

TÍTULO:

Trabajo: Metodologías de modelado de amenazas

ALUMNO:

Felipe Trejo Garcia


MATERIA:

Seguridad en el Software

PROFESOR:

M.G.T.I. OMAR URIEL DOMINGUEZ MENDOZA

FECHA: 14/Dic/2020



Contenido

Caso Teórico:	3
Introducción al Modelado de Amenazas.....	3
Estudio de metodologías existentes.	14
Descripción de una metodología en profundidad.	20
Caso Práctico	25
Ejercicio práctico de modelado de amenazas, utilizando una herramienta de modelado	25
Objetivo:	25
Realización de diagrama DFD.....	25
Valoración de amenazas, método DREAD.....	27
Calificación de amenazas.....	28
Conclusiones.....	31
Referencias bibliográficas	32

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Caso Teórico:

Introducción al Modelado de Amenazas.

El modelado de amenazas es una técnica eficaz para ayudar a proteger sistemas, aplicaciones, redes y servicios. Ayuda a identificar amenazas potenciales y estrategias de reducción de riesgos en una etapa temprana del ciclo de vida del desarrollo.

El modelado de amenazas utiliza un diagrama de flujo de datos que muestra gráficamente cómo funciona el sistema. Luego aplica un marco de trabajo para ayudarlo a encontrar y solucionar problemas de seguridad.

Los sistemas lanzados sin haber sido previamente modelados por amenazas ponen en riesgo tanto a clientes como organización.

Cuando usar el modelado de amenazas

Utilice el modelado de amenazas siempre que diseñe nuevos sistemas o actualice los existentes. Ejemplos incluyen:

- » Crear un nuevo microservicio de Azure que informe sobre el uso de recursos en la nube de su organización con fines presupuestarios
- » Diseñar una API pública para proporcionar a los clientes acceso a sus datos
- » Agregar una nueva función a una aplicación existente

Quién puede usar modelado de amenazas

Cualquiera con un conocimiento práctico del sistema y un conocimiento básico de seguridad puede trabajar con el modelado de amenazas. Esta técnica se puede aplicar en cualquier:

- » Metodología de software (por ejemplo, Agile o Waterfall)
- » Periodo de implementación (por hora, mensual, anual)

Fases del modelado de amenazas

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

El modelado de amenazas es una técnica utilizada por cualquier persona que sepa cómo funciona su sistema y tenga un conocimiento práctico de la seguridad de la información.

La técnica se divide en cuatro fases diferentes, cada una de las cuales contiene pasos importantes para ayudarlo a crear un diagrama de flujo de datos y analizarlo en busca de posibles amenazas.



Fase	Título	Descripción
1	Diseño	Capturar todos los requisitos del sistema y crear un diagrama de flujo de datos.
2	Interrupción	Aplicar un marco de modelado de amenazas al diagrama de flujo de datos y buscar posibles problemas de seguridad.
3	Corrección	Decidir cómo abordar cada problema con la combinación correcta de controles de seguridad.
4	Verificación	Comprobar que se cumplen los requisitos, se detectan los problemas y se implementan los controles de seguridad.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Paso 1: Diseño

La fase de diseño es la base de las actividades de modelado de amenazas. Recopilará tantos datos como sea posible sobre lo que va a crear y lo que usa para crearlo.

Objetivos

- » Desarrollar una imagen clara de cómo funciona el sistema
- » Enumerar todos los servicios utilizados por el sistema
- » Enumerar todas las suposiciones sobre el entorno y las configuraciones de seguridad predeterminadas
- » Crear un diagrama de flujo de datos con el nivel de profundidad del contexto adecuado

Formulación de preguntas sobre el sistema

Es necesario formular tantas preguntas sobre el sistema como sea posible. Estas son algunas preguntas a tener en cuenta:

Área	Preguntas
Descripción del sistema	¿Qué hace el sistema? ¿Cuáles son los procesos empresariales que controla el servicio? ¿Están claramente definidos?
Entorno del sistema	¿El sistema se creará en la nube o de forma local? ¿En qué sistema operativo se creará? ¿Se usarán contenedores? ¿El sistema es una aplicación, un servicio o algo totalmente diferente?
Escenarios	¿Cómo se usará el sistema? ¿Cómo no se usará?
Permisos	¿El sistema tiene requisitos de acceso de hardware, datos o ejecución de scripts? Si es así, ¿qué son?
Proveedor de servicios en la nube	¿Qué proveedor de servicios en la nube usará el sistema? ¿Qué opciones de configuración de seguridad predeterminadas proporciona? ¿Cómo afectan estas opciones a los requisitos de seguridad del sistema?
Sistema operativo	¿Qué sistema operativo usará el sistema? ¿Qué opciones de configuración de seguridad predeterminadas ofrece? ¿Cómo afectan estas opciones a los requisitos de seguridad del sistema?

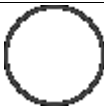


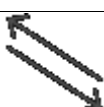

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Área	Preguntas
Propios y de terceros	¿Qué servicios de primera y tercera parte usará el sistema? ¿Qué opciones de configuración de seguridad predeterminadas ofrecen? ¿Cómo afectan estas opciones a los requisitos de seguridad del sistema?
Cuentas	¿Cuáles son los tipos de cuenta que se utilizarán en el sistema, como usuarios y administradores? ¿Estas cuentas serán locales o estarán habilitadas para la nube? ¿Qué acceso necesitan y por qué?
Control de acceso e identidad	¿Cómo ayudará el sistema a proteger esas cuentas? ¿Se basará en Azure Active Directory (Azure AD)? ¿Usará características como las listas de control de acceso (ACL), Multi-Factor Authentication (MFA) y el control de sesión?
Tokens y sesiones	¿El sistema procesará solicitudes como SOAP o API REST? ¿Cómo tratará las distintas sesiones?
Desvío	¿El sistema usará o requerirá puertas traseras? Si es así, ¿cómo funcionará?
Registro, supervisión y copias de seguridad	¿Cuáles son los mecanismos que usa el sistema para registrar eventos de seguridad, supervisar anomalías y realizar copias de seguridad de los datos del sistema? ¿Qué tipos de eventos capturará?
Red	¿Cuáles son todos los sistemas de protección y detección de intrusiones que se usarán? ¿Cómo se cifrará la comunicación?
Datos	¿Qué tipo de datos creará o controlará el sistema? ¿Cuál será el tipo de clasificación de los datos? ¿Cómo confiará el sistema en los orígenes de datos? ¿Cómo analizará los datos? ¿Cuál será el comportamiento de entrada y salida esperado? ¿Cómo se controlará la validación? ¿Cómo se cifrarán los datos en todos los estados?
Administración de secretos	¿Cómo controlará el sistema las claves, los certificados y las credenciales?

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Elementos de diagrama

Un diagrama de flujo de datos muestra el flujo de datos en un sistema determinado. Normalmente, comienza con solicitudes de usuarios o almacenes de datos, y finaliza con almacenes de datos o servicios de análisis. El diagrama de flujo de datos utiliza formas distintas para indicar los elementos que representan.

Elemento	Forma	Definición
Proceso		Tarea que recibe, modifica o redirige la entrada a la salida, como un servicio web.
Almacén de datos		Almacenamiento de datos permanente y temporal, como una caché web y bases de datos administradas por Azure.
Entidad externa		Una tarea, una entidad o un almacén de datos fuera de su control directo, como los usuarios y las API de terceros.
Flujo de datos		Movimiento de datos entre procesos, almacenes de datos y entidades externas, como cadenas de conexión y cargas.
Límite de confianza		Cambios en la zona de confianza a medida que los datos fluyen a través del sistema, como los usuarios que usan Internet para acceder a una red corporativa protegida.

Los elementos del diagrama de flujo de datos también necesitan contexto para ayudar a cualquiera a entender cómo se usan y protegen en el sistema.

Información que se debe incluir en el diagrama de flujo de datos

La cantidad de información que se va a incluir en el diagrama de flujo de datos depende de algunos factores clave:

Factor	Explicación
Tipo de sistema que va a crear	Puede que los sistemas que no controlan datos confidenciales o que se usan internamente no necesiten tanto contexto como un sistema orientado externamente.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Factor	Explicación
Contexto requerido del equipo de seguridad	Los equipos de seguridad son precisos con lo que buscan en los modelos de amenazas. Hable con su equipo de seguridad para confirmar la capa de profundidad requerida.

Si no se incluye el contexto correcto, se producen revisiones de seguridad incompletas y sistemas potencialmente vulnerables.

Capas del diagrama

Para ayudarle a comprender la cantidad de información que se debe incluir, elija entre estas cuatro capas de profundidad de contexto:

Capa de profundidad	Título	Descripción
0	Sistema	Punto de partida para cualquier sistema. El diagrama de flujo de datos contiene los elementos principales del sistema con suficiente contexto para ayudarle a comprender cómo funcionan e interactúan entre sí.
1	Proceso	Enfocarse en los diagramas de flujo de datos de cada parte del sistema mediante diagramas de flujo de datos adicionales. Se usa para cada sistema, especialmente si controla datos confidenciales. El contexto en esta capa debe ayudarle a identificar las amenazas, así como las formas de reducir o eliminar los riesgos de forma más eficaz.
2	Subproceso	Enfocarse en los diagramas de flujo de datos para cada subparte de una parte del sistema. Se usa para sistemas que se consideran críticos. Algunos ejemplos son los sistemas para entornos seguros, los que controlan datos altamente confidenciales o los que contienen una clasificación de alto riesgo.
3	Nivel inferior	Enfocarse en los sistemas muy críticos y de nivel de kernel. Los diagramas de flujo de datos describen cada subproceso hasta el último detalle.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Paso 2: Interrupción

La fase de interrupción es donde se usa el diagrama de flujo de datos para buscar posibles amenazas contra el sistema. El proceso utiliza un marco de modelado de amenazas para ayudarle a buscar las amenazas más comunes y las formas de protegerse ante ellas.

Objetivos

- » Elegir entre los enfoques centrados en la "protección del sistema" o la "comprensión del atacante"
- » Usar el marco STRIDE para identificar amenazas comunes (descrito más adelante)

Limitación del enfoque

Comience por elegir si quiere buscar maneras de proteger el sistema o recopilar tanta información como pueda sobre un atacante y sus motivos. Algunos ejemplos son los siguientes:

Foco	Ejemplo de lo que puede encontrar
Sistema	Encuentra un problema con una conexión sin cifrar entre el usuario y el sistema.
Atacante	Obtiene más información sobre los medios, la motivación y las formas de proteger los puntos de entrada del sistema.
Recursos	Identifica los recursos críticos en función de aspectos como la administración de datos clasificados y se centra en la protección de esos recursos.

Selección de un marco de amenazas

A continuación, seleccione un marco para ayudar a generar posibles amenazas en el sistema. Microsoft suele usar STRIDE, un acrónimo de las seis categorías de amenazas principales para proporcionar una lista de amenazas completa pero no exhaustiva.

El marco le ayuda a formular algunas preguntas importantes acerca del sistema:

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Amenaza	Definición	Pregunta	Ejemplo de amenaza
Suplantación	El atacante quiere hacerse pasar por alguien o algo	¿Se autentican ambos lados de la comunicación?	Se envía un correo electrónico a los usuarios desde una cuenta que parezca legítima con vínculos malintencionados y datos adjuntos para capturar sus credenciales, sus datos y el acceso al dispositivo.
Manipulación	El atacante cambia los datos sin autorización	¿Cómo puedo saber que alguien no puede cambiar los datos en tránsito, en uso o en reposo?	Modificación de la memoria mediante un control débil de llamadas API para producir bloqueos y revelar mensajes de error confidenciales.
Rechazo	El atacante dice que no ha hecho nada	¿Se puede asociar cada acción a una identidad?	Notificación de que no se han eliminado registros de base de datos.
Divulgación de información	El atacante ve datos que no debería ver	¿Cómo puedo saber que alguien no puede ver los datos en tránsito, en uso o en reposo?	Acceso a documentos y carpetas no autorizados con controles de seguridad débiles.
Denegación de servicio	El atacante pone el sistema fuera de servicio	¿Hay áreas en el sistema donde el recurso está limitado?	Desbordamiento de la red con solicitudes.
Elevación de privilegios	El atacante tiene acceso no autorizado a los datos	¿Cómo sabe que alguien puede realizar esta acción?	Extracción de datos mediante el aprovechamiento de puntos débiles de la memoria o la lógica de control de entrada.

Paso 3: Corrección

La fase de corrección es aquella en la que se decide el destino de todas las amenazas. Cada amenaza STRIDE se asigna a uno o varios controles de seguridad, que ofrecen diferentes funciones y tipos entre los que elegir.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Objetivos

- » Medir cada amenaza con un marco de priorización o una barra de errores de seguridad
- » Realizar un seguimiento de cada amenaza como una tarea o un elemento de trabajo en un servicio de administración de errores
- » Generar recomendaciones de control de seguridad que se asignan a las amenazas STRIDE
- » Seleccionar uno o varios tipos y funciones de control de seguridad para abordar cada amenaza
- » Resolver tareas

Configuración de un flujo de trabajo de seguimiento de amenazas

Clasificación por orden de prioridad de las amenazas

Para empezar, mida cada amenaza con un marco de priorización o una barra de errores de seguridad. Este proceso le ayuda a organizar los recursos para solucionar los problemas que la organización considere más importantes.

El proceso utiliza tres variables clave:

Variable Descripción

Impacto	Usa categorías de STRIDE para asignar el impacto.	▪
Gravedad	Usa la barra de errores interna o el marco de priorización para asignar la gravedad mediante los peores casos posibles.	▪
Riesgo	Usa un cálculo de la eficacia del control de seguridad y el costo de implementación.	▪

Creación de tareas

Después, agregue cada amenaza a una solución de administración de errores como Azure DevOps Services. Algunas de las ventajas son las siguientes:

- » Refuerza la propiedad del problema
- » Realiza un seguimiento del historial de forma eficaz

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

- » Le ofrece la posibilidad de usar plantillas estandarizadas para los ejercicios de prioridad y resolución

Valoración de la efectividad y el costo de las amenazas

Visite cada recomendación de control de seguridad asignada a las amenazas STRIDE. Anote las que sean más eficaces y menos costosas de implementar. Estos son algunos ejemplos:

Amenaza	Control de seguridad	Ejemplo de control de seguridad
Suplantación	Autenticación	Envío y recepción de mensajes firmados con firmas digitales para autenticar el origen y garantizar la integridad de los mensajes.
Manipulación	Integridad	Validación de la entrada para evitar el procesamiento de cargas malintencionadas y el control inadecuado de un comportamiento inesperado.
Rechazo	Sin rechazo	Creación y protección de los registros de seguridad que contienen acciones de los usuarios y marcas de tiempo.
Divulgación de información	Confidencialidad	Aplicación de listas de control de acceso para garantizar que los usuarios adecuados puedan acceder a los datos correctos.
Denegación de servicio	Disponibilidad	Uso de recursos elásticos para administrar el uso creciente o decreciente.
Elevación de privilegios	Autorización	Ejecución del servicio con la mínima cantidad de acceso posible.

Adición de detalles de control de seguridad a cada problema

Agregue los detalles a cada problema en la solución de administración de errores y, después, resuelva cada uno de ellos siguiendo una de las soluciones siguientes. Variarán ligeramente entre organizaciones:

Resolución	Descripción
Reducción	El problema se solucionará con correcciones de errores o un cambio de diseño para reducir o eliminar el impacto de la amenaza, así como su gravedad.
Transferencia	Otro sistema o equipo controlará el problema.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Resolución	Descripción
Evasión	Se eliminará el elemento del sistema que contiene el problema.
Aceptación	El riesgo se aceptará sin una solución. Esto requerirá la aprobación de un responsable de toma de decisiones de riesgo autorizado, que puede basarse en la gravedad de la amenaza. Las amenazas de gravedad crítica pueden requerir la aprobación del liderazgo senior, mientras que un riesgo de defensa en profundidad puede ser aprobado por un ingeniero senior. Hable con el equipo para obtener instrucciones estratégicas.

Paso 4: Verificación

La fase de verificación es el último paso del proceso de modelado de amenazas y suele tener lugar antes de implementar el sistema. Implica asegurarse de que se cumplen los requisitos, se validan las suposiciones y se implementan los controles de seguridad.

Objetivos

- » Confirmar que se cumplen todos los requisitos de seguridad nuevos y anteriores para el sistema
- » Configurar el proveedor de servicios en la nube, el sistema operativo y los componentes para cumplir los requisitos de seguridad
- » Asegurarse de que todos los problemas se abordan con los controles de seguridad adecuados
- » Realizar una verificación manual y automatizada del sistema antes de la implementación

Comprobación de los requisitos y establecimiento de valores predeterminados

Para empezar, compruebe que se cumplan todos los requisitos creados en la primera fase.

Ejemplos:

- » Planes de seguridad de red
- » Implementación de la solución de administración de secretos
- » Sistemas de registro y supervisión

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

- » Controles de identidad y acceso

Después, asegúrese de que los valores de configuración predeterminados de los proveedores de servicios en la nube, los sistemas operativos y los componentes se han modificado para cumplir todos los requisitos de seguridad.

Ejemplos:

- » Habilitar el cifrado de datos transparente de Azure SQL Database para proteger los datos en disco
- » Usar el control de acceso basado en roles (RBAC) para asignar permisos a los usuarios, los grupos y las aplicaciones
- » Habilitar el Firewall de Windows en todos los perfiles

Deben resolverse todos los problemas registrados en la solución de administración de errores y deben verificarse todas las correcciones.

Ejecución de la verificación

La última parte implica la ejecución de la verificación manual y automatizada. En Microsoft, los sistemas están sujetos a un proceso de verificación antes de la implementación, que puede constar de escáneres automatizados, revisiones de código y pruebas de penetración. El proceso se puede aplicar antes de cada implementación o en intervalos de tiempo, como cada 6 o 12 meses.

Si responde afirmativamente a cualquiera de las preguntas siguientes, es posible que le interesen ritmos de verificación más rápidos:

- » ¿El sistema se utilizará externamente?
- » ¿Controla datos confidenciales?
- » ¿Tengo que cumplir normativas?
- » ¿Mi organización requiere procesos de seguridad adicionales, como implicaciones de privacidad, riesgo operativo o requisitos de desarrollo?

Estudio de metodologías existentes.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

STRIDE y derivaciones asociadas

Inventado en 1999 y adoptado por Microsoft en 2002, STRIDE es actualmente el método de modelado de amenazas más maduro. STRIDE ha evolucionado con el tiempo para incluir nuevas tablas específicas de amenazas y las variantes STRIDE-per-Element y STRIDE-per-Interaction.

STRIDE evalúa el diseño detallado del sistema. Modela el sistema in situ. Al construir diagramas de flujo de datos (DFD), STRIDE se utiliza para identificar entidades del sistema, eventos y los límites del sistema. STRIDE aplica un conjunto general de amenazas conocidas en función de su nombre, que es un mnemónico, como se muestra en la siguiente tabla:

	Amenaza	Propiedad violada	Definición de la amenaza
S	Identidad de Suplantación	Autenticación	Pretender ser alguien o algo distinto a ti mismo
T	Manipulación de datos	Integridad	Modificando algo en el disco, memoria, u otra parte
R	Repudio	No-repudio	Alegando que no hizo algo o no fue responsable; puede ser honesto o falso
I	divulgación de información	Confidencialidad	Proporcionar información a alguien no autorizado para acceder a ella
D	Negación de servicio	Disponibilidad	Agotar los recursos necesarios para brindar el servicio
E	Elevación de privilegio	Autorización	Permitir a alguien hacer algo que no está autorizado para hacer

STRIDE se ha aplicado con éxito a sistemas ciber físicos y cibernéticos. Aunque Microsoft ya no mantiene STRIDE, se implementa como parte del ciclo de vida de desarrollo de seguridad de Microsoft (SDL) con la herramienta de modelado de amenazas, que todavía está disponible. Microsoft también desarrolló un método similar llamado DREAD, que también es un mnemónico (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) con un enfoque diferente para evaluar las amenazas.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

PASTA

El Proceso de Simulación de Ataques y Análisis de Amenazas (PASTA) es un marco de modelado de amenazas centrado en el riesgo desarrollado en 2012. Contiene siete etapas, cada una con múltiples actividades, que se ilustran en la Figura a continuación:

1-Definir Objetivos	<ul style="list-style-type: none"> • Identificar los objetivos comerciales • Identificar los requisitos de seguridad y cumplimiento • Análisis de Impacto del Negocio
2-Definir el alcance técnico	<ul style="list-style-type: none"> • Capture los límites del entorno técnico • Capture las dependencias de infraestructura / aplicación / dependencia de software
3-Descomposición de la aplicación	<ul style="list-style-type: none"> • Identificar casos de uso / definir puntos de entrada de aplicaciones y niveles de confianza • Identificar actores / activos / servicios / roles / fuentes de datos • Diagrama de flujo de datos (DFD) / límites de confianza
4-Análisis de Amenazas	<ul style="list-style-type: none"> • Análisis de escenarios probabilísticos de ataques • Análisis de regresión sobre eventos de seguridad • Correlación y análisis de la inteligencia de amenazas
5-Análisis de vulnerabilidades y debilidades	<ul style="list-style-type: none"> • Consultas de informes de vulnerabilidad existentes y seguimiento de problemas • Amenaza al mapeo de vulnerabilidades existente utilizando árboles de amenazas • Diseñar análisis de fallas usando casos de uso y abuso • Enumeraciones de puntajes (CVSS / CWSS) (CWE / CVE)
6-Modelado de ataque	<ul style="list-style-type: none"> • Análisis de superficie de ataque • Attack tree development / Attack library Mgt. • Ataque a la vulnerabilidad y análisis de exploits utilizando árboles de ataque
7- Análisis de riesgo e impacto	<ul style="list-style-type: none"> • Calificar y cuantificar el impacto empresarial • Identificación de contramedidas y análisis de riesgo residual • Estrategias de mitigación de riesgos de identificación

PASTA tiene como objetivo unir los objetivos comerciales y los requisitos técnicos.

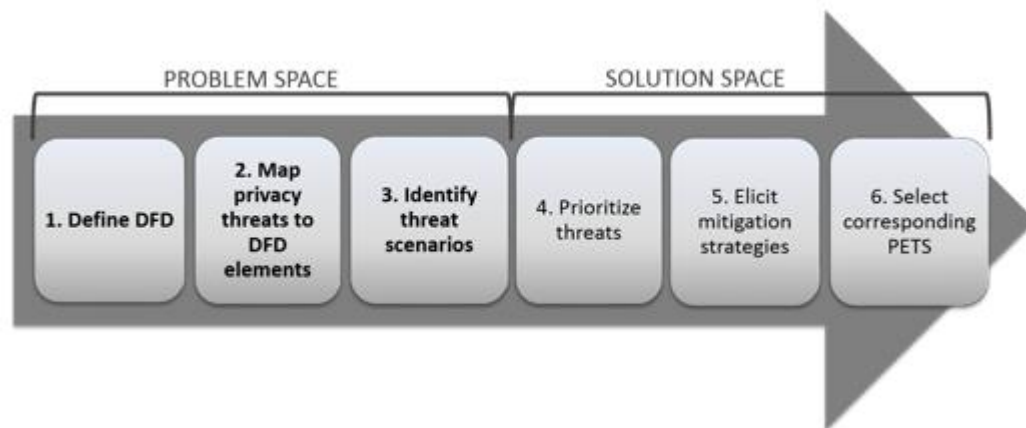
Utiliza una variedad de herramientas de diseño y elicitación en diferentes etapas. Este método eleva el proceso de modelado de amenazas a un nivel estratégico al involucrar a los tomadores de decisiones clave y al requerir información de seguridad de las

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

operaciones, la gobernanza, la arquitectura y el desarrollo. Ampliamente considerado como un marco centrado en el riesgo, PASTA emplea una perspectiva centrada en el atacante para producir un resultado centrado en los activos en forma de enumeración y puntuación de amenazas.

LINDDUN

LINDDUN (linkability, identifiability, nonrepudiation, detectability, disclosure of information, unawareness, noncompliance) se centra en cuestiones de privacidad y se puede utilizar para la seguridad de los datos. LINDDUN, que consta de seis pasos (ver figura), proporciona un enfoque sistemático para la evaluación de la privacidad.



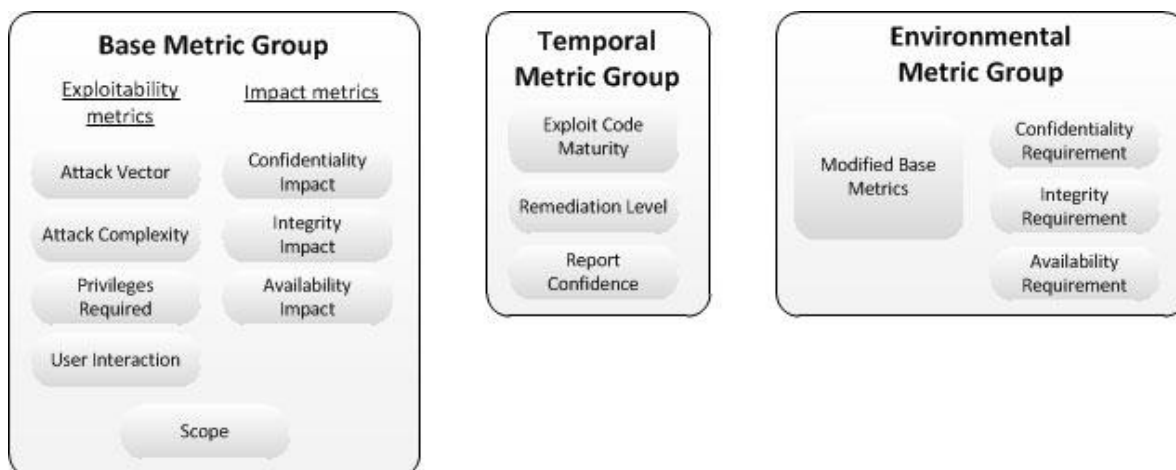
LINDDUN comienza con un DFD del sistema que define los flujos de datos, los almacenes de datos, los procesos y las entidades externas del sistema. Al iterar sistemáticamente sobre todos los elementos del modelo y analizarlos desde el punto de vista de las categorías de amenazas, los usuarios de LINDDUN identifican la aplicabilidad de una amenaza al sistema y crean árboles de amenazas.

CVSS

The Common Vulnerability Scoring System (CVSS) captura las características principales de una vulnerabilidad y produce una puntuación de gravedad numérica. CVSS fue desarrollado por NIST y es mantenido por el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) con el apoyo y contribuciones del Grupo de Interés Especial de CVSS. El CVSS proporciona a los usuarios un sistema de puntuación común

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

y estandarizado dentro de diferentes plataformas cibernéticas y ciberfísicas. Una puntuación CVSS se puede calcular con una calculadora que está disponible en línea.



Una puntuación CVSS se deriva de los valores asignados por un analista para cada métrica. Las métricas se explican ampliamente en la documentación. El método CVSS se usa a menudo en combinación con otros métodos de modelado de amenazas.

Trike

Trike se creó como un marco de auditoría de seguridad que utiliza el modelado de amenazas como técnica. Analiza el modelado de amenazas desde una perspectiva defensiva y de gestión de riesgos.

Como ocurre con muchos otros métodos, Trike comienza definiendo un sistema. El analista crea un modelo de requisitos enumerando y comprendiendo los actores, los activos, las acciones previstas y las reglas del sistema. Este paso crea una matriz actor-activo-acción en la que las columnas representan activos y las filas representan actores.

Cada celda de la matriz se divide en cuatro partes, una para cada acción de CRUD (crear, leer, actualizar y borrar). En estas celdas, el analista asigna uno de tres valores: acción permitida, acción no permitida o acción con reglas. Se adjunta un árbol de reglas a cada celda.

Después de definir los requisitos, se crea un diagrama de flujo de datos (DFD). Cada elemento se asigna a una selección de actores y activos. Iterando a través del DFD, el analista identifica amenazas, que caen en una de dos categorías: elevaciones de

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

privilegios o denegaciones de servicio. Cada amenaza descubierta se convierte en un nodo raíz en un árbol de ataque.

Para evaluar el riesgo de ataques que pueden afectar los activos a través de CRUD, Trike usa una escala de cinco puntos para cada acción, en función de su probabilidad. Los actores se califican en escalas de cinco puntos por los riesgos que se supone que presentan (menor número = mayor riesgo) para el activo. Además, los actores son evaluados en una escala tridimensional (siempre, a veces, nunca) por cada acción que pueden realizar en cada activo.

Tarjetas de seguridad

Las tarjetas de seguridad identifican ataques inusuales y complejos. No son un método formal, sino más bien una especie de técnica de lluvia de ideas. Con la ayuda de una baraja de cartas, los analistas pueden responder preguntas sobre un ataque, como

- » ¿Quién podría atacar?
- » ¿Por qué se podría atacar el sistema?
- » ¿Qué activos son de interés?

¿Cómo se pueden implementar estos ataques?

Este método utiliza una baraja de 42 cartas para facilitar las actividades de descubrimiento de amenazas: Impacto humano (9 cartas), Motivaciones del adversario (13 cartas), Recursos del adversario (11 cartas) y Métodos del adversario (9 cartas). Las diferentes categorías dentro de cada dimensión se muestran en la Tabla.

Impacto Humano	Motivaciones del adversario	Recursos del adversario	Métodos del adversario
<ul style="list-style-type: none"> • La biosfera • Bienestar emocional • Bienestar financiero • Datos personales • Bienestar físico • Relaciones • Bienestar social • Impactos inusuales 	<ul style="list-style-type: none"> • Acceso o conveniencia • Curiosidad o aburrimiento • Deseo u obsesión • Diplomacia o mercadería • Malicia o venganza • Dinero • Política • Protección • Religión • Auto promoción 	<ul style="list-style-type: none"> • Pericia • Un mundo futuro • Impunidad • Capacidades internas • Conocimiento interno • Dinero • Poder e influencia • Hora • Herramientas • Recursos inusuales 	<ul style="list-style-type: none"> • Ataque encubrimiento • Ataque indirecto • Manipulación o coerción • Ataque multifase • Agresión física • Procesos • Ataque tecnológico • Métodos inusuales

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

	<ul style="list-style-type: none"> • Visión del mundo • Motivaciones inusuales 		
--	--	--	--

hTMM

El Método de modelado de amenazas híbridas (hTMM) fue desarrollado por la SEI en 2018. Consiste en una combinación de SQUARE (Método de ingeniería de requisitos de calidad de seguridad), Tarjetas de seguridad y actividades PnG. Las características específicas del método incluyen ningún falso positivo, ninguna amenaza pasada por alto, un resultado consistente independientemente de quién esté realizando el modelado de amenazas y la rentabilidad.

Los principales pasos del método son

- » Identifique el sistema a modelar las amenazas.
- » Aplique tarjetas de seguridad según las sugerencias de los desarrolladores.
- » Elimine los PnG improbables (es decir, no hay vectores de ataque realistas).
- » Resuma los resultados utilizando el soporte de herramientas.
- » Continúe con un método formal de evaluación de riesgos.

Descripción de una metodología en profundidad.

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

La Evaluación de vulnerabilidades, activos y amenazas operativamente críticas (OCTAVE) es un marco de trabajo para identificar y gestionar los riesgos de seguridad de la información. Define un método de evaluación integral que permite a una organización identificar los activos de información que son importantes para la misión de la organización, las amenazas a esos activos y las vulnerabilidades que pueden exponer esos activos a las amenazas. Al reunir los activos de información, las amenazas y las vulnerabilidades, la organización puede comenzar a comprender qué información está en riesgo. Con este conocimiento, la organización puede diseñar e implementar una estrategia de protección para reducir la exposición general al riesgo de sus activos de información.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

OCTAVE fue desarrollado en 2001 en la Carnegie Mellon University (CMU), para el Departamento de Defensa de los Estados Unidos. El marco ha pasado por varias fases evolutivas desde ese momento, pero los principios y objetivos básicos han permanecido iguales. Existen dos versiones: OCTAVE-S, una metodología simplificada para organizaciones más pequeñas que tienen estructuras jerárquicas planas, y OCTAVE Allegro, una versión más completa para organizaciones grandes o aquellas con estructuras multinivel.

Cómo funciona

OCTAVE es una metodología de evaluación de riesgos flexible y autodirigida. Un pequeño equipo de personas de las unidades operativas (o comerciales) y el departamento de TI trabajan juntos para abordar las necesidades de seguridad de la organización. El equipo se basa en el conocimiento de muchos empleados para definir el estado actual de la seguridad, identificar los riesgos para los activos críticos y establecer una estrategia de seguridad. Puede adaptarse a la mayoría de las organizaciones.

A diferencia de la mayoría de los otros métodos de evaluación de riesgos, el enfoque OCTAVE se basa en prácticas de seguridad y riesgo operacional y no en tecnología. Está diseñado para permitir que una organización:

- » Dirija y gestione las evaluaciones de riesgos de seguridad de la información por sí mismos
- » Tome las mejores decisiones basadas en sus riesgos únicos
- » Centrarse en proteger los activos de información clave
- » Comunique de forma eficaz la información de seguridad clave

Fases de OCTAVE

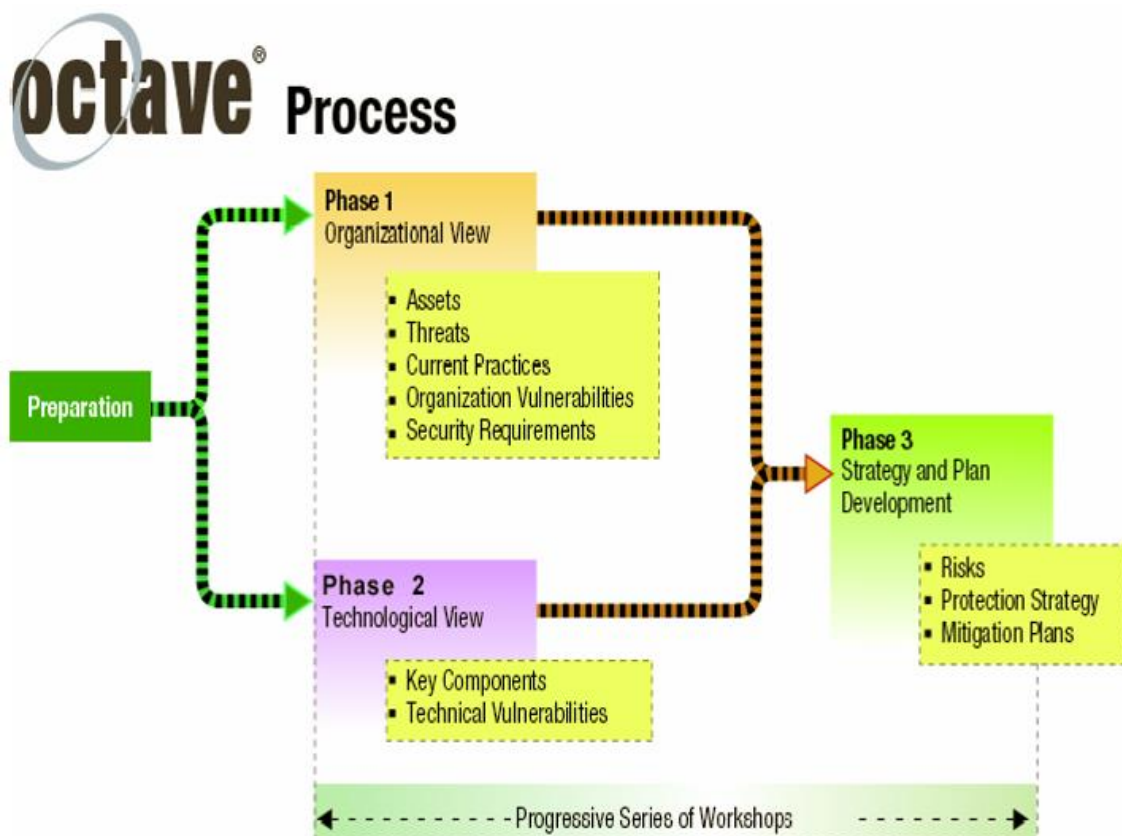
OCTAVE se organiza en torno a estos tres aspectos básicos que permiten al personal de la organización reunir una imagen completa de las necesidades de seguridad de la información de la organización. Las fases son:

- » Fase 1: Crear perfiles de amenazas basados en activos: esta es una evaluación organizacional. El equipo de análisis determina qué es importante para la organización (activos relacionados con la información) y qué se está haciendo

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

actualmente para proteger esos activos. Luego, el equipo selecciona los activos que son más importantes para la organización (activos críticos) y describe los requisitos de seguridad para cada activo crítico. Finalmente, identifica las amenazas a cada activo crítico, creando un perfil de amenaza para ese activo.

- » Fase 2: Identificar las vulnerabilidades de la infraestructura: esta es una evaluación de la infraestructura de la información. El equipo de análisis examina las rutas de acceso a la red, identificando clases de componentes de tecnología de la información relacionados con cada activo crítico. Luego, el equipo determina en qué medida cada clase de componente es resistente a los ataques de red.
- » Fase 3: Desarrollar planes y estrategias de seguridad: durante esta parte de la evaluación, el equipo de análisis identifica los riesgos para los activos críticos de la organización y decide qué hacer con ellos. El equipo crea una estrategia de protección para la organización y planes de mitigación para abordar los riesgos de los activos críticos, basándose en un análisis de la información recopilada.



Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Metodologías OCTAVE

Existen tres metodologías OCTAVE distintivas disponibles para uso público: el método OCTAVE, OCTAVE-S y OCTAVE Allegro. La introducción de OCTAVE Allegro no pretende suplantar las metodologías OCTAVE anteriores. OCTAVE Allegro es una variante que proporciona un proceso simplificado centrado en los activos de información. Sin embargo, cada método OCTAVE tiene una amplia aplicabilidad y los usuarios de estos métodos pueden seleccionar el enfoque que mejor se adapte a sus necesidades particulares de evaluación de riesgos de seguridad de la información.

- » El método OCTAVE fue la primera metodología consistente con OCTAVE que se introdujo [Alberts 2001]. El enfoque se define mediante una guía de implementación de métodos (procedimientos, orientación, hojas de trabajo, catálogos de información) y capacitación. El método se lleva a cabo en una serie de talleres dirigidos y facilitados por un equipo de análisis interdisciplinario formado por unidades de negocio de toda la organización (p. Ej., Alta dirección, directores de áreas operativas y personal) y miembros del departamento de TI [Alberts 2002]. El público objetivo del método OCTAVE son las grandes organizaciones con 300 empleados o más. Más específicamente, fue diseñado para organizaciones que

- tener una jerarquía de varias capas
- mantener su propia infraestructura informática
- tener la capacidad de ejecutar herramientas de evaluación de vulnerabilidades
- tener la capacidad de interpretar los resultados de las evaluaciones de vulnerabilidad

Como se describió anteriormente, el método OCTAVE se realiza en tres fases.

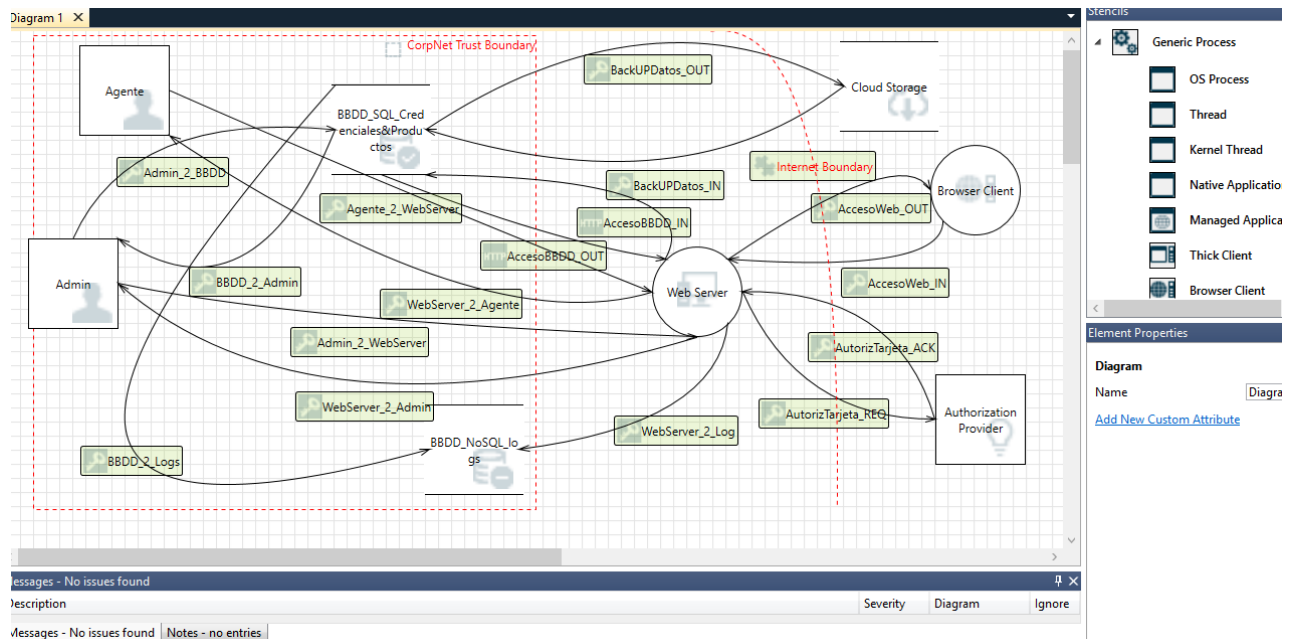
- » OCTAVE-S: El desarrollo de OCTAVE-S fue apoyado por el programa de Inserción, Demostración y Evaluación de Tecnología (TIDE) en el SEI, 4 con el objetivo de llevar un enfoque basado en OCTAVE a las pequeñas organizaciones manufactureras. La versión más actual del enfoque OCTAVE-S, la versión 1.0,

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

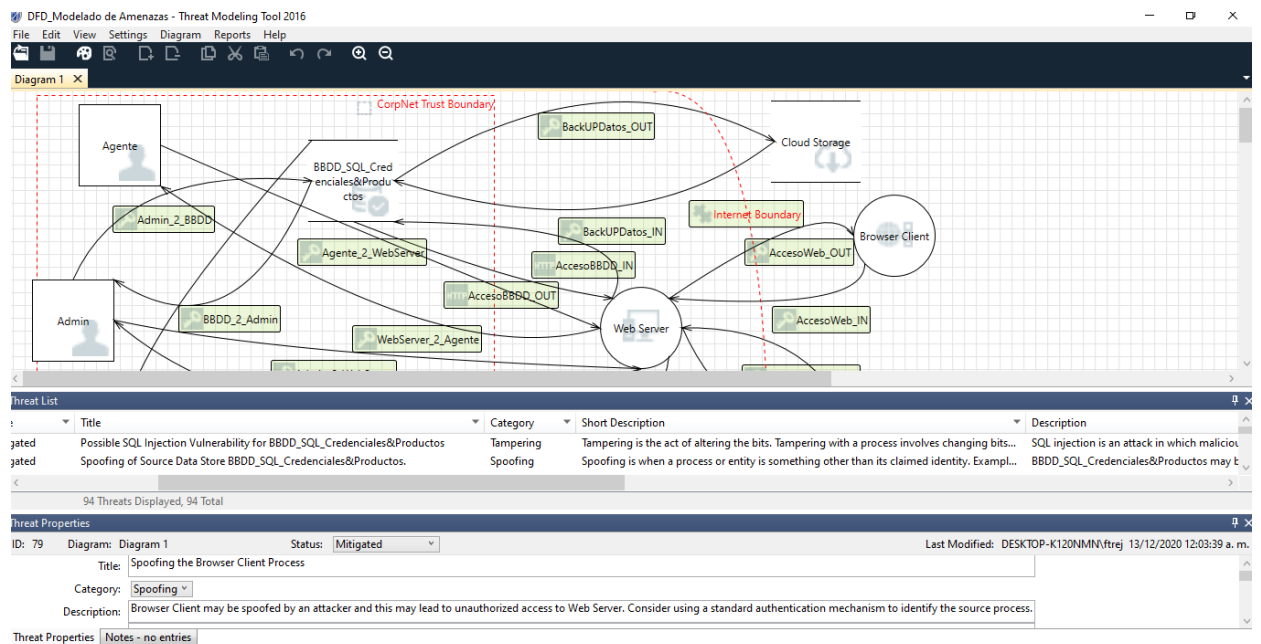
está diseñada específicamente para organizaciones de aproximadamente 100 personas o menos. De acuerdo con los criterios OCTAVE, el enfoque OCTAVE-S consta de tres fases similares. Sin embargo, OCTAVE-S es realizado por un equipo de análisis que tiene un amplio conocimiento de la organización. Por lo tanto, OCTAVE-S no se basa en talleres formales de obtención de conocimientos para recopilar información porque se supone que el equipo de análisis (generalmente compuesto de tres a cinco personas) tiene conocimiento práctico de los activos importantes relacionados con la información, los requisitos de seguridad, las amenazas y las amenazas. prácticas de seguridad de la organización. Otra diferencia significativa en OCTAVE-S es que está más estructurado que el método OCTAVE. Los conceptos de seguridad están integrados en las hojas de trabajo y la guía de OCTAVE-S, lo que permite a los profesionales de la seguridad y los riesgos con menos experiencia abordar una amplia gama de riesgos con los que pueden no estar familiarizados. Una última característica distintiva de OCTAVE-S es que requiere un examen menos extenso de la infraestructura de información de una organización. Debido a que las organizaciones pequeñas pueden no tener los recursos para obtener y ejecutar herramientas de vulnerabilidad, OCTAVE-S fue diseñado para incluir un examen limitado de los riesgos de infraestructura a fin de eliminar una barrera potencial para la adopción.

- » OCTAVE Allegro: El enfoque OCTAVE Allegro está diseñado para permitir una evaluación amplia del entorno de riesgo operativo de una organización con el objetivo de producir resultados más sólidos sin la necesidad de un conocimiento extenso de evaluación de riesgos. Este enfoque se diferencia de los enfoques anteriores de OCTAVE al centrarse principalmente en los activos de información en el contexto de cómo se utilizan, dónde se almacenan, transportan y procesan, y cómo están expuestos a amenazas, vulnerabilidades e interrupciones como resultado. Al igual que los métodos anteriores, OCTAVE Allegro se puede realizar en un entorno colaborativo, estilo taller, y se apoya con guías, hojas de trabajo y cuestionarios, que se incluyen en los apéndices de este documento. Sin embargo, OCTAVE Allegro también es adecuado para personas que desean realizar una evaluación de riesgos sin una amplia participación, experiencia o aportes organizativos. El enfoque OCTAVE Allegro consta de ocho pasos que se organizan en cuatro fases. En la fase 1, la organización desarrolla

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	



Vista en modo diseño.



Vista en modo análisis.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Valoración de amenazas, método DREAD

TABLA DE CALIFICACION DE AMENAZAS

	High (3)	Medium (2)	Low (1)
Daño potencial	El atacante puede recuperar datos extremadamente sensibles y corromperlos o destruirlos.	El atacante puede recuperar datos confidenciales, pero hacer poco más	El atacante solo puede recuperar datos que tienen poco o ningún potencial de daño
Reproducibilidad	Siempre funciona, no requiere una ventana de tiempo o casos extremos específicos	Depende del tiempo; funciona solo dentro de una ventana de tiempo	Rara vez funciona
Explotabilidad	Cualquiera podría hacerlo	El atacante debe tener algo de conocimiento y habilidad	El atacante debe tener mucho conocimiento y habilidad
Usuarios afectados	La mayoría o todos los usuarios	Algunos usuarios	Pocos o ningún usuario
Descubrimiento	El atacante puede descubrir fácilmente la vulnerabilidad	El atacante podría descubrir la vulnerabilidad	El atacante tendrá que excavar para descubrir la vulnerabilidad.

Calculo de Riesgo

Amenaza	Probabilidad de Ocurrencia (P)			Impacto Potencial (I)		P	I	Riesgo
	R	E	DI	D	A	(R+E+DI)	(D+A)	PxI
Spoofing del almacenamiento datos destino BBDD_SQL_Credenciales&Productos	2	2	1	2	2	5	4	20
Potencial vulnerabilidad de inyección SQL para BBDD_SQL_Credenciales&Productos	2	2	3	3	3	7	6	42
Potencial consumo excesivo de recursos para el servidor web o BBDD_SQL_Credenciales&Productos	3	3	3	3	3	9	6	54
Spoofing del proceso del servidor web	2	2	2	3	2	6	5	30
El almacenamiento de datos de BBDD_SQL_Credenciales&Productos podría estar dañado	2	2	3	2	1	7	3	21
El almacen de datos niega escritura en BBDD_SQL_Credenciales&Productos	3	2	3	3	3	8	6	48
Detección de flujo de datos	2	2	3	3	3	7	6	42
Flujo de datos AccesoBBDD_IN esta potencialmente interrumpido	3	3	3	3	3	9	6	54
Almacén de datos es inaccesible	3	2	3	3	2	8	5	40
Spoofing del almacenamiento de datos origen BBDD_SQL_Credenciales&Productos	3	2	3	2	3	8	5	40

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Calificación de amenazas

Descripción de Amenaza	D	R	E	A	D	TOTAL	CALIFICACIÓN
Spoofing del almacenamiento datos destino BBDD_SQL_Credenciales&Productos	2	2	2	2	1	9	Bajo
Potencial vulnerabilidad de inyección SQL para BBDD_SQL_Credenciales&Productos	3	2	2	3	3	13	Muy alto
Potencial consumo excesivo de recursos para el servidor web o BBDD_SQL_Credenciales&Productos	3	3	3	3	3	15	Muy alto
Spoofing del proceso del servidor web	2	2	2	2	2	10	Medio
El almacenamiento de datos de BBDD_SQL_Credenciales&Productos podría estar dañado	1	2	2	1	3	9	Bajo
El almacén de datos niega escritura en BBDD_SQL_Credenciales&Productos	3	2	2	3	3	13	Muy alto
Detección de flujo de datos	3	2	2	3	3	13	Muy alto
Flujo de datos AccesoBBDD_IN esta potencialmente interrumpido	3	3	3	3	3	15	Muy alto
Almacén de datos es inaccesible	2	3	2	2	3	12	Alto
Spoofing del almacenamiento de datos origen BBDD_SQL_Credenciales&Productos	3	3	2	3	3	14	Muy alto

Descripción de Amenaza 1	Spoofing of Destination Data Store BBDD_SQL_Credenciales&Productos
Objetivo Amenaza	Los datos se escriben en el objetivo del atacante
Clasificación Amenaza	Spoofing
Calificación Riesgo	Bajo
Técnica de ataque	DDoS attack, Malware, Pharming
Contramedidas	Single Sign on, IPSec Protección de secretos, No almacenamiento de secretos Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital.

Descripción de Amenaza 2	Potential SQL Injection Vulnerability for BBDD_SQL_Credenciales&Productos
Objetivo Amenaza	Modificar datos en el servidor SQL
Clasificación Amenaza	Tampering, Malware
Calificación Riesgo	Muy alto
Técnica de ataque	Inyección SQL de Unión, SQL Inyección de Error, Inyección SQL Ciega tiempo, Inyección SQL Ciega de Boolean, Inyección SQL Fuera de banda
Contramedidas	Códigos de autenticación de mensajes, Firmas digitales Protocolos resistentes a la manipulación, Listas de control de acceso ACL Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Descripción de Amenaza 3	Potential Excessive Resource Consumption for Web Server or BBDD_SQL_Credenciales&Productos
Objetivo Amenaza	Interrupción de servicios o colapso del servidor
Clasificación Amenaza	Denial Of Service
Calificación Riesgo	Muy Alto
Técnica de ataque	Uso de botnets
Contramedidas	Calidad de servicio Listas de control de acceso ACL Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital.

Descripción de Amenaza 4	Spoofing the Web Server Process
Objetivo Amenaza	Acceso no autorizado a la base de datos.
Clasificación Amenaza	Spoofing
Calificación Riesgo	Medio
Técnica de ataque	Crear páginas web falsas y redirigir a los usuarios
Contramedidas	Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital. Protección de secretos, No almacenamiento de secretos Single Sign on, IPSec

Descripción de Amenaza 5	The BBDD_SQL_Credenciales&Productos Data Store Could Be Corrupted
Objetivo Amenaza	Dañar la base de datos
Clasificación Amenaza	Tampering
Calificación Riesgo	Bajo
Técnica de ataque	Malware
Contramedidas	Protocolos resistentes a la manipulación, Listas de control de acceso ACL Códigos de autenticación de mensajes, Firmas digitales Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital.

Descripción de Amenaza 6	Data Store Denies BBDD_SQL_Credenciales&Productos Potentially Writing Data
Objetivo Amenaza	Borrar evidencia de ataques
Clasificación Amenaza	Repudiación
Calificación Riesgo	Muy alto
Técnica de ataque	Audit Log Manipulation
Contramedidas	Sellado de tiempo Procesos de Autenticación: Hash, firma digital. Procesos de Auditoria

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Descripción de Amenaza 7	Detección de flujo de datos
Objetivo Amenaza	Leer los datos que fluyen a través de la base de datos
Clasificación Amenaza	Divulgación de información
Calificación Riesgo	Muy alto
Técnica de ataque	Uso de sniffers
Contramedidas	Protección de secretos Protocolos seguros, Encriptado Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital.

Descripción de Amenaza 8	El acceso al flujo de datos BBDD_IN esta potencialmente interrumpido
Objetivo Amenaza	Interrumpir el flujo de datos en cualquier dirección a través del límite de confianza
Clasificación Amenaza	Denial Of Service
Calificación Riesgo	Muy alto
Técnica de ataque	Uso de botnets
Contramedidas	Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital. Calidad de servicio Listas de control de acceso ACL

Descripción de Amenaza 9	Almacén de datos inaccesible
Objetivo Amenaza	Impedir acceso a la base de datos al otro lado del límite de confianza
Clasificación Amenaza	Denial Of Service
Calificación Riesgo	Alto
Técnica de ataque	Uso de botnets
Contramedidas	Listas de control de acceso ACL Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital. Calidad de servicio

Descripción de Amenaza 10	Spoofing of Source Data Store BBDD_SQL_Credenciales&Productos
Objetivo Amenaza	Entrega de datos falsos al servidor web
Clasificación Amenaza	Spoofing
Calificación Riesgo	Muy alto
Técnica de ataque	Phishing
Contramedidas	Procesos de Autenticación, Autorización y Auditoria (AAA): Hash, firma digital. Single Sign on, IPSec Protección de secretos, no almacenamiento de secretos

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Conclusiones

La metodología elegida para dar una descripción mas detallada fue OCTAVE, me pareció un concepto interesante por las siguientes razones:

Sus aspectos principales son el riesgo operacional, prácticas de seguridad y tecnología, método profundo y flexible, contribuye a la gestión de riesgos, tiene una priorización de mitigación incorporada, resultados consistentes con repetición y es escalable.

La herramienta de modelado de amenazas de Microsoft facilita el modelado de amenazas para todos los desarrolladores a través de una notación estándar para visualizar los componentes del sistema, los flujos de datos y los límites de seguridad.

También ayuda a los modeladores de amenazas a identificar las clases de amenazas que deben considerar en función de la estructura de su diseño de software. Esta herramienta ha sido diseñada pensando en los expertos que no son de seguridad, lo que facilita el modelado de amenazas para todos los desarrolladores al proporcionar una guía clara sobre la creación y el análisis de modelos de amenazas.

A nivel de seguridad, debemos considerar a los productos software como soluciones únicas, en constante cambio para corregir vulnerabilidades, añadir controles y adaptarse a las regulaciones y amenazas cambiantes.

Este proceso podrá a veces parecer tedioso, pero el enorme valor que aporta la seguridad correctamente aplicada a un proyecto sobrepasa considerablemente los costos asociados.

Es importante considerar que un solo ciberataque exitoso y público puede derrumbar el prestigio empresarial construido por décadas, acabar con la confianza de los usuarios, generar pérdidas por robo de dinero e información y sanciones legales de los entes reguladores.

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	

Referencias bibliográficas

Shevchenko, N. (2018, 3 December). Threat Modeling: 12 Available Methods
https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

Alberts, C. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.
<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473>

Juuso, S. (2019, mayo). Evaluation of Threat Modeling Methodologies A Case Study.
https://www.theseus.fi/bitstream/handle/10024/220967/Selin_Juuso.pdf?sequence=2&isAllowed=y

Rodsan, R. (2019). Introduction to threat modeling - Learn. Microsoft Docs.
<https://docs.microsoft.com/en-us/learn/modules/tm-introduction-to-threat-modeling/>

Modelado de Amenazas -OWASP. (2017). Owasp.org. Retrieved 19 December 2017, from https://www.owasp.org/index.php/Modelado_de_Amenazas

PAe – MAGERIT v.3: metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catalogo de Elementos. Método. Ministerio de Hacienda y Administraciones (2017). Administracionelectronica.gob.es. Retrieved December 2017, from: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WjIIJt_ibIV

CAPEC - CAPEC-333: WASC Threat Classification 2.0 (Version 3.3)
<https://capec.mitre.org/data/definitions/333.html>

Asignatura	Datos del alumno	Fecha
Seguridad en el Software	Apellidos: Trejo Garcia	14/Dic/2020
	Nombre: Felipe	