Asignatura	Datos del alumno	Fecha
Diseño y Desarrollo de Programas Informáticos Seguros	Apellidos: Paz López	27/11/2021
	Nombre: Angel Ramón	

Contenido

INTRODUCCION....2

METODOLOGIAS....3

- CORAS (CONSULTATIVE OBJECTIVE RISK ANALYSIS SYSTEM).....3
- CIGITAL'S ARCHITECTURAL RISK ANALYSIS PROCESS. 4
- OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION) 5
- PTA TECHNOLOGIES CALCULATIVE THREAT MODELING METHODOLOGY (CTMM). 5
- TRIKE. METODOLOGÍA DE EVALUACIÓN DE AMENAZAS. 6
- TAM (Microsoft Threat Analysis And Modeling). 7
- PASTA (Process For Attack Simulation And Threat Analysis). 8

CUADRO COMPARATIVO 10

PROPUESTA DE UNA NUEVA METODOLOGÍA DE AMENAZAS 12

CONCLUSIONES 13

REFERENCIAS 14

INTRODUCCION

Vivimos en un mundo en una era actualizada donde las empresas, organizaciones hasta las mismas personas dependemos de la tecnología de la información usando herramientas para realizar hasta las actividades más simples de la vida cotidiana, y para lograr objetivos y metas en el ámbito laboral; pero el uso de ello también trae un abanico de problemas e inconvenientes de usar estas herramientas sino se está utilizando de manera correcta, ya que en ello hay amenazas y vulnerabilidades asociadas a estas herramientas tecnológicas, que si no nos percatamos o no somos conscientes de ello podríamos tener resultados negativos como ser víctimas de ataques para robar información y con ello no lograr nuestros objetivos y metas en el ámbito laboral y hasta personal. En esta actividad estaremos estudiando y analizando el modelado de amenazas el cual es un proceso estructurado y sistemático de seguridad para el desarrollo de software cuyo objetivo es el de identificar todas las posibles amenazas y vulnerabilidades a la que un sistema de información puede ser susceptible, cuantificar el impacto, mitigar los ataques, proteger los recursos y hasta identificar posibles consecuencias, es por ello que el modelado de amenazas se considera la primera linea de defensa para la seguridad de una aplicación. Analizaremos algunas metodologías del modelado de amenazas mencionando sus características y haciendo una comparación de sus características ya que varios tienen diferentes énfasis y veremos que metodologías tienen cosas en común.

METODOLOGIAS

➢ CORAS (CONSULTATIVE OBJECTIVE RISK ANALYSIS SYSTEM).

Es un Proyecto desarrollado por SINTEF el cual fue financiado por la Unión europea con la finalidad de proporcionar un framework para aquellos sistemas donde la seguridad es crítica con el objetivo de facilitar los descubrimientos de las vulnerabilidades de los sistemas, inconsistencias y redundancias, en otras palabras, es un método de análisis de riesgos cuyo resultado es un diagrama.

CORAS se basa en tres componentes para realizar un análisis de riesgos en los sistemas proporcionando un método basado en modelos:

- ✓ Un Lenguaje de Modelado de riesgos basados en el Lenguaje UML
- ✓ La metodología CORAS que consiste en describir los pasos de todo el análisis de los procesos de las actividades con el fin de construir diagramas CORAS. Esta metodología hace un enorme uso de los diagramas.
- ✓ Una Herramienta para documentar y crear informes de todo el análisis y procesos de la metodología CORAS

Los siete pasos para trabajar con la metodología CORAS basado en entrevistas con los expertos son:

1. **Análisis de alto nivel:** en el cual se recopila la información mediante entrevistas y otros datos de recopilación para así analizar y documentar la información obtenida, con el fin de identificar las amenazas, vulnerabilidades, escenarios de los posibles ataques que pueda tener una organización.
2. **Aprobación:** En esta sección se describen a detalle los objetivos, los alcances o límites de la metodología para presentarlo a la dirección más alta de la organización para así desarrollar el análisis de riesgos de la forma eficaz y eficiente.
3. **Identificación de riesgos:** Se identifican todos los riesgos, amenazas, posibles escenarios a la que puede estar expuesta la organización
4. **Estimación de riesgos:** Se identifica y se documenta el impacto generado por un ataque y las probabilidades de los incidentes identificados en los anteriores pasos.
5. **Evaluación del riesgo:** Se documenta toda la evaluación con respecto a los riesgos que se puedan identificar para su ajuste fino y correcciones.

6. **Tratamiento del riesgo:** las medidas que se realizaran a los riesgos identificados, se identifican las salvaguardas que se necesitaran para el apaleamiento de las amenazas.

Tipos de Diagramas de CORAS.

1. **Diagrama superficial de activos:** Este tipo de diagramas muestra una visión general de los daños que pueden tener los activos, y como estos pueden afectar a otros.
2. **Diagrama de amenazas:** Muestra una visión general de todo el proceso inicial de una amenaza todos los eventos secuenciales que este podría generar hasta las consecuencias que tienen sobre los activos.
3. **Diagrama superficial de riesgo:** Este diagrama nos muestra las amenazas y todo tipo de riesgos que podrían suscitarse. Al riesgo se le asigna un valor
4. **Diagrama de tratamiento:** muestra las soluciones y contramedidas propuestas de manera general para tratar los riesgos
5. **Diagrama superficial del tratamiento:** Es un resumen donde se añaden los escenarios posibles y las relaciones de los elementos propuesto en el tratamiento del riesgo.

➢ CIGITAL'S ARCHITECTURAL RISK ANALYSIS PROCESS.

Es un framework de modelado de amenazas creado por la empresa CIGITAL que es una empresa dedicada al software, cuyo framework tiene como propósito realizar un análisis de gestión de riesgos en una arquitectura de un software, identificando las fallas y los riesgos en los que están expuestos los activos, priorizando los mismos según el impacto que los riesgos ocasionan. Este método consta de cuatro procesos:

1. **Identificación de activos**: en este proceso se identifican los activos más importantes con lo que cuenta la organización.
2. **Análisis de riesgos:** Se identifican las amenazas y los riesgos a los que se esta expuesto para su debido análisis.
3. **Mitigación de riesgos:** En este proceso se analizan los mecanismos y salvaguardas necesarios para mitigar los riesgos y amenazas identificadas.
4. **Gestión y medición de riesgos:** Medición del impacto y probabilidades de las amenazas y riesgos.

➢ OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)

Desarrollado en la Universidad de Carnegie Mellon es un método de planificación y evaluación cuyo objetivo es evaluar los riesgos de una organización, identificando y administrando los riesgos de seguridad de la información, esta metodología define un método de evaluación integran para identificar los activos que son importantes para el cumplimiento de los objetivos de la organización, las amenazas a esos activos, y las vulnerabilidades a los que pueden estar expuestos los activos a las amenazas.

OCTAVE consiste en tres fases:

- ✓ Evaluación Organizacional: consiste en la Creación de perfiles de amenazas basadas en los activos.
- ✓ Evaluación de la Infraestructura de la Información: consiste en la identificación de las vulnerabilidades o fallos de infraestructura
- ✓ Evaluación de Riegos: consiste en desarrollar y planificar estrategias de seguridad con respecto a los activos críticos de la empresa con el fin de brindar la documentación necesaria para la toma de decisiones.

OCTAVE divide los activos en dos tipos:

- ✓ Sistemas (Hardware, Software y Datos)
- ✓ Personas

OCTAVE se considera una de las metodologías mas completas ya que involucra elementos y procesos completos en cuanto al análisis de la información: Activos, amenazas, vulnerabilidades, los recursos con que cuenta la organización y las salvaguardas para la mitigación de los riesgos.

➢ PTA TECHNOLOGIES CALCULATIVE THREAT MODELING METHODOLOGY (CTMM).

Metodología creada propiamente por la empresa PTA Technologies con el nombre PTA CTMM (Calculative Threat Modeling Methodology) cuya finalidad es de permitir la constante actualización de las amenazas que van apareciendo en el transcurso del tiempo, esta metodología se basa en calcular el nivel riesgo y las respectivas contramedidas y tratamiento de manera de que se realicen de manera automática en función de los activos.

El analista debe conocer y documentarse en primer lugar con la aplicación o sistema a evaluar recopilando toda información que le fuera útil ya que se pueden presentar distintos escenarios y dependiendo de la información obtenida se decide lo que se va a modelar (Descripción funcional del sistema con sus respectivos diagramas de arquitectura del software con su respectiva documentación e informes y un diccionario de términos con el fin de dar significado a los vocablos utilizados en el documento).

Los pasos que propone esta metodología del CTMM

1. Identificación de los activos, determinando cuales activos son los de mayor valor para protegerlos antes los riesgos y no sufrir daños críticos, es necesario determinar prioridades.
2. Identificación de las vulnerabilidades, determinar las vulnerabilidades a las que pueden estar expuestos los activos.
3. Definición de las Salvaguardas, se establecen los tratamientos y las contramedidas en función a las vulnerabilidades y del coste o presupuesto que estas generarían al aplicarlas.
4. Creación de escenarios de las posibles amenazas y planes de mitigación, primero es identificar los distintos elementos de las amenazas y sus diferentes parámetros mediante una descripción breve del escenario, identificar en primer lugar las amenazas que puedan afectar los activos y su nivel de riesgo.

La herramienta que acompaña la metodología PTA permite el uso de las etiquetas para poder distinguir las áreas, elementos de la arquitectura del sistema para una mejor comprensión y distinción de ellos.

- ## TRIKE. METODOLOGÍA DE EVALUACIÓN DE AMENAZAS.

Es un framework de modelado de amenazas, es un marco de trabajo conceptual que aportan a la comunidad Open Source una metodología y una herramienta eficaz que facilita el proceso para el modelado, este modelo permite crear un sistema robusto para la toma de decisiones ya la metodología permite al analista describir de forma completa todas las características de seguridad con la que cuenta un sistema en todos los niveles desde su iniciación con respecto al diseño y arquitectura hasta su finalización de lo que es la

implementación. Cabe mencionar que Trike viene siendo una alternativa a STRIDE que es un modelo para clasificación de amenazas como Spoofing, Ataques DOS, Repudio, Revelación de información entre otros y DREAD es un modelo que nos permite realizar una valoración o puntuación del daño potencial que puede ser generada por una vulnerabilidad si esta fuese a ser atacada, valoración o puntuación de cuantos usuarios han sido afectados, valoración o puntuación de la facilidad de descubrimiento de la vulnerabilidad, y estas tanto DREAD como STRIDE son metodologías propuestas por Microsoft.

El objetivo de TRIKE es automatizar todos los procesos repetitivos del modelado de amenazas, apoyando al analista para que este solo tenga que hacer el respectivo análisis del sistema a evaluar. Lo que diferencia la metodología Trike con STRIDE Y DREAD es que con Trike utiliza un enfoque basado en los riesgos con implementación con sus respectivos modelados de amenazas y los distintos riesgos, y los otros dos utilizan un modelado de amenazas mixto (Ataques, Amenazas, Debilidades) además que se puede distinguir por los niveles altos de automatización la perspectiva defensiva del sistema y el grado de formalismo presentado en la metodología.

Herramientas que utiliza Trike:

- ✓ Spreadsheet
- ✓ Standalone Tool

➢ TAM (Microsoft Threat Analysis And Modeling).

Es una Herramienta creada por Microsoft lo cual es un elemento básico del Ciclo de vida del desarrollo de seguridad (SDL) lo cual permite a los analistas de sistemas a identificar las amenazas y mitigar el impacto de los problemas de seguridad en una fase temprana. Es una herramienta que fue diseñada de forma práctica para que sea de fácil utilización para toda persona entre las características más destacables que posee esta herramienta tenemos:

- ✓ Creación de modelos básicos mediante asistente, que ayudara al usuario la creación del modelado de forma fácil.
- ✓ Posee una biblioteca de ataques por defecto con su respectiva guía, conceptos y hasta las contramedidas necesarias tipo guía descriptiva.
- ✓ Cuenta con navegación usando el componente treeview
- ✓ Generación de informes y estadísticas

- ✓ Tutoriales en video
- ✓ Cuenta con un sistema de medición de riesgos

Con la herramienta cualquier analista podrá:

- ✓ Comunicar el diseño de seguridad de cualquier sistema en la cual se está trabajando.
- ✓ Analizar el diseño de todas las posibles amenazas y problemas de seguridad.
- ✓ Sugerir y administración mitigaciones de los problemas de seguridad que se pueden encontrar en las aplicaciones.

La herramienta TAM se utiliza más que todo con el fin de identificar las amenazas en las que esta expuestas todos los sistemas de información y aplicaciones en todo el proceso de desarrollo desde su diseño hasta en su implementación y lo cual esta metodología o herramienta cuenta con los siguientes pasos:

1. Identificar los objetivos de seguridad e identificar los activos
2. Crear una descripción general de la arquitectura de la aplicación
3. Descomponer la aplicación
4. Identificar las amenazas
5. Identificar las vulnerabilidades
6. Documentar las amenazas
7. Asignar prioridades a las amenazas

➢ PASTA (Process For Attack Simulation And Threat Analysis).

Es una metodología basada en la gestión del riesgo que considera cuyo objetivo es alinear los objetivos del negocio con los requerimientos técnicos para identificar las prioridades para poder realizar la mitigación de riesgos.

PASTA es un proceso que consiste en una simulación de ataques y análisis de amenazas, con esto esta metodología crea una imagen completa de las amenazas y las vulnerabilidades posibles que puedan existir en las aplicaciones simulando en estar en la piel de un atacante y ver desde su perspectiva y combina los resultados con el análisis de riesgo, con los resultados obtenidos se informan las decisiones sobre el riesgo y las principales correcciones.

La metodología PASTA consta de siete pasos centradas en el riesgo el cual es un proceso dinámico para la clasificación, enumeración, clasificación y gestión de amenazas.

1. Definir los objetivos: En este paso se debe identificar y definir cuáles son los objetivos del negocio o de la organización, definir sus prioridades, comprender hasta los objetivos y finalidades de sus productos o aplicaciones.
2. Definir el alcance: En esta etapa se identifica el alcance que pueden tener los activos y los componentes de estos, comprendiendo la superficie del ataque y crear una imagen de lo que se quiere proteger, identificar como está configurado las aplicaciones, que aplicaciones tienen dependencia de otras de manera interna y donde y como se utilizan las aplicaciones de terceros.
3. Observar la descompensación de la aplicación: En esta etapa se debe factorizar la aplicación e identificar los controles de la aplicación, se debe mapear las relaciones que existen entre los componentes, identificar los roles y los permisos de accesos a los usuarios para no tener problemas de seguridad con respecto a la autenticación, identificar los activos, comprender los controles de aplicación que protegen todos los procesos y transacciones de la aplicación.
4. Análisis de amenazas: En este paso se identifican todas las amenazas
5. Identificación de Vulnerabilidades: Se identifican todas las debilidades y vulnerabilidades dentro del diseño y código de las aplicaciones a analizar o evaluar.
6. Simulación de Ataques: En esta etapa se simula en realizar ataques para poder explotar vulnerabilidades o fallos que pueda tener una aplicación determinando la viabilidad de las amenazas por medio de los patrones de ataque.
7. Análisis de Riesgos: En la última etapa se analizan los riesgos, debilidades y vulnerabilidades que se hayan encontrado en las etapas anteriores y se centra en la mitigación y la corrección de ello.

CUADRO COMPARATIVO

METODO	TIPO DE MODELADO	HERRAMIENTAS	CONOCIMIENTO INTERNO	ORIENTACION
CORAS	Análisis de Riesgos	Gestión de Casos Lenguaje Grafico UML Editor Grafico CORAS	Conocimiento basado en Diagramas	Contribuir a la reducción de riesgos y la adopción de unas correctas contramedidas
CIGITAL	Análisis de Riesgos arquitectónico	Editor de Diagramas	Conocimiento basado en Diagramas	Identificar las fallas y los riesgos en los que están expuestos los activos, mitigación de los riesgos y medición del impacto y probabilidades
OCTAVE	Evaluación y Gestión de Riesgos		Conocimiento en recopilación de la información de la organización (Activos, Amenazas, Vulnerabilidades a las que esta expuestos los activos)	Planificación y Evaluación de riesgos de una organización
PTA	Evaluación de Riesgos de Amenazas	La herramienta que acompaña la		Evaluar los riesgos operativos y de seguridad en sus sistemas y

		metodología PTA permite el uso de las etiquetas PTA Professional Edition		a crear una política de mitigación de riesgos adecuada
TRIKE	Enfoque basado en riesgos	Spreadsheet Standalone Tool	Capacidad de distinguir los niveles altos de automatización de la perspectiva defensiva del sistema	Ayudar al Analista a describir de forma completa y precisa todas las características de seguridad en un sistema.
TAM	Análisis y modelado de Amenazas	Microsoft Tam v2	Conocimientos básicos ya que la herramienta de forma automatizada ayuda al analista a crear un modelado de amenazas con solo seguir el asistente.	Identificar las amenazas y mitigar el impacto de los problemas de seguridad en una fase temprana
PASTA	Gestión del Riesgo		Los 7 pasos centradas en el riesgo	Guiar a los Analistas, modeladores de amenazas a través de actividades de modelado de amenazas de aplicaciones centradas en el riesgo. Un proceso estratégico para mitigar los riesgos.

PROPUESTA DE UNA NUEVA METODOLOGÍA DE AMENAZAS

La nueva metodología es con un enfoque a la gestión de riesgos con el propósito identificar los activos, riesgos, amenazas y vulnerabilidades, estudiar a profundidad los riesgos que se identifican mediante pasos específicos, evaluar los riesgos que se han identificado y analizado y sacar mediciones de la severidad o el impacto del riesgo, tanto su probabilidad de ocurrencia, probabilidad de detección y el nivel de riesgo o criticidad y capacidad de poder controlar los riesgos mediante la acción de controles, políticas, asignando responsables y por ultimo dar el seguimiento debido a los riesgos y amenazas.

Fases de la Metodología:

1. Identificación de activos
2. Identificación de riesgos, vulnerabilidades y amenazas
3. Estudio detallado de riesgos, vulnerabilidades y amenazas
    - Determinar probabilidad
    - Determinar consecuencias
4. Evaluación del riesgo, vulnerabilidades y amenazas
    - Índice de Impacto
    - Probabilidad de Ocurrencia
    - Probabilidad de Detección
5. Control y Mitigación del riesgo, vulnerabilidades y amenazas
6. Seguimiento de riesgos, vulnerabilidades y amenazas

CONCLUSIONES

El modelado de amenazas es un proceso estructurado en la cual se planifica y optimiza la seguridad de los sistemas, aplicaciones, redes, identificando los riesgos, amenazas, vulnerabilidades, y realizar su debido análisis del impacto y las probabilidades de cada riesgo o amenaza encontrada, como así también priorizar las recomendaciones debidas para la mitigación de ataques con el fin de proteger los activos y recursos. El seguimiento de una metodología por parte de los Analistas o un modelador de amenazas es un factor clave para mejorar la seguridad de una aplicación o un sistema, red.

Es de gran importancia que cada organización o empresa implemente una metodología para la gestión y análisis de riesgos asociados en todos los procesos y actividades que se realicen en el interior para identificar, evaluar y mitigar los riesgos y vulnerabilidades.

REFERENCIAS

- ✓ *Análisis y Modelado de Amenazas—PDF Descargar libre*. (s. f.). Recuperado 9 de noviembre de 2021, de https://docplayer.es/2030391-Analisis-y-modelado-de-amenazas.html

- ✓ ¿Qué es el modelado de amenazas? Ejemplos. (s. f.). *Ciberseguridad*. Recuperado 9 de noviembre de 2021, de https://ciberseguridad.com/herramientas/modelado-amenazas-ejemplos/

- ✓ *Architectural Risk Analysis | CISA*. (s. f.). Recuperado 9 de noviembre de 2021, de https://1-us--cert-cisa-gov.translate.goog/bsi/articles/best-practices/architectural-risk-analysis/architectural-risk-analysis?_x_tr_enc=1&_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=nui,sc
- ✓ Mogollón, A. (s. f.). *Análisis Comparativo: Metodologías de análisis de Riesgos*. 9.