RISK ANALYSIS IN SECURITY OF INFORMATION

Article Information:

Received: October 21, 2013
Accepted: December 23, 2013

Keywords: Analysis of risks, controls, Risk analysis methodologies, Information security, Vulnerabilities.

Abstract: This article is centered in identifying which is the methodology Risk analysis that provides a better chance in making decisions within an organization, since information has become one of the most important assets from the business and its use is necessary to ensure the security and business continuity. There are several methodologies for risk analysis as: OCTAVE, MEHARI, MAGERIT, CRAMM, NIST SP 800-30 and EBIOS, those are oriented towards the same goal and which have characteristics that make them attractive in the business scope. From the study made in enterprise ECO - VOLTIO, it has been determined that MAGERIT seems to be the most effective and complete because it protects the information regarding for integrity, confidentiality, availability and other important features to ensure the security of the systems and processes of the organization. The application of risk analysis methodologies will help organizations gain more control over their assets, its value and threats that may impact them, forcing them to select security measures to ensure the success of their processes and increased competitiveness in the business world.

ANÁLISIS DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

Ana Abril[1], Esp., Jarol Pulido[2], Esp., John A. Bohada[3], Ph.D.

Grupo de Investigación MUISCA, Especialización en Seguridad de la Información, Facultad de Ingeniería, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.

[1]adcae@hotmail.com, [2]jarol1503@hotmail.com, [3]jbohada@jdc.edu.co

Información del artículo:

Clasificación: Artículo de Revisión

Recibido: 21 de octubre de 2013
Aceptado: 23 de diciembre de 2013

Palabras Claves: Análisis de riesgos, Controles, Metodologías de análisis de riesgos, Seguridad de la información, Vulnerabilidades.

Resumen: Este artículo se enfoca en exponer algunas opciones y permitir generar argumentos sólidos para identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información, la cual se ha convertido en uno de los activos más importantes del ámbito empresarial e implica una adecuada utilización y preservación para garantizar la seguridad y la continuidad del negocio. Existen varias metodologías de análisis de riesgos como: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30, las cuales se orientan hacia el mismo objetivo, pero tienen características propias que las hacen atractivas para las empresas en todos los sectores. A partir del estudio realizado en la empresa ECO – VOLTIO, se logra determinar que MAGERIT resulta ser la opción más efectiva y completa ya que protege la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización. La aplicación de metodologías de análisis de riesgos es de utilidad a las organizaciones para tener un mayor control sobre sus activos, su valor y las amenazas que pueden impactarlas, obligándolas a implementar medidas de seguridad que garanticen el éxito de sus procesos y una mayor competitividad en el mundo empresarial.

1. INTRODUCCIÓN

Con el crecimiento y auge de las Nuevas Tecnologías de la Información y la Comunicación (NTIC) [1], los avances en los servicios y modelos de comunicaciones e información, el uso continuo y generalizado a nivel global de la Internet; también se han aumentado los ataques a los sistemas informáticos, lo que ha llevado a las empresas a buscar estrategias que les permitan ejecutar análisis que prevengan, controlen y reduzcan los riesgos asociados a la violación o vulnerabilidad de su información. Para esta tarea es importante conocer los elementos que componen cada modelo, entre ellos están los recursos del sistema de información necesarios para que la organización funcione correctamente y el alcance de los objetivos propuestos, los eventos que pueden desencadenar un incidente que produzca daños en sus activos, la posibilidad de la materialización de una amenaza, las consecuencias de la misma, la posibilidad de que se genere un impacto en los bienes de la organización y finalmente los procedimientos que se llevan a cabo para reducir un riesgo [2]. "El análisis de riesgos pretende dar respuesta a tres interrogantes: saber qué se quiere proteger, contra quién y cómo se va a hacer" [3].

Es de vital importancia que en las empresas se establezcan objetivos empresariales y, a partir de ellos, políticas de seguridad que permitan controlar la realización de los procesos para así optimizar el análisis de riesgos [4]. Con la implementación de este imperativo estudio en las empresas, se debería garantizar la continuidad del negocio, asegurando los principios de la seguridad de la información.

Las organizaciones están expuestas día a día a amenazas tanto internas como externas que ocasionan robo de identidad e información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que pueden afectar la sostenibilidad de la entidad, por lo anterior, se cuestiona si las empresas conocen y aplican metodologías para el análisis de riesgos y protección de los principios de seguridad de la información o por el contrario desconocen los modelos que traigan protección de los principios de seguridad de la información.

Mediante esta investigación se darán a conocer las diferentes metodologías soportadas, utilizando para ello un caso de estudio aplicado a una organización, las razones por las que es importante su aplicación y finalmente recomendaciones sobre el modelo que se considera brinda una mejor oportunidad de toma de decisiones ante un riesgo inminente.

2. METODOLOGÍAS DE ANÁLISIS DE RIESGOS

Existen metodologías que permiten hacer un uso adecuado del análisis de riesgos y así asegurar los sistemas de información de las organizaciones. Entre las principales tenemos: OCTAVE [5], MEHARI [6], MAGERIT [7], CRAMM [8], EBIOS [9], NIST SP 800:30 [10]. En la tabla 1 se hace referencia a las fases que componen cada una de las metodologías mencionadas anteriormente.

Tabla 1. Fases de las metodologías para el análisis de riesgos

FASES	METODOLOGÍAS							
	1	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**
Caracterización del sistema	X	X	X	X	X	X	X	X
Identificación de amenazas	X	X	X		X	X	X	X
Identificación de vulnerabilidades	X		X			X		X
Análisis de controles	X	X	X	X	X		X	X
Determinación de la probabilidad								X
Análisis de impacto								X
Determinación del riesgo	X	X	X	X	X	X		X
Recomendaciones de control	X	X	X	X		X	X	X
Documentación de resultados	X			X				X
Establecimiento de parámetros			X		X			
Necesidades de Seguridad	X					X	X	

(1) OCTAVE, (1A) OCTAVE S, (1B) OCTAVE ALLEGRO,

(2) MEHARI, (3) MAGERIT, (4) CRAMM, (5) EBIOS, (6) NIST SP 800 – 30

La metodología OCTAVE está compuesta por tres fases en las cuales se tienen en cuenta cada uno de los aspectos señalados en la tabla anterior, lo que le permite a las organizaciones que, después de su implementación, se haga un plan de actividades detallado, implementado, monitoreado y controlado periódicamente [6] [11]. Cada una de las versiones de OCTAVE tiene algunas variaciones en cuanto a su concepción y a las actividades que se deben realizar en cada una de las fases [7]. Por otro lado, se menciona la metodología MEHARI que, al igual que la anterior, está comprendida por tres fases a partir de las cuales las empresas pueden tomar medidas oportunas para asegurar la continuidad del negocio. En seguida, encontramos MAGERIT conformada por cinco fases [12], las cuales se fundamentan en los siguientes elementos: activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas, los cuales deben ser proporcionados por el responsable de cada proceso a evaluar [13]. A continuación encontramos la metodología CRAMM compuesta por tres fases para realizar el proceso de análisis y gestión de riesgos [14], al igual que OCTAVE y MEHARI [15] [16] . Luego encontramos la metodología EBIOS, en la cual se llevan a cabo los siguientes pasos: estudio de contexto, expresión de las necesidades de seguridad, estudio de las amenazas, expresión de los objetivos de seguridad y determinación de los requerimientos de seguridad [17]. Finalmente, se menciona la metodología NIST SP 800-30 con su respectivo procedimiento [18] [19].

A continuación se hace una breve descripción de las mismas.

2.1 OCTAVE

La metodología OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation) [5], desarrollada por el Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa [20]. Por tanto, se tienen en cuenta las necesidades de la empresa donde se está implementando, permitiendo reducir los riesgos de seguridad de información, para lograr una mayor protección a estos elementos dentro del sistema. OCTAVE equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que a partir de éstos, los entes empresariales puedan tomar decisiones de protección de información basado en los principios de la seguridad de la información [20]. Esta metodología persigue dos objetivos específicos que son: concientizar a la organización que la seguridad informática no es un asunto solamente técnico y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos [21].

Hasta la fecha han sido publicadas tres metodologías de este tipo: OCTAVE que ha sido definida para grandes organizaciones de trecientos o más empleados, OCTAVE – S que se enfoca para pequeñas empresas, por ejemplo, PYMES con veinte a ochenta empleados y finalmente, OCTAVE ALLEGRO que permite analizar riesgos con mayor enfoque en activos de información [22], cada una de estas metodologías ejecuta las fases mencionadas con algunas variaciones dependiendo de las necesidades.

Con una metodología de análisis de riesgos como OCTAVE la empresa puede obtener beneficios como: dirigir y gestionar adecuadamente sus evaluaciones de riesgos, tomar decisiones basándose en los mismos, proteger los activos de información y, por último, comunicar de forma efectiva la información clave de seguridad [8] los cuales se derivan de las siguientes características: en primera medida, se establecen equipos auto dirigidos dentro de la organización con la finalidad de dar solución a las necesidades de seguridad que esta puede tener. Y por otro lado, se dice que este método es FLEXIBLE ya que es adaptable a todo tipo de organización independientemente del

entorno porque se basa en los riesgos, la capacidad de recuperación y la experiencia que se tenga en este tema [24]. Finalmente, es importante mencionar que OCTAVE busca asegurar la continuidad del negocio, identificar y medir riesgos, establecer controles para mitigarlos, conservar la información (activo más importante) e intervenir en todas las dependencias de la organización, ya que de esta manera puede aprovechar al máximo el conocimiento de los distintos niveles de la empresa [25].

2.2 MEHARI

MEHARI (Method for Harmonized Analysis of Risk) [26], es definida por la organización francesa especializada en la seguridad de los sistemas de información (CLUSIF) como una metodología que proporciona un conjunto de herramientas que permiten hacer un análisis de riesgos cualitativo y cuantitativo, cuando sea necesario para tener una adecuada gestión de seguridad [27]. De lo anterior, se deduce que está diseñada para acompañar los procesos de análisis de riesgos empresariales tanto actuales como futuros. En la metodología MEHARI se hace un análisis de la seguridad basado en tres criterios básicos: confidencialidad, integridad y disponibilidad [9].

2.3 MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es reconocida por ENISA (Agencia Europea de Seguridad de las Redes y de la Información) [28] y promovida por el Consejo Superior de Administración Electrónica con el fin de sistematizar el análisis de los riesgos que pueden presentar los activos de una organización [10]. Esta metodología es importante porque el crecimiento de la tecnología dentro de las organizaciones se está dando de manera exponencial y, por lo tanto, es necesario minimizar los riesgos asociados al uso de los sistemas garantizando la autenticidad, confidencialidad, integridad, disponibilidad [29] y trazabilidad[30] [31] de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización; de igual manera, presenta una guía de cómo llevar a cabo el análisis de riesgos y se divide en 3 libros, el primero describe la estructura del modelo de gestión de riesgos, el segundo presenta el inventario para enfocar el análisis de riesgos y el último compila una guía de técnicas de trabajo para dicho fin [32] [33].

MAGERIT fue creada con el fin de cumplir con objetivos como conocer el estado de seguridad de los sistemas de información y la implementación de medidas de seguridad, garantizar que no hayan elementos que queden fuera del análisis para que haya una profundidad adecuada en el mismo, mitigar las vulnerabilidades y asegurar el desarrollo del sistema en todas las fases de desarrollo [34]. Estos objetivos han posicionado a MAGERIT como una de las metodologías más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones [35] [36] [37].

2.4 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) [38], es el método de análisis y control de riesgos de la Central Computer and Telecommunications Agency (CCTA) del gobierno británico, permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las organizaciones día a día y es definida como una metodología que aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad de la información de un sistema y de sus activos [39] [40]. Cabe resaltar que CRAMM realiza un análisis de riesgos cualitativo y cuantitativo por lo que se conoce como una metodología mixta, ésta se apoya de una herramienta de gestión, lo que permite a las organizaciones tener una visión clara y priorizada de las amenazas a las que está expuesta y que pueden afectar los recursos y la continuidad del negocio [41], basándose en una matriz donde las filas representan los activos y las columnas los

riesgos que podrían afectar la integridad, disponibilidad y confidencialidad de los mismos [42], por otro lado, CRAMM proporciona información acerca de las características de funcionamiento del sistema y una identificación profunda y clara de los activos que se encuentran más expuestos [43].

Los elementos que se deben tener en cuenta para realizar un adecuado análisis de riesgos con la metodología CRAMM son: activos, vulnerabilidades, riesgos, amenazas, contramedidas, implementación y auditoría, los cuales permiten obtener un mejor resultado y asegurar la continuidad de negocio.

2.5 EBIOS

EBIOS (Expresión de las Necesidades e Identificación de los Objetos de Seguridad) [44], es una metodología francesa de gestión de riesgos, fue creada por la dirección Central de seguridad de los sistemas de Información de Francia DCSSI, con el fin de posibilitar la comunicación con los clientes internos y externos para contribuir al proceso de la gestión de riesgos de seguridad de los sistemas de información [45], de igual manera, ayuda a la empresa a tener un mayor reconocimiento en sus actividades de seguridad ya que esta tiene compatibilidad con las normas internacionales como la ISO.

Este procedimiento permite a la organización tener un mayor conocimiento de sus activos y las necesidades de seguridad identificando las amenazas y vulnerabilidades a las que se encuentran expuestos para su posterior mitigación.

2.6 NIST SP 800:30

SP 800:30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información) [46], Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI (Tecnología de la Información), proporciona un guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica [47]. Por otro lado, esta guía provee fundamentos para la administración de riesgos así como la evaluación y mitigación de los riesgos identificados dentro del sistema de TI con el objetivo de apoyar a las organizaciones con todo lo relacionado a Tecnología [24].

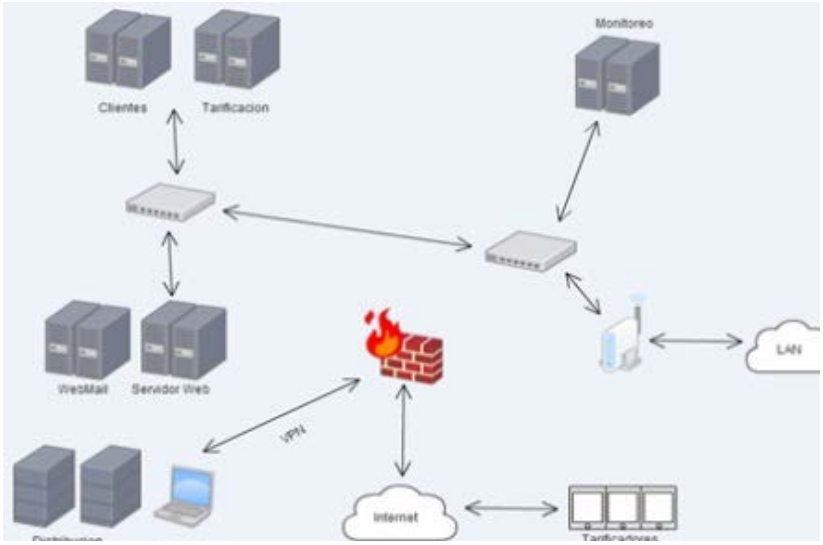
La metodología NIST SP 800:30 está compuesta por nueve fases: caracterización del sistema, la cual permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa; identificación de amenazas, es donde se definen las fuentes de motivación de las mismas; identificación de vulnerabilidades, en esta fase desarrolla una lista de defectos o debilidades del sistema que podrían ser explotadas por una amenaza; análisis de controles; determinación de la probabilidad; análisis de impacto; fase de determinación del riesgo, ayuda a evaluar el riesgo en el sistema de información, recomendaciones de control en donde se proporcionan los controles que podrían mitigar el riesgo identificado disminuyéndolo hasta un nivel aceptable, finalmente está la documentación de resultados la cual genera un informe con la descripción de amenazas y vulnerabilidades, midiendo el riesgo y generando recomendaciones para la implementación de controles [48][49].

3. APLICACIÓN DE METODOLOGÍAS DE ANÁLISIS DE RIESGOS EN UNA EMPRESA

En la actualidad, uno de los factores más importantes que se debe tener en cuenta en todo tipo de organizaciones es la seguridad de la información, ya que los incidentes relacionados con ésta comprometen los activos de las empresas y las ponen en riesgo, lo anterior genera la necesidad de implementar sistemas de seguridad a partir de un análisis de riesgos y minimizar así consecuencias no deseadas.

La empresa prototipo para la aplicación de las metodologías de análisis de riesgos se llama ECO – VOLTIO, la cual se dedica a gestionar proyectos relacionados con nuevas formas de generación, trasmisión y mejoras de energía. Esta empresa cuenta con una infraestructura tecnológica que, aunque es pequeña, permite el cumplimiento de los objetivos misionales de la organización conforme se ve reflejado en la Figura 1.

Figura 1. Infraestructura Tecnológica de ECO_VOLTIO



Fuente: los autores, 2013

Los activos de la empresa ECO- VOLTIO están expuestos a amenazas que aprovechan las vulnerabilidades que generan un riesgo e impacto significativo en el funcionamiento de la empresa, lo que afecta la integridad de la información y continuidad en el mercado, éstos se encuentran expuestos en la tabla 2.

Tabla 2. Variables aplicadas a las metodologías de análisis de riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES
Documentación	Incendio	Existe una alarma contra incendios, pero no está conectada con la estación de bomberos local.
Personal	Pandemias H1N1	Falta de seguimiento a la salud de los empleados continuo.
Servidores	Hacker	Puertos abiertos innecesarios.
Antivirus	Virus	Falta de antivirus.
Software tarificación	Alteración de datos	Bajos niveles de seguridad a la BD.
Bases de datos	Pérdida de información	Falta de backup.
Switch	Descarga eléctrica	Falta de mantenimiento preventivo a las redes eléctricas.
Sistema contable	Fraude interno	Falta de incentivos a los empleados.
Firewall	Carencia de actualización	Falta de cronograma de actualizaciones periódicas.
LAN	Pérdida de comunicación	Falta de un plan de contingencia.
Internet	Pérdida de conexión	Falta de protocolos de seguridad para red externa.
Equipos tecnológicos	Daño de hardware	Falta de mantenimiento preventivo.

Las variables mencionadas anteriormente se tienen en cuenta para todo análisis de riesgos y deben ser evaluadas según algunos criterios de medición dependiendo de la metodología seleccionada para dicho fin. Por ejemplo, para categorizaciones dadas a los activos, se dan de acuerdo con el valor que tienen para la organización: muy alto (MA) $30.000.000, alto (A) $20.000.000, medio (M) $10.000.000 y bajo (B) $1.000.000. Para las vulnerabilidades que pueden presentar los activos, se da una clasificación numérica de esta forma: Extremadamente frecuente (EF) valor 5, Muy frecuente (MF) valor 4, Frecuente (F) valor 3, Frecuencia normal (FN) valor 2 y Poco frecuente (PF) valor 1.

En la tabla 3 se aclara la clasificación del nivel de impacto que pueden tener las amenazas sobre los activos de la organización.

Tabla 3. Escala de valoración de impacto

TABLA DE IMPACTO			
VALORACIÓN			**DESCRIPCIÓN**
A	Alta	3	La ejecución de una vulnerabilidad (1) puede causar una alta pérdida económica de los principales activos tangibles o recursos; (2) puede significativamente violar, dañar, impedir alcanzar la misión de la organización, reputación, o intereses; o (3) puede causar la muerte humana o lesiones graves.
M	Media	2	La ejecución de la vulnerabilidad (1) puede resultar en la pérdida económica de activos de la empresa o recursos; (2) puede violar, dañar, o impedir alcanzar la misión de la organización, reputación, o intereses; o (3) puede resultar en lesiones personales.
B	Baja	1	La ejecución de la vulnerabilidad (1) puede causar la pérdida de algunos recursos o activos tangibles o (2) puede evidenciar un daño en la misión de la organización, reputación o intereses.

Luego de la determinación de la probabilidad se obtienen los índices (Alta, media, baja) para medir la ocurrencia de algún evento que represente un riesgo para la organización y la escala de valoración de ese riesgo, tal y como se muestra en la tabla 4.

Tabla 4. Escala de valoración de ocurrencia de un evento y del riesgo

VALORACIÓN			EVENTOS	RIESGOS
A	Alta	3	La fuente de amenazas es altamente motivada y suficientemente capaz de ser ejecutada y los controles para prevenir esta probabilidad son realizados, pero no efectivos.	Si se evalúa un riesgo como alto, existe la necesidad de aplicar medidas correctivas. Un sistema de información puede continuar operando, pero el plan de acciones correctivas debe ser puesto en práctica tan pronto como sea posible.

VALORACIÓN			EVENTOS	RIESGOS
M	Media	2	La fuente de amenaza es motivada y capaz, pero los controles aplicados pueden dificultar la ejecución exitosa de la vulnerabilidad.	Si se evalúa un riesgo como medio, acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones en un período razonable de tiempo.
B	Baja	1	La fuente de amenaza es pobremente motivada, existen controles realizados para prevenir las amenazas, existe dificultad para la ejecución de la vulnerabilidad.	Si un riesgo se evalúa como bajo, se debe determinar acciones de acuerdo con las necesidades y la obtención de un nivel de riesgo aceptable.

Los anteriores parámetros fueron usados en la aplicación de las metodologías: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30 en la empresa mencionada anteriormente; cabe resaltar que estas metodologías están orientadas al mismo objetivo con algunas variaciones en su procedimiento.

Con el fin de determinar la metodología que brinda una mejor oportunidad de toma de decisiones ante un riesgo inminente en la organización se planteó el siguiente formato (tabla 6), en el cual se evalúan diferentes aspectos de las metodologías tratadas.

Tabla 6. Comparación de las metodologías implementadas en ECO – VOLTIO

ANÁLISIS		1	2	3	4	5	6
TIPO DE ANÁLISIS	CUALITATIVO						
	CUANTITATIVO						
	MIXTO	X	X	X	X	X	X
TIPO DE RIESGO	INTRÍNSECO			X			X
	EFECTIVO	X		X	X		X
	RESIDUAL		X	X		X	X
ELEMENTOS	ACTIVOS	X		X	X	X	X
	VULNERABILIDADES	X	X	X	X	X	X
	AMENAZAS	X	X	X	X	X	X
	CONTROLES	X	X	X	X	X	X
	PROCESOS			X			
	ALCANCE		X		X		X
	PROBABILIDAD						X
	IMPACTO			X			X
	VALORACIÓN DE ACTIVO			X	X		
OBJETIVOS	AUTENTICIDAD			X		X	
	INTEGRIDAD	X	X	X	X	X	X
	CONFIDENCIALIDAD	X	X	X	X	X	X
	DISPONIBILIDAD	X	X	X	X	X	X

(1) OCTAVE, (2) MEHARI, (3) MAGERIT, (4) CRAMM, (5) EBIOS, (6) NIST SP 800 – 30

En esta tabla se evidencian las características propias de las metodologías OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30, las cuales fueron recopiladas durante el desarrollo de las mismas para determinar cuál metodología cumple con estos parámetros y genera mayor confianza para la mitigación de riesgos.

4. ANÁLISIS DE LAS METODOLOGÍAS APLICADAS

A partir de la comparación de las metodologías OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30 en la empresa ECO – VOLTIO y teniendo en cuenta los aspectos mencionados en la tabla 8- Comparación de las metodologías implementadas en ECO – VOLTIO, se determinó que la metodología que brinda un mayor cubrimiento del riesgo, asociado a la seguridad de la información en una empresa es la MAGERIT, en la medida que contempla un análisis de riesgos más detallado, teniendo en cuenta la mayoría de los elementos que forman parte de los objetivos misionales de la organización, protegiendo los datos en los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad con algunos aspectos adicionales como su confiabilidad y que no permite arbitrariedades del analista, lo que la hace diferente a las otras metodologías mencionadas.

Por otra parte, es importante mencionar que esta metodología tiene en cuenta el riesgo efectivo (inicial), el riesgo residual (después de los controles) y el riesgo intrínseco (probabilidad de materialización de una amenaza) con el fin de asegurar desde todo ángulo los activos de la organización. Una de las principales ventajas que tiene esta metodología para las empresas dentro de sus sistemas de gestión de seguridad es que cuenta con una herramienta propia y permite dar un primer paso para una certificación, ya que se encuentra alineada con los estándares ISO (Organización Internacional para la Estandarización) [50].

Cabe resaltar que las otras metodologías tratadas en este artículo son también usadas en diferentes organizaciones por ser las más reconocidas y porque realizan un análisis de riesgos homólogo al de MAGERIT. Algunas de las desventajas de las otras metodologías frente a esta son: que no incorporan las medidas de la eficacia de las salvaguardas, no administran el tipo de riesgo residual, no trabajan objetivos de seguridad como la trazabilidad. Metodologías como CRAMM, NIST SP 800 - 30 y OCTAVE tienen que pagar el costo de la licencia más allá del costo de la implementación del análisis y del mantenimiento lo que las hace menos atractivas para las empresas que buscan su aplicación para el análisis de riesgos.

5. RAZONES POR LAS CUALES SE DEBEAPLICARUNAMETODOLOGÍA DE ANÁLISIS DE RIESGOS EN LA EMPRESA

En este entorno empresarial, creciente y complejo es importante que las empresas tomen conciencia de aplicar continuamente una metodología de análisis de riesgo para garantizar el rendimiento de los sistemas y procesos dentro de la organización, algunas de las razones por las que las empresas deben utilizarla son:

- Permite tener claramente identificados los activos y las políticas de seguridad para que a partir de estos se puedan tomar decisiones y hacer mejoras en los procesos internos de la organización.
- Se garantiza la continuidad de negocio ya que permite tener en cuenta componentes y factores tanto internos como externos que intervienen en los objetivos misionales de la organización.
- Proporciona herramientas que permiten mitigar los riesgos a los que está expuesta la organización por medio de la creación de planes

de contingencia y controles que aseguren el los sistemas de información.

- Por medio de los procesos de auditabilidad, MAGERIT permite encontrar inconsistencias dentro del sistema que no han sido identificadas y no se sospechaba de su existencia.
- Con la ayuda de las metodologías de análisis de riesgos, las empresas pueden optimizar sus procesos y obtener un retorno de inversión.

6. CONCLUSIONES

- El análisis de riesgo a nivel empresarial es una excelente herramienta para generar planes de contingencia y continuidad del negocio, debido a que permite a las empresas mitigar el riesgo y garantizar el rendimiento de los sistemas informáticos. Cabe resaltar que es imposible eliminar un riesgo en su totalidad, lo que se puede hacer con la implementación de metodologías es reducirlo para que no genere ningún daño representativo al sistema informático de la organización.
- Las metodologías de análisis de riesgos le ayuda a las organizaciones a tener un mayor control sobre sus activos, su valor y minimizar las amenazas que pueden impactarlas obligándolas a seleccionar medidas de seguridad que garanticen el éxito de sus procesos y una mayor competitividad en el sector que se desenvuelven.
- La metodología MAGERIT es una buena opción que permite a las organizaciones una mayor asertividad en la toma de decisiones, debido a que su análisis de riesgos es más completo y tiene en cuenta elementos empresariales que otras metodologías no contemplan.

REFERENCIAS

[1] Ministerio de Educación y Ciencia, Secretaría General de Educación, Instituto Superior de Formación del Profesorado. La Acción Tutorial: Su Concepción y su Práctica. [On line]. Disponible en http://books.google.com.co/books?id=8Gg0qAwn4cMC&pg=PA220&dq=concepto+ NTIC&hl=es&sa=X&ei=ECiuUsujMemmsQSD04GYDQ&ved=0CDwQ6AEwAw#v=onepage&q=concepto%20NTIC&f=false

[2] E. Daltabiut, L. Hernández, G. Mallén, J. Vázquez, La seguridad de la información, México: Limusa Noriega Editores S.A., 2009.

[3] J. Areitio Bertolín, Seguridad de la información, redes, informática y sistemas de información, Madrid-España: Cengage Learning Paraninfo S.A., 2008.

[4] V. Aceituno Canal, Seguridad de la información, México: Limusa Noriega Editores, 2008.

[5] R. Gómez, D. Pérez, Y. Donoso, A. Herrera, (2010, junio), Metodología y gobierno de la gestión de riesgos de tecnología de la información, Revista de Ingeniería SCIELO, [On line]. Disponible en http://www.scielo.unal.edu.co/scielo.php ?script=sci_arttext&pid=S0121-49932010000100012&lng=es&nrm=

[6] M. Muñoz, (2013, agosto), Security Consultant ETEK International, Introducción a OCTAVE. [On line]. Disponible en http://www.acis.org.co / memorias/JornadasSeguridad/IVJNSI/ MauricioMunoz-IVJNSI.pdf

[7] J. M. Matalobos, (2013, septiembre), Análisis de Riesgos de Seguridad de la Información, Universidad Politécnica de Madrid, [On line]. Disponible en http://oa.upm.

es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

[8] J. A. Peña Ibarra, Vicepresidente internacional ISACA, (2013, octubre), Metodologías y normas para el análisis de riesgos: ¿Cuál debo aplicar?, [On line]. Disponible en http://www.isaca.org/ chapters7/Monterrey/Events/Documents/ 20100302%20 Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

[9] Y. Campos, Administración de riesgos en las tecnologías de información, Universidad Nacional Autónoma de México. Disponible en http://www.ptolomeo.unam.mx:8080/ xmlui/bitstream/handle/132.248.52.100/1025/Tesis.pdf?sequence=1

[10] H. Leteller, (2013, julio), Consultor Alfresco y J2EE en Blaunia, Seguridad de los sistemas de información, Metodología MAGERIT. [On line]. Disponible en: http://www.belt.es/expertos/home2_experto.asp?id=5374

[11] R. Gómez, D. Pérez, (2010, junio), Metodología y gobierno de la gestión de riesgos de tecnología de la información, Universidad de Los Andes, [On line]. Disponible en http://www.scielo.org.co/ scielo. php?pid=S012199320100001000 12&script=sci_arttext

[12] A. Carvajal, (2013, septiembre), Análisis y gestión de riesgos: base fundamental de SGSI, caso: Metodología MAGERIT, Globaltek Security, [On line]. Disponible en http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

[13] J. Cocho, Director de proyecto y Romo S. Consultor principal SEMA- GROUP, (2013, septiembre), Metodología de análisis de gestión de riesgos de los sistemas de información, [On line]. Disponible en http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

[14] MC. Crespo, (2013, enero) El análisis de riesgos dentro de una auditoría, Informática: pasos y posibles metodologías, Universidad Carlos II de Madrid, [On line]. Disponible en http://earchivo.uc3m.es/bitstream/handle /10016/16802/PFC_Carmen_Crespo_Rin.pdf?sequence=1

[15] J. Baños y P. Carrera, (2013, Octubre), Elaboración del plan de disponibilidad del TI para la empresa RELIANCE, Escuela Politécnica Nacional, [On line]. Disponible en http://bibdigital.epn.edu.ec/bitstream /15000/2405/1/CD-3137.pdf

[16] A. Huerta, (2013, marzo), Introducción al análisis de riesgos – Metodologías I, [On line]. Disponible en http://www.securityartwork.es/2012/03/30/introduccion-alanalisis-de-riesgos-metodologias-i/

[17] R. Gil, Sistematización de la gestión de riesgos de seguridad informática en la red de la Universidad Centro Occidental Lisandro Alvarado. [On line]. Disponible en https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&cad=rja&ved=0CGMQFjAJOAo&url=http%3A%2F%2Friesgosdeseguridad.wikispaces.com%2Ffile%2Fview%2Ftrabajo%2Bde%2Bgrado.%2Bpor%2Braul%2Bgil%2B0312.doc&ei=TGBjUo-lJonu8ATLtoDQAQ&usg=AFQjCNEJjqdnRx1z3ZARdEoyOOijVOuJcg&bvm=bv.55139894,d.eWU

[18] Instituto Nacional de Tecnologías de la Comunicación (INTECO), Guía avanzada de gestión de riesgos. [On line]. Disponible en https://www.google.com.co/url?sa=t& rct=j&q=&esrc=s&source=web&cd=30&cad=rja&ved=0CG0QFjAJOBQ&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2FteW3c753nhRRK6a0e7iZKg&ei=bTRkUqzZB4fa8ASC-

jIB4&usg=AFQjCNGNHP8zxXy5j0ct-NID4ESBSaxvj2A&sig2=k-5NDyu19zdM2Cg-r4gvyQ&bvm=bv.55139894,d.eWU

[19] J. Borbón, Buenas prácticas, estándares y normas, Revista Seguridad y Defensa Digital. [On line]. Disponible en http://revista. seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas

[20] T. Freire, Directora de la Colección Biblioteca de Economía y Finanzas, Dirección y gestión de los sistemas de información en la empresa. [On line]. Disponible en http://books.google.com.co/ books?id=OqlSVYn0fI0C&pg=PA180&dq=-gestion+de+riesgos+metodologia+octave&hl=es&sa=X&ei=MOVlUqrEC4LA-9QSJh4Ag&ved=0CCwQ6AEwAA#v=onepage&q=gestion%20de%20riesgos%20metodologia%20octave&f=false.

[21] M. C. Gallardo, P. O. Jácome, (2013, agosto), Análisis de riesgos informáticos y elaboración de un plan de contingencia TI para la empresa eléctrica Quito S.A., [On line]. Disponible en http://bibdigital.epn. edu.ec/bitstream/15000/3790/1/CD-3510.pdf

[22] E. Cárdenas, (2013, octubre), Metodologías para el análisis. Universidad técnica de Manabí (UTM), [On line]. Disponible en http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

[23] J. A. Betolini, (2013, agosto). Gestión de riesgos de seguridad y privacidad de la información, Universidad de Deusto, [On line]. Disponible en http://www.conec tronica.com/Seguridad/Gesti%C3%B3n-de-riesgos-de-seguridad-y-privacidad-de-lainformaci % C3%B3n.html

[24] CERT, 2013, septiembre, Metodología OCTAVE, [On line]. Disponible en http://www.cert.org/octave/

[25] M. Baldeón, C. Coreonel, Plan maestro de seguridad informática para la UTIC DE LA ESPE con lineamientos de la norma ISO /IEC 27002. [On line]. Disponible en http://repositorio.espe.edu.ec/bitstream/21000/6026/1/AC-GS-ESPE-034491.pdf

[26] European Union Agency for Network And Information Security. [On line]. Disponible en http://rminv.enisa.europa.eu/methods/m_mehari.html

[27] CLUSIF, Metodología MEHARI, 2010. [On line]. Disponible en http://www.clusif.asso. fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf

[28] Y. Tapias, (2013, julio), Mejoramiento de la Seguridad En PYMES, [On line]. Disponible en http://aprendiendosecinfo. blogspot.com/

[29] Oficina Asesora de Sistemas, (2013, agosto), Proceso de desarrollo OPEN–UP/OAS, Universidad Distrital Francisco José de Caldas, [On line]. Disponible en http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

[30] Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Metodologías de análisis y gestión de riesgos de los sistemas de información, libro 1: guía de técnicas, [On line]. Disponible en http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.UmMfU3BFXpU

[31] UNAD, Sistema de Gestión de Seguridad de la Información SGSI, dimensiones de seguridad, [On line]. Disponible en http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-enlinea/3221_dimensiones_de_seguridad.html

[32] C. Gutiérrez, (2013, mayo), Metodología MAGERIT: metodología práctica para gestionar riesgos, [On line]. Disponible en

http://www.elsemanario.com/noticias/tecnologia/85028-magerit-metodologia-practica-para-gestionar-riesgos.html

[33] L. Camalo, (2013, agosto), Gestión de Riesgos 2010, [On line]. Disponible en http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

[34] J. Eterovic, G. Pagliari, Metodología de Análisis de Riesgos Informáticos. [On line]. Disponible en http://www.cyta.com.ar /ta1001 /v10n1a3.htm

[35] E. Ferrero, (2006), Análisis y gestión de riesgos del servicio IMAT del sistema de información del I.C.A.I. Madrid, Universidad Pontificia Comillas, [On line]. Disponible en http://www.iit.upcomillas.es/pfc/resumenes/44a527e27a231.pdf

[36] A. Lucero, J. Valverde, Análisis y gestión de riesgos de los sistemas de la cooperativa de ahorro y crédito Jadin Uzuayo (Ecuador), Utilizando la metodología MARGERIT. [On line]. Disponible en http://dspace.ucuenca.edu.ec/bitstream/123456789/1342/1/tcon640.pdf

[37] Ministerio de Administraciones Públicas, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [On line]. Disponible en http://www.pilar-tools.com/magerit/v2/meth-es-v11.pdf

[38] M. Fernández Manuel, Estudio de una estrategia para la implementación de los sistemas de gestión de seguridad de la información, Universidad de CÁDIZ (España). [On line]. Disponible en http://www.mfbarcell.es/conferencias/Metodolog%C3%ADas%20de%20seguridad_2.pdf

[39] R. Valbuena, Seguridad en redes de telecomunicaciones e informática. 2010. [On line]. Disponible en http://seguridad digitalvenezuela.blogspot.com/2010/07/cramm-software-para-el-manejo-de.html

[40] M. Crespo, (2013, enero), El análisis de riesgos dentro de una auditoría informática: pasos y posibles metodologías, Universidad Carlos III de Madrid, [On line]. Disponible en http://e-archivo.uc3m.es/bitstream/handle/10016/16802/PFC_Carmen_Crespo_Rin.pdf;jsessionid=8EA401088DD103F1324990EBA6FD6CC5?sequence=1

[41] F. Martus, V. Mesa, Seguridad, Editorial MAT, S.L., España, 2006.

[42] E. Landazuri, C. Roberto, J. C. Merino, Manual de procedimientos para ejecutar la auditoría informática en la Armada del Ecuador, Facultad de Ingeniería en Sistemas e Informática, ESPE-Ecuador, 2005. [On line]. Disponible en http://repositorio.espe. edu.ec/handle/21000/741

[43] Department of Information and Communication Systems Engineering, Risk analysis of a patient monitoring system using Bayesian Network modeling, University of the Aegean, GR 83200 Karlovasi, Samos, Greece. [On line]. Disponible en http://www.science direct. com/science/article/pii/S15320464050010 97

[44] D. Maques, A. Marcano, Modelo de estrategias integrales de seguridad para la infraestructura de red de datos, Caso de estudio universidad de oriente núcleo MONAGAS. [On line]. Disponible en http://www.laccei.org/LACCEI2012-Panama/RefereedPapers/RP099.pdf

[45] Secretaria General de la Defensa Nacional Francesa, Dirección Central de la Seguridad de los Sistemas de Información, Método EBIOS. Septiembre 2013. [On line]. Disponible en http://www.ssi.gouv.fr /archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf

[46] Comisión Interamericana de Telecomunicaciones, (2009, septiembre), Organización de los Estados Americanos, INFO@CITEL,

Gestión de Riesgos de Seguridad, [On line]. Disponible en http://www.oas.org/en/citel/infocitel/2009/septiembre/seguridad_e.asp

[47] NIST SP 800-30, (2013, octubre), Estándar para la evaluación del riesgo técnico, [On line]. Disponible en http://searchsecurity.techtarget.in/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation

[48] V. N. Avalos, (2013, septiembre), Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica NIST SP 800 – 30, Escuela Politécnica del Ejército, ESPE-Ecuador, [On line]. Disponible en http://repositorio.espe.edu.ec/bitstream/21000/2333/1/T-ESPE-021816.pdf

[49] Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas, UPIICSA, (2013, septiembre), Metodologías de análisis, [On line]. Disponible en http://upiicsa-ha4cm1. blogspot.com/2012/05/ha4cm1-gonzalez-jazmin.html

[50] ISO, Organización Internacional para la Estandarización. [On line]. Disponible en http://www.iso.org/iso/home.html