Investigación CORAS

Jorge René García Rosado - 558828
Fernando Cepeda - 342741
Mauricio Cortés - 350429
David Jimenez - 557168
Kevin Luna - 378142

Introducción

- Desarrollado a partir del año 2001 por SINTEF
  - Organización noruega que se dedica a la elaboración de proyectos de investigación.
- Significa “Construct a platform for Risk Analysis of Security critical system”
- Es una metodología de análisis de riesgos informáticos en una organización basada en la elaboración de modelos que consta de siete pasos, basadas fundamentalmente en entrevistas con los expertos.

¿Qué proporciona este método?

- Un lenguaje gráfico basado en UML para la definición de los modelos (activos, amenazas, riesgos y salvaguardas), y guías para su utilización a lo largo del proceso.
- Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos, que permite su gestión y reutilización.
- Representación textual basada en XML del lenguaje gráfico.
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

Los 7 pasos

1. Presentación.
2. Análisis de alto nivel.
3. Aprobación.
4. Identificación de riesgos.
5. Estimación de riesgos.
6. Evaluación de riesgos.
7. Tratamiento del riesgo.

1.- Presentación.

- Reunión para presentar los objetivos y alcance del análisis y recabar información inicial.

2.- Análisis de alto nivel

- Se identifican amenazas, vulnerabilidades, escenarios e incidentes, se usan entrevistas para verificar la comprensión de la información obtenida y se analiza la documentación.

3.- Aprobación

- Descripción precisa del objetivo, alcance y consideraciones a analizar: Se necesita la aprobación del cliente para terminar este paso.

4.- Identificación de riesgos

- Taller de análisis con personas con experiencia para identificar el mayor número de posibles incidentes, amenazas y vulnerabilidades.

5.- Estimación de riesgos

- Estimación de probabilidades e impactos de los incidentes identificados en el paso anterior.

6.- Evaluación de riesgos

- Se emite un informe con los riesgos, el cual se le entrega al cliente y normalmente da lugar a ajustes.

7.- Tratamiento de riesgo

- Se identifican posibles tratamientos para los riesgos y se realiza un análisis costo/beneficio.

Bibliografía

- Manuel, M. (2009). Análisis de riesgos de seguridad de la información. Recuperado de: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf
- Acevedo N. & Satizábal C. (2016). Risk management and prevention methodologies: a comparison. Sistemas & Telemática, 14(36), 39-58.

Damos nuestra palabra de que hemos realizado esta actividad con integridad académica.