Universidad de Costa Rica
Seguridad de Sistemas Computacionales
CI0143 - I Semestre 2022

Desarrollo (Parte I), Seguridad (Parte II) y Evaluación (Parte III)
de una Aplicación Web
Fecha entrega: 7 junio 2022

Prof. Ricardo Villalón Fonseca

1. Objetivo General

Establecer la seguridad (Parte II) de una aplicación web simple y la infraestructura tecnológica que la soporta, para ser evaluada en un entorno de producción, posiblemente hostil.

2. Objetivos Específicos

1. Construir una propuesta de seguridad para la aplicación web desarrollada en la Parte I de esta tarea y la infraestructura tecnológica que la soporta.
2. Implementar los controles de seguridad propuestos para la aplicación y la infraestructura.
3. Instalar la aplicación en un servidor como una versión para producción.

3. Descripción General

Esta tarea consiste en construir e implementar una solución de seguridad para la aplicación web creada en la parte I de esta tarea así como para la infraestructura tecnológica que la soporta, con el fin de desarrollar habilidades básicas en procesos de seguridad de los componentes tecnológicos para un servicio en producción.

Para especificar y delimitar el proceso de seguridad se deben considerar los siguientes aspectos:

- Componentes del servicio a asegurar.
- Objetivos de seguridad.
- Metodología de seguridad.
- Definición de políticas y controles de seguridad.
- Puesta en operación del servicio.
- Documentación de seguridad.

4. Componentes del servicio a asegurar

Debe considerar/incluir al menos los siguientes elementos o componentes como parte de su ámbito de responsabilidad al realizar el proceso de seguridad.

- Toda la información gestionada por la aplicación web.
- La aplicación web así como de cualquier otra aplicación de software, incluyendo el sistema operativo del equipo donde se ejecute la aplicación. Si la aplicación requiere más de un servidor para operar, debe incluir en su solución de seguridad todas las aplicaciones de software de los equipos.
- Los equipos y otros componentes de hardware (aunque sean virtuales) que conformen el servicio.

Tenga en cuenta que, dado que el ambiente de producción será la Nube Académica Computacional, la seguridad del hardware debe considerar todos los componentes que estén en su dominio de acción, y validar (potencialmente proponer) las condiciones mínimas requeridas en la seguridad de la plataforma de la nube, aún cuando no sea posible tener control de las mismas. Este último requerimiento tiene como objetivo considerar la seguridad ofrecida por la plataforma de nube, que en condiciones reales usualmente se reflejaría por medio de un contrato de nivel de servicio o Service Level Agreement (SLA).

5. Objetivos generales de seguridad

Establezca objetivos de seguridad para todos los componentes y subcomponentes del servicio bajo su responsabilidad, según corresponda. Para este proyecto, al menos identifique, especifique e implemente requerimientos apropiados de integridad, confidencialidad, autenticación, autorización y auditoría.

6. Metodología de seguridad

Se utilizará como metodología general el procedimiento estudiado en clase, el cual se resume de forma gráfica en la figura 1.

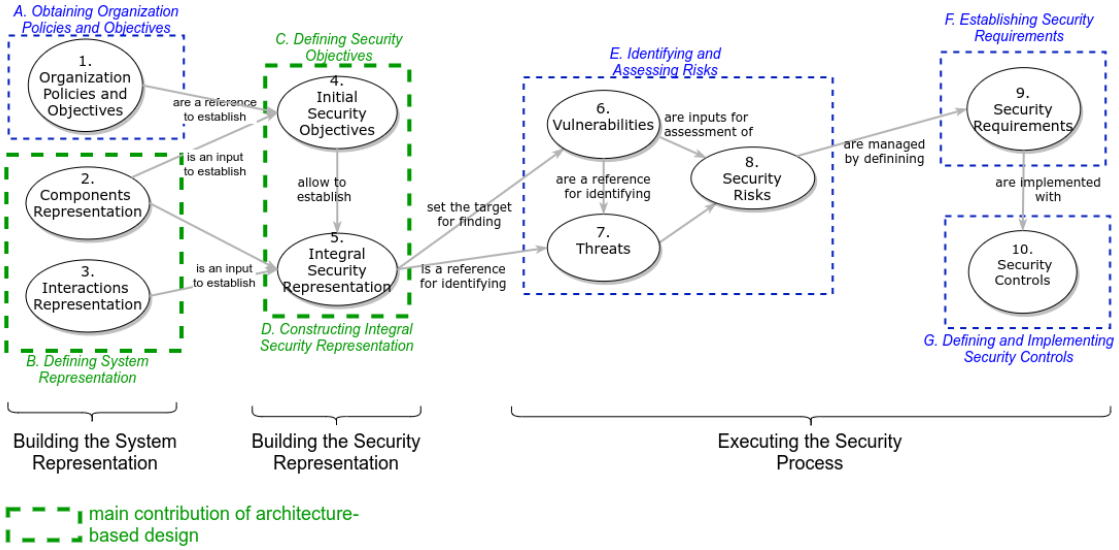

Figura 1: Modelo del Proceso de Seguridad.

1. Establezca objetivos de seguridad para componentes del sistema, a partir de los objetivos generales definidos en el apartado anterior.

2. Construya una representación para los componentes de su sistema, usando un patrón del todo-y-las-partes, con el fin de lograr una organización de componentes que sea apropiada para desarrollar el proceso de seguridad.

3. Construya diagramas de interacción para los casos de uso de su sistema, con base en los componentes del sistema y tomando en consideración la lógica funcional de su aplicación, así como otros componentes externos o internos que sean parte del proceso.

4. Identifique relaciones de representación entre componentes del sistema y que sean relevantes para el proceso de seguridad.

5. A partir de los objetivos de seguridad para los componentes del sistema, y por medio de las relaciones de seguridad, realice un proceso de identificación de vulnerabilidades y amenazas, que permita establecer los riesgos relevantes para su sistema.

6. Aplique un esquema de valoración de riesgos (según se defina en el curso), defina un umbral de tolerancia de acuerdo con su apetito al riesgo, y establezca cuáles riesgos serán mitigados y cuáles serán asumidos.

7. Para los riesgos seleccionados defina requerimientos/políticas técnicas de seguridad, que establezcan acciones concretas, en ánimo de alcanzar un nivel de seguridad apropiado para el sistema, en relación con los objetivos establecidos.

8. Defina e implemente controles de seguridad para atender los requerimientos establecidos en la políticas de seguridad.

9. Repita el proceso de aseguramiento realizado, considerando riesgos residuales y nuevos riesgos que puedan surgir a partir de la adición de los controles de seguridad.

7. Puesta en operación del servicio

Para la puesta en operación del servicio, reserve uno o más computadores en la plataforma de la NAC, según las indicaciones que le serán proporcionadas en el curso. Luego, instale los servicios de servidor que necesite, realice las configuraciones de seguridad que considere apropiadas, instale y publique la aplicación.

8. Documentación de seguridad

Para cada uno de los pasos indicados anteriormente, documente apropiadamente el trabajo realizado. Como parte de la estructura de documentación, de forma complementaria, se incluyen como parte de este enunciado una guía de documentación de un servicio, una de documentación de un equipo y una breve guía de estilo de documentación que puede usar como referencia o apoyo para organizar el contenido sus documentos.