Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria

Astrid Estefanía Pacheco Fernández
Luis Ignacio Suarez Santamaría
Juan Hover González Chacón
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes
{ae.pacheco, Luis.suarez, jh.gonzalez}@uniandes.edu.co

Resumen

Este artículo describe cómo aplicar la metodología OCTAVE (Operationally Critical Threat Asset, and Vulnerability Evaluation) para la identificación de Amenazas y Vulnerabilidades en una entidad bancaria, para posteriormente construir un plan de mitigación de los riesgos identificados.

Esta metodología se desarrolla en tres fases. En la primera fase se realizan workshops en tres niveles de la organización (Gerencia, Área Operacional, y Staff) para identificar desde su perspectiva, los riegos asociados a los activos más críticos de la banca virtual. En la fase dos se hace un análisis de riesgo de la infraestructura crítica que soporta los activos de información identificados en la fase uno; y en la fase tres, se lleva a cabo un análisis multidimensional de los riesgos identificados previamente para desarrollar posteriormente estrategias de protección y mitigación sobre estos riesgos.

Además, este artículo presenta un análisis sobre las ventajas y desventajas de la metodología a la hora de hacer una evaluación de riesgos frente a otras metodologías.

Abstract

This paper describes how to apply the OCTAVE (Operationally Critical Threat Asset, and Vulnerability Evaluation) methodology for the identification of Threats and Vulnerabilities in a banking institution, in order to subsequently build a mitigation plan to address the identified risks.

This methodology is developed in three phases. In the first phase, workshops are conducted at three levels of the organization (Enterprise, Operational Area, and Staff) to identify from their perspective the risks associated with the most critical assets of virtual banking. In phase two, a risk analysis of the critical infrastructure that supports the information assets identified in phase one is performed; and in phase three, a multidimensional analysis of the previously identified risks is carried out in order to subsequently develop protection and mitigation strategies for these risks.

Additionally, this paper presents an analysis will be made of the advantages and disadvantages of the methodology when performing a risk assessment compared to other methodologies.

I. CONTEXTO

OCTAVE (Operationally Critical Threat Asset, and Vulnerability Evaluation), es una metodología de evaluación de riesgos desarrollada por el SEI (Software Engineering Institute) en Estados Unidos, que busca cubrir los riesgos operacionales y prácticas de seguridad, a través de tres fases, procesos y actividades, para lograr elaborar una vista detallada de las necesidades de seguridad de una organización.

El SEI ha divulgado distintas versiones de la metodología, a lo largo de los años, a partir de su primera publicación en el año 2.000. Las principales versiones existentes en la actualidad son:

- OCTAVE versión 2.0. Esta versión fue diseñada para empresas con más de 300 empleados, con infraestructura propia, con una estructura organizacional multinivel y que tengan la capacidad de poder efectuar ejecución de herramientas de identificación de vulnerabilidades e interpretación de los resultados de estas. Esta versión establece los procedimientos, guías, catálogos y entrenamiento para ser aplicados a distintos niveles de la organización, con el fin de lograr una perspectiva desde lo estratégico, táctico y operativo. Este último aspecto también incluye la tecnología que soporta los activos a ser gestionados, buscando alinear a la organización integralmente en torno de estos, para perfilar las amenazas, vulnerabilidades y riesgos y desarrollar un plan de mitigación efectivo. El método de levantamiento de información se basa en workshops [1].

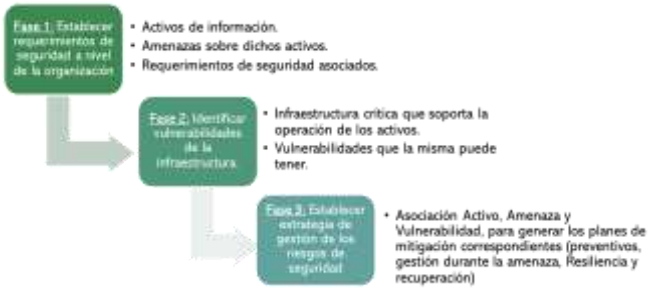

Fig. 1. Arquitectura OCTAVE Versión 2.0. [1]

- OCTAVE – S. Está orientado a organizaciones pequeñas, de menos de 100 empleados. Al igual que la primera versión de OCTAVE, está compuesta por tres fases. Sin embargo, el levantamiento de la información, no se efectúa con base en workshops. Se presume que el equipo ejecutor de la metodología cuenta con el conocimiento profundo y detallado de los activos de la organización, sus requerimientos de seguridad, sus amenazas y en general, las prácticas de seguridad de la organización. [2]
- OCTAVE Allegro. Está hecho para grupos que quieren realizar una evaluación de riesgos sin tener que efectuar un gran involucramiento de la organización, para recibir conocimiento experto de todos los activos [2].
- OCTAVE FORTE. Esta es la versión más reciente de OCTAVE y está diseñada para implementar un modelo de gestión de riesgos operacionales asociados a la empresa. Aborda todas las formas de riesgo, desde una perspectiva holística, logrando que los riesgos de ciberseguridad sean analizados y manejados de la misma manera que todo el portafolio restante de riesgos de la organización.[3]

Para efectos del trabajo contemplado en este proyecto, se considera la revisión de la versión original 2.0.

II. Descripción de la Propuesta

A. Descripción del problema

El CSIRT de Asobancaria (Equipo de apoyo parala respuesta a incidentes de Ciberseguridad para el sector financiero colombiano), ha expuesto y generado documentos de advertencia sobre el crecimiento de los ataques y delitos a través de los canales virtuales [4]. Es así como en su informe de Cibercriminalidad del pasado mes de diciembre del 2020, manifiesta cómo los delincuentes también han pasado a una operación virtual, ante las limitaciones de movilidad que el aislamiento y la pandemia han determinado, para la población en general.

Fig. 2. Informe Incremento de Amenazas CSIRT Financiero Asobancaria diciembre 2020 [5]

Como se puede observar, el crecimiento en delitos, comparando año a año, contra el periodo de la pandemia, determina un crecimiento más pronunciado en dichas actividades ilícitas. Así mismo en general, hay un gran crecimiento en estos ataques cuando se compara el año 2019 contra el 2020.

Teniendo en cuenta lo anterior, se deduce la importancia de tener una correcta identificación y tratamiento de los riesgos asociados a las amenazas y vulnerabilidades más importantes de una entidad bancaria, con el fin de realizar un correcto análisis, teniendo en cuenta los resultados que generan herramientas de protección como IDS/IPS, cortafuegos, etc., así como el conocimiento del negocio y sus riesgos asociados, desde el punto de vista de la organización.

Dados los anteriores antecedentes, es necesario que las entidades bancarias realicen una evaluación formal e integral de amenazas y vulnerabilidades sobre sus activos de información e infraestructura que los soporta, para diseñar, construir e implementar un plan de gestión que pueda mitigar las brechas identificadas.

B. Propuesta de solución

Implementación de una metodología de identificación de amenazas y vulnerabilidades en una entidad bancaria, para elaborar y aplicar un plan de gestión de las brechas encontradas. A este respecto, se plantea el uso de la metodología OCTAVE (Operationally Critical Threat Asset, and Vulnerability Evaluation), puesto que incluye la vista organizacional y operativa del negocio, para aprovechar el conocimiento y experiencia de la misma institución, lo cual difícilmente puede aportar un consultor externo. Así mismo, es necesario efectuar la evaluación propuesta, puesto que el nivel de seguridad y continuidad configurado corresponde a una solución general que, si bien se fundamenta en buenas prácticas, desconoce las características propias de la organización, operación y tecnología que se emplea para ofrecer el servicio, lo cual puede generar vacíos, que de materializarse podrían ocasionar efectos devastadores legales, financieros y reputacionales.

Por otra parte, la elección de OCTAVE, como la metodología de evaluación de amenazas, vulnerabilidades y riesgos, para este trabajo, se basa en el siguiente análisis. Las metodologías que cubren el alcance mencionado se clasifican en cualitativas y cuantitativas, de acuerdo con el método que incorporan para medir el nivel de criticidad de cada riesgo identificado. Las que abordan la evaluación del riesgo a través de información numérica, fórmulas y cálculos son de naturaleza cuantitativa. Las principales de esta categoría son:

- Método IS Risk Analysis. [6]Es un modelo con 4 etapas secuenciales bajos las cuales determina niveles de relevancia de las funciones del negocio y sus activos de información asociados. Para cada amenaza y riesgo de no disponibilidad de dicho negocio, efectúa un análisis de pérdida anual esperada con base en una formulación matemática. Dicho análisis, no solamente incluye los costos del posible reemplazo del activo comprometido, sino que también considera la pérdida de ingresos que dicha situación genera para el negocio. También incorpora a la formulación la probabilidad de materialización del riesgo junto con un nivel de relevancia del activo afectado, desde la perspectiva de la continuidad operacional. Lo más destacado de esta metodología es que finaliza con un resultado cuantitativo financiero, que permite ser comparado contra la inversión requerida para mitigar cada riesgo evaluado. Sin embargo, sus cuatro etapas incluyen una formulación matemática compleja, que puede ser difícil de seguir para la alta gerencia y para las distintas áreas de la organización.

- Método ISRAM (Information Security Risk Analysis Method) [7]. Es una metodología que establece 7 etapas para su desarrollo. Incluye una serie de encuestas para ser aplicadas a los miembros del personal operativo y gerencia de la organización para relevar la probabilidad y consecuencia de la materialización de las vulnerabilidades de seguridad identificadas. Incluye una formulación matemática que permite traducir las encuestas en resultados cuantitativos con un valor de riesgo final. Cada valor individual puede ser empleado para la toma de decisiones sobre la estrategia de gestión. Tiene como desventaja que finalmente los resultados obtenidos se basan en la valoración subjetiva de las encuestas y adicionalmente, la formulación matemática es compleja, lo cual dificulta su aplicación en las organizaciones.

Por otra parte, las metodologías que evalúan los riesgos a través de juicio experto, utilizando calificaciones asignadas en categorías discretas, se consideran de tipo

cualitativas. Las principales de esta categoría son (tomado de los artículos relacionados en [7] y [8]):

- OCTAVE. Es una metodología elaborada por el SEI, que busca cubrir los riesgos operacionales y prácticas de seguridad, a través de tres fases, procesos y actividades, para lograr elaborar una vista detallada de las necesidades de seguridad de una organización. Tiene como ventaja que puede ser ejecutado por un pequeño grupo de personas, obteniendo información de múltiples niveles de la organización, para lograr construir una vista estratégica, táctica, operacional y tecnológica de los riesgos de la empresa. Esto hace que OCTAVE sea muy comprensible en su utilización, pues coincide con los aspectos que conforman la organización como un todo. Sin embargo, tiene como desventaja que los riesgos son evaluados a través de un rango de valores (alto, medio y bajo), que son combinados en una matriz, junto con su probabilidad, para establecer un posible impacto. Este resultado, al carecer de una valoración financiera, no permite determinar la pertinencia de las estrategias de gestión y mitigación junto con su correspondiente inversión.

- CORAS (Construct a platform for Risk Analysis of Security Critical Systems). Este método fue construido por la IST (Information Society Technologies) patrocinado por la Unión Europea. Utiliza UML para describir la relación entre los empleados con su medio ambiente de trabajo y los riesgos resultantes de dicha relación. Las decisiones de gestión de los riesgos identificados son representadas en diagramas de clases asociados a cada activo. La principal fortaleza de CORAS, es que incluye un esquema de comunicación fluido entre las distintas partes de la organización junto con un análisis eficiente sobre los riesgos identificados, asociados a los activos detallados. Su principal desventaja es que al igual que OCTAVE, no considera una valoración financiera cuantitativa de los riesgos, con lo cual no es posible soportar las decisiones de inversión que la gestión de dichos riesgos puede implicar.

De acuerdo con la anterior descripción, la metodología que mejor interpreta la estructura de la organización en todos sus niveles es OCTAVE, pues está diseñada para incorporar los aspectos estratégicos, tácticos, operativos y tecnológicos, lo cual es la estructura misma de la empresa. Sin embargo, para cubrir la falencia de la evaluación cualitativa del riesgo, se propone incorporar una valoración tipo ALE (Annual Loss Expectancy) para los riesgos más críticos. Dicha valoración se calcula con base en la siguiente fórmula [8]:

$$ALE = SLE\ x\ ARO$$

ARO = Frecuencia anual de materialización del riesgo

Donde SLE (Single Loss Expectancy) corresponde a la fórmula:

$$SLE = AV\ x\ EF$$

AV = Valor del Activo de información para la organización

EF = Nivel de exposición del activo al riesgo considerado

Adicionalmente, se propone también incluir un ejercicio de análisis de correlación de riesgos, puesto que la consideración inicial de la metodología los supone independientes. Sin embargo, en la práctica, riesgos considerados menores, pueden activar otros riesgos mayores, por tanto, su gestión debe ser considerada para buscar una mitigación efectiva.

III. SOLUCIÓN

A continuación, se detallan las actividades desarrolladas para llevar a cabo la evaluación de riesgos utilizando como principal referencia la metodología de OCTAVE V2.

Fase 1 - Establecer requerimientos de seguridad a nivel de la organización.

Durante esta etapa se examina la organización realizando un acercamiento y obteniendo información del personal que labora en la compañía. Se interactúa con diferentes personas de la organización en diferentes niveles con la única idea de que contribuyan con su conocimiento, experiencia y puntos de vista únicos al ejercicio.

- *Proceso 1: Identificar el conocimiento empresarial:* el primer proceso OCTAVE, define las actividades para identificar los activos más importantes, las amenazas, y las estrategias de

protección con las que cuenta la organización desde la perspectiva de la alta gerencia.

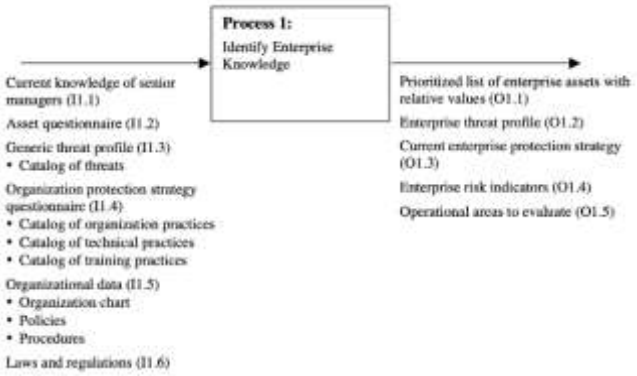

Fig 3. OCTAVE Process 1, Identify Enterprise Knowledge.[1]

En este proceso es importante que el equipo que lidere los workshops tenga amplio conocimiento de los activos a evaluar con el fin de garantizar que se recolecte información que ayude exitosamente al desarrollo de todos los procesos de la metodología.

OCTAVE brinda una guía de cómo realizar los workshops, mas no un formato, por lo que se debe preparar adecuadamente los mismos antes de programar a los participantes de la alta gerencia. En este sentido es importante que los Workshops den respuesta a los siguientes interrogantes:

- Activos de información más importantes en el área a evaluar.
- Amenazas existentes asociadas a los activos de información.
- Políticas de protección existentes.
- Vulnerabilidades asociadas a los activos de información.
- Requerimientos de seguridad asociados a los activos de información.

Por otro lado, OCTAVE allegro puede ser usado para complementar el uso de la metodología, ya que brinda un worksheet de áreas de preocupación donde detalla amenazas, vulnerabilidades y riesgos, también ilustra un árbol de amenazas que es muy útil para identificar dichas amenazas de los activos de información de una manera clara y rápida.

- *Proceso 2: Identificar el conocimiento de las áreas operativas*: el segundo proceso de OCTAVE, define las actividades para determinar el punto de vista de las áreas operativas respecto a los activos más importantes, las amenazas, y las estrategias de protección con que cuenta la organización.

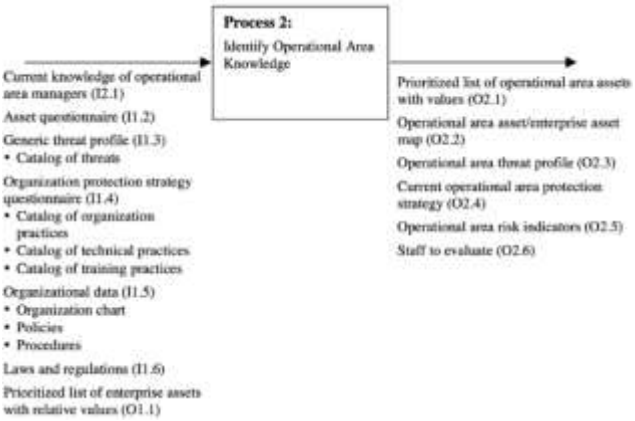

Fig 4. OCTAVE Process 2, Identify Operational Area Knowledge.[1]

El proceso 2 se busca obtener respuesta a los mismos interrogantes planteados en el proceso 1, sin embargo, esta vez desde una perspectiva operacional, la cual cubre un alcance táctico de la organización. Es importante que los Workshops den respuesta a los siguientes interrogantes, los cuales son:

- Activos de información más importantes en el área a evaluar.
- Amenazas existentes asociadas a los activos de información.
- Políticas de protección existentes.
- Vulnerabilidades asociadas a los activos de información.
- Requerimientos de seguridad asociados a los activos de información.

En este caso el aporte es desde la gerencia de operación, su experiencia desde la gestión con los clientes internos y externos, sus áreas de preocupación muchas de ellas, asociadas a incidentes que se han presentado.

Al igual que en el proceso 1, es muy importante el conocimiento del equipo que maneja el Workshop, con el fin de conducir a los involucrados a describir estas necesidades, dando énfasis en su área de conocimiento sobre los activos.

- *Proceso 3: Identificar el conocimiento del personal*: el tercer proceso OCTAVE, define las actividades

para determinar el punto de vista de los activos más importantes, las amenazas, y las estrategias de protección con las que cuenta la organización desde la perspectiva de las personas que trabajan directamente con dichos activos o indirectamente (áreas de soporte, por ejemplo).

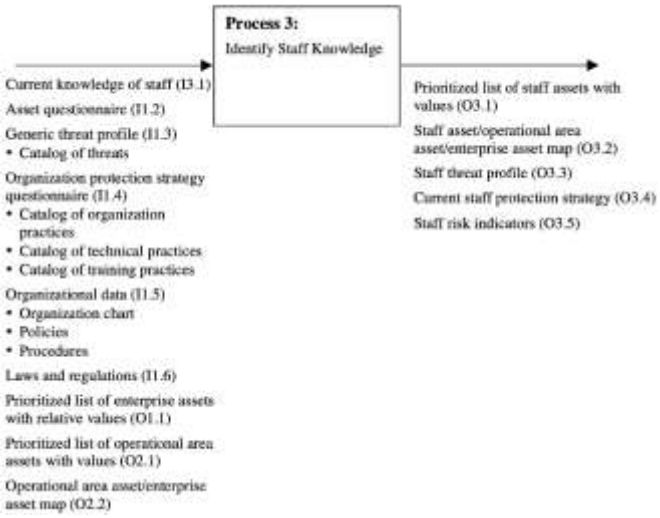

Fig 5. OCTAVE Process 3, Identify Staff Knowledge.[1]

En el proceso 3, se busca obtener respuesta a los mismos interrogantes planteados en los procesos 1 y 2, sin embargo, esta vez desde una perspectiva de personas que trabajan directa o indirectamente con el área a evaluar, como equipo de TI, marketing, equipo de proyectos, etc. Es importante que los Workshops den respuesta a los siguientes interrogantes:

- Activos de información más importantes en el área a evaluar.
- Amenazas existentes asociadas a los activos de información.
- Políticas de protección existentes.
- Vulnerabilidades asociadas a los activos de información.
- Requerimientos de seguridad asociados a los activos de información.

En este nivel el personal que interviene en la evaluación tiene un mayor conocimiento de los activos, porque los gestiona continuamente. Lo cual da una vista mucho más detallada de los mismos y de las brechas de seguridad, así como las vulnerabilidades que pueden tener los procesos y procedimientos mismos.

- *Proceso 4: Establecer los requerimientos de seguridad:* el cuarto proceso de OCTAVE se construye con base en la información recolectada en los primeros procesos. Las diferentes perspectivas son recolectadas y combinadas de acuerdo con su naturaleza (amenazas, actividades de protección, indicadores de riesgo y activos), y se determinan los requerimientos de seguridad para los activos identificados. Este proceso aporta suficiente información que conformará la base para el diseño de la estrategia de protección en la organización. La meta de este proceso es combinar los diferentes puntos de vista recolectados durante los procesos anteriores, para crear una figura más clara respecto a los activos, amenazas e indicadores de riesgo y así, determinar los requerimientos de seguridad en toda la organización y los fundamentos para una estrategia de protección.

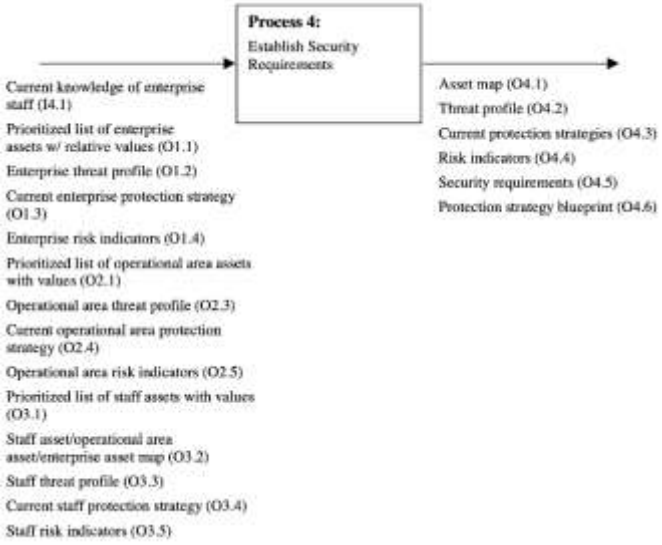

Fig 6. OCTAVE Process 4, Establish Security Requirements.[1]

Como resultado de los workshops, se identifican por parte de cada área participante diferentes focos de atención e información que, desde su perspectiva son los de mayor relevancia, importancia y cuidado con respecto al área evaluada.

Con estos resultados, se puede analizar el Mapa Estratégico Institucional de la entidad financiera a fin de determinar si la información y áreas de preocupación expuestas por los diferentes participantes en las primeras etapas de la aplicación de la metodología, agregan valor al negocio y se encuentran alineadas a los objetivos organizacionales.

Por otro lado, con la información detallada de los workshops realizados en los procesos 1, 2 y 3 y su análisis, se busca construir como resultado:

- Mapa de activos consolidado
- Perfil de riesgo consolidado
- Estrategias de protección consolidado
- Indicadores de riesgos
- Requerimientos de seguridad consolidado
- Estrategias de protección

Fase 2 - Identificar vulnerabilidades de la infraestructura

Esta fase de OCTAVE, utiliza la información recopilada durante los procesos de la fase 1. Con dicha información, se identifican los componentes de la infraestructura de mayor prioridad tanto a nivel de componentes físicos como computacionales, para establecer las vulnerabilidades de estos y que su vez, generan una exposición de riesgos para los activos de la organización, que son soportados en dichos componentes. La principal meta de la fase 2, es identificar políticas y procedimientos faltantes al igual que componentes de la infraestructura vulnerables.

- *Proceso 5: Mapeo de los activos de alta prioridad sobre la infraestructura que los soporta*: con base en los activos y amenazas identificados durante la fase 1, se determinan los componentes de mayor prioridad en la infraestructura que los soporta. La infraestructura de información hace referencia tanto a la infraestructura de computación como a la infraestructura física. La principal meta de este proceso es identificar los componentes más críticos o de mayor prioridad en dicha infraestructura, con el fin de poder ser examinados a detalle y lograr establecer posibles vulnerabilidades.

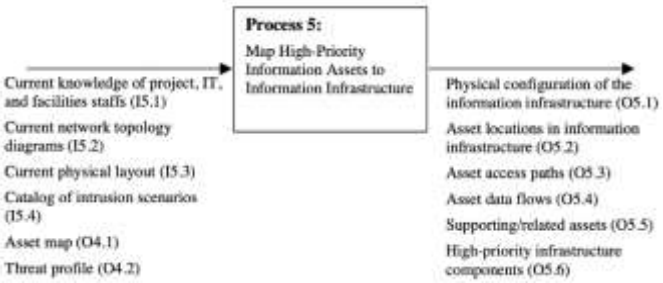

Fig 7. OCTAVE Process 5, Map High-Priority Information Assets to Information Infrastructure.[1]

En el proceso 5, es muy importante la participación y conocimiento del área de TI, para obtener información de:

- Rutas de acceso de los activos de información
- Flujos de los activos de información
- Ubicación física de los activos de información
- Arquitectura de red de los activos de información

Con esta información se puede examinar con detalle los activos de información y su infraestructura asociada, con el fin de identificar sus vulnerabilidades en el proceso 6.

- *Proceso 6: Ejecutar una evaluación de vulnerabilidades en la infraestructura*: define las actividades para evaluar las vulnerabilidades de los componentes de la infraestructura de información identificados en el proceso 5. Entre dichos componentes también se contemplan infraestructuras de terceras partes, que están directamente relacionadas con los activos analizados y sus servicios asociados. La meta principal es establecer las vulnerabilidades presentes en la infraestructura existente y así mismo, lograr la identificación de procedimientos o políticas inexistentes o parcialmente implementadas.

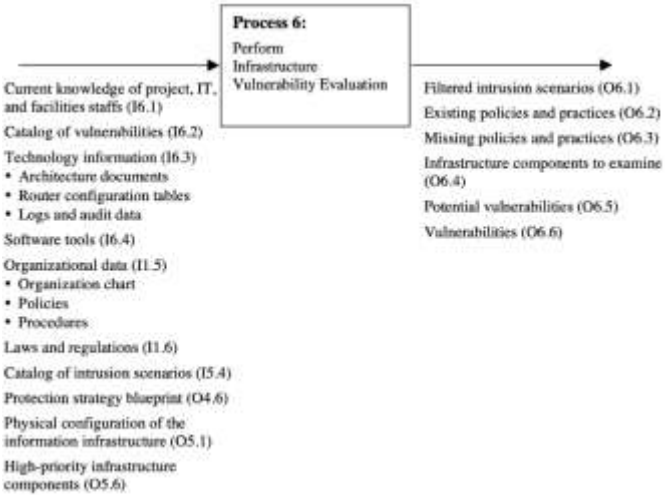

Fig 8. OCTAVE Process 6, Perform Infrastructure Vulnerability Evaluation.[1]

Para identificar las vulnerabilidades presentes en la infraestructura se realizan las siguientes actividades:

- Verificar si existen escenarios de intrusión para ser evaluados
- Identificar políticas y prácticas existentes
- Identificar ausencia de políticas y prácticas existentes.

Al realizar estas actividades se obtienen las vulnerabilidades presentes en el área que gestiona la infraestructura evaluada.

Fase 3 – Desarrollar un plan y una estrategia de seguridad.

La fase 3 de OCTAVE, determina la estrategia de gestión de riesgos de seguridad, analiza la información sobre amenazas y vulnerabilidades de los activos en el contexto de escenarios de intrusión, para identificar y priorizar el riesgo asociado a dichos escenarios para la empresa. La meta principal de la fase 3, es identificar los riesgos sobre la banca virtual y desarrollar una estrategia de protección que mitigue los de mayor prioridad.

- *Proceso 7: Conducir un análisis de riesgo multidimensional*: determina las actividades para identificar y priorizar los riesgos en la organización asociados a la banca virtual. Para esto, los riesgos son definidos con base en el conocimiento del equipo de trabajo al igual que su entendimiento de los escenarios de intrusión, activos expuestos, impacto sobre el negocio, amenazas, prácticas de protección existentes y faltantes y la probabilidad de materialización de dichas amenazas, por lo cual este análisis se conoce como multidimensional. La meta principal de este proceso es generar una lista priorizada de riesgos basados en impacto y probabilidad.

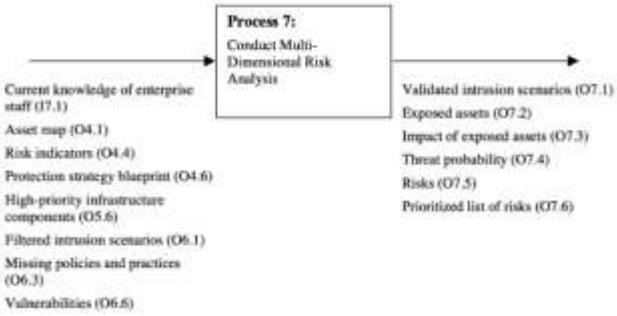

Fig 9. OCTAVE Process 7, Conduct Multi-Dimensional Risk Analysis.[1]

Durante esta etapa de la aplicación de la metodología se realiza la definición y priorización de riesgos de acuerdo con el método especificado al inicio del documento, en el cual se evalúa y se determinan los aspectos de mayor importancia para la estrategia del banco y se plantea un ejercicio típico de probabilidad vs impacto para su valoración y posterior priorización.

En este proceso se puede usar como base los ejercicios realizados en la identificación de las áreas de preocupación.

- *Proceso 8: Desarrollar una estrategia de protección*: define las actividades para desarrollar e implementar una estrategia de protección en la organización, reduciendo los riesgos de seguridad de información. La meta principal de este proceso es producir una estrategia de protección para mitigar los riesgos y un plan de gestión continuo.

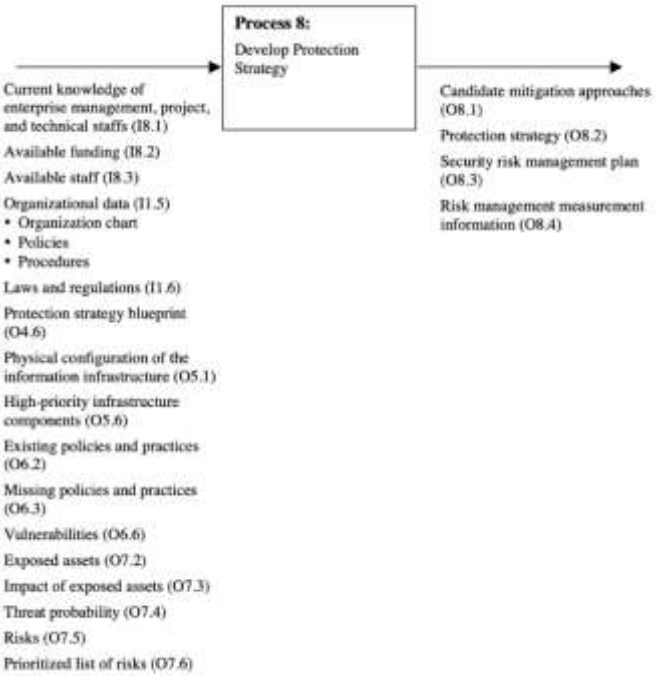

Fig 10. OCTAVE Process 8, Develop Protection Strategy.[1]

En este proceso, para desarrollar las estrategias de protección, se realiza la definición de controles asociados a cada uno de los riesgos identificados en el proceso 7. Para cada uno de los controles identificados, se efectúa una valoración de los riesgos luego de su aplicación con el fin de determinar la efectividad de este y su eficacia de cara a la mitigación del riesgo.

Para establecer la prioridad en la implementación de los controles se determina inicialmente la valoración numérica de cada ejercicio de riesgos y se adiciona el costo asociado a cada implementación para facilitar la toma de decisiones y la clasificación dentro de la priorización de ejecución.

Para costear el proyecto y decidir cuáles riesgos se mitigarán y cuáles no, es importante realizar un cálculo de pérdida esperada, ya que determinará qué inversiones son razonables e inclusive la manera de autofinanciación o mitigación del riesgo mismo (provisión en el cobro de comisiones o seguros contratados).

Para la implementación de las estrategias de protección se puede hacer un despliegue de controles que mayor afectación positiva tienen sobre el riesgo, para después contemplar la capacidad y esfuerzo de su desarrollo, si el recurso humano actual puede realizarlo como ejercicio de mejora en los procesos actuales y finalmente, teniendo en cuenta el presupuesto requerido para implementación.

Adicionalmente, como parte del ejercicio de análisis de riesgos, no planteado dentro de la metodología de OCTAVE, pero sin embargo, útil para minimizar los riesgos, es importante realizar una revisión de riesgo motor, ya que a partir de los riesgos identificados inicialmente, se encuentra que estos pueden ser disparados por otros riesgos y en algunos casos aumentar su criticidad. Por ejemplo, si hay un riesgo de fuga de información y este se materializa, dicha información puede ser aprovechada por los delincuentes disparando el riesgo de vishing o fishing, ya que un delincuente podría utilizar la información de los clientes para hacer campañas de vishing o de fishing, logrando obtener los datos restantes de identificación, autenticación, para materializar los fraudes. En este contexto, estos riesgos están correlacionados y al materializarse el riesgo motor, el plan de gestión debe ser integral.

IV. VENTAJAS Y DESVENTAJAS DE LA METODOLOGÍA

Durante la implementación de la metodología se encontraron en cada proceso ventajas y desventajas las cuales son presentadas a continuación:

Ventajas procesos 1, 2 y 3 Identificar el conocimiento de la organización en los niveles de alta gerencia, área operacional y staff

- ✓ Se obtiene conocimiento de problemas y debilidades de los cuales no se tiene visibilidad en el día a día de la operación.
- ✓ Aunque desde cada área se da un enfoque diferente de acuerdo con su rol en la organización, se identificó solo un activo de información en el área evaluada lo que permite enfocar los esfuerzos de aplicación de la metodología.
- ✓ Se Preparar adecuadamente los workshops permite gestionar adecuadamente al grupo para recolectar la información relevante para el análisis multidimensional de los riesgos, lo cual es una de las ventajas de la metodología de OCTAVE, sobre otras metodologías que solo realizan validación general de listas de requerimientos, sin contexto.
- ✓ Identificar detalles operativos del servicio permite desarrollar estrategias de gestión de protección alineadas con el negocio, lo cual es una ventaja sobre otras metodologías que trabajan sólo una lista de requisitos general, sin un contexto específico.
- ✓ Al ser la metodología desarrollada por personal interno de la organización puede generar un vínculo de confianza fundamental para obtener información relevante y de manera continua.
- ✓ Contar con una lista de prácticas de protección sirve para evaluar la madurez de la gestión de los riesgos en la organización, lo cual es un aporte directo de la metodología.

Desventajas procesos 1, 2 y 3 Identificar el conocimiento de la organización en los niveles de alta gerencia, área operacional y staff

- De acuerdo con los workshops realizados, es importante corroborar la información entregada. Se recibieron criterios o prácticas realizadas, sin embargo, en actividad de campo efectuada se identificó que no todas las prácticas mencionadas se estaban cumpliendo.
- Si los participantes no cuentan con el tiempo requerido para el desarrollo de los workshops, es posible obtener información incompleta y en algunos casos sin relevancia, generando atrasos en la implementación de la metodología. Por tanto, OCTAVE tiene una dependencia directa sobre la calidad de los workshops en comparación con otras metodologías que no utilizan este tipo de actividades.
- La información recopilada en los workshops virtuales es relevante para el desarrollo de la metodología, sin embargo, no genera cercanía con los participantes, disminuyendo así la probabilidad de recopilar toda la información de valor para la organización. Así mismo, se incrementa la probabilidad de interpretaciones incorrectas frente a los temas tratados. Nuevamente, OCTAVE tiene una dependencia directa sobre la calidad de los workshops en comparación con otras metodologías que no utilizan este tipo de actividades.

Ventajas proceso 4 Establecer los requerimientos de seguridad

- ✓ La elaboración de las áreas de preocupación con la información de los procesos 1, 2 y 3, permite identificar adecuadamente los requerimientos de seguridad y apoyar el desarrollo de los demás procesos alineados con las necesidades expresadas por las áreas participantes de los workshops. Esto permite que la metodología responda específicamente a la casuística de la organización, lo cual es una ventaja de esta.
- ✓ El poder identificar el conocimiento del cliente, influye directamente en las decisiones que se deben tomar a nivel de seguridad.
- ✓ Las áreas de preocupación consolidadas en los arboles de intrusión, son más fáciles de visualizar y comprender.
- ✓ Se combinan estrategias de protección con las áreas de preocupación para establecer los riesgos relevantes.

Desventajas proceso 4 Establecer los requerimientos de seguridad

- Es necesario establecer un glosario de términos, con el fin de garantizar que se mitigue la ambigüedad de expresiones o palabras asociadas a componentes del servicio.
- Teniendo en cuenta que OCTAVE usa una valoración de riesgo es cualitativa, es necesario apoyarse en otras metodologías cuantitativas.
- El no hacer una correlación de riesgos, genera un análisis parcial ya que los mismos se contemplan de manera independiente, lo cual no es lo que sucede en la vida real, pues los riesgos tienen relaciones de causa efecto o de concurrencia. OCTAVE los analiza de manera independiente, por tanto, fue necesario hacer una evaluación adicional.

Ventajas procesos 5 y 6 Identificar vulnerabilidades de la infraestructura

- ✓ Correlacionar las áreas de preocupación identificadas en los procesos 1, 2 y 3 con la infraestructura que los soporta permite identificar los posibles puntos neurálgicos de falla.
- ✓ Al identificar los flujos de información y rutas de acceso y combinarlas con prácticas de protección y vulnerabilidades, se determina si los riesgos identificados continúan igual o se vuelven más relevantes.

- ✓ Los árboles de amenazas de OCTAVE Allegro entregan información de amenazas de infraestructura, propia y externa y de los activos de información, que operan sobre las mismas.
- ✓ Se obtuvieron resultados rápidos al tener la información de los procesos 1, 2, 3 y 4.

Desventajas procesos 5 y 6 Identificar vulnerabilidades de la infraestructura

- ➢ Es importante llegar a un buen nivel de detalle para identificar puntos únicos de falla.
- ➢ Para que la identificación de las vulnerabilidades de infraestructura sea correcta se debe garantizar que la información se encuentre actualizada y documentada.
- ➢ Es necesario hacer actividades de campo para garantizar que la información documentada sea consistente con lo que ocurre en la operación.
- ➢ Es necesario apoyarse en formatos propios de la organización y otras fuentes ya que la metodología no los suministra.

Ventajas procesos 7 Conducir un análisis de riesgo multidimensional

- ✓ Con la metodología se puede hacer una valoración de riesgos adecuada para garantizar que la aplicación de estrategias de protección sea sustentable, debido a la inclusión de las diferentes dimensiones consideradas como importantes para la organización.
- ✓ En este proceso se obtiene una vista general de percepción de la infraestructura correlacionada con activos de información identificados en los procesos 1, 2, 3 y 4, facilitando la identificación de riesgos asociados a dicha infraestructura y su impacto directo en los activos de información.
- ✓ Se puede identificar el riesgo residual con base en los riesgos identificados previamente y sus controles.

Desventajas proceso 7 Conducir un análisis de riesgo multidimensional

- ➢ La probabilidad de riesgos es subjetiva, por lo que es necesario analizar incidentes del pasado de otras fuentes para reducir esta subjetividad.
- ➢ Al ser los riesgos evaluados a través de un rango de valores (alto, medio y bajo), y combinados en una matriz, junto con su probabilidad, para establecer un posible impacto, este resultado, al carecer de una valoración financiera, no permite determinar la pertinencia de las estrategias de gestión y mitigación junto con su correspondiente inversión.

Ventajas procesos 8 Desarrollar una estrategia de protección

- ✓ El desarrollo de este proceso permite contar con un plan de protección alineado con las prioridades y riesgos identificados, así como las capacidades para poderlos gestionarlos.
- ✓ Se facilita la incorporación de diferentes criterios para determinar la priorización de implementación del plan de protección.
- ✓ Se considera la inversión de las distintas aproximaciones para seleccionar estrategias de mitigación.

Desventajas proceso 8 Desarrollar una estrategia de protección

- ➢ La metodología no sugiere un criterio cuantitativo para hacer la valoración de riesgos, por lo que es necesario hacer la valoración con pérdida esperada u otras metodologías de estimación cuantitativas existentes.

V. CONCLUSIONES

Cada grupo de la organización analiza la situación desde una perspectiva estratégica, táctica y operativa, que es como funciona realmente la entidad. Esto es

muy conveniente porque permite darle una respuesta integral de gestión a todos los niveles de la empresa.

Con los workshops se puede identificar los perfiles de conocimiento de tecnología de los clientes de la entidad financiera, lo cual resulta altamente relevante, porque a partir de esta perspectiva, las estrategias de gestión se pueden adaptar específicamente a dichos perfiles, para que sean mucho más efectivas.

La clave fundamental de la metodología está enfocada en las personas entrevistadas, ya que son las que dan el contexto y punto de partida sobre los activos claves de información con base en el cual se fundamentan las siguientes etapas de la metodología.

Evaluar los diferentes niveles de la organización ayuda a identificar riesgos que no estaban contemplados en la evaluación de riegos, a través de métodos de aseguramiento de estándares como ISO27001, por ejemplo, identificar el tipo de cliente que utiliza un servicio de la entidad y su vulnerabilidad técnica asociada a los ataques cibernéticos. Así mismo, sirve para solucionar y ajustar de inmediato algunos componentes de la infraestructura.

Al combinar los workshops funcionales con los correspondientes de infraestructura y tecnología, se logran identificar vulnerabilidades y amenazas en distintas áreas y con distintas prioridades.

Al hacer un análisis multidimensional se logra identificar más fácilmente en dónde son requeridos más esfuerzos en tiempo, costos y asignación de personal.

Con esta metodología se logra identificar de una manera clara y detallada en qué riesgos invertir recursos para solucionar o bajar su probabilidad de impacto u ocurrencia.

Se identificaron algunos vacíos en la metodología asociados a herramientas o plantillas de referencia, para la elaboración de los workshops y evaluación de riesgos, las cuales deberían lograr que la ejecución y evolución de los procesos a lo largo del trabajo, se pudieran realizar de una forma más consistente con el método expuesto, por lo cual al inicio se encontraron algunas dificultades en como planear y desarrollar los workshops con las personas elegidas de la banca virtual.

La metodología debe ser continua en el tiempo, particularmente en el seguimiento a los controles y también es oportuno efectuar reevaluaciones, cuando hay cambios relevantes con el fin de identificar nuevos riesgos.

Comparado con otras metodologías como PCI e ISO 27001, en esta metodología se tiene inclusión del personal y su conocimiento, por lo cual es importante la combinación de varias metodologías y no limitarse a la utilización de solo una.

Comparada con otras metodologías como ISO y PCI que aborda un tema general de riesgos, la metodología OCTAVE es más especializada en garantizar que se apliquen los controles que son más acordes con la operación y las características del negocio y la organización.

Los workshops ayudan a construir los requerimientos de seguridad y en general, a detallar las distintas ópticas de la organización, en cuanto a la estrategia, táctica, operación y la infraestructura tecnológica.

Para que la gestión de riesgos tenga un mayor impacto, lo que la metodología enseña es que es importante tener espacios de diálogo continuos con los clientes, con el fin de establecer nuevas áreas de preocupación o cambios en las prioridades de estas.

Antes de iniciar los workshops es importante establecer las áreas que son requeridas y relevantes para obtener toda la información necesaria que servirá de entrada en los diferentes procesos.

Para llevar a cabo una evaluación de riesgos integral es importante soportase en otras estrategias de análisis como la valoración de pérdida esperada y la correlación de riesgos, ya que estas ayudan a

identificar de manera más clara las alternativas de controles razonables para mitigar los riesgos encontrados y la prioridad de dichos riesgos, que se debe determinar para su tratamiento.

REFERENCIAS

[1] Christopher J. Alberts, Sandra G. Behrens, Richard D. Pethia, William R. Wilson. (June 1999). Introduction. En Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0(2-62). Pittsburgh, PA 15213-3890: Carnegie Mellon Software Engineering Institute.

[2] Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University: Software Engineering Institute.

[3] Brett Tucker (2020). Advancing Risk Management Capability Using the OCTAVE FORTE Process. Carnegie Mellon University: Software Engineering Institute.

[4] OEA and Asobancaria, "DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA." Oct. 2019, [Online]. Available: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf.

[5] CSIRT FINANCIERO ASOBANCARIA. (22/12/2020). Cibercriminalidad en Colombia. INFORME DE AMENAZAS, I, 17.

[6] Mike Tierney. (October 13, 2020). annual-loss-expectancy-and-quantitative-risk-analysis. February 27,2021, de Netwrix blog Sitio web: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/.

[7] Ping Wang and Melva Ratchford. (2018). Integrated Methodology for Information Security Risk Assessment. En Information Technology –14th International Conference on Information Technology New Generations (156-159). Las Vegas, Nevada, USA: Department of Electrical and Computer Engineering University of Nevada.

[8] Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. Proceedings of SAICSIT 2005, pp. 95–103.