15, si todos los impactos son altos, al multiplicar la probabilidad por el impacto se genera la Fig. 2.

probabilidad	Amenaza	5	6	7	8	9	10	11	12	13	14	15
	1	5	6	7	8	9	10	11	12	13	14	15
	2	10	12	14	16	18	20	22	24	26	28	30
	3	15	18	21	24	27	30	33	36	39	42	45

Fig. 2: Impacto por Probabilidad

Debido a que solo pueden ocurrir como mínimo 1 amenaza y como máximo 16 según el perfil de riesgo, el valor del riesgo se calcularía usando la fórmula 1:

$$VR = VIP \times CA \quad (1)$$

Donde:

VR: Valor del Riesgo

CA: Cantidad de Amenazas

Por lo que podemos concluir que el valor VIP toma el mínimo valor (5) y solo se manifiesta 1 amenaza, el VR mínimo será 5. De igual forma, el máximo valor del VIP (45) y se manifiestan las 16 amenazas, el VR máximo será 720.

Con los valores de riesgo mínimo y máximo, la empresa podrá definir el rango para el nivel bajo, medio y alto de riesgo.

Para obtener el valor total riesgo de cada activo, solo se deberá multiplicar el impacto de cada amenaza identificada por activo por la probabilidad, y luego sumarlos, así con este valor se podrá identificar en qué nivel se encuentra el riesgo y saber si es bajo, medio o alto según como la empresa lo haya definido como se mencionó anteriormente.

Deberá contemplar una matriz de riesgo para poder mostrar los valores de riesgo según el color verde, para riesgo bajo; color amarillo, para riesgo medio; y color rojo, para riesgo alto. Es decisión de cada empresa cómo realizar su matriz de riesgo.

En este punto la empresa deberá tomar medidas necesarias de cómo abordar el riesgo. En este artículo, se adaptará el enfoque de la ISO/IEC 27005 que indica que para el tratamiento de riesgo existen 4 enfoques los cuales son aceptar, mitigar, transferir y eliminar a diferencia de OCTAVE-S que solo tiene el tratamiento de aceptar o mitigar el riesgo.

Una vez definido el enfoque de tratamiento de riesgo, se tendrá que identificar qué medidas se deberán tomar para reducir el riesgo y llegar al riesgo residual, por lo que se ha empleado la fórmula 2 basada en la efectividad de los controles de la ISO/IEC 27002 y las actividades de mitigación de OCTAVE-S para aquellos riesgos que decidan mitigarse.

$$VRR = VR/VPEA \quad (2)$$

Donde:

VRR: Valor del Riesgo Residual

VPEA: Valor Promedio de Efectividad de Controles

Para poder calcular el VPEA, se calcula del promedio de los valores obtenidos de las multiplicaciones del valor de la periodicidad y el valor de cada uno de los controles. La periodicidad se define con los valores de 1 a 3, donde 1 significa ocasional, 2 es periódico y 3 es permanente. El valor de control se define en el rango de 1 a 4, donde 1 es inexistente, 2 si el control es detectivo, 3 si es correctivo y 4 es preventivo. Si la multiplicación es mayor 9, el valor de la efectividad de controles es 4; si es menor a 9 y mayor igual a 6, es 3; si es menor a 6 y mayor igual a 2, es 2; si es entre 0 y 1, es 1 [21].

Al finalizar, se podrá identificar los cambios necesarios que se debe realizar a la estrategia de protección actual de la empresa para poder contrarrestar los riesgos identificados.

4. Caso de Estudio

4.1. Organización

El modelo se implementó en una PYME peruana del sector arcilla - cerámica para el proceso de ventas. Esta PYME se encarga de la producción y venta de estos productos, ya sea a clientes naturales o clientes corporativos. Específicamente llega a través de tres sectores: retail, tipo depósito y constructoras.

La empresa tiene alrededor de 24 productos en su cartera, los cuales son necesarios para la construcción de viviendas. Dicha empresa peruana no realizaba una gestión de riesgos continuamente, debido al tiempo que este pueda requerir, por no contar un personal especializado para realizarlo y porque su presupuesto era reducido. Debido a esto, la empresa ha sufrido cuantiosas pérdidas económicas y robo de información confidencial, estos datos no serán brindados debido a la confidencialidad de la información.

4.2. Implementación

Se identificó qué personas se iban a relacionar al proyecto para poder brindar la información correspondiente. En este caso, las áreas críticas para evaluar identificados fueron ventas y producción. Considerando que el área de ventas es un proceso core de la empresa, y se tiene que proteger toda la información relacionada al proceso, se decidió implementar el modelo en este proceso.

Dentro del equipo de trabajo seleccionado se encuentra el gerente de administración y finanzas, jefe del área de sistemas, personal de apoyo del área de ventas, así como las autoras de este artículo.

4.2.1Fase 1: Construcción de perfil de amenazas

Para esta fase se necesita como entradas la información de la empresa, información de TI, las recomendaciones de auditorías pasadas enfocadas al proceso a evaluar, las cuales fueron obtenidas con el apoyo del jefe de sistemas.

Siguiendo nuestro modelo planteado, en la fase 1 se encontraron 35 activos, los cuales 9 de estos son activos críticos según su confidencialidad, integridad y

disponibilidad, definidas entre un consenso con el jefe de sistemas y el personal de ventas, ya que es importante tener ambos puntos de vista.

Los activos identificados fueron el software de virtualización, ERP, Computadoras/Laptops, Sistemas operativos, Certificados electrónicos y correo electrónico mostrados en la Tabla 1, cabe mencionar que no se indican los 3 restantes debido a la confidencialidad de los datos.

Tabla 1: *Tabla de activos*

Activos	Disponibilidad	Integridad	Confidencialidad
Software de virtualización	Alto	Alto	Alto
ERP	Alto	Alto	Alto
Computadoras/Laptops	Alto	Alto	Alto
Sistemas opertivos	Alto	Alto	Alto
Certificados electrónicos	Alto	Alto	Alto
Correo Electrónico	Alto	Alto	Alto

Asimismo, se evaluó las prácticas organizacionales encontrando que la mayoría de ellas no están totalmente formalizadas y documentadas, las cuales se encuentran en su mayoría un nivel medio según la información recopilada en las áreas mostradas en la Tabla 2.

Tabla 2: *Tabla evaluación de prácticas organizacionales*

Áreas	Nivel
Concientización de la seguridad y capacitación	Medio
Estrategia de seguridad	Medio
Administración de la seguridad	Medio
Políticas de seguridad y regulaciones	Medio
Administración de seguridad colaborativa	Medio
Plan de contingencia / Recuperación ante desastres	Medio
Control de acceso físico	Medio
Monitoreo y Auditoría de seguridad física	Medio
Administración de sistemas y red	Medio
Monitoreo y Auditoría de seguridad TI	Medio
Autenticación y autorización	Medio
Gestión de la vulnerabilidad	Medio
Cifrado	Bajo
Arquitectura y diseño de seguridad	Medio
Gestión de incidentes	Medio

En esta fase se identifica las amenazas de cada activo, logrando reconocer el siguiente grupo de amenazas como revelación, modificación, pérdida o destrucción e interrupción, tal como se muestra en la Fig. 3.

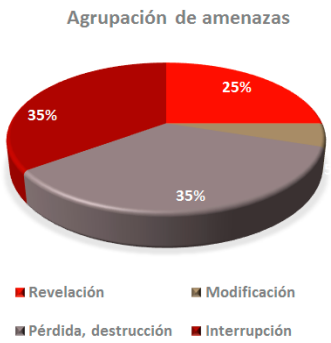

Fig. 3: Agrupación de amenazas

Finalmente, teniendo como salidas la lista de activos ya mencionadas, la lista de vulnerabilidades relacionadas a las prácticas de seguridad de la información, la lista de escenarios, el perfil de las amenazas y criterios de impacto.

De cada amenaza identificada, se identificaron escenarios de incidentes que podrían ocurrir si se presentara la amenaza, los cuales tienen consecuencias en pérdida tiempo operacional, pérdida de tiempo en investigación, reputación de la empresa y tiempo invertido en recuperación de cambios.

4.2.2 Fase 2: Identificar vulnerabilidades de Infraestructura:

Para poder realizar esta fase se necesita tener la información de TI, la lista de activos y la lista de vulnerabilidades de la Fase 1. Como siguiente paso, se procede a identificar los componentes de infraestructura, se identifican cuáles son los más críticos y de estos se encuentra sus vulnerabilidades, en esta fase se descubrió un activo crítico de infraestructura para el proceso de ventas, el cual no había sido identificado en la fase 1. Este activo crítico es el servidor de producción de la empresa, el cual fue añadido a la lista de activos críticos teniendo un total de 10. Algunas de las vulnerabilidades encontradas de los activos y las prácticas de seguridad se muestran en la tabla 3.

Tabla 3: *Tabla de vulnerabilidades*

Vulnerabilidades
Falta de concientización y capacitación formal.
Falta de aprobación de documentos de políticas por gerente.
Falta de validación de concienciación en empleados.
Falta de monitoreo de políticas.
Falta de revisión periódica y comunicación de documentos.
Falta de documentación formal.
Falta de presupuesto para actividades de seguridad.
Falta de proceso formal de gestión de riesgos.
Falta realizar pruebas periódicas correspondientes a los planes.
Falta de gestión adecuada sobre el control de acceso.
Falta de formalización en verificación de los requisitos.
Falta de control por divulgación de información (sanción).
Falta de capacitación sobre el sistema.
Falta de control en la red interna.
Falta de control de filtros de correo electrónico.
Falta de configuración con recomendaciones de seguridad.
Falta de actualización de parches.
Falta de control en medios de almacenamiento.
Falta de control en instalación no autorizada.

Como paso final se agruparon las vulnerabilidades logrando lo siguiente tal como se aprecia en la Fig. 4.

Finalmente, se identificó una lista de escenarios de incidentes con las consecuencias relacionadas. Como salidas se identifica, la lista de vulnerabilidades, la lista de activos críticos de infraestructura.

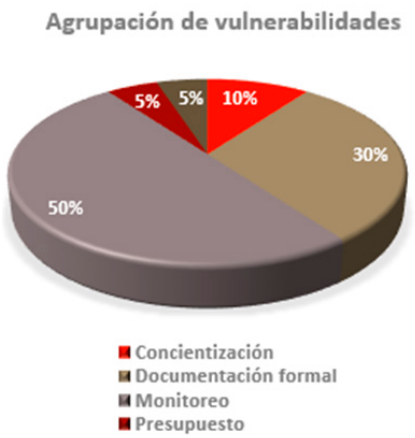

Fig. 4: Agrupación de vulnerabilidades

4.2.3 Fase 3: Planes y estrategias de seguridad

Para esta fase se necesita tener los criterios de impacto, el perfil de amenazas, criterios de probabilidad. Se evaluó el impacto de cada amenaza identificada de cada activo crítico y la probabilidad. Luego de ello se completa como se encuentra la protección en las áreas de prácticas de seguridad de cada activo crítico. Para obtener el nivel de tolerancia de riesgo, el resultado nos devolvió que como mínimo se había completado 1 amenaza y como máximo habían sido 12, por lo que el mínimo nivel del riesgo es 5 y el máximo es 540. De esta forma la empresa definió los rangos donde se especifica el nivel de riesgo tal como se muestra en la Tabla 4.

Tabla 4: *Tabla de nivel de riesgo*

Nivel	Mínimo	Máximo
Bajo	5	100
Medio	101	199
Alto	200	540

Con los valores de la probabilidad y el impacto del riesgo por cada activo crítico se encontraron los siguientes resultados de la Tabla 5.

Tabla 5: *Tabla de valor de riesgos*

Activo	Valor Riesgo
Software de virtualización	216
ERP	208
Computadoras/Laptops	139
Sistemas operativos	85
Certificados electrónicos	68
Correo Electrónico	59

Según lo definido por la empresa el nivel de riesgo por cada activo se muestra en la Tabla 6.

Tabla 6: *Tabla de nivel de riesgo*

Activo	Nivel de Riesgo
Software de virtualización	Alto
ERP	Alto
Computadoras/Laptops	Medio
Sistemas operativos	Bajo
Certificados electrónicos	Bajo
Correo Electrónico	Bajo

Con esta información se procedió a escoger que enfoque debe seguirse, si mitigar, transferir, evitar o eliminar.

La organización decidió mitigar todos los riesgos encontrados, por lo que se le ofrecieron controles para cada uno de ellos obteniendo como riesgo residual. Para esto se propusieron controles de carácter preventivo, correctivo y detectivo tal como se muestra en la Figura 5.

Fig. 5: Agrupación de controles

Algunos de los controles propuestos a la empresa de productos de arcilla cerámica se muestran en la Tabla 7.

Tabla 7: *Tabla de controles propuestos*

Controles propuestos
Formalización y revisión de los documentos relacionados a los planes de recuperación
Revisión ocasional de los documentos formales, y los que no sean formales comunicarlos oportunamente
Acuerdos de confidencialidad o de no divulgación.
Toma de conciencia, educación y formación de la Seguridad de la Información
Protección de la información de registro
Monitorear periódicamente si las políticas están actualizadas y se están cumplimiento, crear indicadores
Incorporar información sobre los planes de BCP, RPD en el programa de capacitación de seguridad
Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Documentar formalmente los procesos, políticas, normas y procedimientos
Capacitación sobre los sistemas a utilizar
Sistema de Gestión de Contraseñas
Registro de eventos realizados por un usuario, logs
Controles de redes
Políticas y procedimientos de transferencia de información
Realizar un proceso formal de gestión de riesgos
Mensajes electrónicos
Análisis y especificación de requisitos de seguridad de la información
Procedimientos de operación documentados
Transferencia de medios de soporte físicos
Restricciones sobre la instalación de Software

Finalmente, con dicha información se pudo elaborar la estrategia de protección, plan de mitigación, la lista de riesgos con prioridad que se obtiene con el valor de riesgo de cada activo, lista de riesgos aceptados definidos por la empresa, la lista de controles e indicadores que se podrían monitorear mostrados en la Tabla 8, según los controles proporcionados para la empresa. Como resultado se calculó el valor del riesgo inherente y residual en la fase 3, así, se obtuvo como resultado la Tabla 9.

Tabla 8: *Tabla de indicadores*

Indicadores
Cumplimiento de gerente en formalización de políticas, procedimientos y planes.
Cumplimiento de revisión semestral de políticas, procedimientos y planes.
Cumplimiento de documentar y firmar acuerdos de confidencialidad.
Entrenamiento en seguridad de la información.
Verificar los incidentes de seguridad de la información de alteración y acceso no autorizado.
Verificar el entrenamiento en seguridad de la información.
Cumplimiento de pruebas de plan de continuidad de negocio y seguridad de la información.
Verificar las juntas con la dirección.
Verificar la capacitación en los sistemas.
Verificar el cumplimiento de realización de proceso de gestión de riesgos.
Cumplimiento de políticas de contraseñas.
Cumplimiento de implementación de logs de auditoría
Cumplimiento de dispositivos según requerimientos de seguridad en redes
Incumplimiento de política de correo electrónico
Cumplimiento de los requerimientos de seguridad de la información en los sistemas
Cumplimiento de medios que cumplen los requerimientos de seguridad de la información
Cumplimiento de política de instalación de software no autorizado

Tabla 9: *Tabla de Riesgo Residual*

Activo	Valor Riesgo	Valor Riesgo Residual	Reducción
Software de virtualización	216	109	50%
ERP	208	101	51%
Computadoras/Laptops	139	60	57%
Sistemas operativos	85	51	40%
Certificados electrónicos	68	23	66%
Correo Electrónico	59	28	53%

Se realizó la matriz de riesgo de acuerdo a los valores de riesgos identificados mostrada en la Figura 6, y la matriz de riesgo residual si la empresa realiza los controles identificados anteriormente mencionados mostrada en la Figura 7.

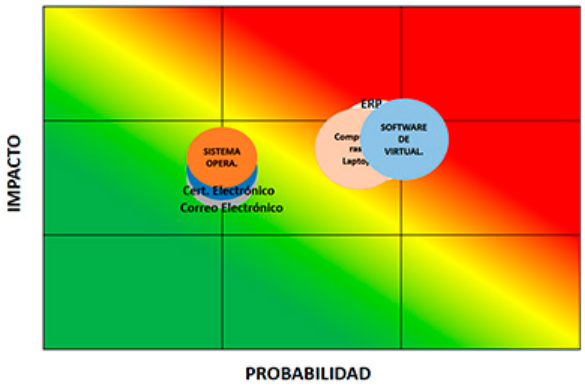

Fig. 6: Matriz probabilidad - impacto Riesgo actual

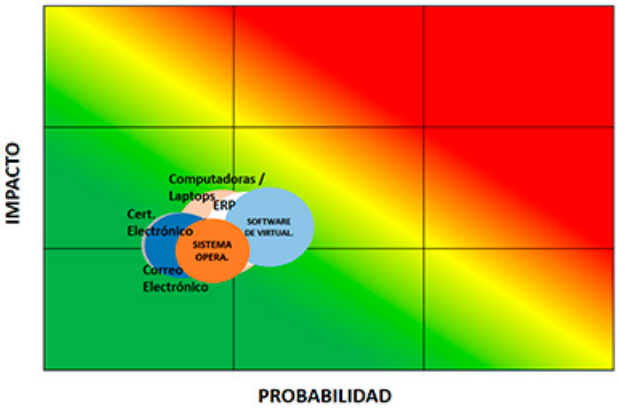

Fig. 7: Matriz probabilidad – impacto Riesgo Residual

Con los valores asignados a los controles identificados se logró calcular el riesgo residual, como se mencionó anteriormente en la propuesta del modelo en la fase 3. En la Tabla 9 se observa el porcentaje de reducción de riesgo, el cual fue calculado según la variación del riesgo actual y el riesgo residual. Con esto se observa que la PYME podría reducir sus riesgos en 53% implementando los controles propuestos.

Realizar un análisis de riesgo les tomaba 2 semanas, con el modelo implementado se logró disminuir 15 horas del tiempo total, logrando una reducción de tiempo en 25% aproximadamente.

Con el modelo implementando se logró capacitar al personal para que puedan realizar un análisis de riesgo regularmente.

5. Conclusiones

En este trabajo se ha propuesto un modelo de Gestión de Riesgos de Seguridad de la Información para PYMES peruanas, que introduce el cálculo del riesgo residual en base a la efectividad de los controles propuestos de la ISO de acuerdo con las amenazas identificadas lo que permite proponer un modelo completamente gratuito para las PYMES.

Los resultados de la implementación del modelo con caso de estudio en una PYME del sector arcilla - cerámica se observa que el nivel de riesgos se reduce en un

53%. Además, se han propuesto a la empresa 17 indicadores para verificar el cumplimiento de los controles.

6. Agradecimiento

Los autores agradecen a la Universidad Peruana de Ciencias Aplicadas por el financiamiento parcial a esta investigación, asimismo a David Mauricio por sus comentarios y recomendaciones.

7. Referencias

[1] N. Feng, J. W. Harry y M. Li, «A security risk analysis model for information systems,» Information Sciences, 2013.

[2] Banco Interamericano de Desarrollo (BID); Organización de los Estados Americanos (OEA), «Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?,» 2016.

[3] Gestión, Perú: pérdidas económicas por ciberdelitos ascienden a más de US$ 4,000 millones, 2016.

[4] Ernst & Young, «A prueba de ataques cibernéticos,» Desde Adentro, 2016.

[5] V. Lalanne, M. Munier y A. Gabillon, «Information Security Risk Management in a World of Services,» IEEE, 2013.

[6] R. Hoffman, M. Kiedrowicz y J. Stanik, «Risk management system as the basic paradigm of the information security management system in an organization,» MATEC Web of Conferences, 2016.

[7] ISO/IEC, Information technology — Security techniques — Information security risk management, 2011.

[8] A. Behnia, R. A. Rashid y J. A. Chaudhry, «A Survey of Information Security Risk Analysis Methods,» Smart Computing Review, vol. 2, pp. 81-94, Febrero 2012.

[9] F. G. Pacheco, «The Need for Formal Education on Information Security,» IEEE LATIN AMERICA TRANSACTIONS, pp. 668-670, Febrero 2013.

[10] A. Hakemi, J. S. Ryul , S. R. Jeong, I. Ghani y M. G. Sanaei, «Enhancement of VECTOR Method by Adapting OCTAVE for Risk Analysis in Legacy System Migration,» KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, pp. 2118-2138, 6 Junio 2014.

[11] J. Mouna, B. A. R. Latifa y K. Ridha, «A Multidimensional Approach Towards a Quantitative,» Procedia Computer Science, pp. 507-514, 2015.

[12] P. Shedden, A. Ahmad, H. Tscherning, W. Smith y R. Scheepers, «Asset Identification in Information Security Risk Assessment: A Business Practice Approach,» Communications of the Association for Information Systems, vol. 39, pp. 297-320, Setiembre 2016.

[13] P. Shamala, R. Ahmad y M. Yusoff, «A conceptual framework of info structure for information security risk assessment (ISRA),» Information security and applications, pp. 45-52, 2013.

[14] L. Beranek, «Risk analysis methodology used by several small and medium enterprises in the Czech Republic,» Information Management & Computer Security, vol. 19, nº 1, pp. 42-52, 2011.

[15] S. S. Alireza, A. B. Rouzbeh y C. Mohamed, «Taxonomy of Information Security Risk Assessment,» Computers & Security, 2015.

[16] A. Behnia, R. A. Rashid y J. A. Chaudhry, «A Survey of Information Security Risk Analysis Methods,» Smart Computing Review, vol. 2, pp. 81-94, Febrero 2012.

[17] A. J. An Wang, Information security models and metrics, 2005.

[18] J. Chanchala y K. S. Umesh, «Information security risks management framework –A step towards mitigating security risks in university network,» Journal of Information Security and Applications, pp. 128-137, 2017.

[19] C. Montenegro y D. Moncayo, «Information Security Risk in SMEs: A Hybrid Model Compatible with IFRS,» de 2016 6th International Conference on Information Communication and Management, 2016.

[20] S. Faris, M. Ghazouani, H. Medromi y A. Sayouti, «Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk,» International Journal of Computer Applications, vol. 103, nº 8, pp. 36-42, Octubre 2014.

[21] SENASA, «Instructivo para identificar, medir, controlar y monitorear los riesgos operacionales,» Costa Rica, 2010.