



Noviembre 2018 - ISSN: 1988-7833

EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT

Julio, Alvarado-Zabala, MSC
Universidad Agraria del Ecuador
jalvarado@uaqraia.edu.ec

Joselin, Pacheco-Guzmán
Universidad Agraria del Ecuador
joselin-p2011@hotmail.com

Ivette Martillo-Alchundia
Universidad Agraria del Ecuador
imartillo@uaqraia.edu.ec

Datos Autores

Julio Ramón Alvarado Zabala: Ingeniero en Sistemas Computacionales; Master en Diseño Curricular; Profesor Titular Auxiliar de la carrera de Tecnología en Computación e Informática en la Unidad Académica Programa Regional de Enseñanza El Triunfo de la Facultad de Ciencias Agrarias en la Universidad Agraria del Ecuador.

Joselin Yomira Pacheco Guzmán: Tecnóloga en Computación e Informática, graduada del Programa Regional Enseñanza El Triunfo de Facultad de Ciencias Agrarias de la Universidad Agraria del Ecuador. Estudiante de Pregrado de la Carrera de Ingeniería en Computación e Informática de la Facultad de Ciencias Agrarias en la Universidad Agraria del Ecuador.

Ivette Shirley Martillo Alchundia: Ingeniera en Computación e Informática; Master en Diseño Curricular; Profesor Titular Auxiliar de la carrera de Tecnología en Computación e Informática en la Unidad Académica Programa Regional de Enseñanza El Triunfo de la Facultad de Ciencias Agrarias en la Universidad Agraria del Ecuador

Para citar este artículo puede utilizar el siguiente formato:

Julio, Alvarado-Zabala, Joselin, Pacheco-Guzmán e Ivette Martillo-Alchundia (2018): "El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT", Revista Contribuciones a las Ciencias Sociales, (noviembre 2018). En línea:

<https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html>

RESUMEN.

Las administraciones públicas y empresas privadas hoy en día requieren de un mayor control en cuanto a los sistemas que operan con información, por lo cual el análisis y gestión de riesgos es considerado de suma importancia en el contexto del negocio. Este análisis constituye una herramienta esencial para el auditor, pues comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas expuestas. Por tanto, el análisis y gestión de riesgos es fundamental dentro de cualquier organización, pues si un análisis de riesgos está mal elaborado o no sigue una metodología preestablecida podría causar el desperdicio los esfuerzos por proteger activos. En la actualidad son muchos los riesgos que afectan a la seguridad de la información, existen distintas metodologías apegadas a estándares y normas, y que su implementación permite mejorar los sistemas de gestión de riesgos. Este artículo muestra que tipo de estándares, normas y metodologías se deben considerar al momento de realizar un análisis de riesgos, pero en particular se enfatizará en el uso de una metodología, para este caso MAGERIT y cómo articularla en el proceso de gobernabilidad de TI para un mejor desempeño.

Palabras claves: Tecnología de información, análisis de riesgos de TI, gobiernos de TI.

ABSTRAC

Public administrations and private companies today require greater control over systems that operate with information, so risk analysis and management is considered of paramount importance in the context of the business. This analysis constitutes an essential tool for the auditor, since it includes the identification of computer assets, their vulnerabilities and exposed threats. Therefore, risk analysis and management is fundamental within any organization, because if a risk analysis is poorly designed or does not follow a pre-established methodology, efforts to protect assets could be wasteful. At present, there are many risks that affect the security of information, there are different methodologies adhered to standards and standards, and that their implementation allows to improve the systems of risk management. This article shows what kind of standards, norms and methodologies should be considered when carrying out a risk analysis, but in particular will be emphasized in the use of a methodology, for this MAGERIT case and how to articulate it in the process of IT governance for a better performance.

Key words: Information technology, IT risk analysis, IT Governance.

I. INTRODUCCIÓN

Hoy en día son muchos los riesgos que enfrentan las organizaciones y que por lo general el capital con el que se cuenta para protegerlas no es suficiente, por eso es muy importante recalcar que tanto la administración como toda la sociedad dependen mucho de las TI para poder cumplir con su misión propuesta. Es por ello que se debe llevar a cabo un plan de seguridad elaborado en base a un análisis de riesgo previo que va a permitir tenerlos identificados y controlados esos riesgos.

Respecto al análisis de riesgos es ampliamente utilizado dentro del contexto del negocio y las interrelaciones con otras funciones, tales como: recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, entre otros, por lo tanto el análisis de riesgos es considerado como uno de los elementos fundamentales dentro de cualquier proceso de implantación de un sistema de gestión de seguridad de la información, porque es ahí donde se cuantifica la importancia que tienen los activos para la seguridad de cualquier organización. Los resultados del análisis de riesgos permiten a la gestión de los mismos recomendar las medidas adecuadas para controlar los riesgos identificados y poder reducir sus posibles daños.

Debido a tantos efectos negativos que se han visto en las organizaciones por las vulnerabilidades en los sistemas, es que se han implementado el uso de distintas metodologías que son de gran importancia, pues gracias a la predicción, análisis y monitoreo de los riesgos se podría mitigar su impacto y saber cuánto valor de activo de información está en juego para poder protegerlo adecuadamente, es decir que gracias a las metodologías como: EBIOS, MEHARI, NIST SP 800: 30, OCTAVE, CRAMM, MAGERIT, entre otras, las empresas contarán con una adecuada administración del riesgo informático.

Observando las necesidades que las organizaciones tienen hoy en día en cuanto a los riesgos en TI, es que hemos decidido presentar este artículo, el cual se ha enfocado en tres puntos: primero en mostrar un marco de referencia en cuanto a estándares, normas, metodologías, entre otras, que son de gran importancia en el análisis y gestión de riesgos; segundo enfoque mostramos MAGERIT como una metodología comprobada con algunos ejemplos de casos de éxito en distintas empresas y finalmente nuestro artículo mostrando los aspectos más relevantes del gobierno de TI respecto a la gestión de los riesgos.

II. DESARROLLO

2.1 Marco de referencia en cuanto a estándares, normas, metodologías para el análisis y gestión de riesgos.

Muchas organizaciones hoy en día son dependientes de la tecnología, el desarrollo de las mismas y lo sofisticado de estas han colaborado en la automatización de muchos procesos y actividades que se realizan, sin embargo, las dependencias en el uso de tecnologías también provocan que las organizaciones queden expuestas a riesgos y a explotar sus vulnerabilidades. Es por ello que para todo tipo de organizaciones es muy importante implementar medidas de seguridad de la información, ya que distintos tipos de riesgos, amenazas potenciales y vulnerabilidades que existen en su entorno podrían causar algún daño para un activo, en cuanto a la violación de la información.

Cabe mencionar que para muchas empresas la información y la tecnología que la soportan representan sus más valiosos activos ya que el gobierno de TI, facilita que la empresa aproveche al máximo su información para obtener oportunidades y ventajas competitivas dentro de las organizaciones, para la seguridad de su información, así como de todos sus activos (Barahona, 2011). Entre algunos ejemplos de activos de información están: documentación del sistema, ficheros, bases de datos, manuales de usuarios, software del sistema, aplicaciones, contratos y acuerdos, entre otros, los cuales permiten generar, procesar, almacenar y transmitir información (ISOTOOLS EXCELLENCE, 2014).

Aunque existen distintos tipos de medidas para solucionar problemas de la seguridad en los SI. Arévalo et al.(2009), afirma que la inseguridad sigue siendo un problema el cual no ha sido resuelto y una de las principales razones es porque frecuentemente siguen apareciendo muchas amenazas: evolución del malware, virus, entre otros, por lo que una organización debe considerar los cambios en los riesgos, ya que parten de dos orígenes: el surgimiento de nuevas amenazas y la adopción de tecnologías que proveen origen a aquellos riesgos no previstos, todos estos cambios van a producir la posibilidad de riesgos imprevistos y también la creación de vulnerabilidades que antes no existían en los SI.

Debido a todas esas causas, el análisis de riesgos actúa como una herramienta que permite establecer un marco sistemático para así obtener los indicadores adecuados para llevar a cabo acciones de control, mitigación o eliminación de peligrosos riesgos e impactos adversos. Por lo tanto, existen variada estructura documental para realizar el análisis de riesgos como: estándares, normas y metodologías que van a permitir disminuir los riesgos y amenazas que continuamente siguen apareciendo.

Según manifiesta en su trabajo, Amutio (2010), con el pasar del tiempo se ha venido desarrollando una colección significativa de normas en el campo de la seguridad de las TI, la evolución de la normalización y el enfoque tradicional de desarrollo de normas centradas en aspectos de la tecnología se ha inclinado sustancialmente con prácticas de gestión, servicios y gestión de riesgos. La ISO es la Organización Internacional de Normalización y IEC es la Comisión Electrotécnica Internacional, estas dos entidades internacionales quienes establecen el sistema especializado en normalización a nivel mundial. Esta Organización tiene más de 18000 normas publicadas, cabe mencionar algunas de las normas más importantes en cuanto a su aplicación y la relevancia de sectores las cuales son: normas relacionadas con la calidad; con la gestión de la seguridad; con la calidad en la investigación y el desarrollo; con la calidad en el medio ambiente y la sostenibilidad (NORMAS ISO, 2014).

También están algunas normas como: ISO 27005 y ISO/IEC 27001 que son muy necesarias para la identificación de riesgos y vulnerabilidades relacionadas con sistemas de tecnología de la información, ya que permiten la gestión de los riesgos, estableciendo controles de seguridad para el recurso de la información, los estándares ISO para la identificación de riesgos-27005, es el estándar internacional que se encarga de los SGSI o Sistemas de Gestión de Seguridad de la Información, quienes a su vez permite suministrar las directrices para la seguridad de la información en una empresa y está diseñada como soporte para poder aplicar estos sistemas basado en un enfoque de gestión de riesgos, además cuenta con siete pasos que son: establecimiento del contexto, identificación del riesgo, estimación del riesgo, evaluación del riesgo; tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo (Espinosa, Martínez y Amador, 2014).

Mientras que los estándares ISO para sistemas de seguridad de la información-27001, está basada en un enfoque de riesgo empresarial, establecida para mantener y mejorar la seguridad de la información ya que se la puede emplear en cualquier tipo de organización, además que explica cómo diseñar un SGSI y establecer controles de seguridad (Gómez y Álvarez, 2012).

2.2 Metodologías para el análisis de riesgos en sistemas de información.

En cuanto a las metodologías de análisis de riesgos, existen diversas metodologías para desarrollar los análisis de riesgos, la selección de la metodología más apropiada en cada caso depende de la disponibilidad de información y el nivel de detalle que se desee alcanzar, entre las metodologías más importantes están: EBIOS, MEHARI, MAGERIT, NIST SP 800:30, OCTAVE, entre otras.

La seguridad total es inalcanzable pero mediante el proceso que se ha ido desarrollando del sistema de seguridad por medio de distintos estándares, normas y metodologías se puede obtener un nivel de seguridad altamente satisfactorio que permita reducir al mínimo los riesgos, sin embargo el objetivo del presente estudio es mostrar las características más relevantes de una metodología que facilita el proceso de análisis e identificación de los riesgos y vulnerabilidades en sistemas de información, en el caso particular de este artículo se presenta a MAGERIT como herramienta o marco de trabajo que ayude en la realización del proceso antes mencionado.

2.3 Metodología MAGERIT para el análisis y gestión de riesgos de TI.

Existen diversas metodologías para el gobierno de las TI, la idea no es usar todas ellas en todo momento. Por lo cual es que se debe saber analizar y seleccionar aquella metodología que mejor se adapte a cada organización. Cabe mencionar que a pesar de que pueda haber un sin número de metodologías que den solución a determinada problemática, cada una de ellas fueron creadas para resolver una matriz específica, con un enfoque específico y con un nivel de granularidad distinto.

En definitiva, es de primordial importancia el saber elegir la metodología más apropiada en cada caso, lo cual va a depender de la disponibilidad de la información y el nivel de detalle que se desee alcanzar.

Es por ello que se destaca MAGERIT, metodología de análisis y gestión de riesgos de TI, que permite dividir los activos de la organización en varios grupos, para poder identificar así los riesgos y tomar las medidas apropiadas para controlarlos o impedir cualquier tipo de inconveniente (Llavisaca, 2010).

Esta metodología fue elaborada por el Consejo Superior de Administración Electrónica de las administraciones públicas de España, que indica que la gestión de riesgos es fundamental en las guías del buen gobierno, el resultado de esta metodología se lo expresa en valores económicos, la primera versión se hizo en 1997, actualizada en 2012 en su versión 3 (Portal administración electrónica-PAE, 2012). Tiene la finalidad de poder dar satisfacción al principio de la proporcionalidad del cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información (Amutio, 2012).

2.3.1 Principales características

MAGERIT, es una de las metodologías más utilizadas ya que se encuentra en idioma español, entre las principales ventajas de su implementación se encuentra el hecho de que: las decisiones que se toman serán fundamentadas y fácilmente defendibles; ofrece un método sistematizado para analizar los riesgos; permite ayudar a identificar y planificar medidas necesarias poder reducirlos y brindan herramientas que permitan facilitar el análisis de los riesgos, mientras que entre sus desventajas está en que la metodología resulta costosa ya que tienen que traducir de manera directa las valoraciones en valores económicos (Carvajal, 2012).

Por otro lado, esta metodología de análisis y gestión de riesgos MAGERIT persigue objetivos directos e indirectos. Dentro de los objetivos directos están: concienciar a los responsables de todas las organizaciones de la existencia de riesgos, dando a conocer la necesidad de poder gestionarlos; permitir ofrecer un método sistemático para analizarlos; descubrir y planear un tratamiento oportuno en caso de que los riesgos ataquen los activos de información, mientras que los indirectos son: preparar a la organización para procesos de evaluación, auditoría, certificación y acreditación (Cordero y García, 2015).

2.3.2 Desarrollo del análisis y gestión de riesgos

MAGERIT se desarrolla mediante tres libros que permiten realizar el análisis y gestión de los riesgos. Los cuales son: métodos, catálogo de elementos, guía técnica

El primer libro de MAGERIT: método, es una guía detallada para el análisis de gestión de los riesgos y la estructura del proyecto de implementación de la metodología. En sus contenidos se describe la estructura que debe tener el modelo de la gestión de los riesgos, en el cual se tratan sobre temas como: método de análisis de riesgos, los cuales poseen tres tipologías de métodos: métodos cualitativos, métodos cuantitativos y métodos semi cuantitativos que son utilizados para determinar cuál es el nivel de los riesgos dentro de los negocios (Comunidad de Madrid, 2016); procesos de gestión de riesgos, estos procesos actúan mediante dos pasos: la evaluación y el tratamiento de los riesgos; proyectos de análisis de riesgos, se realizan mediante tareas como: actividades preliminares las cuales incluyen: el estudio de oportunidad, la elaboración del análisis de riesgos y la comunicación de resultados; planes de seguridad, que se planifican en tres niveles de detalle: plan director, plan anual y plan de proyecto; desarrollo de SI, durante este desarrollo se pueden identificar dos tipos de actividades diferenciadas: la seguridad del SI y la seguridad del proceso de desarrollo (Alcivar, 2012).

El segundo libro de MAGERIT: catálogo de elementos, es una especie de inventario que las empresas pueden usar para enfocar el análisis de los riesgos. En sus contenidos propone un catálogo referente a: tipos de activos; dimensiones de valoración de los activos, que incluyen: disponibilidad, integridad de los datos, confidencialidad, autenticidad y trazabilidad; Criterios de valoración de los activos, en estos criterios se puede utilizar cualquier escala de valores, frecuentemente la valoración es cualitativa, quedando a discreción del usuario; amenazas típicas sobre los SI y las salvaguardias a considerar para proteger SI (Alcivar, 2012).

El tercer libro de MAGERIT: guías técnicas permiten a los usuarios encontrar guías técnicas tanto específicas como generales para realizar proyectos de análisis y gestión de los riesgos. Dentro de las guías técnicas específicas para el análisis de gestión están: el análisis mediante tablas, que tienen como objetivo estandarizar y especificar las valoraciones, estimaciones dentro de un rango establecido; análisis algorítmico, existen dos enfoques algorítmicos: el modelo cualitativo, que busca una valoración relativa del riesgo que corren los activos y el modelo cuantitativo que ambiciona responder a la pregunta de cuánto más y cuánto menos; arboles de ataque, constan de: nodos con atributos, riesgo residual y la construcción del árbol. Mientras que las guías técnicas generales contienen: técnicas gráficas, existen diferentes tipos de graficas: técnicas graficas por puntos y líneas, técnicas gráficas por barras, técnicas graficas por área y técnicas gráficas por radar; Valoración DELPHI, esta valoración se realizó en las siguientes tareas: identificación de activos, dependencia entre activos, valoración de los activos, identificación de las amenazas, calificación de riesgos, valoración de las amenazas y valoración de las salvaguardias existentes; secciones de trabajo, estas sesiones pueden ser de varios tipos: entrevistas, reuniones y presentaciones en función de las personas que participen en ellas, el objetivo que se persiga y el modo de llevarlas a cabo (Alcivar, 2012).

2.4 Ejemplos de casos de éxito de la metodología MAGERIT

Algunas empresas han vivido experiencias realmente complejas que han demostrado la necesidad de incurrir a utilizar metodologías para realizar el análisis y gestión de riesgos.

Para citar un ejemplo de la implementación de la metodología MAGERIT para la seguridad de la información en la empresa Pesquera e Industrial Bravito S.A de la ciudad de Machala, pues en ella no se había realizado ningún estudio basado en estándares o metodologías de seguridad de información, por tal motivo se había escogido a MAGERIT para lograr que la información sea reservada, completa y segura. La situación actual en la que se encontraba la empresa en ese tiempo era alarmante ya que en sus procesos no implementaba medidas de seguridad apropiada, por lo cual provocaba que existiera inseguridad, sin embargo, gracias al análisis de riesgos permitió a la empresa sistematizar las medidas actuales y mejorarlas con algunas otras que fueron suficientes para lograr un nivel de seguridad estable (Gaona, 2013).

2.4.1 Desarrollo del análisis y gestión de riesgos para la empresa Pesquera e Industrial Bravito S.A.

Antes de iniciar con las etapas de análisis y gestión de riesgos (AGR) de los sistemas de información de la empresa Pesquera e Industrial Bravito S.A. Se realizó las siguientes tareas: estudio de oportunidad, determinación del alcance del proyecto, planificación del proyecto y lanzamiento del proyecto.

El proyecto AGR se desarrolló mediante la metodología MAGERIT versión 3. En base a las actividades preliminares que anteriormente fueron mencionadas, se informó que el proyecto estaba autorizado y listo para su ejecución.

2.4.2 Análisis de riesgos

Mediante el análisis de riesgos se alcanzó los siguientes objetivos: determinar los activos más significativos que posee la empresa, establecer las amenazas a las que están expuestos cada activo, escoger las salvaguardias más apropiadas para los activos y estimar el impacto si se materializara alguna amenaza.

El análisis de riesgos realiza para lograr los objetivos que se presentan en la tabla 1.

Tabla 1. Actividades del análisis de riesgos.

Actividades:

- Determinar los activos más significativos de la empresa
- Establecer la amenaza a las que están expuestos los activos
- Escogimiento de salvaguardias apropiadas
- Estimación de impacto su se llegase a presentar alguna amenaza

Fuente: (Gaona, 2013).

2.4.2.1 Identificación de activos

La identificación de activos es una actividad crítica, pues una correcta identificación permitió después realizar una valoración correcta y establecer la dependencia de los activos. El resultado de esta actividad se muestra en la tabla 2.

Tabla 2. Caracterización de activos.

Activos	Identificación
Servicios internos	[TELF_PIB] Telefonía IP
Software Aplicativo	[INTERNET_PIB] Internet [SIS_PIB] BIZNET. [OFF_PIB] Ofimática [AV_PIB] Antivirus [OS_PIB] Sistema Operativo [OTR_PIB] Otros
Equipos	[SDB_PIB] Servidor de base de datos [PRINT_PIB] Medios de impresión [PC_PIB] Computador de escritorio [ROUTER_PIB] Router
Comunicaciones	[IPPHONE_PIB] Telefonía IP [WIFI_PIB] Red WIFI [LAN_PIB] Red LAN [IEX_PIB] Internet
Medios	[CD_PIB] CD
Equipamiento auxiliar	[GEN_PIB] Generador eléctrico [CABLING_PIB] Cableado [MOB_PIB] Mobiliario [SISVG_PIB] Sistema de vigilancia [ANT_PIB] Antenas [RAD_PIB] Radios [SAI_PIB] Sistema de alimentación interrumpida [AUXOTR_PIB] Otros equipos auxiliares
Instalaciones	[BUILDING_PIB] Edificio
Personal	[JF_PIB] Jefa de departamento financiero [DBA_PIB] Mantenimiento BD [SP_PIB] Mantenimiento EQ [JC_PIB] Jefa de departamento de contabilidad [JLC_PIB] Jefe de departamento de logística y compras

[JP_PIB] Jefa de departamento de personal
 [AC_PIB] Auxiliar de contabilidad
 [D_PIB] Digitadora

Fuente: (Gaona, 2013).

Dependencia entre activos

La en la **Figura 1** muestra la dependencia existente entre los activos de la empresa. Se aprecia que el sistema BIZNET es fundamental para el desarrollo de las actividades en la organización, por esta razón es que se encuentra en el nivel más alto.

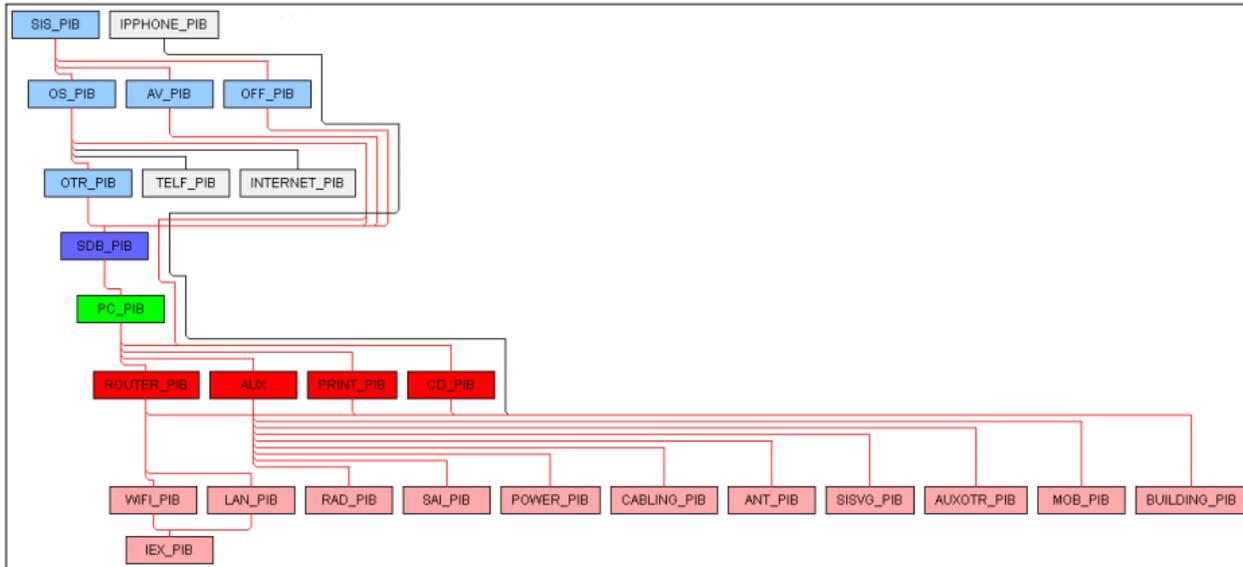


Figura1. Dependencia de activos. Fuente: PILAR 5.2.9

Valoración de activos

La valoración de activos se realizó bajo las dimensiones en que los activos son relevantes, para el caso se empleó las siguientes: [D] disponibilidad, [I] integridad de datos, [C] confidencialidad de datos, [A] autenticidad de los usuarios y de la información, [T] trazabilidad de los servicios de datos; y la estimación de la valoración se lo hizo en escala de valores de 1 a 10 donde el valor más bajo es considerado como un activo despreciables y la valoración más alta como activo de gran importancia. La siguiente Tabla 4, muestra el resultado de la valoración de activos.

Tabla 3. Valoración de activos

Activos	Dimensiones				
	D	I	C	A	T
[TELF_PIB]	[6]			[7]	[7]
[INTERNET_PIB]	[8]			[8]	[8]
[SIS_PIB]			[9]	[9]	[9]
[OFF_PIB]					[7]
[AV_PIB]					[7]
[OS_PIB]					[7]
[OTR_PIB]					[5]
[SDB_PIB]		[9]	[9]	[9]	[9]
[PRINT_PIB]					[6]
[PC_PIB]					[8]
[ROUTER_PIB]					[8]
[IPPHONE_PIB]		[7]			
[WIFI_PIB]					[7]

[LAN_PIB]			[7]
[IEX_PIB]		[7]	[7]
[CD_PIB]		[7]	[7]
[CABLING_PIB]	[7]		
[MOB_PIB]	[7]		
[SISVG_PIB]	[7]		
[ANT_PIB]	[7]		
[RAD_PIB]	[7]		
[SAI_PIB]	[7]		
[AUXOTR_PIB]	[5]		
[BUILDING_PIB]		[8]	
[JF_PIB]		[8]	
[DBA_PIB]		[7]	
[SP_PIB]		[7]	
[JC_PIB]		[8]	
[JLC_PIB]		[8]	
[JP_PIB]		[8]	
[AC_PIB]		[7]	
[D_PIB]		[6]	

Fuente: (Gaona, 2013).

2.4.2.2 Caracterización y valoración de las amenazas

Para la realización de esta actividad se utilizó la herramienta PILAR la cual ha sido desarrollada bajo el enfoque de MAGERIT, esta herramienta categoriza las amenazas como: [N] desastres naturales, [I] desastres de origen industrial, [E] errores y fallos no intencionados, [A] ataques intencionados, con el objetivo de caracterizar el entorno al que cada activo se enfrenta. En la Tabla 5 se muestra el resultado de la caracterización de amenazas de algunos activos, junto con su respectiva valoración donde se toma en cuenta la degradación del valor del activo y su probabilidad de ocurrencia. Para la degradación del valor se utiliza [MA] muy alta, [A] alta, [M] media, [B] baja, [MB] muy baja; y para la probabilidad de ocurrencia se utiliza [CS] casi seguro, [MA] muy alto, [P] posible, [PP] poco probable, [MB] muy bajo, [MB] muy rara.

Tabla 4. Valoración y probabilidad de amenazas

Activos	Amenazas	P	D	I	C	A	T
[SIS_PIB]	[I.5] avería de origen físico o lógico	P	A				
	[E.20] vulnerabilidad de los programas	P	B	M	M		
	[E.21] errores de mantenimiento/actualización	P	B	B	M		
[OFF_PIB]	[A.5] suplantación de identidad del usuario	P	A	A	A		
	[E.1] errores de los usuarios	P	M	M	M		
	[E.20] vulnerabilidad de los programas	P	M	M	M		
[AV_PIB]	[E.21] errores de mantenimiento/actualización	P	M	B			
	[E.8] difusión de servicio dañino	PP	B	B	B		
	[E.8] difusión de servicio dañino	PP	B	B	B		
[OS_PIB]	[E.20] vulnerabilidad de los programas	P	M	M	M		
	[E.21] errores de mantenimiento/actualización	P	M	M			
	[I.5] avería de origen físico o lógico	P	M				
[SDB_PIB]	[E.1] errores de los usuarios	PP	M	M	M		
	[E.8] difusión de servicio dañino	PP	B	B	B		
	[E.20] vulnerabilidad de los programas	P	B	M	M		
	[E.21] errores de mantenimiento/actualización	P	M	B			
	[A.7] uso no previsto	P	B	B	B		
	[N.1] daños por fuego	P	A				
	[N.2] daños por agua	P	A				
[N.*] desastres naturales	P	A					
[I.3] contaminación medioambiental	P	A					
[I.5] avería de origen físico o lógico	P	A					

	[I.7] condiciones inadecuadas de temperatura	MA	MA				
	[E.2] errores de administrador de sistema	P	M	M	M		
	[E.23] errores de mantenimiento de equipos	P	M				
	[A.11] acceso no autorizado	MA		A	A		
[PC_PIB]	[A.23] manipulación de hardware	MA	A		A		
	[I.*] desastres industriales	P	B				
	[I.5] avería de origen físico o lógico	P	M				
	[I.7] condiciones inadecuadas de temperatura	PP	M				
	[A.6] abuso de privilegio de acceso	PP	M	M	M		
[IPPHONE_PIB]	[A.7] uso no previsto	P	M	B	M		
	[A.7] uso no previsto	P		M	M		
	[A.9] re encaminamiento de mensajes	P			M		
	[A.10] alteración de secuencia	P		M			
	[A.12] análisis de tráfico	P			A		
	[A.14] interceptación de información	P			A		
	[I.8] fallo de servicio de comunicación	PP	B				
	[E.10] errores de secuencia	P		M			
	[A.5] suplantación de identidad del usuario	P		M	M	M	
	[A.9] re encaminamiento de mensajes	P			M		

Fuente: (Gaona, 2013).

2.4.2.3 Valoración de las salvaguardias

esta actividad consta de dos sub-tareas: identificación de las salvaguardias pertinentes y valoración de las salvaguardias. La Figura 2, ofrece una detallada descripción acerca de salvaguardias identificadas como convenientes para proteger el sistema y también su valoración determinada por su nivel de eficiencia donde 0% es determinado como nivel L0, 10% nivel L1, 50% nivel L2, 90% nivel L3, 95% nivel L4 y 100% nivel L5.

aspecto	top	salvaguarda	dudas	fuente	come...	reco...	target	cap...	PILAR
SALVAGUARDIAS									
G	PR	[H] Protecciones Generales				0	L5	L1	L3-L4
G	PR	[S] Protección de los Servicios				6	L5	L0-L1	L2-L3
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7	L5	L0-L1	L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7	L5	L0-L1	L2-L4
G	PR	[COM] Protección de las Comunicaciones				9	L5	L1	L2-L5
G	PR	[MP] Protección de los Soportes de Información				6	L5	L1	L2-L4
G	PR	[ALX] Elementos Auxiliares				6	L5	L1	L2-L3
F	PR	[I] Protección de las Instalaciones				7	L5	L1	L2-L4
P	PR	[PS] Gestión del Personal				5	L5	L1	L2-L3

Figura 2. Caracterización y valoración de las salvaguardias. Fuente: PILAR 5.2.9

2.4.2 Estimación y gestión del riesgo,

Luego de realizadas las tareas anteriores se elabora un documento en el cual se informa cual es el impacto potencial y residual ante la materialización de alguna amenaza, para luego realizar una estimación del nivel de riesgo a las que se someten los activos. La Figura 3, muestra la interpretación de resultados, producto de la realización de la actividad.

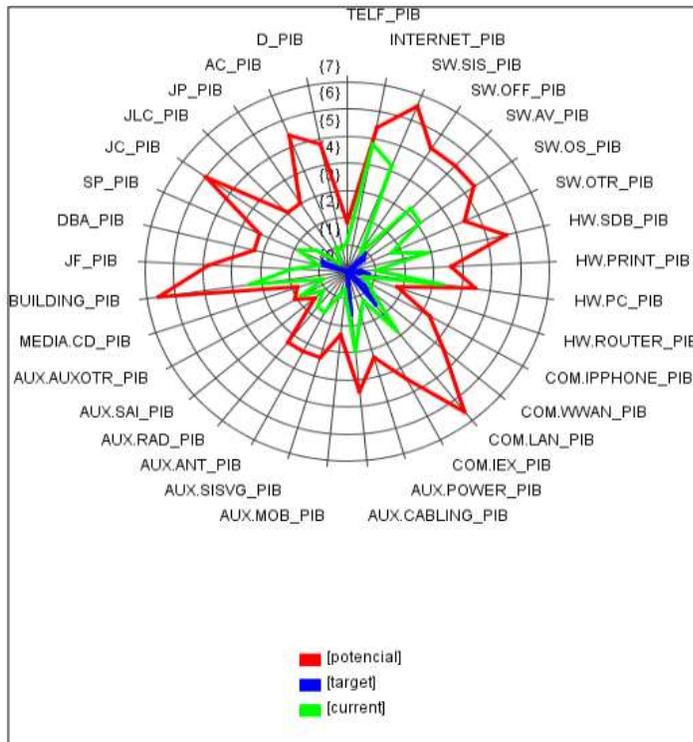


Figura 3. Interpretación de los resultados sobre la estimación de riesgos de activos Fuente: PILAR 5.2.9

Después de haber realizado el análisis de riesgos queda a la vista los impactos y los riesgos que están expuestos la empresa. La siguiente actividad a emprender corresponden a la toma de decisiones concerniente a identificar los riesgos críticos y clasificarlos, para luego elaborar un plan de seguridad adecuado cuyo objetivo es panificar la protección adecuada de los activos.

2.5 Gobierno de TI respecto a la gestión de los riesgos.

Dentro del proceso que se quiere realizar para el análisis de riesgos, una vez que se tiene claro el marco de referencia y la metodología a aplicar para llevar este proceso, es necesario tener unas directrices claras orientadas hacia los procesos de misión crítica dentro de la organización. Es por esta razón que, unido a lo anterior, se hace necesario entender cómo se enmarcan estos estándares y metodologías dentro del gobierno de TI.

El Gobierno TI es un conjunto de procedimientos, estructuras y comportamientos utilizados para dirigir y controlar la organización hacia el logro de sus objetivos, su principal objetivo es entender las cuestiones y la importancia estratégica de TI para permitir a la organización que mantenga sus operaciones e implemente las estrategias necesarias para sus proyectos y actividades futuras. Este gobierno conduce a la empresa a tomar total ventaja de su información logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva (Ali, 2011).

Una de las situaciones que afectan a los gobiernos de TI es que comúnmente los confunde con marcos de trabajo referentes a buenas prácticas de administración y control de tecnología de la información, en contraparte ISO 38500 ha aportado con tratar de resolver confusión describiendo a los Gobierno de TI como el sistema ligado a la gestión utilizado por los niveles más altos de dirección.

Por otro lado, (Coello, 2008). acerca de los marcos de trabajo de gestión y control de TI, indica que estos brindan modelos que ayudan en la administración de los riesgos con el propósito de lograr los objetivos planteados en dicho proceso, aunque también enfatiza en que son parte esenciales de un los Gobierno de TI, es prioritario para este dedicar sus esfuerzos en la entrega de valor. También anota que los beneficios que ofrece un buen Gobierno de TI están íntimamente re correlación al: alineamiento estratégico, menores afectaciones riesgos, incremento en la calidad de servicios TI, reducción de costos, mejorar tiempos de respuestas ante acontecimientos

La importancia que las TI han alcanzado hoy en día no está en discusión, ha pasado de ser un componente de soporte o un departamento de asesoría, para formar parte totalmente fundamental para cualquier empresa. En muchas organizaciones, TI es indispensable para mantener, fortalecer y lograr objetivos de expansión en cualquier organización.

IV. CONCLUSIÓN

La metodología MAGERIT que ofrece un método sistemático para identificar y analizar los riesgos que pueden causar algún tipo de daño dentro de la empresa, como es la violación de la seguridad de los SI, en base a los daños que podrían causar los riesgos MAGERIT implementa medidas de control que permitan tener los riesgos mitigados. Fue elaborada por el Consejo Superior de Administración Electrónica de España, para saber, que tanto la administración como toda la sociedad dependen mucho de las TI para poder cumplir con su misión propuesta. Sin duda esta metodología es de gran utilidad para las organizaciones que trabajan con SSGI, pues permite identificar cuáles son los riesgos más críticos para una empresa.

MAGERIT versión 3 se ha estructurado en tres libros que son utilizados para el análisis de control de riesgos: el primer libro métodos, donde se describe la estructura que debe tener el modelo de la gestión de los riesgos; el segundo libro es el catálogo de elementos, este libro es una especie de inventario que las empresas pueden usar para enfocar el análisis de los riesgos y el tercer libro es una guía de técnicas, en donde se describen diferentes técnicas frecuentemente utilizadas en el análisis de riesgos.

Sin embargo, existen diversas metodologías para desarrollar el análisis y gestión de riesgos, la selección de la metodología más apropiada en cada caso depende de la disponibilidad de información y el nivel de detalle que se desee alcanzar. Entre las cuales están: EBIOS, MAGERIT, NIST SP 800:30, MEHARI, OCTAVE y CRAMM. La diferencia que tiene MAGERIT frente a otras metodologías, es que presenta una guía completa de cómo llevar a cabo paso a paso el análisis de riesgos, porque cuenta con tres libros, mientras que otras metodologías implementan diferentes métodos o formas para desarrollar el análisis y gestión de los riesgos.

V. REFERENCIAS

- Alcivar, B. (2012). *Libro I - Método*. Madrid: Esquema Nacional de seguridad (ENS).
- Alcivar, B. (2012). *Libro II - Catálogo de Elementos*. Madrid: Esquema Nacional de Seguridad (ENS).
- Alcivar, B. (2012). *Libro III - Guía de Técnicas*. Madrid: Esquema Nacional de Seguridad (ENS).
- Ali, N. (2011). *Implantación de Gobierno de TI*. Valencia: network-sec.
- Amutio, M. (2010). *Normalización en seguridad de las tecnologías de la información*. España: Ministerio de la presidencia.
- Amutio, M. (2012). *MAGERIT versión 3*. España: Portal administración electrónica(PAe-CTT).
- Arévalo, O., Escalante, K., Guevara, N., Jiménez, M., Montoya, A., & Orellana, J. (2009). *Metodología de análisis de riesgos de la empresa la casa de las baterías S.A de C.V.* San Salvador: Universidad Tecnológica de El Salvador.
- Barahona, M. (2011). *Protección de los activos de información*. Chile: Universidad Técnica Federico Santa María.
- Carvajal, A. (2012). *Análisis y gestión de riesgos, base fundamental del SGSI, metodología MAGERIT*. Colombia: Asociación Colombiana de Ingenieros de Sistemas (ACIS).
- Coello, H. (8 de Diciembre de 2008). *ITIL, COBIT, CMMI, PMBOK: Como integrar y adoptar los estándares para un buen Gobierno de TI*. Obtenido de <https://helkyncoello.wordpress.com/2008/12/08/itil-cobit-cmmi-pmbok-como-integrar-y-adoptar-los-estandares-para-un-buen-gobierno-de-ti/>
- Comunidad de Madrid. (2016). *Análisis y cuantificación del Riesgo*. Madrid: Comunidad de Madrid.
- 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*. Armenia: Universidad San Buenaventura Medellín (USBMED).
- 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 e Industrial Bravito S.A en la ciudad de Machala*. Cuenca: Universidad Politécnica Salesiana sede Cuenca.
- Gómez, L., & Álvarez, A. (2012). *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. Madrid: Asociación Española de Normalización y Certificación (AENOR).
- ISOTOOLS EXCELLENCE. (19 de Agosto de 2014). *ISO 27001 con los activos de la información de la empresa*. Obtenido de <https://www.isotools.org/2014/08/19/iso-27001-activos-información-empresa-3/>
- Llvisaca, M. (2010). *Análisis y gestión de riesgos para el servidor RADIUS del laboratorio de la facultad de ingenierías de sistemas*. Quito: Escuela Politécnica Nacional (EPN).
- Norma técnica Ecuatoriana-NTE. (2013). *Tecnologías de información, técnicas de seguridad, código de práctica para los controles de seguridad de la información (ISO/IEC 27002:2013 + Cor 2: 2015, IDT)*. Ecuador: Norma técnica Ecuatoriana (INEN).
- Portal administración electrónica-PAe. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. España: Portal administración electrónica (PAe).

