ANALISIS DE RIESGOS EN SISTEMAS

Unidad 3: Método de análisis y gestión de riesgos II

Objetivo específico 3: El alumno aprenderá a formalizar las actividades conociendo la caracterización de las amenaza y las salvaguardas, para poder realizar una estimación del riesgo así como la documentación que se debe de elaborar y la lista de control que se debe de llevar a cabo

.

Conceptos a desarrollar en la unidad: Formalización de las actividades, Caracterización de las amenazas, Caracterización de las salvaguardas, Estimación del estado de riesgo, Documentación y Lista de control

Introducción

En este tema se abordara la manera de cómo se deben de formalizar las actividades del método de análisis de riesgos, como se lleva a cabo las diferentes caracterizaciones tanto de las amenazas como de las salvaguardas que se llevan a cabo durante el análisis de riesgos, teniendo en cuenta la estimación del estado de riesgos, además de elaborar los diferentes documentos y llevar a cabo la lista de control con la cual podemos ir evaluando y asi poder llevar a cabo un control de los riesgos a los cuales os enfrentamos

3.1 Formalización de las actividades

Este conjunto de actividades tiene los siguientes objetivos:

- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Informar de las áreas del sistema con mayor impacto y/o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

MAR.1: Caracterización de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, de- terminando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado “modelo de

valor”. Sub-tareas:

Tarea MAR.11: Identificación de los activos **Tarea MAR.12:** Dependencias entre activos **Tarea MAR.13:** Valoración de los activos

MAR.2: Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

El resultado de esta actividad es el informe denominado “mapa de

riesgos”. Sub-tareas:

Tarea MAR.21: Identificación de las amenazas

Tarea MAR.22: Valoración de las amenazas

MAR.3: Caracterización de las salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

El resultado de esta actividad se concreta en varios informes:

- declaración de aplicabilidad
- evaluación de salvaguardas
- insuficiencias (o vulnerabilidades del sistema de protección)

Sub-tareas:

Tarea MAR.31: Identificación de las salvaguardas pertinentes

Tarea MAR.32: Valoración de las salvaguardas

MAR.4: Estimación del estado de riesgo

Esta actividad procesa todos los datos recopilados en las actividades anteriores para

- realizar un informe del estado de riesgo: estimación de impacto y riesgo
- realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

Sub-tareas:

Tarea MAR.41: Estimación del impacto

Tarea MAR.42: Estimación del riesgo

Es frecuente que las tareas relacionadas con los activos (MAR.1) se realicen concurrentemente con las tareas relacionadas con las amenazas sobre dichos activos (MAR.2) e identificación de las salvaguardas actuales (MAR.3), simplemente porque suelen coincidir las personas y es difícil que el interlocutor no tienda de forma natural a tratar cada activo "verticalmente", viendo todo lo que le afecta antes de pasar al siguiente.

3.1.1 Tarea MAR.1: Caracterización de los activos

Esta actividad consta de tres sub-tareas:

MAR.11: Identificación de los activos

MAR.12: Dependencias entre activos

MAR.13: Valoración de los activos

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar que parte del valor del sistema se soporta en cada activo. Podemos resumirlo en la expresión "conócete a ti mismo".

MAR: Análisis de riesgos ***MAR.1: Caracterización de los activos*** ***MAR.11: Identificación de los activos***
Objetivos • Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados
Productos de entrada • Inventario de datos manejados por el sistema • Inventario de servicios prestados por el sistema • Procesos de negocio • Diagramas de uso • Diagramas de flujo de datos • Inventarios de equipamiento lógico • Inventarios de equipamiento físico • Locales y sedes de la Organización • Caracterización funcional de los puestos de trabajo

MAR: Análisis de riesgos
MAR.1: Caracterización de los activos
MAR.11: Identificación de los activos

Productos de salida

- Relación de activos a considerar
- Caracterización de los activos: valor propio y acumulado
- Relaciones entre activos

Técnicas, prácticas y pautas

- Ver “Libro II – Catálogo”.
- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones

Esta tarea es crítica. Una buena identificación es importante desde varios puntos de vista:

- materializa con precisión el alcance del proyecto
- permite las interlocución con los grupos de usuarios: todos hablan el mismo lenguaje
- permite determinar las dependencias precisas entre activos
- permite valorar los activos con precisión
- permite identificar y valorar las amenazas con precisión
- permite determinar qué salvaguardas serán necesarias para proteger el sistema

Caracterización de los activos

Para cada activo hay que determinar una serie de características que lo definen:

- código, típicamente procedente del inventario
- nombre (corto)
- descripción (larga)
- tipo (o tipos) que caracterizan el activo
- unidad responsable. A veces hay más de una unidad. Por ejemplo, en el caso de aplicaciones cabe diferenciar entre la unidad que la mantiene y la que la explota.
- persona responsable. Especialmente relevante en el caso de datos. A veces hay más de un responsable. Por ejemplo en caso de datos de carácter personal cabe diferenciar entre el responsable del dato y el operador u operadores que lo manejan.
- ubicación, técnica (en activos intangibles) o geográfica (en activos materiales)
- cantidad, si procede como puede ser en el caso de la informática personal (por ejemplo 350 equipos de sobremesa)
- otras características específicas del tipo de activo

MAR: Análisis de riesgos
MAR.1: Caracterización de los activos
MAR.12: Dependencias entre activos

Objetivos

- Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior

Productos de entrada

- Resultados de la tarea T1.2.1, Identificación
- Procesos de negocio
- Diagramas de flujo de datos
- Diagramas de uso

Productos de salida

- Diagrama de dependencias entre activos

Técnicas, prácticas y pautas

- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

Para cada dependencia conviene registrar la siguiente información:

- estimación del grado de dependencia: hasta un 100%
- explicación de la valoración de la dependencia
- entrevistas realizadas de las que se ha deducido la anterior estimación

MAR: Análisis de riesgos
MAR.1: Caracterización de los activos
MAR.13: Valoración de los activos

Objetivos

- Identificar en qué dimensión es valioso el activo
- Valorar el coste que para la Organización supondría la destrucción del activo

Productos de entrada

- Resultados de la tarea MAR.11, Identificación de los activos
- Resultados de la tarea MAR.12, Dependencias entre activos

Productos de salida

- **Modelo de valor**: informe de valor de los activos

Técnicas, prácticas y pautas

- Ver “Libro II – Catálogo”.
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

Para la adquisición de este conocimiento puede ser necesario entrevistar a diferentes colectivos dentro de la Organización:

- dirección o gerencia, que conocen las consecuencias para la misión de la Organización
- responsables de los datos, que conocen las consecuencias de sus fallos de seguridad
- responsables de los servicios, que conocen las consecuencias de la no prestación del servi-

cio o de su prestación degradada

- responsables de sistemas de información y responsables de operación, que conocen las consecuencias de un incidente

Para cada valoración conviene registrar la siguiente información:

- dimensiones en las que el activo es relevante
- estimación de la valoración en cada dimensión
- explicación de la valoración
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

3.1.1 Tarea MAR.2: Caracterización de las amenazas

Esta actividad consta de dos sub-tareas:

MAR.21: Identificación de las amenazas

MAR.22: Valoración de las amenazas

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cómo de probable es que pase. Podemos resumirlo en la expresión “conoce a tu enemigo”.

MAR: Análisis de riesgos ***MAR.2: Caracterización de las amenazas*** ***MAR.21: Identificación de las amenazas***
Objetivos • Identificar las amenazas relevantes sobre cada activo
Productos de entrada • Resultados de la actividad MAR.1, Caracterización de los activos • Informes relativos a defectos en los productos. Esto es, informes de vulnerabilidades.
Productos de salida • Relación de amenazas posibles
Técnicas, prácticas y pautas • Catálogos de amenazas (ver "Catálogo de Elementos") • Árboles de ataque (ver "Guía de Técnicas") • Entrevistas (ver "Guía de Técnicas") • Reuniones • Valoración Delphi (ver "Guía de Técnicas")

En esta tarea se identifican las amenazas significativas sobre los activos identificados, tomando en consideración:

- el tipo de activo
- las dimensiones en que el activo es valioso
- la experiencia de la Organización
- los defectos reportados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- explicación del efecto de la amenaza
- entrevistas realizadas de las que se ha deducido la anterior estimación
- antecedentes, si los hubiera, bien en la propia Organización, bien en otras organizaciones que se haya considerado relevantes

MAR: Análisis de riesgos
MAR.2: Caracterización de las amenazas
MAR.22: Valoración de las amenazas

Objetivos

- Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse

Productos de entrada

- Resultados de la tarea MAR2.1, Identificación de las amenazas
- Series históricas de incidentes
- Informes de defectos en los productos
- Antecedentes: incidentes en la Organización

Productos de salida

- **Mapa de riesgos**: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos

Técnicas, prácticas y pautas

- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

En esta tarea se valoran las amenazas identificadas en la tarea anterior, tomando en consideración:

- la experiencia (historia) universal
- la experiencia (historia) del sector de actividad
- la experiencia (historia) del entorno en que se ubican los sistemas
- la experiencia (historia) de la propia Organización
- los informes anexos a los reportes de defectos proporcionados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Sabiendo que existen una serie de posibles agravantes, como se describe en la sección X.

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- estimación de la frecuencia de la amenaza
- estimación del daño (degradación) que causaría su materialización
- explicación de las estimaciones de frecuencia y degradación
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

3.1.2 Tarea MAR.3: Caracterización de las salvaguardas

Esta actividad consta de dos sub-tareas:

MAR.31: Identificación de las salvaguardas pertinentes

MAR.32: Valoración de las salvaguardas

El objetivo de estas tareas es doble: saber qué necesitamos para proteger el sistema y saber si tenemos un sistema de protección a la altura de nuestras necesidades.

MAR: Análisis de riesgos
MAR.3: Caracterización de las salvaguardas
MAR.31: Identificación de las salvaguardas pertinentes

Objetivos

- Identificar las salvaguardas convenientes para proteger el sistema

Productos de entrada

- modelo de activos del sistema
- modelo de amenazas del sistema
- indicadores de impacto y riesgo residual
- informes de productos y servicios en el mercado

Productos de salida

- Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias
- Relación de salvaguardas desplegadas

Técnicas, prácticas y pautas

- Catálogos de salvaguardas (ver "Catálogo de Elementos")
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones

Para cada salvaguarda conviene registrar la siguiente información:

- descripción de la salvaguarda y su estado de implantación
- descripción de las amenazas a las que pretende hacer frente
- entrevistas realizadas de las que se ha deducido la anterior información

Para determinar las salvaguardas pertinentes es frecuente recurrir a catálogos de salvaguardas o al consejo de personas expertas. De una u otra forma dispondremos de una colección de salva guardas para elegir, de forma que el complejo problema de encontrar lo que necesitamos se reduce al problema más sencillo de descartar lo que no necesitamos.

En el proceso de descarte hay varias razones para eliminar una salvaguarda propuesta:

- porque no es apropiada para el activo que necesitamos defender
- porque no es apropiada para la dimensión de seguridad que necesitamos defender
- porque no es efectiva oponiéndose a la amenaza que necesitamos contrarrestar
- porque es excesiva para el valor que tenemos que proteger (desproporcionada)
- porque disponemos de medidas alternativas

MAR: Análisis de riesgos
MAR.3: Caracterización de las salvaguardas
MAR.32: Valoración de las salvaguardas

Objetivos

- Determinar la eficacia de las salvaguardas pertinentes

Productos de entrada

- Inventario de salvaguardas derivado de la tarea MAR.31

Productos de salida

- **Evaluación de salvaguardas** : informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad
- **Informe de insuficiencias (o vulnerabilidades)**: relación de salvaguardas que deberían estar pero no están desplegadas o están desplegadas de forma insuficiente

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

En esta tarea se valora la efectividad de las salvaguardas identificadas en la tarea anterior, tomando en consideración:

- la idoneidad de la salvaguarda para el fin perseguido
- la calidad de la implantación
- la formación de los responsables de su configuración y operación
- la formación de los usuarios, si tienen un papel activo
- la existencia de controles de medida de su efectividad
- la existencia de procedimientos de revisión regular

Para cada salvaguarda conviene registrar la siguiente información:

- estimación de su eficacia para afrontar aquellas amenazas
- explicación de la estimación de eficacia
- entrevistas realizadas de las que se ha deducido la anterior estimación

3.1.3 Tarea MAR.4: Estimación del estado de riesgo

En esta tarea se combinan los descubrimientos de las tareas anteriores (MAR.1, MAR.2 y MAR.3) para derivar estimaciones del estado de riesgo de la Organización.

Esta actividad consta de tres tareas:

MAR.41: Estimación del impacto

MAR.42: Estimación del riesgo

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

MAR: Análisis de riesgos
MAR.4: Estimación del estado de riesgo
MAR.41: Estimación del impacto

Objetivos

- Determinar el impacto potencial al que está sometido el sistema
- Determinar el impacto residual al que está sometido el sistema

Productos de entrada

- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas

Productos de salida

- Informe de impacto (potencial) por activo
- Informe de impacto residual por activo

Técnicas, prácticas y pautas

- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

En esta tarea se estima el impacto al que están expuestos los activos del sistema:

- el impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- el impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

MAR: Análisis de riesgos
MAR.4: Estimación del estado de riesgo
MAR.42: Estimación del riesgo

Objetivos

- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

Productos de entrada

- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas
- Resultados de la actividad MAR.4, Estimaciones de impacto

MAR: Análisis de riesgos
MAR.4: Estimación del estado de riesgo
MAR.42: Estimación del riesgo

Productos de salida

- Informe de riesgo (potencial) por activo
- Informe de riesgo residual por activo

Técnicas, prácticas y pautas

- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

En esta tarea se estima el riesgo al que están sometidos los activos del sistema:

- el riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- el riesgo residual, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

3.2 Documentación

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Informes y evaluaciones de defectos de los productos, procedentes de fabricantes o de centros de respuesta a incidentes de seguridad (CERTs).

Documentación final

- **Modelo de valor**

  Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

- **Mapa de riesgos**:

  Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

- **Declaración de aplicabilidad:**

  Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.

- **Evaluación de salvaguardas:**

  Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.

- **Informe de insuficiencias o vulnerabilidades:**

  Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.

- **Estado de riesgo:**

  Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

Esta documentación es un fiel reflejo del estado de riesgo y de las razones por la que este riesgo no es aceptable. Es fundamental entender las razones que llevan a una valoración determinada de riesgo para que el proceso de gestión de riesgos esté bien fundamentado. El proceso de gestión de riesgos partirá de estas valoraciones para atajar el riesgo o reducirlo a

niveles aceptables.

3.4 Lista de control

√	actividad	tarea
	Se han identificado los activos esenciales: información que se trata y servicios que se prestan	MAR.11
	Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad	MAR.13
	Se han identificado los demás activos del sistema	MAR.11
	Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, mediante identificación de las dependencias)	MAR.12
	Se han identificado las amenazas posibles sobre los activos	MAR.21
	Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas	MAR.22
	Se ha estimado la probabilidad de que dichas amenazas se materialicen	MAR.23
	Se han estimado los impactos y riesgos potenciales, inherentes al sistema	MAR.4
	Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales	MAR.31
	Se ha valorado el despliegue de las salvaguardas identificadas	MAR.32
	Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas	MAR.4