Revista CIENCIA Y TECNOLOGÍA
ISSN 1810-6781 Rev. Cienc. Tecnol. 18(3): 71- 78, (2022)

Evaluación de riesgos en activos de tecnologías de información en una MIPYME

Risk evaluation in information technology assets in a MIPYME

Pedro Huaman, Liz Sofia Raymunda[1,*]; Rodríguez Novoa, Francisco Elías[2]

[1] Facultad de Ciencias Físicas y Matemáticas, Universidad Nacional de Trujillo, Av. Juan Pablo II s/n – Ciudad Universitaria, Trujillo, Perú.
[2] Facultad de Ingeniería, Universidad Nacional de Trujillo, Av. Juan Pablo II s/n – Ciudad Universitaria, Trujillo, Perú.

* Autor correspondiente: lspedroh@gmail.com (L. Pedro)
DOI: 10.17268/rev.cyt.2022.03.07

RESUMEN

Esta investigación tuvo como objetivo evaluar los riesgos en activos de tecnologías de información en una MiPyme empleando un modelo de evaluación basado en buenas prácticas. El tipo de investigación es descriptiva, y para validar el modelo se empleó el método de juicio de expertos junto coeficiente de concordancia W de Kendall y la prueba Chi-cuadrado. Como resultado, se obtuvo un modelo de evaluación de riesgos que emplea elementos de las metodologías MAGERIT y OCTAVE-S, así como de los estándares internacionales ISO 27005 e ISO 3100. El modelo fue validado y aplicado exitosamente en una MiPyme de transporte urbano de la provincia de Trujillo, donde se identificaron 19 activos críticos; los cuales permitieron identificar 248 riesgos en activos de tecnologías de información, siendo 06 de ellos no aceptables para los cuales se elaboraron 02 planes de tratamiento de riesgos.

Palabras clave: Evaluación de riesgos; activos de tecnologías de información; MiPyme.

ABSTRACT

This research goal was evaluating the risk in the information technology assets in a MiPyme using an evaluation model based on good practices. The research is descriptive, and the proposed model was validated using the expert judgement method with the Kendall's concordance coefficient W and the Chi-square test. As a result, we proposed an information technology asset risk evaluation model using components of the methodologies MAGERIT and OCTAVE-S, and the international standards ISO 27005 and ISO 31000. The model was validated and successfully applied to an urban transportation MiPyme of Trujillo province, there were identified 19 critical assets which allowed to identify 248 potential asset risks of which 06 are not acceptable, for which 02 risk treatment plans were proposed.

Keywords: Risk evaluation; information technology assets; MiPyme.

1. INTRODUCCIÓN

Las organizaciones modernas buscan ofrecer servicios de alta calidad a sus clientes, empleando para ello diversas infraestructuras de tecnologías de información, tales como routers, firewalls, servidores, estaciones de trabajo, protocolos de red y paquetes de software (Wickboldt et al., 2011); las cuales están más que presentes en las actividades cotidianas de las empresas y de las personas debido a soluciones como cloud computing, internet de las cosas, dispositivos móviles, y muchas otras más tecnologías relacionadas al internet; lo que indica que las tecnologías de información se han vuelto omnipresentes y esenciales para cualquier empresa (Barafort et al., 2017). Las tecnologías de información tienen un rol muy importante en todas las organizaciones debido a los importantes beneficios que brindan, pero a la vez esta dependencia las vuelve vulnerables a posibles fallas y ataques (Tøndel et al., 2014).

Según estudio económico realizado por Comisión Económica para América Latina y el Caribe CEPAL (2016), las micro, pequeña y mediana empresas tienen un porcentaje significativo, no solo expresado en números sino en puestos de empleo. Las MiPymes representan el 99.5% del tejido empresarial formal en el Perú; y en el año 2016, las MiPymes emplearon al 59,9% de la PEA ocupada y el 88,8% de la PEA del sector privado (Ministerio de Producción, 2018). Actualmente, las tecnologías de información significan una ventaja competitiva que está siendo adoptada por las micro, pequeña y mediana empresa como fuente de innovación y crecimiento. Las tec-

Fecha de envío: 15-03-2022 Fecha de aceptación: 02-08-2022 Fecha de publicación: 30-09-2022

nologías de información y comunicaciones permiten desarrollar nuevos modelos de negocios en donde las pequeñas unidades económicas juegan un rol cada vez más importante como algunas aplicaciones que nacieron en pequeña escala, y se han desarrollado equiparando oportunidades generando un umbral de crecimiento (Ponce y Zevallos, 2017).

Las pequeñas y medianas empresas tienen problemas y retos diferentes a las grandes empresas debido a fuerzas laborales más pequeñas, menores presupuestos y ambientes computacionales más simples; sin embargo, requieren mejorar sus niveles de servicio para lograr los objetivos del negocio, controlar costos y adaptar su infraestructura tecnológica a sus necesidades (Cruz-Hinojosa y Gutiérrez-de-Mesa, 2016). Además, es claro que las empresas requieren una rápida respuesta a las nuevas oportunidades del negocio para satisfacer las necesidades de los clientes internos y externos a través de una comunicación efectiva entre las tecnologías de información y las estructuras empresariales (Barros et al., 2015). Los empleados de las pequeñas empresas conocen la existencia de modelos y buenas prácticas relacionadas con tecnologías de información, pero les parecen distantes y utópicos dado que su dedicación al trabajo productivo y solución de los problemas diarios, no les motiva a invertir tiempo y esfuerzo en definir e implementar nuevos procesos; y al no contar con áreas de calidad no están acostumbrados a establecer nuevas prácticas laborales pese a necesitar procedimientos basados en modelos y buenas prácticas que sean simples de aplicar a sus servicios (Mesquida y Mas, 2015).

Todos los negocios están expuestos a riesgos independiente de su tamaño y tipo, cerca del 90% de las caídas de servicio son debidos a problemas de comunicaciones o redes, fallas en hardware y/o software, o errores de los operadores; dichas caídas dañan sus finanzas y reputación (Bennett, 2007). La dependencia en la comunicación digital y otras tecnologías de red ha aumentado rápidamente debido a los beneficios que brinda el ciberespacio, pero también ha abierto nuevas oportunidades para las actividades criminales en línea (Lagazio et al., 2014). Actualmente, es inevitable que alguna organización independiente de su tamaño sea víctima de un algún ataque, lo que generaría pérdidas directas por la interrupción del servicio, daños generados por la caída del sistema, y pérdidas indirectas como las de tipo legal y las que afectan la reputación de la empresa (Ab Rahman y Choo, 2015). En este panorama, es evidente que muchas MiPymes no cuentan con un proceso de evaluación de riesgos sobre los activos de tecnologías de información que facilite su identificación y evaluación, pese a que es necesario. Por tanto, la investigación se justifica en la falta de un modelo de evaluación de riesgos en activos de tecnologías de información para MiPymes del sector servicios en la provincia de Trujillo dado que las referencias más cercanas son de pequeñas empresas colombianas, ecuatorianas o españolas, las cuales presentan características diferentes a las de nuestro país o región. Además, se propone un modelo que facilitara el proceso de evaluación de riesgos en activos de tecnologías de información en una MiPyme del sector transporte en la provincia de Trujillo, el cual brinda información importante para el tratamiento de dichos riesgos.

El objetivo de la investigación es evaluar los riesgos en activos de TI en una MiPyme empleando un modelo de evaluación basado en buenas prácticas. Para lograr este objetivo se ha realizado una investigación bibliográfica de trabajos relacionados como la evaluación de riesgos de tecnologías de información en la Dirección de Tecnologías de Información y desarrollo de sistemas del Instituto de Tecnología Sepuluh Nopember (ITS) de Indonesia empleando COBIT 5 como modelo de referencia (Astuti et al., 2017), la aplicación de la metodología OCTAVE Alegro para evaluar los riesgos en los sistemas de información en la Universidad de Thamrin en Indonesia (Suroso y Fakhrozi, 2018), el diseño de un método de evaluación de seguridad de TI dirigido a microempresas alemanas (Heidenreich, 2017), una propuesta de proceso de análisis y gestión de riesgos para pequeñas y medianas empresas españolas RAM-SME posee elementos de MAGERIT e ISO 27002 (Sánchez et al., 2010), la adaptación de la metodología OCTAVE-s y la norma ISO/IEC 27005:2011 para el análisis y gestión del riesgo en la seguridad de la información en la Universidad del Cauca y su aplicación en el proceso de Inscripciones y Admisiones de la División de Admisión, Registro y Control Académico (DARCA) (Espinosa et al., 2014), un modelo de gestión de riesgos de TI para contribuir en la continuidad del negocio de las micro financieras de la región Lambayeque (Vásquez y Alva, 2018), una propuesta de modelo de gestión de riesgos de TI para las empresas del sector de saneamiento del norte del Perú aplicada a los procesos comerciales de la empresa EPSEL S.A (Moscoso et al., 2018).

2. MATERIALES Y MÉTODOS

Para la evaluación de riesgos en activos de tecnologías de información se elaboró un modelo el cual fue aplicado a una MiPyme de transporte de servicio público urbano de la provincia de Trujillo.

La técnica elegida para la validación del modelo propuesto es la de juicio de expertos considerando los criterios (categorías) propuestas por Escobar-Pérez y Cuervo-Martínez (2008), las cuales ya han sido empleados en otras investigaciones relacionadas a la gestión de riesgos en activos de tecnologías de información en nuestro país.

La plantilla empleada sigue los lineamientos de la técnica propuesta, considerando las cuatro categorías que se muestran en la Tabla 1.

Tabla 1. Criterios considerados para la aceptación del modelo propuesto

Categoría	Descripción
Suficiencia	Los ítems que pertenecen una misma dimensión bastan para obtener la medición de ésta.
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.
Coherencia	El ítem tiene relación lógica con la dimensión o indicador que está midiendo.
Relevancia	El ítem es esencial o importante, es decir debe ser incluido.

Para la evaluación de las respuestas de los expertos se empleó el coeficiente de concordancia W de Kendall, y la prueba de hipótesis Chi-cuadrado obteniéndose W=0,667, X^2=16.000 y p=0,042, siendo el valor de p<0,05 se validó la concordancia del juicio aprobatorio de los expertos. Para procesamiento de los datos se empleó el software SPSS 21.

3. RESULTADOS Y DISCUSIÓN

El presente trabajo incluye el modelo propuesto, su validación y posterior aplicación en la MiPyme seleccionada.

3.1 Modelo propuesto

El modelo propuesto contiene elementos de la norma ISO 31000 que es el estándar internacional que rige la gestión de riesgos; la norma ISO 27005 especializada en gestión de riesgos en sistemas de seguridad de información, permite delimitar el proceso de evaluación de riesgos y a su vez brinda un catálogo de vulnerabilidades y criterios de priorización. Además, considera elementos de metodologías como MAGERIT que proporciona un catálogo de activos y amenazas; así como, criterios de evaluación, y OCTAVE-S que proporciona criterios de evaluación del riesgo, y el establecimiento del contexto sugerido por la norma ISO 3100.

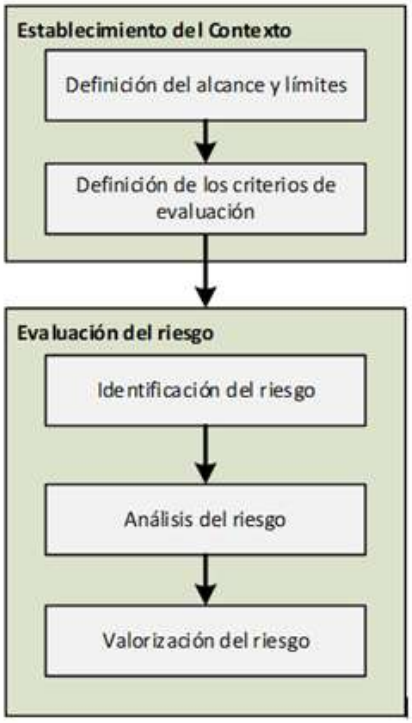

Figura 1. Modelo propuesto.

Es importante resaltar que el equipo de trabajo para la evaluación riesgos considerando el tamaño de las MiPymes será de tres integrantes, lo cual se encuentra dentro del rango sugerido por la metodología OCTAVE-S.

El modelo propuesto se divide en dos etapas. La primera denominada establecimiento del contexto tiene por objetivo mapear todo el ambiente que rodea a la organización de forma específica; esta etapa se divide en dos procesos principales: definición del alcance y límites donde se realiza una revisión del estado actual de la empresa y se delimitan los procesos incluidos en la evaluación; y la definición de criterios de evaluación de activos de tecnologías de información, de impacto de una amenaza, de probabilidad y de riesgo, también se debe indicar el nivel de aceptación del riesgo.

Para la definición de los criterios de evaluación se emplearon escalas de cinco niveles; en el caso de la evaluación de activos se emplearon las tres dimensiones sugeridas por la metodología MAGERIT: confidencialidad, integridad y disponibilidad (Gobierno de España, 2012a). Mientras que para la evaluación del impacto se emplearon los cinco aspectos sugeridos por la metodología OCTAVE-S: financieros, legales, reputación/confianza del cliente, seguridad/salud y productividad (Carnegie Mellon, 2005). En el caso de los criterios de evaluación de probabilidad se brinda una escala sugerida la cual puede ser modificada, y con respecto al nivel de evaluación del riesgo se considerado la matriz propuesta por la metodología MAGERIT (Gobierno de España, 2012c) cuyos niveles fueron renombrados para manejar un vocabulario común, la cual se muestra en la siguiente Figura 2, donde MA representa muy alto(a), A es alto(a), M es medio (a), B es bajo (a) y MB es muy bajo (a).

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Figura 2. Matriz de riesgos adaptada de MAGERIT.

La segunda etapa denominada evaluación del riesgo tiene por objetivo evaluar el riesgo en los activos de tecnologías de información en el proceso o procesos seleccionados previamente, para lo cual se divide en tres procesos principales: identificación del riesgo, análisis del riesgo y valorización del riesgo Estos procesos permiten obtener como salida de esta etapa una lista de riesgos codificados y priorizados. Es importante indicar que en esta etapa se realiza mediante reuniones o sesiones de trabajo del equipo y de visitas a las instalaciones, para lo cual se emplearán una serie de formatos y escalas que servirán como documentación del proceso.

En el proceso de identificación del riesgo se realizan las actividades requeridas para poder identificar los riesgos sobre los activos críticos, este proceso posee dos actividades de vital importancia: identificar los activos críticos, e identificar las amenazas y vulnerabilidades sobre estos, para lo cual se elaboró una base de datos que vincula los activos de tecnologías de información con las amenazas y vulnerabilidades a los que se encuentran expuestos, luego de revisión y comparación del catálogo de activos de MAGERIT (Gobierno de España, 2012b) y la lista de amenazas y vulnerabilidades proporcionada por la norma ISO 27005 (ISO, 2018). Luego, el proceso de análisis del riesgo busca determinar el impacto del riesgo de una amenaza y determinar la probabilidad de que una amenaza aproveche una vulnerabilidad para materializarse, determinación del impacto y de la probabilidad. Después viene la valorización del riesgo donde se emplea la matriz mostrada en la Figura 2 y finalmente los riesgos serán priorizados considerando el nivel de aceptación del riesgo establecido previamente.

3.2 Aplicación del modelo

La MiPyme seleccionada pertenece al sector de transporte público urbano, es una organización de naturaleza jurídica privada, constituida como sociedad anónima, conforme al Código Civil, la Ley General de Sociedades, la Ley General de Transporte Terrestre y Marítimo, con un capital social aportado por sus asociados, cuyo obje-

to principal es prestar servicios de transporte urbano de pasajeros y el de gestar actividades y servicios complementarios a su labor principal.

En la empresa se siguió el modelo propuesto , el cual consta de dos etapas: en la primera etapa, se realiza el establecimiento del contexto empezando por el proceso de definición del alcance y limites, lo cual requirió una revisión de la situación actual de la empresa: su misión, visión, objetivos organizacionales, políticas, estructura organizacional, procesos y servicios, personal, organismos reguladores y principales proveedores; así mismo, se debe determinar que procesos formaran parte de la evaluación, en este caso se consideraron dos procesos: el proceso de facturación y el proceso de control de frecuencias. En el proceso siguiente llamado definición de los criterios de evaluación se definieron los criterios de evaluación, lo cual incluye determinar el nivel de selección de activos críticos, definir los criterios de evaluación del impacto de un riesgo considerando cinco aspectos (financieros, legales, reputación/confianza del cliente, seguridad y salud, y productividad), criterios de evaluación de la probabilidad, y el criterio de aceptación del riesgo.

En la segunda etapa denominada evaluación del riesgo, se inició con el proceso de identificación de del riesgo consiste en la identificación de activos críticos, considerando las dimensiones de seguridad de la información: confidencialidad, integridad y disponibilidad, identificándose 19 activos críticos distribuidos en los niveles ALTO y MUY ALTO, tal como se muestra en la Tabla 2. Posteriormente, se realizó la identificación de riesgos considerando la base de datos de amenazas y vulnerabilidades sobre activos de tecnologías de la información; identificándose un total de 248 riesgos sobre los activos críticos.

Tabla 2. Clasificación de activos por nivel de criticidad

Nivel de criticidad	Cantidad
Muy Bajo	1
Bajo	16
Medio	22
Alto	15
Muy Alto	4
Total	58

El segundo proceso denominado análisis del riesgo se procede a determinar el impacto y la probabilidad empleando los criterios evaluación previamente seleccionados. El tercer proceso denominado valorización del riesgo consiste en la estimación del riesgo empleando la matriz de riesgos mostrada en la Figura 2, y posteriormente considerando el criterio de aceptación del riesgo establecido se identificaron 06 riesgos no aceptables, cuyo nivel de riesgo es ALTO, la clasificación de riesgos por niveles se encuentra en la Tabla 3.

Tabla 3. Clasificación riesgos por niveles

Nivel riesgo	Cantidad
Muy Bajo	32
Bajo	146
Medio	64
Alto	6
Muy Alto	0
Total	248

Posteriormente los riesgos no aceptables identificados, fueron analizados y se elaboraron 02 planes de tratamiento de riesgos. El primer de tratamiento de riesgos considera el aseguramiento y estabilidad del fluido eléctrico mientras que el segundo plan de tratamiento de riesgos está relacionado a la gestión de copias de seguridad considerando la elaboración de un procedimiento.

El modelo propuesto es cualitativo, considerando que las MiPymes son empresas pequeñas con recursos limitados y generalmente carecen de áreas de calidad; por lo cual, requieren de un modelo de fácil comprensión y aplicación, y que motive a una posterior extensión de su uso.

La prueba elegida para la validación del modelo fue empleada previamente en trabajos similares, la cual propone un instrumento adaptable, una rúbrica para la evaluación, el coeficiente de concordancia W de Kendall y la prueba Chi-cuadrado. El valor del coeficiente W de Kendall obtenido presenta valores más altos que en los tra-

bajos de (Vásquez y Alva, 2018) y (Moscoso et al., 2018), mostrando un mayor grado de concordancia entre los juicios de los expertos.

Durante la evaluación se notó la importancia de la definición previa de los criterios de evaluación siendo de gran utilidad porque permitió uniformizar criterios durante el proceso de evaluación. La definición de criterios proviene de OCTAVE-s, y no se encuentra claramente definida en MAGERIT por lo cual muchos de los antecedentes que se enfocan fuerte en MAGERIT no lo describen, esta definición de criterios si es considerada en la adaptación de la metodología OCTAVE-s aplicada al proceso de Inscripciones y admisiones en la división de admisión registro y control académico (DARCA) de la Universidad del Cauca (Espinosa et al., 2014).

Los formatos y colores elegidos y la uniformidad en los niveles de las escalas facilitaron el proceso de evaluación. Los colores elegidos corresponden los usados por la Metodología MAGERIT, dichos colores no fueron considerados en los antecedentes dado que los autores establecieron sus propios colores. Además, los niveles de las escalas empleados fueron de diferentes tamaños.

El brindar una clasificación de tipos de activos y la base de amenazas y vulnerabilidades por activos es una característica de este trabajo, no se observó en los antecedentes, pues aquellos que se centran en MAGERIT, solamente cuentan con el catálogo de activos y amenazas; pero las vulnerabilidades no son incluidas; mientras que los que se basan en la Norma ISO 27005 descuidan el catálogo de activos.

El modelo fue probado en una empresa de transportes de servicio urbano, identificándose 248 riesgos potenciales, de los cuales 06 son considerados NO ACEPTABLES. Con relación a los antecedentes, el número de riesgos NO ACEPTABLES identificados es menor, pero se debe considerar que se trata de empresas de mayor tamaño como empresas financieras (Vásquez y Alva, 2018), de saneamiento (Moscoso et al., 2018), o en una universidad (Espinosa et al., 2014). Sin embargo, es importante resaltar que el número de riesgos identificados no es menor, y se podría considerar que se debe la determinación del criterio de aceptación donde se puede observar la influencia del punto de vista de los representantes de la empresa.

4. CONCLUSIONES

El modelo propuesto considera elementos de las metodologías MAGERIT, OCTAVE-S y la norma ISO 27005, e ISO 31000 tratando de proporcionar un modelo sea claro y coherente que proporcione información relevante y suficiente.

La prueba, formatos y estadísticos empleados para la validación del modelo fueron empleados en trabajos similares previamente y permitieron validar el modelo empleando el juicio de expertos con el coeficiente concordancia W de Kendall, el cual es útil para determinar el grado de concordancia entre las calificaciones de los expertos, y la prueba Chi-cuadrado que permitió validar el modelo propuesto.

El modelo propuesto fue aplicado en una empresa de servicio de transporte público de la ciudad de Trujillo, donde se empezó con un análisis de la situación actual y la selección de los criterios de evaluación. Posteriormente, se realizó el análisis de los activos de tecnologías de información, detectándose un total de 19 activos críticos.

A partir de dichos activos críticos se identificaron 248 riesgos sobre dichos activos, de los cuales 06 fueron detectados como no aceptables en base a los criterios de evaluación seleccionados. Durante la evaluación se observó la utilidad de los formatos elaborados, así como de la lista de tipos de activos elaborada y la base de datos de amenazas y vulnerabilidades por tipo de activo de tecnologías de información.

REFERENCIAS BIBLIOGRÁFICAS

Ab Rahman, N.; Choo, K. 2015. A survey of information security incident handling in the cloud. Computers and Security. 49:45-69

Astuti, H.; Muqtadiroh, F.; Tyas Darmaningrat, E.; Putri, C. 2017. Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk. Procedia Computer Science. 124:569-576

Barafort, B.; Mesquida, A; Mas, A. 2017. Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards & Interfaces. 54:176-185.

Barros, M.; Salles, C.; Gomes, C.; Silva, R.; Costa, H. 2015. Mapping of the Scientific Production on the ITIL Application Published in the National and International Literature. Procedia Computer Science. 55: 102-111.

Bennett, J. 2007. Business continuity and availability planning. Infosecurity. 4(3):38.

Carnegie Mellon. 2005. OCTAVE-S Implementation Guide, Version 1. Disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795

CEPAL. 2016. Estudio Económico de América Latina y el Caribe La Agenda 2030 para el Desarrollo Sostenible y los desafíos del financiamiento para el desarrollo. Naciones Unidas. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/40326/86/S1600799_es.pdf

Cruz-Hinojosa, N.; Gutiérrez-de-Mesa, J. 2016. Literature review of the situation research faces in the application of ITIL in Small and Medium Enterprises. Computer Standards & Interfaces. 48:124-138.

Escobar-Pérez, J.; Cuervo-Martínez, Á. 2008. Validez De Contenido Y Juicio De Expertos: Una. Avances en Medición. 6:27-36.

Espinosa, D.; Martínez, J.; Amador, S. 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 AC. Revista de Ingenierías USBmed. 5(2):33.

Gobierno de España. 2012a. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I- Método. Ministerio de Hacienda y Administraciones Públicas. 127pp.

Gobierno de España. 2012b. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos. 75pp.

Gobierno de España. 2012c. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro III- Guía de Técnicas. 42 pp.

Heidenreich, M. 2017. How to design a method for measuring IT security in micro enterprises for IT security level measuring? A literature analysis. 2017 Communication and Information Technologies (KIT). 1-9.

ISO. 2018. ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management. 56 pp.

Lagazio, M.; Sherif, N.; Cushman, M. 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security. 45:58-74.

Mesquida, A.; Mas, A. 2015. Integrating IT service management requirements into the organizational management system. Computer Standards & Interfaces.37:80-91.

Ministerio de Producción. 2018. MiPyme en cifras. Disponible en: http://ogeiee.produce.gob.pe/images/oee/Mipyme-en-cifras-2016.pdf

Moscoso, L.; Peña, E.; Soto, M. 2018. Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú. Tesis para optar al grado de Maestro. Universidad Católica Santo Toribio de Mogrovejo. Disponible en: http://tesis.usat.edu.pe/bitstream/20.500.12423/1409/1/TM_SotoCastrillonMariadelCarmen_PenaNuñezEdgard_MoscosoAnayaLissette.pdf

Ponce, F.; Zevallos, E. 2017. La innovación en la micro y la pequeña empresa (MYPE): no solo factible, sino accesible. Revista de Ciencias de la Gestión. 2(2):48-68.

Sánchez, L.; Ruiz, C.; Fernández Medina, E.; Piattini, M. 2010. Managing the Asset Risk of SMEs. 2010 International Conference on Availability, Reliability and Security. 422-429.

Suroso, J.; Fakhrozi, M. 2018. Assessment of Information System Risk Management with Octave Allegro at Education Institution. Procedia Computer Science. 135:202-213.

Tøndel, I.; Line, M.; Jaatun, M. 2014. Information security incident management: Current practice as reported in the literature. Computers & Security. 45:42-57.

Vásquez, F.; Alva, J. 2018. Modelo de gestión de riesgos de TI para contribuir en la continuidad del negocio de las microfinancieras de la región Lambayeque Tesis para optar al grado de Maestro. Universidad Católica Santo Toribio de Mogrovejo. Disponible en: http://tesis.usat.edu.pe/handle/usat/1373

Wickboldt, J.; Bianchin, L.; Lunardi, R.; Granville, L.; Gaspary, L.; Bartolini, C. 2011. A framework for risk assessment based on analysis of historical information of workflow execution in IT systems. Computer Networks. 55(13):2954-2975.

ANEXOS

IDENTIFICACIÓN DE ACTIVOS CRÍTICOS								P03-01				
Fecha 24/02/2021												
N°	Código	Activo	Descripción	Ubicación	Responsable	Tipo	Valoración de activos					
							C	I	D	Total	Nivel	Crítico
1	IPE-001	Datos de Carácter personal	Información personal	Central	Gerente General	Información	3	3	1	2.3	Baja	--
2	IES-001	Información estratégica	Plan operativo	Central	Gerente General	Información	3	4	1	2.7	Media	--
3	IVA-001	Información valiosa	Libros contables	Central	Gerente General	Información	3	3	2	3.3	Media	--
4	IVA-002	Información valiosa	Contratos y Actas	Central	Gerente General	Información	3	3	2	3.3	Media	--
5	IVA-003	Información valiosa	Información confidencial	Central	Gerente General	Información	4	5	4	4.3	Alta	SI
6	IBK-001	Copias de seguridad	Copias de seguridad Servidor	Central	Gerente General	Información	3	3	3	3	Media	--
7	PC-001	Equipos personales	Computadora Contabilidad	Central	Director Economía	Hardware	5	5	3	4.3	Alta	SI
8	PC-002	Equipos personales	Computadora Caja	Central	Cajera	Hardware	4	5	5	4.7	Muy Alta	SI
9	PC-003	Equipos personales	Computadora Control	Central	Controladora	Hardware	3	5	5	4.3	Alta	SI
10	LAP-001	Equipos Móviles	Laptop Gerencia	Central	Gerente General	Hardware	5	4	1	3.3	Media	--
11	PRIN-001	Medios de impresión	Impresora Multifuncional Contabilidad	Central	Director Economía	Hardware	1	1	3	1.7	Baja	--
12	PRIN-002	Medios de impresión	Impresora Multifuncional Control	Central	Controladora	Hardware	2	2	3	2.3	Baja	--
13	PRIN-003	Medios de impresión	Ticketera Caja	Central	Cajera	Hardware	2	4	5	3.7	Alta	SI
14	PRIN-004	Medios de impresión	Ticketera Control	Central	Controladora	Hardware	2	2	3	2.3	Baja	--
15	SRV-001	Servidor	Servidor Dell	Central	Gerente General	Hardware	5	5	5	5	Muy Alta	SI
16	OTR-001	Otros dispositivos	DVR del Sistema de Video vigilancia	Central	Gerente General	Hardware	3	3	1	2.3	Baja	--
17	OTR-002	Otros dispositivos	Sistema de Sonido Control	Central	Controladora	Hardware	1	3	4	2.7	Media	--
18	MED-001	Medios de almacenamiento	Memorias USB	Central	Gerente General	Media	5	3	1	3	Media	--
19	CON-001	Equipos de conexión	Switch Contabilidad	Central	Director Economía	Comunicaciones	1	3	5	3	Media	--
20	CON-002	Equipos de conexión	Switch Presidencia	Central	Gerente General	Comunicaciones	3	5	5	4.3	Alta	SI
21	CONT-001	Equipos de conexión	Modem	Central	Gerente General	Comunicaciones	3	3	5	3.7	Alta	SI
22	LAN-001	Red local	Red Local de la empresa	Central	Gerente General	Comunicaciones	4	4	5	4.3	Alta	SI
23	CEL-001	Telefonía	Teléfono de la empresa	Central	Director Economía	Comunicaciones	1	2	2	1.7	Baja	--
24	NET-001	Internet	Movistar	Central	Director Economía	Comunicaciones	3	3	5	3.7	Alta	SI
25	www-001	Navegación por internet	Servicio de navegación y búsqueda por internet	Central	Director Economía	Servicios	3	3	1	2.3	Baja	--
26	email-001	Correo electrónico	Gmail	Central	Director Economía	Servicios	3	3	1	2.3	Baja	--
27	otro-001	Otro servicio	Control GPS brindado por proveedor	Central	Director de Rutas	Servicios	3	4	5	4	Alta	SI
28	otro-002	Otro servicio	Sistema de alarma	Central	Gerente General	Servicios	4	4	1	3	Media	--
29	SO-001	Sistema operativo	Sistema Operativo Servidor: Windows Server 2016	Central	Gerente General	Software	5	5	5	5	Muy Alta	SI
30	SO-002	Sistema operativo	SO Computadora Contabilidad: Windows 10	Central	Gerente General	Software	5	5	3	4.3	Alta	SI
31	SO-003	Sistema operativo	SO Computadora Caja: Windows 10	Central	Gerente General	Software	4	5	5	4.7	Muy Alta	SI
32	SO-004	Sistema operativo	SO Computadora Control : Windows 10	Central	Gerente General	Software	3	5	5	4.3	Alta	SI
33	SO-005	Sistema operativo	SO Laptop Gerencia: Windows 10	Central	Gerente General	Software	5	4	1	3.3	Media	--
34	OFI-001	Paquetes de software estándar	Antivirus Servidor	Central	Director Economía	Software	4	4	5	4.3	Alta	SI
35	OFI-002	Paquetes de software estándar	Antivirus Computadora Contabilidad	Central	Director Economía	Software	3	4	1	2.7	Media	--
36	OFI-003	Paquetes de software estándar	Antivirus Computadora Caja	Central	Director Economía	Software	3	4	1	2.7	Media	--
37	OFI-004	Paquetes de software estándar	Antivirus Computadora Control	Central	Director Economía	Software	3	4	1	2.7	Media	--
38	OFI-005	Paquetes de software estándar	Antivirus Laptop Gerencia	Central	Director Economía	Software	3	4	1	2.7	Media	--
39	OFI-006	Paquetes de software estándar	Ofimática Contabilidad	Central	Gerente General	Software	3	3	3	3	Media	--
40	OFI-007	Paquetes de software estándar	Ofimática Caja	Central	Gerente General	Software	3	3	4	3.3	Media	--
41	OFI-008	Paquetes de software estándar	Ofimática Control	Central	Gerente General	Software	3	3	1	2.3	Baja	--
42	OFI-009	Paquetes de software estándar	Ofimática Gerencia	Central	Gerente General	Software	3	3	1	2.3	Baja	--
43	SIN-001	Sistemas de información del negocio	Sistema Contable Financiero	Central	Director Economía	Software	5	5	3	4.3	Alta	SI
44	SIN-002	Sistemas de información del negocio	Sistema de Emisión Electrónico de Comprobantes	Central	Director Economía	Software	5	5	3	4.3	Alta	SI
45	SIN-003	Sistemas de información del negocio	Sistema de Control de Frecuencias	Central	Director Economía	Software	3	4	4	3.7	Alta	SI
46	SIT-001	Ambientes Físicos	Local Central	Central	Gerente General	Instalaciones	2	2	5	3	Media	--
47	UIN-001	Usuarios interno	Director de Economía	Central	Gerente General	Personal	4	3	2	3	Media	--
48	UIN-002	Usuarios interno	Contador	Central	Director Economía	Personal	4	3	1	2.7	Media	--
49	UOP-001	Operadores	Asistente Contable	Central	Director Economía	Personal	3	3	3	3	Media	--
50	UOP-002	Operadores	Cajera	Central	Director Economía	Personal	3	3	4	3.3	Media	--
51	UOP-003	Operadores	Controladora	Central	Director de Rutas	Personal	2	2	4	2.7	Media	--
52	UPR-001	Proveedores	Proveedor Sistema Contable Financiero y Emisión Electrónico de Comprobantes	Central	Director Economía	Personal	3	3	1	2.3	Baja	--
53	UPR-002	Proveedores	Proveedor de Sistema de Control de Frecuencias	Central	Director de Rutas	Personal	3	3	1	2.3	Baja	--
54	UPR-003	Proveedores	Proveedor Soporte Técnico	Central	Gerente General	Personal	2	2	1	1.7	Baja	--
55	AIR-001	Equipos de climatización	Ventilador ambiente servidor	Central	Gerente General	Auxiliar	1	1	1	1	Muy Baja	--
56	ESC-001	Suministros esenciales	Tintas impresora Caja	Central	Director Economía	Auxiliar	1	1	3	1.7	Baja	--
57	ESC-002	Suministros esenciales	Tintas impresora Control	Central	Director Economía	Auxiliar	1	1	3	1.7	Baja	--
58	ESC-003	Suministros esenciales	Papel Térmico	Central	Director Economía	Auxiliar	1	1	5	2.3	Baja	--