EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON LA METODOLOGÍA OCTAVE

SAFETY ASSESSMENT INFORMATION WITH THE OCTAVE METHODOLOGY

Departamento de electronica, Facultad de Ingeniería, Institución Universitaria Pascual Bravo
Medellín, Colombia
vramirez@pascualbravo.edu.co

Departamento de Telecomunicaciones, Facultad de Ingeniería, Universidad Santo Tomas de Aquino
Medellín, Colombia
alejo1409@icee.org

Víctor Manuel Gómez Ramírez
Alejandro Ospina Gil

RESUMEN

Se inicia con una introducción a la metodología de evaluación de los riesgos a la seguridad de la información OCTAVE para la protección de los recursos críticos relacionados con la información en las organizaciones. Se describen las principales diferencias de esta metodología frente a otras evaluaciones de la seguridad de la información. Se presentan los tres métodos implementados por el CERT a partir de la metodología OCTAVE y se realizan algunas consideraciones que deben tenerse en cuenta a la hora de realizar una evaluación de este tipo.

PALABRAS CLAVES:

Seguridad de la información, metodología OCTAVE, riesgos de seguridad de la información.

ABSTRACT

It begins with an introduction to the methodology of risk assessment to the OCTAVE information security to protect critical resources related to information in organizations. Describes the main differences of this method compared to other safety evaluations of the information. We present three methods implemented by the CERT from the OCTAVE methodology and makes some considerations to be taken into account when making an assessment of this type.

KEYWORDS:

Information Security, OCTAVE methodology, risks of information security.

1. Introducción

La información se ha convertido no sólo en un activo valioso, sino estratégico en las organizaciones (Melo 2008), y las Tecnologías de la Información (TI) ahora tienen un gran impacto en la forma como las empresas emplean esta información, con el propósito de ser competitivas. Sin embargo, el entorno tecnológico está cada vez más expuesto a incidentes de seguridad; esto hace que las fallas sean ahora más frecuentes y en algunas ocasiones no se pueda reaccionar ante las amenazas sin que se afecte el funcionamiento de la organización. En este sentido, la tendencia es establecer procedimientos que le permitan a las Instituciones estar preparadas para entender y enfrentar de manera proactiva los riesgos a los cuales se enfrentan. Según Viloria (Viloria y Blanco 2009), un plan estratégico bajo una perspectiva de la seguridad de la información (SIF), es un factor crítico de éxito para cualquier empresa madura en el uso y la adopción de los Sistemas de Información (SI) y las Tecnologías de la Información y la Comunicación (TIC).

La seguridad es un conjunto de sistemas, métodos y herramientas destinados a proteger la información, proceso en el cual participan además las personas (CERT 2011). Se dice que el computador más seguro es aquel que está apagado y por lo tanto, desconectado de la red. Pero ni siquiera esto hace a un equipo seguro, porque las amenazas del entorno son muchas y de muy distinto tipo, es por eso que se deben aplicar políticas, metodologías y técnicas de protección de la información.

Aunque la seguridad informática no es un bien medible, sí se pueden desarrollar diversas herramientas para cuantificar la inseguridad informática. En este sentido, la evaluación eficaz de los riesgos de seguridad de la información debería considerar los temas tanto organizacionales como tecnológicos, examinando cómo las personas usan la infraestructura de cómputo de la organización diariamente.

El análisis de riesgos es el primer paso de la gestión de la seguridad de la información de una organización y es necesario para realizar su gestión, es decir, tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos y controlarlos, o sea realizar la gestión de riesgos (Eterovic y Pagliari 2011). Por lo tanto, una evaluación es sumamente importante para cualquier iniciativa de mejora de seguridad, porque genera una visión amplia de los riesgos en la organización, dando una base para mejorar.

Existen en la actualidad diversas estrategias de evaluación de la seguridad como Magerit, Octave y Mehari, entre otras. En este articulo se pretende dar un acercamiento a la metodología de evaluación de riesgos de la seguridad, llamada OCTAVE® y sus ventajas.

2. METODOLOGÍA OCTAVE

a. Definición.

Es una evaluación estratégica, basada en los riesgos y la planeación técnica de la seguridad. Es un proceso auto dirigido, esto significa que las personas de la empresa no sólo participan en la evaluación, sino que asumen la responsabilidad de establecer la estrategia de seguridad una vez se realice la evaluación. Precisamente uno de los aspectos más interesantes de esta metodología, radica en que la evaluación se apoya en el conocimiento del personal de la organización, para capturar el estado actual de las prácticas de seguridad. De esta manera, es más probable determinar los riesgos de los recursos más críticos, priorizar áreas de mejora y proponer la estrategia de seguridad.

A diferencia de las evaluaciones típicas enfocadas en la tecnología, OCTAVE está dirigida a riesgos organizacionales y está enfocada en temas estratégicos relacionados con la práctica, es flexible y puede aplicarse a la medida para la mayoría de las organizaciones. La Tabla 1 resume las diferencias importantes entre OCTAVE y otras evaluaciones.

Fecha de recibo del artículo: 3 de Mayo de 2012
Fecha de aprobación: 12 de Septiembre de 2012

Tabla 1 diferencias clave entre octave y otras metodologías.

OCTAVE	Otras Evaluaciones
Evaluación organizacional	Evaluación de Sistemas
Enfoque sobre prácticas de seguridad	Enfoque sobre prácticas de tecnología
Temas estratégicos	Temas tácticos
Auto dirigido	Dirigido por expertos

b. *Características claves de la metodología*

Como es una evaluación auto dirigida, exige que la organización maneje el proceso de la evaluación y tome las decisiones para proteger la información. Un equipo interdisciplinario, llamado el equipo de análisis, lleva a cabo la evaluación. El equipo incluye personas tanto de las unidades del negocio (las diferentes áreas de la empresa), como del departamento de TI, y ambas perspectivas son cruciales al caracterizar globalmente la organización en cuanto a los riesgos de seguridad de la información.

El equipo de análisis trabaja orientando las necesidades de seguridad de la organización, equilibrando los tres aspectos claves que se ilustran en la Figura 1. El riesgo operacional, las prácticas de seguridad y la tecnología.

La evaluación esta basada en dos de estos aspectos: el riesgo operacional y las prácticas de seguridad. La tecnología sólo se examina en relación a las prácticas de seguridad.

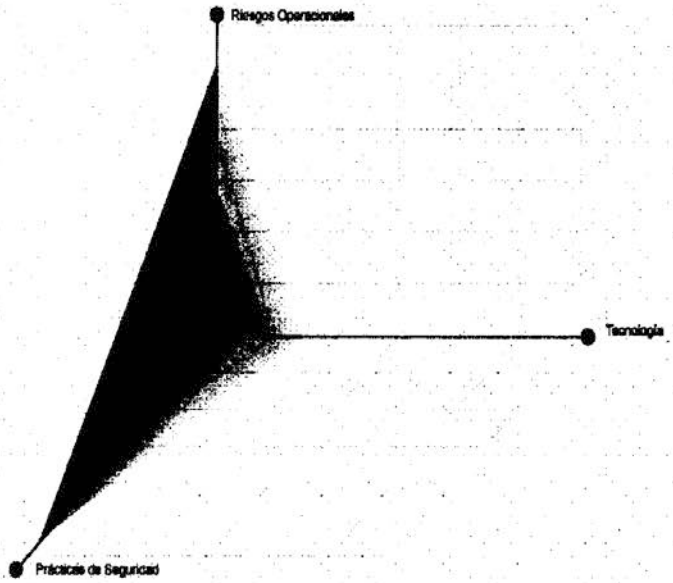

Figura 1 OCTAVE hace un balance de los tres aspectos. Adaptado de CERT 2011.

Como resultado de la evaluación, se toman decisiones de protección de la información, basándose en los riesgos de confidencialidad, disponibilidad e integridad de los recursos críticos relacionados con la información. Todos los aspectos de riesgo (recursos, amenazas, vulnerabilidades, e impacto organizacional), son tenidos en cuenta al momento de tomar una decisión, permitiendo a una organización diseñar la estrategia de protección para los riesgos de seguridad.

A. Face de la metodología OCTAVE

La evaluación es implementada en tres fases ilustradas en la Figura 2:

Fase 1 Construir perfiles de amenazas con base en los recursos: En ésta fase se realiza una evaluación organizacional. El equipo de análisis determina lo que es importante para la organización (recursos relacionados con la información) y también determina que está haciéndose para proteger esos recursos actualmente. El equipo entonces selecciona los recursos que son más importantes para la empresa (los recursos críticos) y describe los

Fecha de recibo del artículo: 3 de Mayo de 2012
Fecha de aprobación: 12 de Septiembre de 2012

requisitos de seguridad para cada recurso crítico. Finalmente, identifica las amenazas a cada recurso crítico, creando un perfil de la amenaza para ese recurso.

Fase 2 Identificar las Vulnerabi lidades de la Infraestructura: Es una evaluación de la infraestructura de la información. El equipo de análisis examina las rutas de acceso a la red, identificando las clases de componentes de tecnología de la información asociados a cada recurso crítico. El equipo determina entonces, hasta que punto cada clase de componente es resistente a los ataques de la red de computadores.

Fase 3 Desarrollar la Estrat egia y los planes de Seguridad : Durante esta parte de la evaluación, el equipo de análisis identifica los riesgos de los recursos críticos de la organización y decide qué hacer sobre ellos. El equipo crea una estrategia de protección para la organización y también planes de mitigación, para manejar los riesgos, basándose en un análisis de la información recogida.

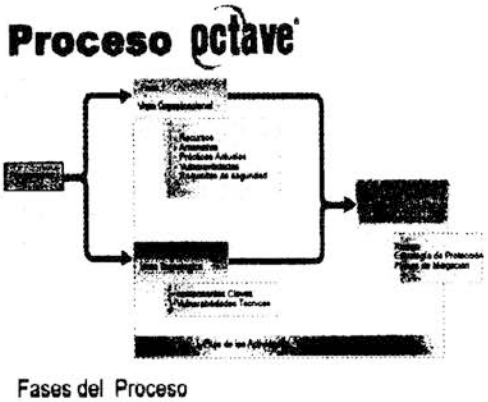

Figura 2 Fases del proceso de evaluación. Adaptado de (CERT 2011).

3. Métodos Consistentes Con La Metodología Octave

1.1 Criterios de la metodología

Los elementos esenciales de la metodología, están reunidos en un conjunto de criterios. Pueden existir muchos métodos o implementaciones consistentes con éstos, pero hay sólo un conjunto de criterios OCTAVE. En este punto, se han desarrollado por el equipo de ingeniería en seguridad cibernética (CERT, por sus siglas en inglés) de la universidad Carnegie Mellon, tres métodos consistentes con los criterios. El Método OCTAVE, se diseñó pensando en las organizaciones grandes, mientras OCTAVE-S se desarrolló para las organizaciones pequeñas. Finalmente, el OCTAVE-Allegro es un método simplificado para evaluar y asegurar la seguridad de la información, que se puede realizar como un taller, en el que es posible adelantar la evaluación, sin la participación extensiva de la organización entre otros aspectos. Además, otros podrían definir métodos para contextos específicos, que sean consistentes con los criterios. La figura 3 ilustra estos puntos.

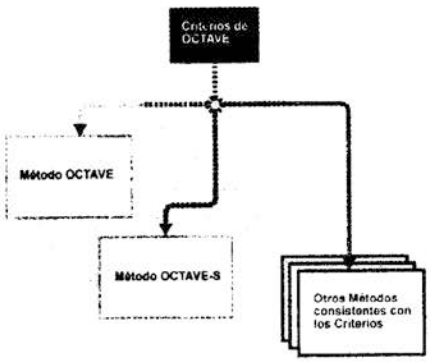

Figura 3 Diferentes implementaciones de OCTAVE. Adaptado de CERT 2011.

Los criterios de OCTAVE se componen en tres partes que son: los principios, los atributos y los resultados. Los principios son los conceptos fundamentales sobre los que se basa la evaluación y definen la filosofía, detrás del proceso de

Fecha de recibo del artículo: 3 de Mayo de 2012
Fecha de aprobación: 12 de Septiembre de 2012

evaluación. Ellos forman la metodología de evaluación y proveen las bases del proceso. Por ejemplo, la auto dirección es uno de los principios de OCTAVE. El concepto de auto dirección significa, que las personas dentro de la organización, están en la mejor posición para realizar la evaluación y tomar decisiones.

Los requisitos de la evaluación están incluidos en los atributos y resultados (salidas). Los atributos son las cualidades distintivas o características de la evaluación. Son los requisitos que definen los elementos básicos de la metodología OCTAVE y definen lo que es necesario para lograr una evaluación con éxito, tanto en los procesos como en las perspectivas organizacionales. Los atributos se derivan de los principios. Por ejemplo, uno de los atributos de OCTAVE es que un equipo interdisciplinario (el equipo de análisis), conformado con personal de la organización, lleve a cabo la evaluación. El principio detrás de la creación de un equipo de análisis, es la auto dirección.

Finalmente, el producto del trabajo (salidas), son los resultados requeridos de cada fase de la evaluación. Ellas definen los resultados que un equipo de análisis debe lograr durante cada fase. Hay más de un conjunto de actividades que pueden producir los resultados o salidas de OCTAVE; por esta razón, la metodología no especifica un único conjunto de actividades. Las salidas definen los resultados que un equipo de análisis debe lograr durante la evaluación y deben estar organizados según las tres fases. Las tablas 2 y 3 listan los principios, actividades y resultados de la metodología OCTAVE.

Tabla 2 principios y atributos de la metodología

Principio	Atributo
Auto dirección	1. Equipo de análisis. 2. Aumento de las capacidades del equipo de análisis.
Medidas adaptables	3. Catálogo de prácticas. 4. Perfil general de amenazas. 5. Catalogo de vulnerabilidades.
Proceso definido	6. Actividades de evaluación definidas. 7. Resultados de la evaluación documentados. 8. Alcance de la evaluación.
Base para un proceso continuo	9. Pasos siguientes. 3. Catálogo de prácticas.
Proyección hacia el futuro	10. Enfoque en el riesgo.
Enfoque en pocos puntos críticos	8. Alcance de la evaluación. 11. Actividades enfocadas.
Administración integrada	12. Temas organizacionales y tecnológicos. 13. Participación de las áreas de negocios y de tecnología de la información. 14. Participación de la alta gerencia
Comunicación abierta	15. Metodología de colaboración.
Perspectiva global	12. Temas tecnológicos y organizacionales. 13. Participación de las áreas de negocios y de tecnología de la información.
Trabajo en equipo	1. Equipo de análisis. 2. Aumento de las capacidades del equipo de análisis. 13. Participación de las áreas de negocios y de tecnología de la información. 15. Metodología de colaboración.

Fecha de recibo del artículo: 3 de Mayo de 2012
Fecha de aprobación: 12 de Septiembre de 2012

Tabla 3 resultados de la evaluación.

FASE	RESULTADO
Fase 1	1.1 Recursos críticos. 1.2 Requerimientos de seguridad para los recursos críticos. 1.3 Amenazas a los recursos críticos. 1.4 Prácticas actuales de seguridad. 1.5 Vulnerabilidades organizacionales actuales.
Fase 2	2.1 Componentes clave 2.2 Vulnerabilidades en la tecnología actual.
Fase 3	3.1 Riesgos en los recursos críticos. 3.2 Medidas del riesgo. 3.3 Estrategia de protección. 3.4 Planes de mitigación de riesgos.

3.2 El método octave

Como se mencionó anteriormente, el método OCTAVE fue ideado para grandes organizaciones, (Ej. A partir de 300 empleados o más). Pero el tamaño no es la única consideración para decidir usarlo. Las organizaciones grandes generalmente tienen una jerarquía de multiniveles y están a menudo desarticuladas o distribuidas geográficamente. Las actividades formales de recolección de datos para determinar qué recursos relacionados con la información son importantes, cómo se usan y cómo son amenazados, se vuelve una razón esencial que motiva a utilizar el método OCTAVE en las grandes compañías. Finalmente, en una organización grande es probable mantener una infraestructura informática propia y tener la habilidad interna de ejecutar herramientas de evaluación de vulnerabilidad, e interpretar los resultados respecto a sus recursos críticos.

El método OCTAVE está estructurado para un equipo de análisis con algún conocimiento de TI y de temas de seguridad, empleando una metodología abierta para recolectar y analizar información.

3.3 El método OCTAVE-S

El método OCTAVE-S se desarrolló para las organizaciones pequeñas, de 20 a 80 personas. Para organizaciones que pueden autorizar un equipo de tres a cinco personas para realizar todas las actividades de la evaluación, sin necesidad de actividades formales de recolección de datos. Aun así, podría decirse que una compañía de 200 personas que tiene una sola locación, podría congregar un equipo de 5 personas que tengan la visión suficiente de la organización, para realizar la evaluación. Por otro lado, una compañía con 90 personas que se encuentren en múltiples localidades, con una estructura sumamente confusa, podría requerir el Método OCTAVE para asegurar que se recojan suficientes datos en la organización y así tener una evaluación exitosa.

OCTAVE-S es más estructurado, permitiendo que el equipo de análisis esté conformado por personal menos experimentado.

3.4 *El metodo OCTAVE- Allegro*

Esta variante del método OCTAVE tiene la característica de que es mas simplificado, pero continua centrándose en los activos de información. El OCTAVE-Allegro es muy apropiado cuando se desea llevar a cabo una evaluación de riesgos sin una amplia participación de la organización. Debido a que es más simplificado, es de gran importancia que se tomen en cuenta también todos los activos importantes que se identifiquen y evalúen, en función de los activos de la información.

El OCTAVE-Allegro está organizado en cuatro fases similares a las implementadas por los otros métodos OCTAVE:

1. Establecer criterios de medición del riesgo de conformidad con los factores que guían la organización.
2. Se crea un perfil de cada activo crítico de información que establece los límites del activo, identifica sus necesidades de seguridad e identifica la totalidad de sus contenedores.

Fecha de recibo del artículo: 3 de Mayo de 2012
Fecha de aprobación: 12 de Septiembre de 2012

3. Identificar amenazas de cada uno de los activos.
4. Después de realizar los respectivos análisis, deben desarrollarse enfoques de mitigación

2. OCTAVE ES PARTE DE UN PROCESO CONTINUO.

Con la evaluación se genera una visión amplia de los riesgos actuales de seguridad de la información dentro de la organización, creando una línea base que puede usarse para enfocarse en las actividades de mejora y de mitigación de riesgos. Pero una evaluación de riegos de seguridad de la información es parte de las actividades de una organización para administrar los riesgos de seguridad de la información. OCTAVE es una actividad de evaluación y no es un proceso continuo como tal. Así, tiene un principio definido y un final. La figura 4 muestra la relación entre estas actividades y dónde encaja una evaluación como OCTAVE. Notar que las actividades para administrar los riesgos están definidas en un ciclo, planear, hacer, verificar y actuar (PHVA).

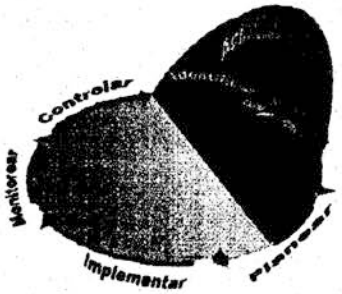

Figura 4 OCTAVE es parte de un proceso continuo. Adaptado de CERT 2011.

Periodicamente, una organización necesitará "restablecer" su línea base con la ayuda de OCTAVE. El tiempo entre las evaluaciones puede predeterminarse (por ejemplo, anualmente), o activarse debido a grandes eventos (por ejemplo, reorganización corporativa o rediseño de la infraestructura de cómputo de la organización). Entre las evaluaciones, una organización puede identificar los nuevos riesgos periódicamente, puede analizar los riesgos respecto a los ya existentes y puede desarrollar los planes de mitigación para ellos.

3. VENTAJAS Y DESVENTAJAS DE LA METODOLOGÍA OCTAVE

Existen diversas ventajas cuando se usa esta metodología:

- Brinda continuidad operacional a la organización.
- Produce certeza y justificación a los costos de la seguridad informática.
- Permite determinar acciones preventivas y correctivas en materia de seguridad.
- Incrementa la productividad de los recursos humanos, financieros y demás que estén involucrados con la seguridad.
- Logra que la seguridad forme parte de la cultura de la organización.

En cuanto a las desventajas o limitantes que generalmente se observa en esta metodología están:

- Al ser un proceso analítico posee un gran número de variables, lo cual hace que el procedimiento pueda ser algo complejo.
- Cada implementación es diferente por lo cual no es aplicable de la misma manera en diversas organizaciones.

Fecha de recibo del artículo: 3 de Mayo de 2012
Fecha de aprobación: 12 de Septiembre de 2012

Las soluciones al problema de seguridad, no son instantáneas ni permanentes, ya que este método involucra tanto la parte tecnológica como la organizacional, por lo que cualquier cambio en la organización, puede afectar considerablemente o no los parámetros definidos con ayuda del método.

4. CONCLUSIONES

Los ataques e incidentes de seguridad, han llevado a la creación de mejores prácticas de seguridad de la información y las evaluaciones de la seguridad, han crecido a la par con este fenómeno.

La seguridad no es un asunto únicamente técnico y la aplicación de evaluaciones del tipo de OCTAVE ayudan a entender que las prácticas operacionales de seguridad son factores que influyen en la disminución de los riesgos de las empresas, permitiendoles entender mejor las distintas formas en que se puede resolver un problema determinado y adoptar una actitud proactiva frente a los riesgos.

Al realizarse una evaluación con OCTAVE, se incrementa la comunicación entre el personal y se enriquece el conocimiento corporativo, obteniéndose múltiples perspectivas de la seguridad en la organización.

Al aplicar una evaluación aumentará la cultura organizacional frente a la seguridad. Se debe tener especial cuidado en aplicar los resultados de esta, es decir, completar el ciclo PHVA (planear, hacer, verificar y actuar), porque si no se hace, desalentara al personal respecto a los esfuerzos hechos en las evaluaciones y generará un ambiente de subvaloración de la seguridad en la empresa.

5. REFERENCIAS

CERT. 2011. «OCTAVE® Information Security Risk Evaluation». http://www.cert.org/octave/.

Eterovic, Jorge Esteban, y Gustavo A Pagliari. 2011. «Metodología de Análisis de Riesgos Informáticos». Técnica Administrativa http://www.cyta.com.ar/ta1001/v10n1a3.htm

Melo, Arean Hernando elasco. 2008. «El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001». Revista de Derecho(029): 333–366.

Viloria, Orlando, y Walter Blanco. 2009 «MODELO SISTÉMICO DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS UNIVERSIDADES». Revista Venezolana de Análisis de Coyuntura(1): 219–240.