

CORAS

<http://coras.sourceforge.net>

CORAS (Consultative Objective Risk Analysis System), es un proyecto creado por la Unión Europea con el objetivo de proporcionar un framework orientado a sistemas donde la seguridad es crítica, facilitando el descubrimiento de vulnerabilidades de seguridad, inconsistencias, y redundancias.

CORAS proporciona un método basado en modelos, para realizar **análisis de riesgos**, y se basa en el uso de tres componentes:

- ✓ Un lenguaje de modelado de riesgos basado en el UML.
- ✓ La metodología CORAS, una descripción paso a paso del proceso de análisis con una directriz para construir los diagramas CORAS.
- ✓ Una herramienta para documentar, mantener y crear los informes del análisis.

Aunque **no es** exactamente **un framework para el modelado de amenazas**, su uso orientado a tal fin, puede contribuir a la reducción de riesgos y la adopción de unas correctas contramedidas.

La metodología CORAS, hace un uso intensivo de los diagramas. Existen 5 tipos diferentes:

Diagrama superficial de activos: Muestra una visión general de los activos y cómo el daño sobre un activo puede afectar al resto.

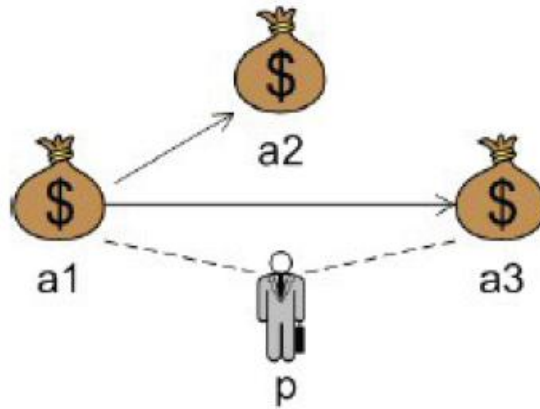
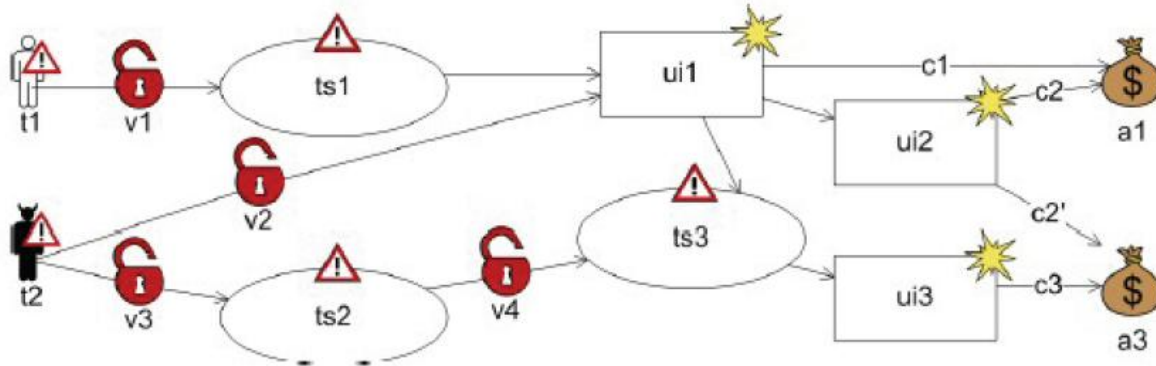


Diagrama de amenazas: Muestra una visión completa de la secuencia de eventos iniciados por las amenazas y las consecuencias que tienen éstas sobre los activos. Sus componentes básicos se muestran en el ejemplo inferior, y son: amenazas deliberadas, amenazas accidentales, amenazas no-humanas, vulnerabilidades, escenarios de amenazas, incidentes no deseados y activos.



Ejemplo de diagrama de amenazas

Diagrama superficial de riesgo: Es un resumen del diagrama de amenazas, mostrando los riesgos. Tiene 5 componentes básicos: amenazas deliberadas, accidentales y no-humanas, riesgos y activos. A cada riesgo se le asigna un valor.

Diagrama de tratamiento: ofrece una visión completa de las contramedidas propuestas. Se basa en el diagrama de amenazas, sustituyendo las consecuencias del impacto sobre los activos con los riesgos procedentes del diagrama superficial de riesgo, y añadiendo los escenarios de contramedidas propuestos.

Diagrama superficial de tratamiento: es un resumen de las contramedidas, añadiendo los distintos escenarios posibles y mostrando las relaciones entre los distintos elementos propuestos para tratar el riesgo.