Polo del Conocimiento

Pol. Con. (Edición núm. 18) Vol. 3, No 4
Abril 2018, pp. 230-244
ISSN: 2550 - 682X
DOI: 10.23857/pc.v3i4.809

Ciencias de la Computación

Artículo de Revisión

Recepción: 22/ 12/ 2017

Aceptación: 05 / 03/ 2018

Publicación: 21/ 04/ 2018

Análisis de riesgos en seguridad de la información

Risk analysis in information security

Análise de risco em segurança da informação

Mayra A. Tejena-Macía[I]
mayratejena@gmail.com

Correspondencia: mayratejena@gmail.com

[I] Magister en Tecnología e Innovación Educativa, Ingeniera en Sistemas, Docente de la Universidad Laica "Eloy Alfaro" de Manabí. Manta, Ecuador.

Resumen

Este trabajo, se enfoca en 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, 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.

Palabras clave: análisis de riesgos; controles; metodologías de análisis de riesgos; seguridad de la información; vulnerabilidades.

Abstract

This article aims to raise the need and importance of designing the process of evaluation of higher education teachers that contributes to the improvement and permanent reinforcement on the quality of university teacher performance. Where the fundamental role of evaluation, in itself is an option for reflection and improvement of reality, and serves as an opportunity and a sense of repercussion both in the personality of the evaluated, as in their environment and in the team that forms part, and hence that evaluation as such is properly understood and positioned to enable the professional advancement of teachers. From this evaluation it should be an activity of analysis, commitment and training of teachers, which allows to assess and prosecute the conception, practice, projection and development of the activity and teacher professionalization. Considering that the modern world is characterized by a constant change and demands of them a high capacity of adaptation like basic condition of survival. Therefore, the process of organizational change

must enable it to improve and restructure universities and their professionals so that they are linked to social, economic and technological forces and finally to achieve a quality education.
Keywords: higher education; evaluation; quality; teaching.

Resumo

Este trabalho consistiu em analisar o uso da e-administração aplicada à gestão humana em instituições públicas do país. Também foi proposto como objetivo parcial, fazer um diagnóstico descritivo sobre a implementação de ferramentas tecnológicas em instituições e sobre a gestão humana em geral, para determinar como os processos são realizados. A metodologia consistiu em um estudo descritivo. Para coletar as informações, utilizou-se observação participante, entrevista estruturada e questionário. A população foi composta pelos trabalhadores de quatro (04) instituições públicas intencionalmente selecionadas. A amostra foi dividida em uma amostra intencional (Diretores) e uma amostra aleatória para os demais trabalhadores de cada instituição. Como resultado da obtenção de altos percentuais de fragilidades em vários dos aspectos avaliados, destacando a importância da implementação de ferramentas de e-Administração, a partir da abordagem de Gestão Humana e Nova Gestão Pública.
Palavras chave: educação superior; avaliação; calidad; docente.

Introducción

Los ataques a los sistemas informáticos han aumentado, como consecuencia a los avances en los servicios y modelos de comunicaciones e información y el auge de las nuevas Tecnologías de la Información y la Comunicación (TIC), 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. 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 (Daltabiut, Hernandez & Guillen,

2009). "El análisis de riesgos pretende dar respuesta a tres interrogantes: saber qué se quiere proteger, contra quién y cómo se va a hacer". (Areitio, 2008)

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.

Metodologías

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, MEHARI, MAGERIT, CRAMM, EBIOS, NIST SP 800:30. 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	

La metodología OCTAVE está compuesta por tres, lo que permite a las organizaciones que, se haga un plan de actividades detallado, implementado, monitoreado y controlado periódicamente (Muñoz, 2013) (Gómez, 2010). 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 (Matalobos, 2013). 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 (Carvajal, 2013), 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. A continuación, encontramos la metodología CRAMM compuesta por tres fases para realizar el proceso de análisis y gestión de riesgos, al igual que OCTAVE y MEHARI. 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. Finalmente, se menciona la metodología NIST SP 800-30 con su respectivo procedimiento.

A continuación, se hace una breve descripción de las mismas.

- **OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation)**

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 (Gomez & col, 2010). 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. 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. (Gallardo & Jácome, 2013)

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.

- **MEHARI (Method for Harmonized Analysis of Risk)**

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. 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.

- **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) (Tapia, 2013) 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 (Leteller, 2013). 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 y trazabilidad de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización.

MAGERIT es una de las metodologías más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones (Ferrero, 20016).

- **CRAMM (CCTA Risk Analysis and Management Method)**

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 (Valbuena, 2010). 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 (Martus, 2006), 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, 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.

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.

- **EBIOS (Expresión de las Necesidades e Identificación de los Objetos de Seguridad)**

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.

- **NIST SP 800:30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información)**

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. 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 (CERT, 2013).

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.

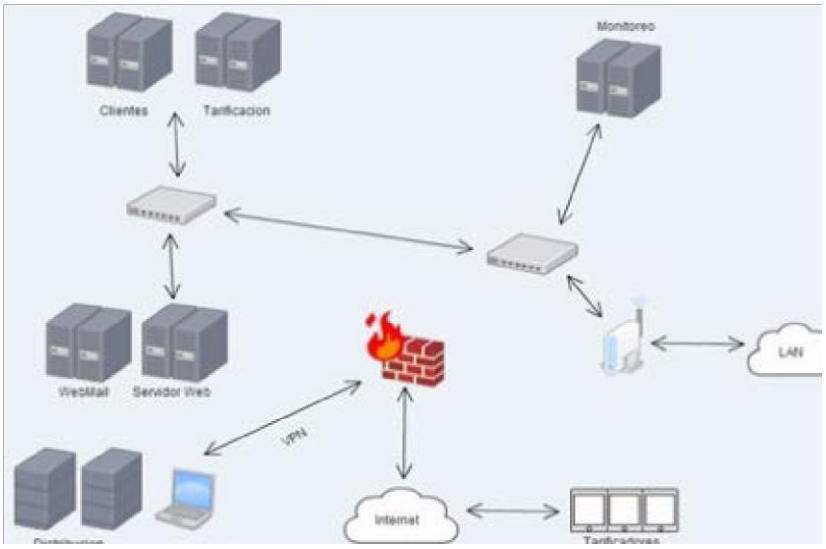
Aplicación de metodologías de análisis de riesgos en una empresa

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 me- cuenta con una infraestructura tecnológica que, todologías de análisis de riesgos se llama ECO – aunque es pequeña, permite el cumplimiento de VOLTIO, la cual se dedica a gestionar proyectos los objetivos misionales de la organización conrelacionados con nuevas formas de generación, forme se ve reflejado en la

Figura 1. Trasmisión y mejoras de energía.



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

Análisis

A partir de la comparación de las metodologías OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30, 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.

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.

Discusión

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 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.

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 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 bibliográficas

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=8Gg 0qAwn4cMC&pg=PA220&dq=concepto+NTIC&hl=es&sa=X&ei=ECiuUsujMemmsQSD04GY DQ&ved=0CDwQ6AEwAw#v=onepage&q=concepto%20NTIC&f=false

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

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

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

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=

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

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

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

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

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

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

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

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

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

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=MOVlUqrEC4LA9QSJh4Ag&ved=0CCwQ6AEwAA#v=onepage&q=gestion%20de%2 0riesgos%20 metodologia%20octave&f=false.

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

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

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

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

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

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

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

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

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

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

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

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

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=8EA401088DD103F 1324990EBA6FD6CC5?sequence=1

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

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.