Ministerio de Modernización
Presidencia de la Nación

Requerimientos y Controles de Seguridad para Aplicaciones

Coordinación de Proyectos e Investigación de Ciberseguridad

Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad

PAIS DIGITAL

Versión 1

Diciembre de 2017

Contenidos

Equipo de Trabajo

- López Lio Rodrigo

- Bellezza Bruno

- Erra Francisco

1. Consideraciones al iniciar un Proyecto de Desarrollo

Es fundamental **considerar la seguridad de una aplicación lo más temprano posible** en el ciclo de desarrollo o adquisición de nuevas aplicaciónes. Las decisiones que se toman en las **etapas iniciales** de análisis de requerimientos y diseño de arquitectura son las que **más influencian los niveles de seguridad** de la aplicación cuando llegue a producción.

Se debe dar **participación al área de seguridad informática desde el comienzo** de un proyecto de desarrollo. La participación del equipo de seguridad, ayuda a entender y mitigar los riesgos asociados al desarrollo y operación de una aplicación con los respectivos datos de los usuarios.

Adicionalmente, se recomienda designar a un **miembro del equipo de desarrollo como responsable de seguridad** para la aplicación. El responsable de seguridad, dirige y verifica el cumplimiento de las actividades de seguridad recomendadas para todo el ciclo de desarrollo.

Se recomienda almacenar la mínima cantidad de datos de los usuarios por el menor tiempo posible para reducir el riesgo de que se produzcan fugas de información.

Este proceso de análisis de requerimientos de seguridad puede aplicarse tanto a nuevos proyectos de desarrollo, proyectos preexistentes o heredados y a proyectos propios o implementados por terceros.

En este documento se explica cómo identificar los requerimientos de seguridad para una aplicación y se ofrece herramientas para entrevistar a los stakeholders y elegir controles de seguridad.

1.1. Metodologías para Identificar Requerimientos de Seguridad

A continuación se presenta una breve comparativa de distintas metodologías para identificar requerimientos de seguridad en un proyecto.

Modelo	SQUARE	KAOS Sec Extension	Secure Tropos
Descripción	Basado en nueve pasos formales.	Basado en Modelos y responsabilidades.	Basado en requerimientos no-funcionales.
Output	Genera requerimientos categorizados y priorizados.	Genera lista de requerimientos y una selección de controles.	Genera diagramas Tropos de seguridad.
Documentación	Casos uso, casos abuso Arboles de ataque. Requerimientos priorizados.	Modelo de Requerimientos de seguridad.	Diagramas Tropos de restricciones, entidades,
Stakeholders	Participación Activa	Participación secundaria.	No incluye entrevistas

2. Definición de Requerimientos de Seguridad

Definir los **requerimientos de seguridad ayuda a reforzar los puntos débiles en la seguridad de una aplicación**. Los requerimientos dependerán de los objetivos de la organización, el marco regulatorio y las buenas prácticas de seguridad vigentes.

*La definición de requerimientos es **un proceso iterativo** adaptado al entorno*. Se deberá conducir entrevistas con **stakeholders** representativos de distintas características del proyecto para lograr un enfoque completo. En este documento se incluye un anexo con preguntas para ayudar a identificar posibles requerimientos de seguridad.

Los requerimientos de seguridad especifican **restricciones sobre el funcionamiento de la aplicación ante abusos,** es decir: *"¿**Qué no deberá hacer la aplicación ante un ataque**?"*

Un **caso de abuso**, refiere a las acciones que toma un atacante para perjudicar el funcionamiento previsto de nuestra aplicación. Por ejemplo, para acceder a una información privada sin autorización.

2.1. Etapas en la Definición de Requerimientos de Seguridad:

La conducción de **este proceso será tarea del responsable de seguridad** designado para la aplicación. Se debe llevarlo a cabo ***antes de tomar decisiones críticas de arquitectura y diseño.***

- **Identificar Objetivos de Seguridad:** Que se busca alcanzar para evaluar los requerimientos necesarios.
- **Definir Documentación deseable:** Que documentos se producirán sobre los requerimientos de seguridad.
- **Enumerar Requerimientos:** Se produce una lista tentativa de requerimientos de seguridad.
- **Categorizar Requerimientos:** Se asigna los requerimientos a distintas categorías.
- **Priorizar Requerimientos:** Se asigna valor relativo a los requerimientos enumerados.

2.2. Ejemplos de Documentación Deseable

- **Diagramas de arquitectura del sistema,** a nivel aplicación, stack y red.
- **Casos de abuso y Arboles de ataque,** complementan casos de uso y pueden aplicarse a distintos sub-componentes de la aplicación.
- **Listado de Requerimientos de Seguridad,** enumera los requerimientos de seguridad que se consideran necesarios para alcanzar los objetivos.
- **Listado de Controles de Seguridad,** se seleccionan en base a los requerimientos de seguridad establecidos.

2.3. Definición de Objetivos de Seguridad

Los objetivos de seguridad que se definan para una aplicación deberán responder a los objetivos organizacionales de los procesos asociados a la aplicación.

Es posible que distintos stakeholders propongan diversos objetivos de seguridad, que incluso pueden contradecirse entre sí. El responsable de seguridad deberá evaluar la prioridad de los objetivos de seguridad propuestos, en función de la compatibilidad con el propósito organizacional de la aplicación.

La definición de objetivos de seguridad priorizados ayudará a inferir los requerimientos de seguridad necesarios.

2.4. Características de requerimientos bien formulados:

Un requerimiento bien planteado deberá cubrir ciertos criterios para ser aceptable. Se recomienda prestar atención a las siguientes características:

- **Concretos**: Lo suficientemente específicos y definidos claramente.
- **Completos**: Cubren todos los puntos clave.
- **Consistentes**: Con niveles similares de abstracción entre sí.
- **Necesarios**: Sirven para ayudar a cumplir objetivos de la aplicación.
- **Verificables**: Permiten comprobar que se cumplen.
- **Explícitos**: No dejan lugar confusiones o ambigüedades.
- **Precisos**: Expresan suficientes detalles con exactitud.
- **No-Conflictivos**: No se contradicen entre sí.

2.5. Enumeración de Requerimientos de Seguridad

Los requerimientos definen ***que debe hacer la aplicación***. En la etapa de diseño se especifica cómo debe hacerlo.

Se recomienda especial atención a prevenir la inclusión de características de arquitectura arbitrarias antes de terminar el proceso de análisis de requerimientos, ya que puede afectar negativamente la seguridad.

Se deberá conducir entrevistas cara a cara con los stakeholders durante el proceso de enumeración de requerimientos, utilizando la metodología que el responsable de seguridad prefiera.

Los requerimientos **Funcionales** de Seguridad describirán **condiciones o capacidades** para garantizar el cumplimiento de requerimientos frente a abusos.

Los requerimientos **No-Funcionales** de Seguridad describirán **propiedades emergentes del sistema,** necesarias para cumplir requerimientos frente a abusos.

2.6. Ejemplos de Requerimientos de Seguridad

- *El sistema debe aplicar mecanismos de autenticación en todos los puntos de entrada.*
- *Se requiere un plan de Continuidad de operaciones para asegurar disponibilidad del sistema.*
- *Las comunicaciones de red del sistema deberán protegerse utilizando cifrado.*
- *El sistema deberá implementar autenticación mediante una pantalla de login.*
- *El sistema deberá identificar y autenticar a todos los usuarios que intenten acceder.*
- *El sistema deberá mantener integridad de datos mediante un registro de modificaciones.*
- *El sistema deberá recuperarse de todo tipo de ataque, fallo o accidente en menos de X minutos.*
- *El backup deberá incluir una copia validada de todos los archivos en el servidor.*
- *El sistema deberá poder recuperar todas sus funcionalidades desde una copia de respaldo.*
- *El sistema deberá proveer información confiable a los usuarios con acceso legítimo.*
- *El sistema deberá asegurar que solo usuarios autenticados puedan acceder a contenidos protegidos.*
- *El sistema deberá proteger la privacidad de comunicaciones con los usuarios.*
- *El sistema deberá implementar redundancia para mantenerse funcionando en caso de desastre.*
- *El sistema deberá tener un mecanismo de control de accesos basado en roles, que determine las funciones que cada usuario puede utilizar.*

2.7. Categorización y Priorización de Requerimientos

El asignar categorías a los requerimientos enumerados ayuda a identificar los requerimientos más importantes y establecer un corte de los que se alcanzará a cumplir en función de las restricciones del proyecto.

Requerimientos Centrales	Requerimientos Generales	Requerimientos Operativos	Otros Requerimientos
Confidencialidad Integridad Disponibilidad Auditabilidad Control de Accesos Confidencialidad	Control de Sesiones Manejo de Errores Configuración de Componentes	Entornos de Deployment Almacenamiento de Datos Anti-Piratería	Adquisición de Software Contratación de Terceros Marco Regulatorio

En la mayoría de los casos no será posible implementar todos los requerimientos elegidos. Los stakeholders pueden elegir que requerimientos se implementarán y en qué orden. Se puede optar por descartar completamente o postergar la implementación de algunos requerimientos.

Existen distintos métodos para la priorización de requerimientos, generalmente, el equipo de desarrollo puede ayudar a evaluar el esfuerzo-beneficio de implementar distintos requerimientos.

3. Anexo: Preguntas para identificar Requerimientos de Seguridad

A continuación se presenta una serie de preguntas para que el responsable de seguridad de una aplicación, pueda dirigir a distintos stakeholders en la etapa inicial de un desarrollo para facilitar la enumeración de requerimientos.

3.1. Preguntas de Seguridad Generales

3.1.1. Seguridad Operativa

¿Cuál será el proceso para identificar y corregir vulnerabilidades en la aplicación?
¿Cuál será el proceso para identificar y corregir vulnerabilidades en sistemas y servicios?
¿Qué nivel de acceso a datos de la aplicación tendrán los administradores de sistemas y redes?
¿Qué requerimientos se definirá para incidentes de seguridad?
¿Cómo accederán los administradores a la infraestructura productiva para mantenerla?
¿Qué controles de acceso físico existirán para proteger los equipos en que corre la aplicación y sus datos?
¿Qué protocolo de acceso existirá para el entorno donde se hosteará la aplicación?

3.1.2. Seguridad en Gestión de Cambios

¿Cómo se controlará los cambios en el código?
¿Cómo se controlará los cambios en la infraestructura?
¿Cómo se despliegará código a producción?
¿Qué mecanismos existirá para detectar violaciones a la gestión de cambios?

3.1.3. Seguridad en Procesos de Desarrollo

¿Qué datos usarán los desarrolladores en entornos de pruebas?
¿Cómo participarán los desarrolladores en el debugging y troubleshooting de la aplicación?
¿Qué requerimientos de control de acceso existirán sobre el código fuente?
¿Qué procesos de programación segura se usará?

3.1.4. Seguridad Organizacional

¿Qué programa de seguridad rige para la organización?
¿Qué entrenamiento de seguridad reciben los desarrolladores y administradores?
¿Qué personal vigilará los procesos y requerimientos de seguridad sobre la aplicación?
¿Qué procedimientos de incorporación y separación de personal existen?
¿Cómo se impone el principio de segregación de responsabilidades?
¿Cómo se protegerá entornos productivos de compromisos a la red interna?
¿Qué requerimientos normativos de seguridad se definirá?

3.2. Seguridad a Nivel Organizacional

3.2.1. Modelo Organizacional

¿Cuál es el objetivo organizacional de la aplicación?
¿Cómo beneficiara a la organización?
¿Cuáles son los objetivos de la organización para desarrollar y mejorar la aplicación?
¿Cómo se promocionará el uso de la aplicación?
¿Qué beneficios les ofrecerá la aplicación a los usuarios?
¿Qué previsiones de continuidad de negocio se definirá para la aplicación?
¿En qué áreas geográficas prestará servicio la aplicación?

3.2.2. Datos

¿Qué datos recibirá, producirá y procesará la aplicación?
¿Cómo se puede clasificar los datos en categorías?
¿Qué beneficio obtendría un atacante si roba o modifica los datos?
¿Qué plan de Backups se definirá para la aplicación?

3.2.3. Usuarios

¿Quiénes serán los usuarios de la aplicación?
¿Cómo van a interactuar los usuarios con la aplicación?
¿Qué expectativas de seguridad tendrán los usuarios?

3.2.4. Terceras Partes

¿Qué terceras partes proveerán datos a la aplicación?
¿Qué terceras partes recibirán datos de la aplicación?
¿Qué terceras partes procesarán datos de la aplicación?
¿Qué mecanismos se usará para compartir datos con terceros además de la aplicación?
¿Qué requerimientos de seguridad se establecerá para los terceros?

3.2.5. Administradores

¿Quiénes tendrán privilegios administrativos sobre la aplicación?
¿Qué funciones administrativas ofrecerá la aplicación?

3.2.6. Marco Regulatorio

¿En qué industrias se usará la aplicación?
¿Qué normativa de seguridad aplica a la industria?
¿Qué normativa de auditoria y compliance rige?
¿Cómo se comunicará, gestionará e implementaran los cambios del marco normativo?

3.3. Seguridad a Nivel Aplicación

3.3.1. Entorno

¿Que frameworks y lenguajes de programación se usarán para crear la aplicación?
¿Qué procesos, código o infraestructura se definirá para la aplicación?
¿Qué bases de dato y servicios soportarán la aplicación?
¿Cómo se protegerán las credenciales para la base de datos, las llaves de cifrado y otros secreteos?

3.3.2. Procesamiento de Datos

¿Qué campos de entrada de datos tendrá la aplicación?
¿Qué campos de salida de datos tendrá la aplicación?
¿Cuál será el flujo de datos entre los componentes internos de la aplicación?
¿Qué requerimientos de validación de entrada de datos se definirá?
¿Qué datos almacenará la aplicación y cómo se almacenarán?
¿Qué datos se necesitará cifrar y que requerimientos se definirá?
¿Qué medidas se tomarán para detectar una filtración de datos?
¿Qué requerimientos de cifrado se establecerá para datos en tránsito?

3.3.3. Accesos

¿Qué niveles de privilegio de usuario soportará la aplicación?
¿Qué requerimientos de identificación y autenticación de usuarios se establecerá?
¿Qué requerimientos de autorización se definirá?
¿Qué requerimientos de control de sesión se establecerá?
¿Qué requerimientos de acceso se establecerá para las URLS?
¿Qué restricciones de acceso se establecerá para los usuarios?
¿Cómo se mantiendrá la identidad de los usuarios entre transacciones?

3.3.4. Monitoreo de la aplicación

¿Qué requerimientos de auditoría de la aplicación se definirá?
¿Qué requerimientos de monitoreo de rendimiento se definirá?
¿Qué requerimientos de monitoreo de seguridad se definirá?
¿Qué requerimientos de manejo y registro de errores se definirá?
¿Cómo se almacenará, protegerá y accederá a los registros de auditoría y debugging?

3.3.5. Diseño de la aplicación

¿Qué prácticas de revisión de diseño de la aplicación se definirá y aplicará?
¿Cómo se almacenará la data cacheada de la aplicación?
¿En qué capas lógicas estarán agrupados los componentes de la aplicación?
¿Qué requerimientos de pruebas y QA se definirá?

3.4. Seguridad a Nivel Infraestructura

3.4.1. Red

¿Qué detalles de red, firewalling y balanceo de carga se definirá?
¿Qué arquitectura de red usará la aplicación?
¿Qué dispositivos de red soportaran la aplicación?
¿Qué requerimientos de rendimiento existirán?
¿Qué redes privadas y públicas soportaran la aplicación?

3.4.2. Sistemas

¿Sobre qué sistemas operativos correrá la aplicación?
¿Qué requerimientos de hardware se definirá?
¿Qué detalles sobre componentes de sistema operativo y hardenizado se definirá?

3.4.3. Monitoreo de Infraestructura

¿Qué requerimientos de red y rendimiento de equipos se definirá?
¿Qué mecanismos de detección de compromiso y código malicioso existirán?
¿Qué requerimientos de seguridad para redes y equipos se definirá?

3.4.4. Virtualización

¿Qué aspectos de la aplicación se prestan a ser virtualizados?
¿Qué requerimientos de virtualización se definirán?
¿Qué partes de la aplicación se prestan a correrse en servicios tipo nube?
¿Qué tipo de servicios nube se usarán?
¿Cómo se evaluaron los riesgos beneficios entre las opciones disponibles?

4. *Anexo: Catálogo de Controles de Seguridad*

4.1. Control de Accesos

- Limitar acceso al sistema para usuarios, procesos y dispositivos autorizados.
- Limitar acceso al sistema solo a transacciones y funciones permitidas para usuarios autorizados.

4.2. Entrenamiento

- Asegurar que los directivos, administradores de sistemas y usuarios de sistemas de la organización, tengan conocimiento de los riesgos asociados a sus actividades, y de las políticas, estándares y procedimientos de seguridad del sistema.
- Asegurar que el personal de la organización esté entrenado como para llevar a cabo sus tareas y responsabilidades relacionadas con la seguridad de la información.
- Proveer entrenamiento de seguridad para reconocer y reportar indicadores de amenazas internas.

4.3. Registros de auditoría

- Crear y mantener los registros de auditoría necesarios para permitir un monitoreo, análisis, investigación y reporte de usos indebidos del sistema.
- Asegurar que las acciones de los usuarios del sistema sean registradas individualmente.

4.4. Gestión de Configuraciones

- Generar y mantener configuraciones básicas e inventario de los activos informáticos de la organización durante el ciclo de desarrollo.
- Establecer y aplicar configuraciones de seguridad para los componentes utilizados en sistemas.

4.5. Identificación y Autenticación

- Identificar a los usuarios del sistema, y a sus correspondientes procesos y dispositivos.
- Antes de permitir acceso al sistema, autenticar la identidad de los usuarios, procesos o dispositivos.

4.6. Respuesta a incidentes

- Establecer capacidades operativas de respuesta a incidentes para sistemas de la organización incluyendo actividades de: preparación, detección, análisis, contención, recuperación y respuesta a usuarios.
- Seguir, documentar y reportar incidentes a las autoridades adecuadas.

4.7. Mantenimiento

- Realizar mantenimiento sobre sistemas de la organización.
- Aplicar controles sobre las herramientas, técnicas, mecanismos y personal que realizan mantenimiento sobre los sistemas.

4.8. Protección de medios

- Proteger los medios de almacenamiento que contienen información de los usuarios.
- Solo permitir acceso a la información de los usuarios a personal autorizado.
- Sanitizar o destruir los medios con información de los usuarios al descartarlos o reutilizarlos.

4.9. Seguridad del Personal

- Auditar a individuos antes de autorizarlos a acceder a sistemas con información personal de los usuarios.
- Asegurar que los sistemas con información de los usuarios se mantengan protegidos durante cambios de personal.

4.10. Protección Física

- Restringir el acceso físico a sistemas, equipamiento y entornos operativos solo a personal autorizado.
- Proteger y vigilar el entorno físico de los sistemas de la organización e infraestructura de soporte.

4.11. Gestión de Riesgos

- Evaluar periódicamente los riesgos a los procesos, activos e individuos de la organización que surjan de utilizar sistemas o información de los usuarios.
- Realizar periódicamente escaneos de vulnerabilidades sobre sistemas y aplicaciones de la organización.
- Reparar las vulnerabilidades descubiertas.

4.12. Auditorías de Seguridad

- Revisar periódicamente los controles de seguridad en sistemas de la organización para determinar si son efectivos.
- Desarrollar e implementar planes de acción destinados a corregir fallos y reducir o eliminar vulnerabilidades en sistemas de la organización.
- Revisar controles de seguridad continuamente para asegurar su efectividad.
- Desarrollar, documentar y actualizar planes de seguridad que describan: límites del sistema, ambientes operativos, implementación de requerimientos de seguridad, y conexiones con otros sistemas.

4.13. Protección de Sistemas y Comunicaciones

- Monitorear, controlar y proteger comunicaciones dentro y hacia afuera de sistemas de la organización.
- Utilizar arquitecturas de diseño, técnicas de desarrollo e ingeniería de sistemas que faciliten la seguridad de la información en sistemas de la organización.

4.14. Integridad de Sistemas e Información

- Identificar, reportar y corregir fallos del sistema rápidamente.
- Proveer protección contra código malicioso a sistemas de la organización.
- Monitorear las alertas de seguridad de fabricantes y aplicar las correcciones recomendadas.

5. *Referencias*

Security Quality Requirements Engineering Methodology
https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14594.pdf

A KAOS Tutorial
http://www.objectiver.com/fileadmin/download/documents/KaosTutorial.pdf

An integrated conceptual model for information system security risk management
https://arxiv.org/ftp/arxiv/papers/1701/1701.01664.pdf

Security Requirements Engineering: Applying SQUARE Framework
https://www.slideshare.net/ramezf/security-requirements-engineering-applying-square-framework

Model-Based Management of Information System Security Risk
https://tel.archives-ouvertes.fr/tel-00402996/document

Modeling Security Risks at the Systems Design Stage
https://brage.bibsys.no/xmlui/bitstream/handle/11250/262641/566044_FULLTEXT01.pdf

OWASP: Application Security Cheat Sheet
https://www.owasp.org/index.php/Application_Security_Architecture_Cheat_Sheet

Protecting CUI in Nonfederal Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Secure Tropos: A security-oriented extensión of the Tropos Methodology
http://www.dit.unitn.it/~pgiorgio/papers/IJSEKE06-1.pdf

Secure Software Systems Engineering: The Secure Tropos Approach
https://pdfs.semanticscholar.org/5292/0882f44cc85df656f7de81cc661a436a7ee8.pdf

Measures and Measurement for Secure Software Development
https://www.us-cert.gov/bsi/articles/best-practices/measurement/measures-and-measurement-secure-software-development