GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT

Hurtado, Martha.
(marthalilianahurtadocruz@hotmail.com)
Universidad Piloto de Colombia

Resumen— Por los múltiples acontecimientos en la actualidad de los llamados delitos informáticos es por lo que existen diversas herramientas destinadas a ayudar a cientos de compañías que existen en el mundo a proteger su activo más importante: la información. El término HACKER muy conocido hoy día, corresponde o hace referencia a una persona que ingresa de manera indebida a los sistemas de información y sin autorización, para provocar daños en los millones de datos que estén almacenados, el ingreso ilegal por así llamarlo es lo que se conoce como una amenaza a la organización y/o empresa.

Es por esta razón, que con los avances tecnológicos se han ido creando de igual forma procedimientos o métodos que ayuden a descubrir con antelación esas vulnerabilidades, conocidas como debilidades dentro de los sistemas, que existen tanto a nivel físico, en el personal que administra los equipos; como a nivel lógico, en lo equipos de seguridad. De esta manera, surgen las llamadas metodologías de los sistemas de información, destinadas a trabajar conjuntamente con los integrantes de una empresa para determinar qué tipos de debilidades poseen, a qué tipo de amenazas están expuestos y como combatirlas o como evitarlas.

Abstract— By multiple events of so called computer related crime is now, so there are varios tools to assist the hundreds of companies that exist in the world to protect your most important asset: information. The term HACKER known today, i sor refers to a person who enters, information systems inappropriately and without authorization to caused amage in the millions of data that are stored, the ilegal entry so call it what referred to as a threat to the organization or company.

This is why, that with the technological advances you have established similarly procedures or methods that help to discover these vulnerabilities, known as weaknesses with in systems, which exist both on the physical level, on the staff in advance It manages the equipment; as a logical level, in the safety equipment. In this way, arise the so-called information systems methodologies, intended to work together with members of a company to determine what types of weaknesses have, what kinds of threats they are exposed and as combat them or as avoid it.

Índice de Términos— Gestión de Riesgo, información, Metodología MAGERIT y OCTAVE.

I. INTRODUCCIÓN

Hoy día la mayoría de compañías a nivel mundial se han enfocado en manejar y cuidar a cabalidad su más valioso activo, en este caso, se determina dos tipos de activos: los primarios que incluyen la información y los secundarios o de apoyo, que incluyen Hardware, Software, Red, Usuarios y Estructura. Compañías que dedican 100% de sus operaciones a proteger y resguardar millones de datos organizados que contienen material confidencial y de la cual dependen cada una de ellas. Por tal razón, cualquier incidente o amenaza contra esta, puede ocasionar impactos adversos en los objetivos de la compañía.

A la existencia de estos riesgos, ya sea internos como fallas ocasionadas por el personal, mala administración de equipos y de información, operacionales, presupuestales, entre otros; y externos como los ambientales, entorno político, económico y legal; que de materializarse podrían afectar la continuidad de las operaciones, el cumplimiento de objetivos y metas y comprometer el patrimonio de la empresa, es lo que a la mayoría de empresas les ha llevado a invertir millones de dólares para determinar y contrarrestar esas vulnerabilidades, físicas y lógicas. Ese riesgo, originario desde el siglo 17 y definida en esa época como una combinación entre la dimensión de las pérdidas y ganancias con las matemáticas, en el siglo 18 como relación entre las pérdidas y ganancias para la economía; y en el siglo 20 se precisó con una negativa enfocada a todo peligro que conlleve a un descenso drástico y catastrófico en la ciencia y la tecnología. [1]

II. GESTIÓN DEL RIESGO

Para hablar de gestión de riesgo, se debe definir inicialmente qué es el riesgo, el cual se define como una probabilidad que ocurra un evento, puede ser previsto y evitado, las amenazas y las vulnerabilidades por separadas no llegan a presentar un daño de grandes magnitudes, en cambio, si se mezclan la probabilidad de daño es mucho más grande.[2] De tal manera, el llamado riesgo informático se desarrolla a la par de la tecnología y cada día son mucho más las vulnerabilidades y amenazas que acechan la información.[2]

Una buena gestión de riesgo en la seguridad de la información de una organización requiere una buena inversión de tiempo, esfuerzo y dedicación. Por lo general, una organización que entienda el valor sustancial de sus activos y desea realizar una inversión para gestionar sus vulnerabilidades, se debe inclinar hacia un sistema de gestión basado en políticas, procesos, recursos, documentación y estructura organizacional; todos estos elementos mezclados, permiten de alguna u otra manera, planificar, desarrollar, controlar y tomar acción. Además, suele acogerse a las normas de la familia ISO 27005. Se debe tener en cuenta que el hecho de plantear una gestión para el riesgo no es solo para proteger sus activos de información, sino procurar que la empresa u organización logre cumplir su misión, por lo que al hablar de gestión se define como un ciclo reiterativo, que identifica, evalúa y ejecuta. [3]

El proceso para la gestión de riesgo, puede observarse en la Figura 1, el cual se encuentra conformado por 5 procesos, los cuáles se describen a continuación:

A. Establecimiento del Contexto.

Este proceso valga la redundacia contextualiza el entorno, en este caso de la empresa, recibiendo toda la información relevante de la misma.

B. Evaluación del Riesgo.

Este proceso trae consigo 3 subprocesos; la identificación, la revisión y el control de riesgos. Identifica de forma cuantitativa y cualitativa los riegos y le da una cierta prioridad a los criterios de evaluación que dependen o estan muy alineados a los objetivos de la organización. De esta manera, se puede controlar y determinar lo que podría generar una pérdida de gran magnitud y el lugar donde puede presentarse. Y por último el proceso de evaluación se encarga de comparar los niveles de criterios de riesgos y los de aceptación, su resultado genera un listado de vulnerabilidades y/o amenazadas pero priorizadas. Para esta evaluación de riesgo se finaliza con un intepretación del mismo, dando uso a la llamada *Matriz de análisis,* en ella, se puede determinar la probabilidad de riesgo versus la magnitud de daño, tomando valores respectivamente desde el 1 hasta el 4, o en otros casos la clasificación del riesgo sería en bajo, moderado, importante y crítico versus las consecuencias. [13] Ver Figura 2. Se debe tener en cuenta que para este proceso se plantean las llamadas metodologías de evaluación.

C. Tratamiento del Riesgo.

Este proceso está encaminado a plantear las posibles medidas de seguridad para reducir o evitar los riesgos y generar contingencias.

D. Consulta del Riesgo.

Este proceso informa de los riesgos existentes a todas las partes interesadas de la organización.

E. Monitoreo del Riesgo.

Este proceso supervisa todas aquellas medidas de seguridad planteadas para contrarrestar los riesgos, con el objetivo de determinar si están funcionando correctamente o están ejecutando la acción para la cual fueron planteadas. Luego de esta implementación se ejecutan las llamadas auditorías internas, documentando todo el proceso y señalando su eficacia.

De esta manera, y con el trascurrir de los años la tecnología ha ido evolucionando, así como los métodos para vulnerar todos los sistemas de información, es así como las normas y los modelos para la gestión de riesgo han ido evolucionando, implementando las conocidas metodologías, se tienen muchas pero las que se analizarán en este artículo son: MAGERIT Y OCTAVE.

Fig. 1. Proceso de Gestión de Riesgos. [2]

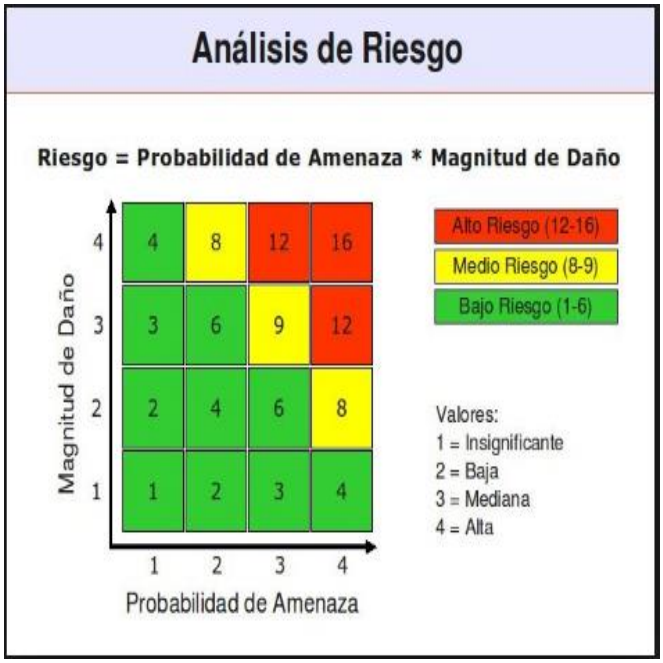

Fig. 2. Matriz de Análisis de Riesgos y Clasificación de Riesgos. [13]

III. METODOLOGÍA OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Es una técnica de evaluación de riesgos desarrollada por el SEI (Software Engineering Institute) en Estados Unidos. Es reconocida a nivel mundial y ha tenido excelente adaptación. [4] Las fases que la componen la catalogan un poco más complicada que las demás metodologías. La misma está enfocada en el riesgo y no en la tecnología como las demás, cuando se usa este tipo de metodología personal de varios departamentos como el operativo, el de tecnología, entre otros; trabajan en conjunto proyectados a la necesidad de seguridad, apoyados por un especialista.

Es necesario considerar, que esta metodología fue desarrollada para ser implementada en organizaciones de más de 300 empleados y se encuentra dividido en tres etapas como se puede observar en la Fig. 3. La fase 1 ***Build asset-based threat profiles***, desarrollar perfiles de amenazas basados en los activos, en la cual se identifican los bienes, las amenazas, prácticas actuales, vulnerabilidades y los recursos de seguridad de la compañía. La fase 2, ***Identify infrastructure vulnerabilities***, identificar las vulnerabilidades de la infraestructura, se basa en los componentes clave y sus correspondientes vulnerabilidades técnicas. Por último, en la fase 3 ***Develop security strategy and plans***, desarrollar estrategias y planes de seguridad, con base a los riesgos, la estrategia de protección y los planes de mitigación. [8]

Buid asset-based threat profiles - Generar perfiles de activos basados en la amenaza.

En esta fase se realiza un análisis para identificar los activos más importantes para la organización y que se está realizando para su protección en la actualidad. Comprende los siguientes cuatro procesos:

1. *Identify enterprise knowledge - Identificar el conocimiento de la empresa.*

El objetivo de este proceso es identificar la perspectiva que tienen los directivos. La Fig. 4 *OCTAVE Proceso 1 Visión Organizacional.* Identificar el conocimiento de la empresa ilustra las entradas que se necesitan para obtener las salidas. Como entradas se puede observar el cuestionario de activos, perfil genérico de las amenazas, catálogo de

amenazas (cuestionario de la estrategia de protección
de la organización), catálogo de prácticas de la organización, técnicas y de entrenamiento, datos organizacionales (organigrama, políticas, procedimientos), por último, las leyes y las regulaciones que la compañía se encuentre obligada a cumplir. Para conseguir la lista priorizada de activos con sus valores relativos, perfil de la amenaza empresarial, la estrategia de protección actual, los indicadores de riesgo, y las áreas operacionales a evaluar. [8] [11] Todo con respecto al conocimiento del área gerencial de la compañía.

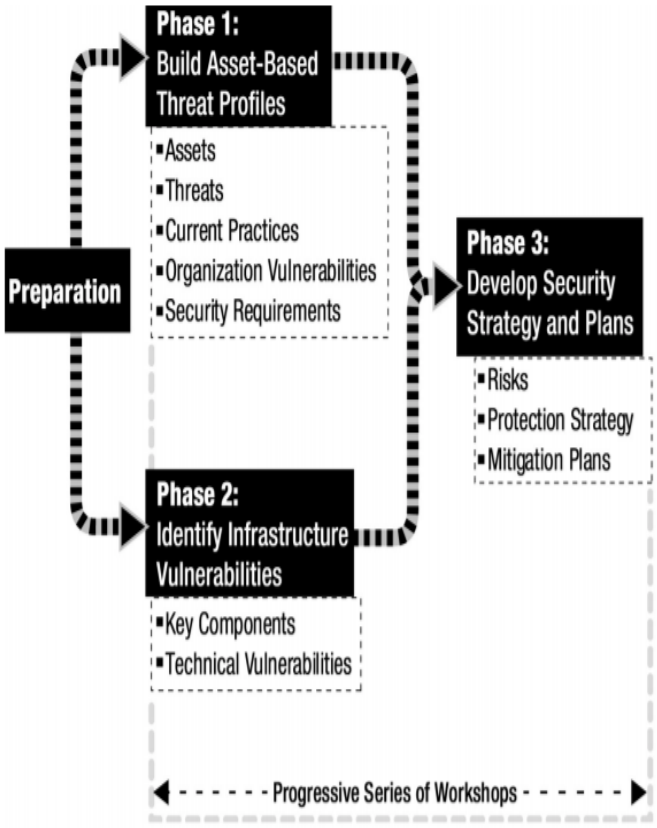

Fig. 3. El método OCTAVE. [6] [11]

Este proceso está compuesto por cinco actividades que se describen a continuación y en las cuáles se explica con mayor detalle las entradas y salidas que le corresponden. [11]

a) Characterize key enterprise assets – Identificar los activos clave de la empresa.

Responde a la pregunta: "¿Qué está intentando proteger?". Dependiendo del conocimiento que la alta gerencia tenga de la empresa y del cuestionario que se les realice. Se obtendrá la lista de los activos que identifican como importantes, con sus respectivos valores relativos para la dirección de la compañía.

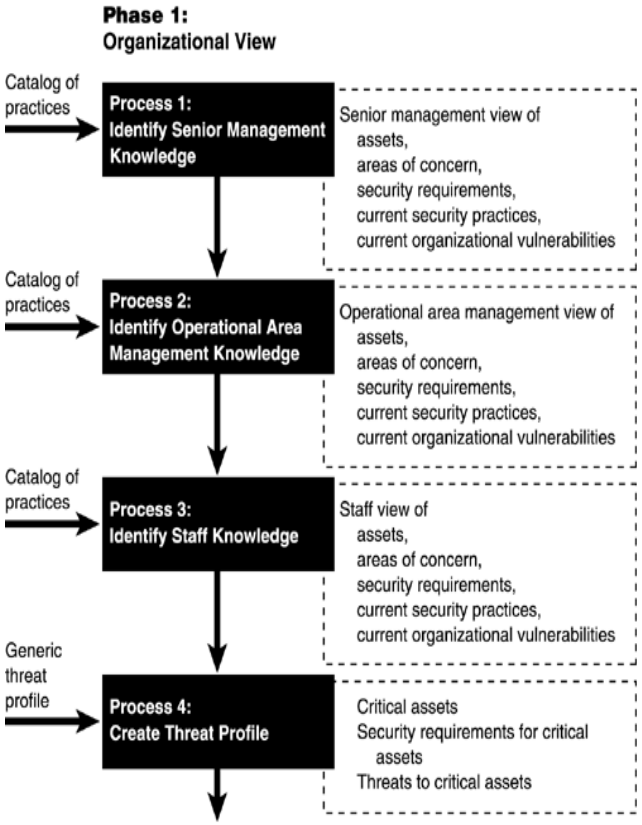

Fig. 4. OCTAVE Proceso 1 Visión Organizacional. [11]

b) Describe threats to assets – Describir las amenazas de los activos.

"¿De qué está intentando proteger sus activos?", es la cuestión en esta actividad. Aquí también es importante el conocimiento que la directiva tiene sobre las amenazas que afectan los activos. Se adquiere el perfil de la amenaza empresarial desde el enfoque directivo.

c) Describe current and planned strategy to protect assets – Describir la estrategia actual y planificada para proteger los activos.

La dirección que conocimiento tiene al respecto de prácticas y políticas que se encuentran actualmente o en planificación para la protección de los bienes.

La pregunta aquí es: "¿Qué está haciendo actualmente para proteger sus activos?". Como resultado se encuentra la estrategia de protección empresarial actual, desde la perspectiva de la alta gerencia.

d) Identify risk indicators – Identificar los indicadores de riesgo.

La salida de esta actividad son los indicadores de riego empresarial, es decir, las preocupaciones de la alta gerencia, dependiendo del cuestionario basado en buenas prácticas técnicas y de capacitaciones en las organizaciones, documentación de políticas y procedimientos, también las leyes y regulaciones que la empresa debe cumplir. El interrogante a esta actividad es: "¿Qué brechas en su estrategia de protección actual están poniendo sus activos en riesgo?".

e) Select operational areas to evaluate – Seleccionar áreas operativas para evaluar.

Esta actividad responde a dos interpelaciones: "¿Qué áreas operativas o funciones de soporte están involucradas con los activos clave que usted identifico?" y "¿Quiénes son los gerentes clave de esas áreas operativas o funciones de apoyo?". De esta forma se obtiene las áreas que son prioridad para evaluar.

2. Identify operational area knowledge - Identificar el conocimiento del área operativa.

De acuerdo al conocimiento actual de los gerentes del área operacional, un cuestionario de activos, perfil genérico de amenazas, cuestionario de la estrategia de protección (catálogo de la organización, técnicas y de entrenamiento), datos organizacionales (organigrama, políticas y procedimientos), leyes y regulaciones que se deban cumplir y la lista despreciando las prioridades de los activos de la empresa con sus respectivos valores relativos, que los jefes de área operativa proporcionen, corresponden a las entradas de esta parte de la metodología.[11]

Para tener como salidas una lista priorizada de activos del área operativa, un mapa en el cual se cruce los activos empresariales identificados por el área gerencial y los activos identificados por el área operativa, un perfil de amenazas, la estrategia actual de protección, los indicadores de riesgo, todo esto correspondiente al área operativa y el personal que se considera debe ser evaluado. [8] Las actividades que corresponden a esta parte de la metodología se describen a continuación.

a) Characterize key operational área assets – Caracterizar los activos clave del área operativa.

Los gerentes de área responden: "¿Qué está intentando proteger?". Depende del conocimiento que se tenga sobre los activos concernientes para obtener la lista de estos.

b) Characterize assets in relation to enterprise assets – Caracterizar los activos en relación con los activos de la empresa.

Es la relación con la lista de los activos identificados en el proceso 1, cuestionando: "¿Cuál es la relación o relaciones entre los activos que ha identificado con los activos que ha identificado la alta gerencia?". Como resultado la o las relaciones documentadas.

c) Describe threats to assets – Describir las amenazas a los activos.

"¿De qué está tratando proteger sus activos?", es el interrogante de esta actividad. En base al conocimiento de los gerentes de área operacional sobre las amenazas a sus activos y con un perfil genérico de estas, la respuesta será el perfil de las amenazas de los activos del área operacional desde su respectivo punto de vista.

d) Describe current and planned strategy to protect assets – Describir la estrategía actual y planificada para proteger los activos.

De acuerdo al conocimiento que los gerentes de área, se da a conocer las buenas prácticas técnicas y de formación, políticas, procedimientos de la empresa y las leyes que esta debe cumplir, responden al interrogante: "¿Qué está haciendo para proteger sus activos?". De esta forma se obtiene la estrategia de protección del área operativa.

e) Identify risk indicators – Identificar indicadores de riesgo.

Teniendo en cuenta un entrenamiento adecuado en seguridad, programa de concientización para el personal y la documentación de políticas y

procedimientos para la protección de los activos, se responde la siguiente pregunta: "¿Qué brechas en su estrategia de protección actual están poniendo sus activos en riesgo?". Arroja los indicadores de riesgo correspondiente al área operacional, dando resultado la expresión de las inquietudes de los riesgos a los que están expuestos sus activos.

f) Select staff to evaluate – Seleccionar personal para evaluar.

En esta actividad se necesita la información recolectada en las anteriores, para escoger líderes o miembros clave de equipo que deban ser evaluados. La indagación es: "¿Quiénes son los miembros clave?".

3. Identify staff knowledge - Identificar el conocimiento del personal.

Detalla las entradas y las salidas que pertenecen a esta parte.

En las entradas se tiene el conocimiento actual del personal, cuestionario de activos, perfil genérico de amenazas, cuestionario de la estrategia de protección actual, catálogo de las prácticas de la organización, técnicas y de capacitación, datos organizacionales (organigrama, políticas y procedimientos), leyes y regulaciones que la compañía está obligada a cumplir, lista priorizada de activos, lista de activos del área operacional y el mapa de cruce de activos. Y se obtiene la lista de activos que el personal identifica, mapa de los activos de la empresa comparado con los activos del área operacional y los del personal, perfil de amenazas, la estrategia actual de protección y los indicadores de riesgo correspondientes a esta área. [8], [11]

A continuación, se describen las actividades que aquí se contemplan.

a) Characterize key staff assets – Caracterizar los activos clave del personal.

"¿Qué está tratando de proteger?" es lo que debe responder el personal en esta actividad, la respuesta dependerá de su conocimiento con respecto a los activos, por medio de un cuestionario. Y de esta forma se consigue la lista priorizada de los activos importantes para el personal.

b) Characterize assets in relation to operational area and enterprise assets – Caracterizar los activos en relación con el área operacional y los activos de la empresa.

Se plantean y relacionan los activos que anteriormente se identificaron como importantes con los que el personal establece con prioridad. La pregunta que hace referencia en esta actividad es: "¿Cuáles son las relaciones entre los activos que ha identificado el personal, con los del área operacional y los pertenecientes a la alta gerencia?". Para obtener la documentación de estas conexiones.

c) Describe threats to assets – Describir las amenazas de los activos.

La cuestión es: "¿De qué está tratando de proteger sus activos?". Que responderán de acuerdo al perfil genérico de amenazas y del conocimiento que posean. Así se obtiene el perfil de amenaza.

d) Describe current and planned strategy to protect assets – Describe la estrategia y planificación para proteger los activos.

La pregunta es ¿Toca aquella estrategia planteada, ser implementada y monitoreada para su efectividad?

4. Create Threat Profile – Creación de Perfiles de Amenazas.

Este proceso integra toda la información contenida en los procesos anteriores, y procede a crear un conjunto de perfiles de amenazas para los activos en estado crítico, por lo general, este tipo de procedimiento suele gestionarse por el equipo de análisis.

Identify Technological Vulnerabilities.

Para esta fase se contemplan los siguientes procesos: Identificación de los componentes clave y la evaluación de los componentes elegidos. Este proceso puede simplificarse en la Figura 5.

5. Identificación de los componentes clave.

Este proceso se encarga de elegir que partes u componentes específicos serán analizados en busca de vulnerabilidades tecnológicas, identifica los

principales sistemas de tecnología y asimismo los activos críticos.

6. Evaluación de componentes.

En esta parte y con los componentes seleccionados se evalúan las vulnerabilidades y con el equipo de los
análisis se procede a ejecutar las herramientas de evaluación para posteriormente analizar el resultado.

La correcta ejecución de este proceso puede mitigar el impacto de la amenaza en la organización.

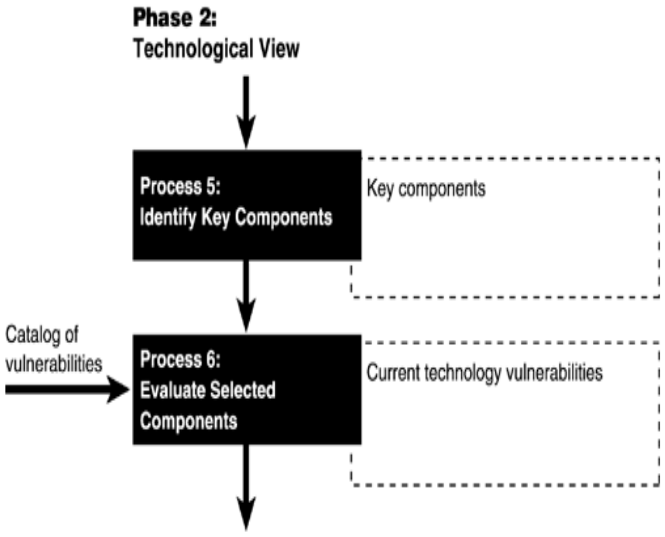

Fig. 5. OCTAVE Proceso 2 Visión Tecnológica. [11]

Develop Security Strategy and Plans

Fase caracterizada por el manejo de los procesos de análisis de riesgo y el desarrollo de una estrategia de contingencia. [11]

7. Análisis de Riesgo.

Proceso encargado de estudiar el impacto de las amenazas a los activos críticos, luego evalúa y crea los criterios para la evaluación de los riesgos.

8. Desarrollo de una estrategia de protección.

Finalmente, el equipo de análisis crea una estrategia para la protección de los activos, esto con el objetivo de contrarrestar o evitar el impacto de la amenaza, este proceso se basa en el análisis de la información recolectada anteriormente.

Se debe tener en consideración, que en vista de las necesidades de cada organización y dependiendo del tamaño de la misma, se diseñaron 3 métodos OCTAVE para suplir esas solicitudes

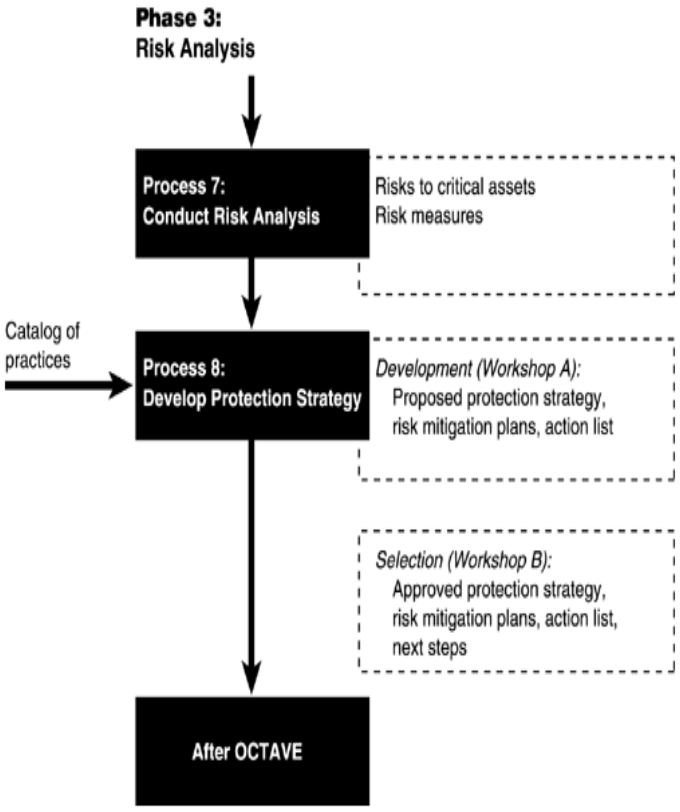

Fig. 6. OCTAVE Proceso 3 Análisis de Riesgo [11]

MÉTODO OCTAVE:

Está compuesto por una serie de talleres y/o programas que son llevados a cabo por la propia organización, aprovechando de esta manera los conocimientos propios de los niveles de la misma. Este grupo se centra únicamente en establecer los puntos críticos y las posibles amenazas, asimismo las vulnerabilidades tantos físicas como lógicas que atente a la organización y plantear la estrategia a utilizar.

Las 2 fases en las que trabaja esta metodología son:

Fase de análisis de Riesgo

Esta fase permite determinar 3 variables: [9]

a) ¿Cuál es?

b) ¿Cuánto vale?
c) ¿Cómo se protege?

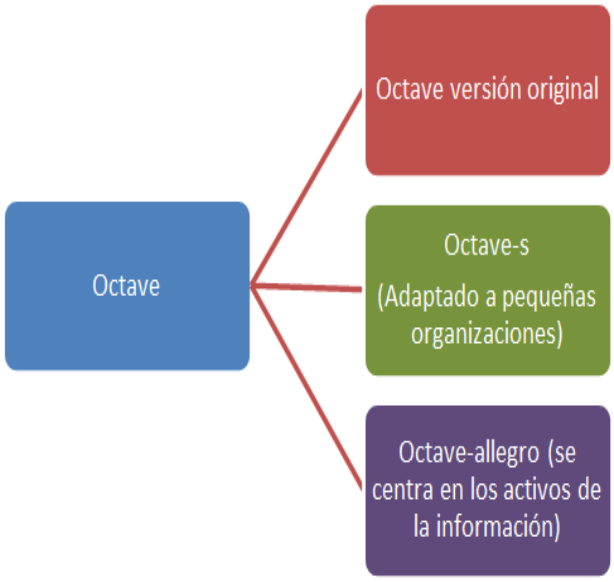

Fig. 7 Tipo de Método OCTAVE. [6]

MÉTODO OCTAVE-S:

Operationally Critical Threat, Asset and Vulnerability Evaluation for Small Organization, fue desarrollado para ser implementado en organizaciones pequeñas de 100 personas o menos utilizando un proceso un poco más reducido que el OCTAVE, pero con los mismos resultados. [5][7] Las dos principales diferencias de este método con el original son:

A. Requiere un grupo de 3 a 5 personas que conozcan a plenitud el desarrollo de la empresa.
B. Solo realiza un barrido de manera superficial a la infraestructura informática.

MÉTODO OCTAVE-ALLEGRO

Es una simplificación del método original y está enfocado solo en los activos de la organización, es perfecta cuando se desea gestionar una evaluación de riesgo, pero sin mucha participación del personal de la empresa, está conformado por 8 pasos organizados en 4 fases. [5][6] Estas son las siguientes:

a. ***Fase 1:*** Evaluación de los participantes desarrollando criterios de medición de riesgo.
b. ***Fase 2:*** Creación de los participantes un perfil de activos críticos.
c. ***Fase 3:*** Los participantes identifican las amenazas a cada uno de los activos.
d. ***Fase 4:*** Los participantes identifican y analizan las amenazas y desarrollan planes de contingencia.

IV. METODOLOGÍA MAGERIT

Acrónimo de Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información, el Consejo Superior de Administración Electrónica de España (CSAE), considera que la sociedad depende mucho de las tecnologías de la información y las comunicaciones para la consecución de los objetivos.[6] El uso de las mismas proporciona mucho beneficios y de igual manera abre una brecha para el surgimiento de riesgos que deben ser neutralizados con las medidas de seguridad que promuevan la confianza de los usuarios que manejen la estructura.

MAGERIT fue creada en el año de 1997 y actualmente ya se encuentra en su segunda versión, los parámetros que esta metodología trabaja están basados en términos como:

A. Activos.
B. Amenazas.
C. Vulnerabilidades.
D. Impacto.
E. Riesgos.
F. Contingencia.

La cuáles son ramales fundamentales en el análisis y gestión del riesgo. Si bien, el avance de la tecnología ha permitido el crecimiento exponencial de los beneficios de la misma, de igual manera, las vulnerabilidades cada día son más y los invasores incrementan el interés de ese llamado juego para romper las barreras y acceder a la información, por tal razón, MAGERIT ha parametrizado el método de trabajo actualizando cada una de sus componentes, renovando cada una de las aplicaciones o programas

abandonados y creando nuevos sistemas de información a la vanguardia de la tecnología.

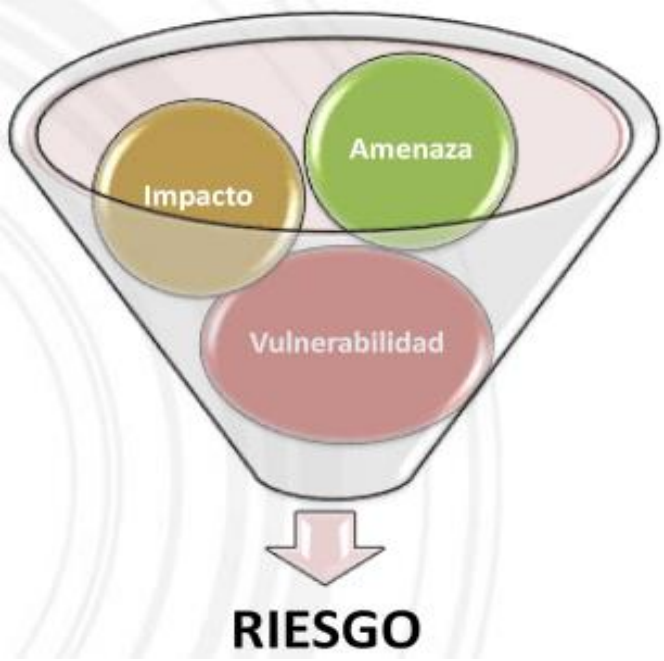

Fig. 8 Términos potenciales del riesgo. [16]

Al conocer y tener respuestas a estas variables y asimismo en conjunto con los objetivos de la organización surge las actividades de tratamiento de los riesgos que son las siguientes: Ver Figura 9

1. Definir el alcance de estudio, es decir, el alcance de las áreas estratégicas donde se va a revisar o mejorar la seguridad.

2. Establecer los activos relevantes de la organización, para así saber su valor y conocer que tanto podría perderse en caso de una amenaza.

3. Determinar a qué vulnerabilidades y/o amenazas están expuestos esos activos.

4. Conocer cuáles son los planes de contingencia (salvaguardas) que pueden contrarrestar las amenazas.

5. Conocer el impacto de presentarse una amenaza sobre el activo.

6. Tratar el riesgo de probabilidad de ocurrencia de esa amenaza.

Fig. 9. Fase de Análisis de Riesgo. [14]

Fase de gestión de Riesgo.

Luego de determinado el impacto y los múltiples riesgos a los que una organización está expuesto, se procede a tomar una serie de decisiones dependiendo de los siguientes factores:

1. La gravedad del impacto.

2. Las obligaciones a las que está comprometida por ley la organización.

3. La obligación a la que está comprometida por reglamento la organización.

4. La obligación a la que está comprometida por contrato la organización.

A partir de la toma de decisiones, se implantan las medidas de seguridad para poder controlar principalmente los riesgos encontrados, y frente a estos proceder a: [10], [11], [12]

A. ACEPTAR EL RIESGO: en vista que la probabilidad de ocurrencia del mismo es baja.
B. TRANSFERIR EL RIESGO: mitigando las consecuencias con los correspondientes seguros. Su probabilidad de ocurrencia es medio.
C. EVITAR EL RIESGO: su probabilidad de ocurrencia es alta.

Y finalmente ejecutar sus salvaguardas para la reducción del impacto. Ver Figura 10.

Fig.10 Fase de Gestión de Riesgos. [15]

V. COMPARACIÓN METODOLOGÍAS OCTAVE-MAGERIT

Entre las comparaciones que se pueden encontrar entre ambas metodologías son:

El OCTAVE está dirigido a diferentes grupos de trabajo desde los más pequeños hasta los más grandes, involucrando participantes de la organización con el propósito de abordar las necesidades que requiera la misma para la protección de la seguridad de la información. Por su parte, MAGERIT lo que promueve es la sensibilización a los responsables de la existencia de riesgos en los sistemas de información y asimismo en la necesidad de identificarlos a tiempo.

La metodología OCTAVE se plantea una gestión de riesgo basada en la operatividad de la organización, y considera la seguridad informática no un tema únicamente técnico, mientras que MAGERIT considera que los riesgos están inmersos dentro de los sistemas de seguridad de la información.

OCTAVE se considera una metodología autodirigida, donde permite que las personas de una organización puedan ser parte del establecimiento y de las estrategias para la protección de la seguridad, esto con el uso de métodos y herramientas; en cambio, MAGERIT focaliza su objetivo en el análisis de los riesgos en los sistemas de Seguridad Informática para descubrirlos de manera oportuna.

MAGERIT fue creado por el Consejo Superior de la Administración Electrónica y OCTAVE fue creada por uno centro de investigación en EE. UU.

OCTAVE es una metodología flexible que puede ser personalizada a cada una de las organizaciones.

OCTAVE maneja talleres, hojas de trabajo y procedimientos para el análisis de los riesgos y la priorización de los mismos en pro del planteamiento de estrategias, en cambio, MAGERIT está relacionado con el uso de medios electrónicos, informativos y tecnológicos con el objetivo de reducir la desconfianza por parte de los usuarios al uso de estos medios.

MAGERIT enfoca sus objetivos en 2 fases:

1. El análisis de riesgo.
2. La gestión del riesgo.

Por su parte, OCTAVE plantea 3 fases:

3. La creación de amenazas.
4. La identificación de vulnerabilidades.
5. El planteamiento de estrategias pro a la mitigación de los riesgos.

Por otra parte, ambas metodologías al momento de iniciar a implementarlas funcionan de manera diferente, OCTAVE establece 4 procesos que sugieren puntos de vista a los activos críticos, las áreas de operatividad importantes, requerimientos de seguridad, las vulnerabilidades y la estrategia a implementar. Sin embargo, MAGERIT inicia su método con el análisis de riesgos a los activos de la organización, su incidencia en ellos y las amenazas a los que están expuestos.

El enfoque de la metodología MAGERIT es dividir los activos de la organización en diversos grupos para determinar una gran cantidad de riesgos, en cambio, OCTAVE trabaja en la planificación con antelación de los sistemas de información basados en lo riesgos.

Sus métodos son totalmente diferentes: Uno plantea la auto dirección y flexibilidad (OCTAVE), en cambio, la otra está basada en un lineamiento sistemático.

Trabaja en pro de las tecnologías de la información y en brindar confianza en el uso de las mismas, mientras que OCTAVE enfoca todo en el riesgo interno u organizacional de la empresa.

Lleva a cabo un proceso de concientización al personal de la organización, con la idea de enseñarles que existen diferentes tipos de riesgos en los sistemas de información y en la importancia de ubicarlos a tiempo. Mientras, que OCTAVE establece los riesgos en cuanto al tipo de activo SOFTWARE, HARDWARE, USUARIO y RED.

Está creado para suplir las necesidades de diferentes entidades, como por ejemplo MAGERIT se enfoca en atender las solicitudes del Gobierno, Organismos, Pymes y compañías comerciales, en cambio, OCTAVE se enfoca para trabajar con empresas pequeñas y medianas.

VI. CONCLUSIONES

Ninguna organización a nivel mundial está exenta de sufrir cualquier tipo de amenaza, y más hoy día, cuando existen muchas personas malintencionadas con objetivos específicos de vulnerar los sistemas ya sea por hobby, beneficio propio y/o por solicitud de un tercero, esto, junto con las herramientas vanguardistas creadas para ser implementadas y romper con esos pilares de seguridad; tales como: la confidencialidad, la integridad y la disponibilidad de aquel activo importante para toda organización como es la "*información",* es lo que provoca la desconfianza en el manejo de los sistemas y el llamado miedo a ser atacados en cualquier momento por los trabajadores. Este sentimiento latente y muy común entre los integrantes de una empresa, ya sea Por los Directivos de la misma, como lo trabajadores de distintas áreas, pero sobre todo de la IT, es lo que genera que las organizaciones quieran adelantarse a las consecuencias de ser arremetidos, como la creación de contingencias con el propósito de saber cómo responder a cualquier ataque para mitigar el impacto de la misma.

Este artículo examina dos metodologías de análisis y gestión de riesgos y establece que ninguna es mejor que otra; cada una fue diseñada para responder a un requerimiento en específico dentro de la organización, una de ellas enfoca a la gestión del riesgo inmerso dentro de las tecnologías de la información, mientras que la otra, pretende trabajar un proceso de planificación para establecer las debilidades internas, esto gracias al personal escogido, aquellos que conocen a plenitud la operatividad de la organización. En pocas palabras, las metodologías analizadas responden o dan solución al llamado de la incertidumbre en la manera de prevenir y/o controlar la amenaza.

Es por esto, que antes de lamentarse con la pérdida de cualquier información, es necesario establecer que estamos dispuestos a hacer como organización para proteger los datos, si lo mejor es anticiparnos y tener claro las vulnerabilidades de un sistema de seguridad y asignarles un nivel de importancia e implementarles los controles necesarios para reducir los contratiempos o esperar a ser atacados para luego actuar y mirar de qué manera podemos reducir los daños.

REFERENCIAS

[1] C. Klüppelberg D, Straub and I. Welpe, Risk-A Multidisciplary Introduction. Springer, 2014.

J. Téllez, "Contratos, riesgos y seguros informáticos", pp 33. 1988.

[2] A. Siler, "Gestión del Riesgo con base en ISO27005 adaptando OCTAVE-S" pp 27. 2014.

[3] E. Osco "Metodologías de Seguridad de la Información".

[4] C. Pardo, G. Vanegas "Hacia un modelo para la gestión de riesgos TI en MiPyMes: MOGRIT.

[5] D. Reyes. "El análisis de riesgos informáticos y su incidencia en la seguridad e integridad de la información"

[6] C. Alberts. "OCTAVE-S Implementation Guide Version 1" 2005.

[7] B. Duque. "Metodología de Gestión de Riesgos" pp -6- 17

[8] Ministerio de Hacienda y Administración Públicas "MAGERIT Vr. 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" Libro 1.

[9] Ministerio de Hacienda y Administración Públicas "MAGERIT Vr. 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" Libro 2.

[10] Ministerio de Hacienda y Administración Públicas "MAGERIT Vr. 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" Libro 3.
[11] C. Alberts, A. Dorofee. "Managing Information Security Risk :The Octave Approach" 2002.
[12] ARL Sura "Sistema de Gestión y Seguridad para la identificación de peligros, evaluación y valoración de riesgos".
[13] B. Zaragoza "Gestión de Proyectos de Software" Instituto Tecnológico de Tijuana 2015.
[14] INCIBE Instituto Nacional de Ciberseguridad "Análisis de Riesgo en 6 pasos" 2017
[15] G. Siqueira "Gestión de Riesgos: Cómo manejar las incertidumbres del proyecto" 2016.
[16] SIGEA "Estándares para evaluar riesgos de seguridad de la información" 2013.

Autor

Martha Liliana Hurtado Cruz, Ingeniera de Telecomunicaciones, estudiante de Postgrado de la Universidad Piloto de Colombia.