TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 4 – UNIDAD 3

Universidad Tecnológica de Pereira

faceIT

Modelos de Evaluación de Riesgos en el Desarrollo de Software

La evaluación de riesgos en el desarrollo de software es un proceso esencial para identificar, evaluar y mitigar vulnerabilidades antes de que se conviertan en amenazas significativas.

En el área de seguridad de la información, las evaluaciones de riesgos se enfocan en los activos de información. Algunas normas como la ISO 27001 son enfáticas en que se deben tener procesos para controlar la seguridad y dar manejo a los riesgos. Algunos pasos que permiten establecer los riesgos para su mitigación son:

1. Establecer y delimitar un marco de evaluación de riesgos

Se deben listar los requisitos legales y contractuales así como las herramientas y modelos de evaluación a utilizar. Un modelo de evaluación permite crear e identificar riesgos y enfocarse en los procesos que permitan mitigar el riesgo.

2. Inventariar los activos de información

Una forma de evaluar los riesgos es teniendo en cuenta los escenarios y los activos. Para poder proteger los activos es necesario conocerlos. Los activos pueden incluir el hardware de la empresa, las redes, el software, los dispositivos, las bases de datos, los medios de información extraíbles, los dispositivos móviles que tengan la información y los archivos en papel y medios físicos.

También es recomendable listar los propietarios o administradores de los activos de información. En las normas ISO es común levantar actas para tener trazabilidad de loas activos y los accesos que estos activos tienen.

En las bases de datos y registros digitales se pueden implementar controles de acceso y sistemas de registro de accesos para saber quién leyó y modificó la información junto con los datos de fecha y hora en la que un cambio o lectura ocurrió. De esta forma se mitigan riesgos, en especial, de ingeniería social

3. Identificar puntos vulnerables y amenazas potenciales

Para cada activo se encuentra la lista de vulnerabilidades y se detallan los procesos y procedimientos que deben efectuarse. En este paso se listan todos los riesgos y los niveles de riesgo que pueden existir por activo.

4. Determinar el impacto de las amenazas

Este paso consiste en determinar el impacto de cada riesgo asignándole una puntuación. Con el puntaje que tiene cada riesgo (basado en el impacto) permite establecer las prioridades al crear estrategias de mitigación y al determinar los niveles de seguridad que van a existir por cada activo.

5. Crear un plan de gestión de riesgos

Dependiendo del nivel de riesgo, es necesario delimitar las acciones utilizando un plan de gestión de riesgos. Los planes suelen tener las instrucciones para evitar los riesgos cuando es posible. Mitigar los riesgos cuando no pueden ser evitados, Transferir los riesgos como estrategia de mitigación (por ejemplo, el uso de pólizas financieras contra demandas por fallos en la seguridad informática).
También se debe definir la forma en la que se está midiendo la gestión de los riesgos.

6 Utilizar una metodología preestablecida de evaluación de riesgos en el software y los activos digitales:

La evaluación de riesgos en el desarrollo de software es crucial para identificar, mitigar y gestionar vulnerabilidades antes de que se conviertan en problemas graves. A continuación, se describen algunos modelos comunes de evaluación de riesgos, con ejemplos prácticos que ilustran cómo se estructuran y aplican en la práctica.

Modelo STRIDE

STRIDE es un marco desarrollado por Microsoft para categorizar y analizar posibles amenazas en sistemas. Su nombre es un acrónimo que representa las principales categorías de amenazas:

- Spoofing (Suplantación de identidad)
- Tampering (Manipulación de datos)
- Repudiation (Repudio de acciones)
- Information Disclosure (Divulgación de información)
- Denial of Service (Denegación de servicio)
- Elevation of Privilege (Elevación de privilegios)

Ejemplo:

En un sistema de banca en línea, el equipo de desarrollo utiliza STRIDE para analizar cada componente. Para el módulo de autenticación, identifican amenazas como la suplantación de identidad (S) mediante el robo de credenciales, y deciden implementar autenticación multifactor (MFA) para mitigarlo. En el módulo de transferencia de fondos, abordan la manipulación de datos (T) mediante la encriptación de las solicitudes.

Estructura en la práctica:

1. Identificar componentes del sistema.
2. Mapear amenazas posibles usando STRIDE.
3. Asignar controles o medidas de mitigación.
4. Revisar regularmente para actualizar las amenazas.

Modelo DREAD

DREAD es un modelo de evaluación de riesgos que cuantifica la gravedad de las amenazas basado en cinco factores:

- Damage Potential (Potencial de daño)
- Reproducibility (Reproducibilidad)
- Exploitability (Explotabilidad)
- Affected Users (Usuarios afectados)
- Discoverability (Descubribilidad)

Ejemplo:

En una aplicación de comercio electrónico, un equipo de seguridad evalúa una vulnerabilidad en la gestión de contraseñas. La clasifican así:

- Potencial de daño: Alto, ya que podría exponer datos sensibles.
- Reproducibilidad: Alta, dado que el ataque es fácil de replicar.
- Explotabilidad: Media, ya que requiere acceso interno.
- Usuarios afectados: Alta, porque involucra a todos los usuarios.
- Descubribilidad: Baja, porque el error está en una sección poco visible.

Estructura en la práctica:

1. Identificar una amenaza específica.
2. Puntuar cada factor en una escala (por ejemplo, de 1 a 10).
3. Calcular un promedio o suma para priorizar la mitigación.
4. Implementar las soluciones según el puntaje de prioridad.

3. Análisis de Impacto y Probabilidad

Este enfoque clasifica los riesgos según dos dimensiones: el impacto potencial y la probabilidad de que ocurran. Se utiliza una matriz de riesgo para visualizar y priorizar los riesgos.
Ejemplo de aplicación:

En un sistema de gestión de inventarios, el equipo identifica el riesgo de una caída del servidor. Lo clasifican como de alto impacto (interrupción de operaciones críticas) pero de baja probabilidad (el servidor tiene redundancia).

Estructura en la práctica:

1. Listar todos los riesgos posibles.
2. Evaluar impacto y probabilidad en escalas definidas.
3. Asignar cada riesgo en la matriz (por ejemplo, bajo, medio, alto).
4. Diseñar estrategias de mitigación para riesgos en la zona roja (alto impacto y alta probabilidad).

Modelo FAIR (Factor Analysis of Information Risk)

FAIR es un modelo que cuantifica los riesgos de seguridad en términos financieros. Se centra en entender los factores que contribuyen al riesgo y su impacto económico.
Ejemplo de aplicación:

Un banco usa FAIR para calcular el costo potencial de una brecha de datos. Evalúan:

- La frecuencia probable de un ataque exitoso.
- El valor de los activos afectados.

Estructura en la práctica:

1. Identificar el activo en riesgo y su valor.
2. Evaluar la frecuencia de amenazas y vulnerabilidades.
3. Calcular el impacto potencial en términos monetarios.
4. Priorizar inversiones en controles según el retorno esperado.

Con la lista la información recopilada y los procedimientos que estén midiendo el desempeño de la seguridad informática e posible facilitar los procesos de auditoría y de certificación conforme a los lineamientos de la norma ISO 270001