UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

DIVISIÓN DE ESTUDIOS DE POSGRADO

TESIS

"Evaluación del nivel de seguridad con patrones"

QUE PARA OBTENER EL TÍTULO DE:

"MAESTRO EN CIENCIAS"

PRESENTA:

OLGA VILLAGRÁN VELASCO

ASESOR:

Dr. Jorge L. Ortega Arjona

Ciudad de México, Noviembre de 2018.

Índice general

Resumen IX

1. Introducción **1**

1.1. Contexto 1

1.2. Problema 3

1.3. Hipótesis 3

1.4. Aproximación 3

1.5. Contribuciones 4

1.6. Estructura de la tesis 4

2. Antecedentes **7**

2.1. ¿Qué es seguridad de la información? 7

2.2. Amenazas a sistemas de información 11

2.2.1. Basados en técnicas de ataque 12

2.2.2. Basados en el impacto de las amenazas 12

2.3. Seguridad en la etapa de diseño de un sistema 13

2.4. Patrones de seguridad 15

2.5. Medición de la seguridad como propiedad de un sistema 19

2.5.1. Medición de la seguridad al implementar Patrones de Seguridad . . . 21

2.6. Resumen 22

3. Trabajo Relacionado **23**

3.1. Metodología para evaluar el nivel de seguridad de un sistema implementando Patrones de Seguridad . . . 23

3.1.1. Introducción . . . 23

3.1.2. Descripción de la metodología . . . 24

3.1.3. Conclusiones del trabajo . . . 25

3.1.4. Semejanzas . . . 26

3.1.5. Diferencias . . . 26

3.2. Evaluación cuantitativa de la seguridad en arquitecturas de software . . . 26

3.2.1. Introducción . . . 26

3.2.2. Descripción de la metodología . . . 27

3.2.3. Conclusiones del trabajo . . . 28

3.2.4. Semejanzas . . . 28

3.2.5. Diferencias . . . 28

3.3. Uso de patrones de seguridad en combinación con métricas de seguridad . . . 29

3.3.1. Introducción . . . 29

3.3.2. Descripción de la metodología . . . 29

3.3.3. Conclusiones del trabajo . . . 31

3.3.4. Semejanzas . . . 31

3.3.5. Diferencias . . . 31

3.4. Resumen . . . 31

4. Evaluación de seguridad al implementar Patrones de Seguridad **33**

4.1. Descripción del método de evaluación . . . 33

4.2. Previos requeridos . . . 35

4.2.1. Requisito de seguridad . . . 35

4.2.2. Patrones de seguridad . . . 36

4.2.3. Modelo de Amenazas 37
4.3. Objetivos de seguridad 39
4.4. Método de evaluación 40
4.5. Interpretación del resultado de la evaluación 48
4.6. Resumen 49

5. Caso de uso del método propuesto **51**

Bibliografía **51**

Índice de Figuras

2.1. Triángulo de objetivos de seguridad *CIA* [35]. 8

3.1. Diagrama de comparación de sistemas. 25

3.2. Gráfica de dependencias obtenida de [11]. 30

4.1. Diagrama a bloques. 34

4.2. Diagrama general de la evaluación del diseño de un sistema. 43

4.3. Selección de objetivo de seguridad correspondiente al requerimiento. 44

4.4. Identificación de la amenaza y ataques correspondientes. 44

4.5. Diagrama del sistema ejemplo. 46

4.6. Indicador de nivel de seguridad en el sistema 48

4.7. Comparación del indicador de nivel de seguridad. 49

Índice de Tablas

2.1. Clasificación de Patrones de Seguridad obtenida de [30] 17

4.1. Ejemplo: Descripción de requerimiento de registro para seguridad de credenciales [22] 35

4.2. Clasificación de requisitos de seguridad 36

4.3. Clasificación de patrones de seguridad 36

4.4. Resumen del Patrón de Seguridad Autorización [6] 37

4.5. Desglose de amenazas del modelo STRIDE 38

4.6. Relación patrones-amenaza de cada objetivo de seguridad 39

4.7. Ejemplo: Registro para seguridad en credenciales 40

4.8. Ejemplo: Descripción de requerimiento de complejidad de contraseñas [22] . 44

4.9. Ejemplo: Registro para seguridad en credenciales 45

Resumen

La seguridad de la información involucra una serie de procesos, herramientas y métodos que al ser implementados en conjunto o individualmente mitigan el daño ocasionado por una amenaza. Poco a poco se da mayor importancia a agregar seguridad en cada una de las etapas del desarrollo de un sistema, utilizando elementos que provean soluciones efectivas y probadas. No obstante, medir qué tan seguro es un sistema es un tema controversial debido a la carencia de evaluaciones que den un resultado confiable y comprobable.

Los Patrones de Seguridad proporcionan una solución probada ante un problema recurrente que coloca a un sistema en peligro de sufrir amenazas. Encontrar una forma de evaluar o aproximar que la implementación de estos patrones proveen de un grado de seguridad al sistema, incentivaría que la industria los utilice de manera cotidiana para aminorar el impacto de dichas amenazas.

En este trabajo, se define un método de evaluación sobre un requisito de seguridad al cual se le da solución aplicado un conjunto de Patrones de Seguridad y analizando como impactan estos en los objetivos de seguridad del sistema. Con esto, se pretende otorgar un dato objetivo para conocer el nivel de seguridad de dicho sistema.

Capítulo 1

Introducción

1.1. Contexto

La información es un activo estratégico para las empresas. La existencia de vulnerabilidades en los sistemas que comprometan la información, pone en riesgo el éxito de la empresa. La seguridad de la información se enfoca en preservar la confidencialidad, integridad y disponibilidad a los datos de un sistema. Debido a la importancia de la información, se crea la rama de la tecnología denominada seguridad informática, encargada de hacer que se cumplan los principios de la seguridad de la información minimizando los riesgos físicos o lógicos a los que esté expuesto el sistema [12, 42, 37].

El área de seguridad de la información es considerada inmadura, uno de los aspectos en los que falta profundizar son los problemas de seguridad asociados al desarrollo de un sistema. Como consecuencia de la inmadurez mencionada, se carece evaluaciones objetivas donde se indique qué tan seguros son los sistemas desarrollados.

Investigaciones recientes se enfocan en generar diseños medibles que indiquen cuán seguro es el sistema que se está diseñando y corregir posibles vulnerabilidades antes de pasar a la etapa de implementación. Los Patrones de Seguridad son una herramienta para diseñar sistemas más seguros [27, 38, 14].

Contar con evaluaciones en seguridad de la información ayuda a la toma de decisiones

relacionadas con dicho activo, ya que el resultado de una evaluación revela la condición de un sistema o la magnitud de un fenómeno ocurrido, lo que permite a los usuarios tomar alguna acción. Entre las razones por las cuales evaluar la seguridad de la información es importante, se encuentra principalmente la económica debido a que se estima una pérdida de entre el 1 % al 5 % la empresa posterior a un ciberataque [2, 38, 5].

Además de las cuestiones económicas que conlleva medir la seguridad de la información, existe la parte tecnológica en el desarrollo de los sistemas. Como lo dijo Lord Kelvin *"Si no puedes medirlo, no podrás mejorarlo"*, la existencia de evaluaciones en esta área también contribuyen a la mejora de la tecnología con la que se desarrollan. Tener una evaluación que indique cuán seguro es el sistema apoya a que los investigadores y desarrolladores de la tecnología mejoren sus productos.

Específicamente, en la etapa de diseño es donde se definen los elementos necesarios para cumplir con los requisitos del sistema. Durante esta etapa intervienen los Patrones de Seguridad, los cuales describen una solución en forma de guías y reglas sobre un problema de seguridad que está asociado a un elemento. Existe una gran variedad de Patrones de Seguridad como la colección mostrada en [34].

Existen métodos que evalúan la seguridad de la información en todas las etapas del desarrollo de un sistema, de la misma forma que existen herramientas para aumentar la seguridad. Por ejemplo, en la etapa de diseño se puede realizar un análisis de ataques o generar un modelo de posibles amenazas.

Se sabe que la seguridad es un tema subjetivo, tornando complejo el querer evaluarlo. No obstante, esta complejidad no ha sido obstáculo para que exista una amplia variedad de estudios enfocados a mejorar el conocimiento que se tiene sobre este tema y de cómo estructurar una evaluación objetiva. Para abordar el problema, primero se debe formalizar el objetivo a alcanzar y las propiedades del sistema, posteriormente se procede a utilizar herramientas formales y automáticas para evaluar la seguridad (las herramientas para evaluar la seguridad deben extrapolarse a cualquier sistema) [2].

1.2. Problema

El problema que aborda esta tesis es la evaluación del nivel de seguridad que otorgan los Patrones de Seguridad como conjunto a un sistema en la etapa de diseño.

Las evaluaciones actuales se enfocan en su mayoría en la etapa de construcción (*build-time*) o durante la etapa de pruebas (*run-time*) donde se tiene parte o el sistema ya desarrollado. La detección de una vulnerabilidad de seguridad en la etapa de pruebas (originada desde la etapa de diseño) genera que tanto diseñadores como desarrolladores hagan modificaciones para minimizarla. La modificación de un sistema ya creado origina problemas ocultos posteriores [4, 11].

1.3. Hipótesis

> *Si se tiene al menos un requisito de seguridad, al incluir en la etapa de diseño Patrones de Seguridad relacionados a un objetivo de seguridad, se puede verificar si el diseño del sistema tiene un nivel de seguridad necesario antes de pasar a la fase de implementación.*

Una evaluación que interactue entre los Patrones de Seguridad y los objetivos de seguridad, que proporcione un parámetro para la toma de decisiones preventivas en la etapa de diseño en lugar de acciones reactivas cuando el sistema o parte de él esté construido.

1.4. Aproximación

Se propone identificar una evaluación que otorgue un parámetro que indique el nivel de seguridad que se proyecta para un conjunto de requisitos de seguridad. Se pretende abordar algunos de los requisitos de seguridad con apoyo de los Patrones de Seguridad.

Las evaluaciones sobre los objetivos de seguridad, dan un indicio de qué tan vulnerable es un sistema ante un ataque.

Se busca que la evaluación conjunte tanto a los objetivos de seguridad, como la eficiencia de los Patrones de Seguridad y las posibles vulnerabilidades desde la etapa de diseño. Para realizar la evaluación, se contempla que desde la fase de análisis se tiene al menos un requisito de seguridad asociado a un requisito funcional.

1.5. Contribuciones

El objetivo principal del presente trabajo es proporcionar una evaluación que contribuya a definir un nivel de seguridad de un sistema a través de incluir Patrones de Seguridad en la etapa de diseño. El análisis de un sistema utilizando esta evaluación apoyaría a diseñadores y desarrolladores en generar sistemas más seguros desde etapas tempranas del desarrollo.

De la misma forma que [21], el presente trabajo se enfoca en promover las buenas prácticas de seguridad desde la etapa de diseño. Un método de prevención es evitar pasar a la etapa de implementación un diseño con vulnerabilidades de seguridad.

1.6. Estructura de la tesis

El presente trabajo se estructura en capítulos, los cuales se describen a continuación:

Capítulo 2 **Antecedentes**

Aquí se presentan los conceptos básicos necesarios para entender el objetivo de la tesis y sus contribuciones, explicando de manera más detallada el por qué de la hipótesis presentada.

Primero, se describe la importancia de proteger la información manipulada por un sistema informático. Después, se describe cómo se encuentra inmersa la seguridad en el diseño de un sistema, donde se explica cómo los Patrones de Seguridad ayudan a prevenir ataques conocidos. Se da una descripción breve de los Patrones de Seguridad y finalmente, se muestran las mediciones relacionadas con la seguridad de los sistemas y las mediciones de los Patrones de Seguridad.

Capítulo 3 **Trabajo relacionado**

En este capítulo, se describe el trabajo relacionado a las métricas asociadas a los Patrones de Seguridad.

Primero, se presenta el artículo titulado "Measuring the level of security introduced by security pattern". En el cual presenta una metodología para comparar dos sistemas sobre el nivel de seguridad que les otorgan los Patrones de Seguridad al ser aplicados.

Posteriormente, se presenta el artículo titulado "Towards a quantitative assessment of security in software architectures". Donde el principal objetivo es proporcionar un valor cuantitativo sobre el nivel de seguridad de un sistema mediante el uso de árboles de requisitos.

Finalmente, se presenta el artículo titulado "Using security patterns to combine security metrics". En este trabajo, se enfocan en seleccionar las métricas correctas relacionadas a los Patrones de Seguridad y cómo interpretar sus resultados.

Capítulo 4 **Evaluación de seguridad al implementar Patrones de Seguridad**

En esta parte de la tesis se presenta de forma general los elementos necesarios para la evaluación propuesta, así como las características que se deben considerar y cómo se debe manipular la información previa requerida.

De manera más detallada, en las subsecciones 4.3, 4.4 y 4.5 se presenta la propuesta de evaluación y cómo interpretar los resultados obtenidos.

Capítulo 5 **Caso de uso del método propuesto**

En este capítulo se utiliza un conjunto de requisitos que representan un diseño de software real, sobre los cuales se aplica el método planteado en el Capítulo 4.

Capítulo 2

Antecedentes

El objetivo de este capítulo es introducir los conceptos de: 1) Qué es la seguridad de la información y su importancia; 2) Cómo se involucra la seguridad en la fase de diseño de un sistema; 3) Qué son los Patrones de Seguridad y 4) Los métodos de medición de seguridad que existen, haciendo énfasis los que se refieren a Patrones de Seguridad.

2.1. ¿Qué es seguridad de la información?

La seguridad de la información tiene el propósito de proteger la información, esto debido a que la información forma parte de los activos de cualquier organización. Proteger la información implica generar controles que preserven los objetivos de integridad, disponibilidad y confidencialidad de los datos [29].

La FISMA (*Federal Information Security Management Act*, por sus siglas en inglés) define tres objetivos de seguridad tanto para la información como para sistemas de información [35, 25]:

Confidencialidad Mantener restricciones sobre el acceso y revelación de información. Este termino incluye dos conceptos:

- Confidencialidad de datos: Asegurar que la información privada o confidencial no está revelada ante individuos no autorizados.

- Privacidad: Asegurar que la información revelada a los individuos sea relacionada con este.

Integridad Prevenir de la modificación o destrucción de la información, incluyendo el no repudio de la información y autenticación. Este termino incluye dos conceptos:

- Integridad de datos: Asegurar que la información y los programas cambian únicamente por una solicitud autorizada o específica.
- Integridad del sistema: Asegurar que un sistema modifica su funcionamiento por cambios autorizados, libre de un cambio no autorizado.

Disponibilidad Asegurar el acceso y uso de la información siempre y cuando sea autorizado, es decir, que el sistema trabaja apropiadamente y no existe una denegación de servicio a usuarios autorizados.

Estos tres conceptos son conocidos como el triángulo CIA (*Confidentiality, Integrity and Availability*, por sus siglas en inglés), el cual representa la relación que tienen estos con la seguridad de la información. No obstante, de estos conceptos se derivan más objetivos de seguridad.

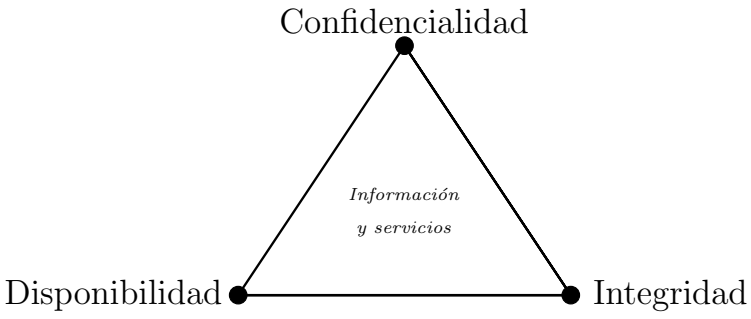

Figura 2.1. *Triángulo de objetivos de seguridad CIA [35].*

En [1] se definen cinco categorías en las que se extrapolan los objetivos de negocio en objetivos de seguridad como se muestra a continuación:

- **Seguridad con prioridad alta**. Determina que es lo que significa *disponibilidad* para el negocio.

- **Seguridad persistente**. Relacionada con el termino de *integridad* que incluye la retención o destrucción de la información de acuerdo con las políticas y objetivos de negocio.
- **Calidad de la información**. Relacionada con la *integridad* que incluye, precisión, relevancia y consistencia de los repositorios.
- **Control de acceso**. Se asegura que lo referente a la *confidencialidad* (protección de la información) sea clara para el negocio.
- **Seguridad técnica**. Cubre la parte de arquitectura de los sistemas de información y el impacto de estos no es directo sobre el negocio.

Proteger la información es de importancia para una organización, por ejemplo [41]:

1. **Proteger la funcionalidad de la organización**. Tiene un impacto en términos de negocio y dinero, ya que podría afectar su funcionalidad.
2. **Permitir que las aplicaciones funcionen de forma segura**. Cuando la operación de la organización depende directamente de las aplicaciones, su impacto radica en que la organización provea del servicio que ofrece de manera correcta y eficiente.
3. **Proteger los datos que la organización recolecta y utiliza**. Si los datos no están protegidos, una organización pierde prestigio ante sus clientes, ya que no brindan garantía de que la información está siendo almacenada o manipulada de manera correcta.
4. **Salvaguarda los bienes tecnológicos de la organización**. Los bienes tecnológicos apoyan a que una organización crezca y consiga sus objetivos, por esto, es de importancia que se salvaguarden.

Para proteger la información se requieren políticas adecuadas. Las políticas de seguridad de la información son un conjunto de criterios descritos en un documento, que sirven para proteger los sistemas y asegurar la información sensible de una organización. Los documentos sobre este tipo se dividen en políticas, estándares, procedimientos, bases y guías, las cuales se detallan a continuación [29, 20]:

- **Las políticas de seguridad de la información** son emitidas para cubrir las expectativas sobre seguridad en los sistemas y ambientes de los usuarios. Se dividen en cuatro niveles:

    1. Organizacional
    2. Programa de seguridad
    3. Usuarios
    4. Sistema y control

- **Los estándares de seguridad de la información** son requisitos más detallados que abordan la selección de metodologías, técnicas y equipos, especificando algún elemento de las políticas de seguridad. Tienen como característica ser obligatorios para todos dentro de la organización.

- **Las guías** también son requisitos detallados, con la diferencia de que no son obligatorios para la organización, más bien son sugerencias de seguridad.

- **Las bases o puntos de referencia**, son los controles de seguridad mínimos que debe cumplir la organización. Detallan los equipos, aplicaciones, configuraciones o actividades relacionados con el control de seguridad en la organización.

- **Los procedimientos** son instrucciones paso a paso de cómo implementar los controles de seguridad definidos en las cuatro políticas anteriores. Principalmente definen el quien y cómo de la aplicación de la seguridad.

La seguridad de la información se divide en las siguientes áreas [13]:

- **Evitar riesgos**. Identifica el valor y riesgo de cada componente de un sistema, incluyendo estrategias para minimizar daños.

- **Disuasión**. Involucra directamente al personal de una empresa, intenta persuadir a estos antes de realizar una acción que perjudique a un sistema.

- **Prevención**. Son los procedimientos que se efectúan para determinar qué necesita protección, quién debe tener accesos y quién es responsable de ciertas actividades para mantener un sistema seguro.

- **Detección**. Aquí se aplican medidas para detectar y reconocer actividades que estén poniendo en riesgo al sistema.

- **Recuperación**. Posterior a un ataque, el área de recuperación se enfoca en devolver al sistema a un estado estable. Esto se realiza mediante respaldos de información, funciones para legitimar a los usuarios que van a acceder de nuevo al sistema, etc.

Dado que un sistema de información crea, procesa, almacena, transmite y/o destruye información, se considera que es seguro si está preparado para minimizar amenazas que comprometan la integridad, confidencialidad y acceso de este recurso. Pensar que un sistema es completamente seguro no es absoluto, ya que la existencia de amenazas no contempladas siempre está latente [24, 31].

2.2. Amenazas a sistemas de información

Se denomina amenaza en los sistemas de información a cualquier acción que dañe o comprometa un recurso como hardware, software, bases de datos, datos, archivos o la red física del sistema. Para que un sistema sea propenso a amenazas, debe existir una vulnerabilidad que se interpreta como una debilidad en el diseño o en el desarrollo del sistema [18].

Actualmente existen métodos que clasifican las amenazas bajo ciertos criterios. Las clasificaciones permiten identificar y entender las características de las amenazas con el objetivo de proteger a los recursos de una organización. Las dos principales clases en las que se dividen estos métodos son basados en técnicas de ataque y basados en el impacto de las amenazas [16, 9].

2.2.1. Basados en técnicas de ataque

En esta clasificación se identifican las amenazas a través de la identificación de especificaciones [9].

- **Análisis paso a paso**. Este método organiza las amenazas en: 1) amenazas de red, 2) amenazas de host y servidor y 3) amenazas de aplicación. La forma en la que se realiza la clasificación es posible cubrir todas las amenazas, aunque su debilidad es que no provee esquema de clasificación mutuamente exclusiva, por ejemplo, un ataque de DoS (*Denial of Service*) afecta tanto a servidores como a la red.

- **Modelo híbrido**. Considera tres criterios principales: 1) frecuencia de la amenaza, 2) área donde la amenaza se focaliza y 3) origen de la amenaza. En particular, esta clasificación se considera dinámica, por ejemplo, una amenaza que tiene una frecuencia alta de aparición puede generar pocas pérdidas o una amenaza que se origine fuera de la organización es más probable que dañe más que una interna.

- **Modelo piramidal**. Se basa en tres factores que identifican las amenazas de alto riesgo en los sistemas de información que son: 1) ¿cuánto sabe el atacante sobre el sistema?, 2) área crítica y 3) pérdidas. Esta clasificación permite identificar las partes vulnerables del sistema y las áreas críticas donde puede afectar una amenaza, una desventaja es que no incluye el impacto de la amenaza.

2.2.2. Basados en el impacto de las amenazas

Los modelos basados en vulnerabilidades o impacto de las amenazas son clasificaciones que agrupan las amenazas del mismo tipo, de las que son más relevantes en impacto y más conocidas [9].

- **STRIDE**. STRIDE son las siglas de *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*, es una clasificación que contempla tanto amenazas de red, host y aplicación. Una de las características de este modelo

es que a cada amenaza le asigna una propiedad de seguridad que es violada y donde impacta.

- **Modelo ISO**. El ISO 7498-2 hace una clasificación en cinco grupos: 1) Destrucción de información y/o recursos, 2) Modificación de la información, 3) pérdida de información y/o recursos, 4) exposición de información y 5) interrupción de servicios. Este modelo presenta una clasificación mutuamente exclusiva aunque no cubre las consecuencias de todos los ataques.

La gran ventaja de estos modelos de clasificación es que desde la fase de diseño se consigue saber cuales amenazas afectarían al sistema que se va a desarrollar.

2.3. Seguridad en la etapa de diseño de un sistema

En la etapa de diseño se define la arquitectura de software o hardware, componentes, módulos, interfaces y datos de un sistema que en conjunto deben satisfacer requerimientos específicos [40].

Al realizar un nuevo sistema o una mejora a uno existente de una empresa, se espera provea un beneficio para esta. La mayoría de los sistemas contienen procesos confidenciales o información sensible de la empresa, por lo tanto, para mantener una postura de seguridad se deben tomar en cuenta las técnicas de seguridad preventivas que eliminen las incertidumbres del comportamiento del sistema en fases posteriores [3].

Un sistema al cual no se le haga una revisión de seguridad desde la etapa de diseño, podría presentar los siguientes problemas [3]:

- Exposición de la información.
- Exhibir la postura de seguridad de la empresa, existiendo la posibilidad de que se refleje en negocio de la empresa.
- En una auditoria, la falta de controles de seguridad en un sistema se convertiría en una evaluación negativa.

- Tomar una medida correctiva ante un problema de seguridad en un sistema ya desarrollado se torna perjudicial para la empresa, principalmente por el costo que conlleva la reparación del problema (en términos de recursos y tiempo) y la dificultad de implementarla (una ingeniería inversa de seguridad se extrapola a un sistema inseguro).

Existen guías que incluyen seguridad en el diseño de un sistema. Estas se expresan en forma de buenas prácticas, principios, algunas políticas, reglas, regulaciones y estándares. El objetivo de las guías es saber qué tan seguro es el diseño de un sistema, las dos principales se describen a continuación [23]:

- **Principios de diseño de seguridad**. Los principios de diseño de seguridad, son reglas probadas para incrementar la seguridad de un sistema, las cuales son aplicadas a problemas específicos. Son identificados durante la etapa de análisis mediante modelado de amenazas. Utilizar estos principios proporciona la ventaja que al identificar una debilidad en el diseño del sistema se pueden tomar decisiones con respecto a la arquitectura e implementación.

- **Patrones de seguridad**. Los Patrones de Seguridad son una solución a un problema de seguridad recurrente, que alienta al rehuso efectivo para construcción de sistemas más robustos. Estos ayudan a manejar un solo requerimiento que es la seguridad de un sistema.

Para incluir la seguridad en el diseño deben existir requisitos de seguridad. El NIST (*National Institute of Standards and Technology* por sus siglas en inglés) en el FIPS 200 muestra un listado de los requisitos de seguridad mínimos que se deben considerar para cualquier sistema de información al que se le quiera incluir seguridad.

En la lista siguiente se muestran los requisitos de seguridad describe el FIPS 200 [26]:

- Control de Acceso
- Conocimiento y Entrenamiento
- Auditoria y Gestión de roles

- Certificación, Acreditación y Evaluaciones de seguridad
- Administración de configuraciones
- Planeación ante contingencias
- Identificación y Autenticación
- Responsable ante incidentes
- Mantenimiento
- Protección de medios de comunicación
- Protección de elementos físicos y entorno de trabajo
- Personal de seguridad
- Evaluaciones de riesgo
- Adquisición de sistemas y servicios
- Protección de sistemas y comunicaciones
- Sistemas e Integridad de la información

2.4. Patrones de seguridad

La definición que Fernández da sobre los Patrones de Seguridad es [34]:

> *"Un Patrón de Seguridad describe la solución a un problema de seguridad recurrente que se genere dentro de un contexto específico y provee un esquema de solución genérico."*

Una de las razones por las cuales los patrones de seguridad son exitosos es que dan una solución que puede ser usada en diferentes situaciones y adaptada para resolver un problema

nuevo dentro del mismo contexto. Capturan la solución y su relación con el problema planteado de manera rápida y accesible. Cabe resaltar que un Patrón de Seguridad se encuentra directamente relacionado con la amenaza y no con la vulnerabilidad [34].

Lo que diferencia a los patrones de seguridad de los patrones tradicionales es el contexto en el que éstos se desenvuelven. Los Patrones de Seguridad tienen una estructura que se compone de los siguientes elementos esenciales: 1) Nombre, 2) Contexto, 3) Problema y 4) Solución. Las características de estos elementos se describen a continuación [34]:

- Contexto. Describe el ambiente y las condiciones en las que el problema de seguridad está ocurriendo.
- Problema. Este se presenta cuando el sistema de software se encuentra en una situación de vulnerabilidad, siendo esta vulnerabilidad una puerta que de motivo a ataques. El problema abarca todos los niveles en la arquitectura del sistema de software.
- Solución. Está fuertemente ligada con el contexto, se diseña para uno o más niveles de la arquitectura del sistema de software y también puede abarcar procesos. La solución estará enfocada según el contexto a la prevención, detección o reacción a un ataque o posible vulnerabilidad.

Algunas de las ventajas del uso de Patrones de Seguridad en el desarrollo de sistemas son [34]:

- Encapsulan el conocimiento básico de seguridad de una forma estructurada y entendible.
- Ayudan a mejorar la integración de la seguridad en los sistemas y empresas.
- Con su uso se extiende la seguridad a todos los niveles de la arquitectura de un sistema.

Clasificar los Patrones de Seguridad sirve para una selección e identificación más adecuada y precisa. Actualmente se han identificado varias clasificaciones con base en criterios o atributos de los patrones, la Tabla 2.1 se muestra una recopilación de las clasificaciones más utilizadas por los investigadores [30].

Clasificación	Atributos
Propósito	Estructural
	De procedimiento
	Ambiente
	Para creación
	Genéricos
Ciclo de vida del sistema	Arquitectónico
	Requisitos
	Diseño
	Análisis
	Implementación
Objetivos de seguridad	Confidencialidad
	Integridad
	Responsabilidad
	Autenticación
	Disponibilidad
	Control de acceso
	Identificación
	No repudio
	Transmisión de datos segura

Tabla 2.1. *Clasificación de Patrones de Seguridad obtenida de [30]*

La lista a continuación muestra algunos Patrones de Seguridad que están incluidos en la clasificación anterior.

Propósito [19, 17]

- **Estructural**. *Account Lockout, Authenticated Session, Client Data Storage, Client Input Filters, Encrypted Storage, Minefield, Network Address Blacklist, Partitioned Application, Password Authentication, Password Propagation, Secure Assertion, Server Sandbox y Trusted Proxy.*
- **De procedimiento**. *Build the Server from the Ground Up, Choose the Right Stuff, Document the Security Goals, Document the Server Configuration, Enroll by Validating Out of Brand, Enroll using Third-party Validation, Enroll with a Pre-Existing Shared Secret, Enroll without Validation, Log for Audit, Patch Proactively, Red Team the Design, Share Responsibility for Security y Test on Staging Server.*
- **Ambiente**. *Limited View y Full View with Errors*
- **De creación**. *Session*

Ciclo de vida del sistema [21].

- **Arquitectónico**. *Distrustful Decomposition, PrivSep (Privilege separation) y Defer to Kernel*
- **Diseño**. *Secure Factory, Secure Strategy Factory, Secure Builder Factory, Secure Chain of Responsibility, Secure State Machine y Secure Visitor*
- **Implementación**. *Secure Logger, Clear Sensitive Information, Secure Directory, Pathname Canonicalization, Input Validation y RAII (Resource Acquisition Is Initialization)*

Objetivos de seguridad [33].

- **Confidencialidad**. *Controlled Access y Secure Data Transmission*
- **Integridad**. *Checkpointed System, Comparator-Checked Fault-tolerant System, Input Guard, Output Guard, Secure Access Layer, Controlled Object Factory, Controlled Process Creator, Server Sandbox*
- **Responsabilidad**. *Replicated System, Session Failover, Session Timeout, Load Balancer, Reverse Proxy*
- **Autenticación y No repudio**. *SAP (Single Access Point) y Check Point*
- **Disponibilidad**. *Secure Logger y Audit Interceptor*
- **Control de acceso**. *Authentication enforcer, Authorization Enforcer, Container-Managed Security, Secure Service Facade, Application Firewall, Demilitarized Zone, Firewall y Single Access Point*
- **Identificación**. *Credential tokenizer, Security Context, Session y Subject Descriptor*
- **Transmisión de datos**. *Obfuscated Transfer Object, Security Association, Secure Message Router y Secure pipe*

Independientemente de la clasificación a la que pertenezcan, los Patrones de Seguridad entran en alguna de las cinco relaciones inter-patrones: *dependencia, beneficios, alternativa, perjudiciales y en conflicto*, que muestran el impacto que tiene aplicar un patrón A junto con un patrón B [33].

Dependencia. Si el patrón A depende del patrón B, entonces es necesario el patrón B para la correcta funcionalidad de A.

Beneficios. Si el patrón A se beneficia del patrón B, entonces, implementar el patrón B incrementa el valor del patrón A.

Alternativa. Los patrones A y B tienen funcionalidad similar, aunque no son identicos.

Perjudiciales. El patrón A se ve perjudicado al implementar el patrón B. Al ser implementados estos patrones se debe verificar que no existan dichos errores en el desarrollo.

En conflicto. El patrón A entra en conflicto con el patrón B, generando inconsistencias. Este caso se da cuando se implementan dos patrones para resolver el mismo problema.

2.5. Medición de la seguridad como propiedad de un sistema

Una de las definiciones más utilizadas para medición es la propuesta por Hermann von Helmholtz en su trabajo denominado *Zählen und Messen*, la cual dice [39]:

> *Es la relación especial que puede existir entre los atributos de dos objetos y la cual designaremos con el nombre de igualdad [...]*
> *Axioma I: Si dos magnitudes son iguales con una tercera, entonces todas ellas son iguales*

Una medición determina [44]:

- Una propiedad o atributo que representa al objeto a ser medido.
- Un estándar que involucra comparar dos objetos entre sí y su relación entre estos basándose en la propiedad.

- Un procedimiento, por el cual se colocan dos objetos bajo las mismas condiciones con el objetivo de observar el resultado y ser capaz de establecer si existe o no una ocurrencia de la relación.

Dado que la definición anterior se enfoca a medir propiedades físicas de los objetos, se requiere una adaptación de esta a la medición del software y aún más a la seguridad sobre este, ya que la seguridad no es una propiedad física, la única forma de medirla es de manera indirecta a través de sus componentes inherentes [44].

Una métrica tiene como objetivo proporcionar un valor escalar que describe una propiedad del sistema, en este caso particular, la propiedad analizada es la seguridad de un sistema. Las métricas de seguridad definidas y usadas en la práctica son relativas debido a que la seguridad es una propiedad que depende de percepciones. Los resultados obtenidos de utilizar una métrica de seguridad, ayudan a la toma de decisiones en varios aspectos de seguridad, que van desde el diseño de una arquitectura, hasta la valoración de la eficiencia y eficacia de las operaciones de seguridad que está ejecutando el sistema [38, 15].

Los principales usos de las métricas de seguridad se pueden incluir en las siguientes categorías:

- **Soporte estratégico**. Brindar garantía de seguridad en un sistema, apoya en la toma de decisiones tales como asignación de recursos, planeación y selección de productos y servicios.
- **Garantía de calidad**. Para minimizar vulnerabilidades en el sistema.
- **Supervisión táctica**. Conocer el estado de un sistema con respecto a la seguridad apoyándose en el control y manejo de riesgos.

Las métricas en seguridad de software se dividen en cuatro categorías [32]:

1. Seguridad desde la perspectiva de ingeniería. Esta categoría se enfoca en verificar procesos.

2. Seguridad desde la perspectiva de negocio. Esta categoría a su vez se divide en nivel organizacional y nivel técnico, el primero se enfoca en los riesgos económicos de mantenimiento y/o procesos y el segundo se enfoca en asegurar al sistema.

3. Seguridad desde la perspectiva de las características. En esta categoría se basan las métricas según la característica de seguridad a analizar.

4. Seguridad desde la perspectiva del sistema. Se enfoca en la parte técnica del sistema, dividiéndose en tres niveles, 1) Métricas a nivel sistema, 2) Métricas a nivel diseño y 3) Métricas a nivel código.

2.5.1. Medición de la seguridad al implementar Patrones de Seguridad

Las investigaciones sobre medición del nivel de seguridad que proporcionan los Patrones de Seguridad se dividen en evaluaciones cuantitativas y cualitativas. Hay evaluaciones que toman de base cómo los Patrones de Seguridad atienden los objetivos de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), otras que se enfocan en identificar las amenazas que los Patrones de Seguridad resuelven.

A continuación se muestran dos metodologías que ejemplifican ambos tipos de evaluaciones a los Patrones de Seguridad:

1. En [43] se muestra una metodología que evalúa el nivel de seguridad que proporcionan los Patrones de Seguridad a la arquitectura de un sistema. Esta metodología selecciona un conjunto de patrones que cumplan cierto objetivo de seguridad de la arquitectura, posterior a eso se les da un peso de acuerdo a la amenaza que mitiguen y con eso obtener un valor que indique sobre las amenazas cuán seguro es la arquitectura.

2. En [10] se muestra una metodología para evaluar las características de los Patrones de Seguridad para verificar el nivel de seguridad que otorgan. La selección de los patrones que analiza se basan en tres criterios: 1) Si es una guía para construir software seguro, 2) Si contemplan hoyos de seguridad de software y 3) Los ataques que mitigan. Esta

metodología contribuye a la selección del conjunto de patrones que mejor otorguen seguridad a un sistema determinado de manera cualitativa.

2.6. Resumen

En este capítulo se presenta una breve introducción a la seguridad de la información, la importancia de incluirla en los sistemas de software y las amenazas a las que están expuestos los sistemas. Se hace un énfasis en la inclusión de la seguridad en la etapa de diseño de un sistema, donde se explica que utilizar guías para proporcionar un nivel de seguridad a un sistema que se esté diseñando disminuye las posibilidades de una amenaza al sistema ya implementado.

Los Patrones de Seguridad al ser parte de las guías para incluir seguridad en el diseño de un sistema y que realmente otorgan un nivel de seguridad debido a la experiencia que involucra la solución propuesta ante ciertas amenazas. También se aborda la clasificación de los patrones y las actuales definiciones de medición de la seguridad como un atributo y la importancia para mejorar la seguridad en los sistemas.

Capítulo 3

Trabajo Relacionado

Este capítulo presentan los trabajos relacionados con el tema de esta tesis, se analizan 1) Metodología para evaluar el nivel de seguridad de un sistema implementando Patrones de Seguridad (*Measuring the level of security introduced by security pattern*), 2) Evaluación cuantitativa de la seguridad en arquitecturas de software (*Towards a quantitative assessment of security in software architectures*) y 3) Uso de patrones de seguridad en combinación con métricas de seguridad (*Using security patterns to combine security metrics*).

Cada sección se organiza presentando una introducción de lo propuesto en el trabajo relacionado, donde se describe el problema, los objetivos y la solución a éste. Brevemente se describe la solución propuesta con los resultados obtenidos y por último se presentan las conclusiones del trabajo.

3.1. Metodología para evaluar el nivel de seguridad de un sistema implementando Patrones de Seguridad

3.1.1. Introducción

Se han buscado formas de evaluar la implementación de Patrones de Seguridad para mejorar la seguridad en los sistemas, muchos autores se enfocan a la evaluación individual de los patrones y no como un todo, por esto en el artículo *"Measuring the level of security*

introduced by security pattern" [7] la pregunta abordada es ¿qué grado de seguridad alcanza un sistema usando los Patrones de Seguridad en su construcción? y la solución propuesta es una metodología para construir sistemas seguros a través del uso de Patrones de Seguridad y su evaluación sobre los posibles ataques definidos como patrones de mal uso.

La metodología consiste en una comparación de dos sistemas construidos bajo los mismos requisitos, con la diferencia que uno de ellos implementa Patrones de Seguridad en el diseño y el otro no. Se consideran las amenazas que pueden sufrir los sistemas y son asociadas a un determinado patrón de mal uso. Entonces, para realizar la evaluación, ambos sistemas son sometidos a la misma cantidad de amenazas y se observa cuantas de ellas consiguen ser mitigadas por cada sistema. El conjunto de relaciones entre amenazas mitigadas por Patrones de Seguridad son comparadas entre los sistemas. Este valor indica qué tan seguro es el software.

3.1.2. Descripción de la metodología

1. **Identificación de amenazas del sistema**. Esta metodología se basa en que existen requisitos previos, entonces, tomando esos requisitos se buscan las posibles amenazas que pudieran afectar al sistema una vez construido. Una vez identificadas, se procede a la elección de Patrones de mal uso que las definan.

2. **Elección de Patrones de mal uso**. Las amenazas a un sistema pueden expresarse como Patrones de mal uso que son una forma de proyectar la amenaza de acuerdo a su objetivo. Existen más de un Patrón de mal uso para realizar cierto tipo de ataques, por lo que los autores asociaron una cantidad de éstos patrones a un tipo de amenaza para la metodología.

3. **Elección de Patrones de Seguridad**. Dado que los Patrones de Seguridad proveen soluciones ante una amenaza específica, los autores utilizaron la asociación amenaza-patrones de mal uso anterior para relacionar a los patrones directamente con la amenaza de seguridad que estos mitigan y su grupo de Patrones de mal uso.

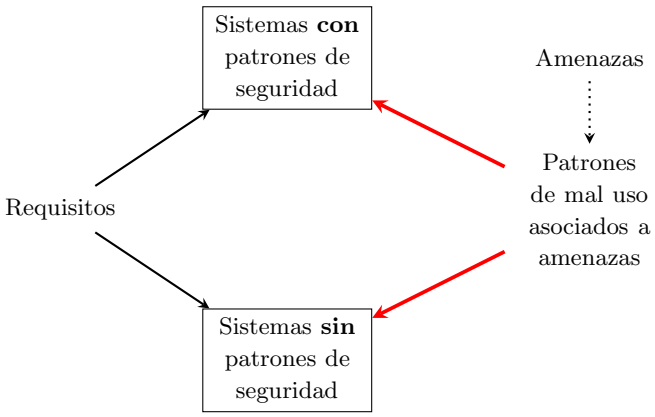

Figura 3.1. *Diagrama de comparación de sistemas.*

4. **Evaluación de los sistemas**. Para la evaluación, la metodología propone la construcción de dos sistemas bajo los mismos requisitos, uno de los sistemas es diseñado con Patrones de Seguridad y el otro sin ellos. Entonces, se realiza la comparación de los sistemas enumerando el conjunto de amenazas mitigadas por cada sistema. La aplicación de la metodología permite una estimación de la seguridad que están adicionando los Patrones de Seguridad.

Como se puede apreciar en la Figura 4.5, ambos sistemas son sometidos a la misma cantidad y tipo de amenazas, por lo que el resultado arrojado de la evaluación da un parámetro que indica el nivel de seguridad que otorga un conjunto de Patrones de Seguridad a un sistema. Una ventaja de esta metodología es que realiza una evaluación de un sistema completo y no solo de un Patrón de Seguridad desde la fase de diseño. Cabe resaltar que la evaluación no determina si los Patrones de Seguridad son implementados correctamente, para ello se requiere pasar a la fase de pruebas.

3.1.3. Conclusiones del trabajo

Un sistema de software que ha sido diseñado utilizando los Patrones de Seguridad es capaz de detener cada amenaza esperada y se puede considerar al sistema seguro a un nivel de modelado. Además, este trabajo plantea definir de manera más precisa la relación entre los patrones de mal uso y las metas de los atacantes para mejorar el análisis del sistema como un todo.

3.1.4. Semejanzas

- Busca identificar si los patrones de seguridad proporcionan un nivel de seguridad a un sistema
- Realiza la evaluación de un sistema completo
- Evalúa un conjunto de Patrones de Seguridad
- Desde la fase de diseño se realiza una estimación de la cantidad de seguridad agregada al utilizar Patrones de Seguridad

3.1.5. Diferencias

- Propone una metodología y no una métrica
- La comparación se realiza una vez construidos los sistemas
- Se enfoca en la relación que existe entre los Patrones de Seguridad y los Patrones de mal uso

3.2. Evaluación cuantitativa de la seguridad en arquitecturas de software

3.2.1. Introducción

La literatura que se encuentra sobre evaluación de la seguridad se enfocan a medir la seguridad después de haber desarrollado un sistema y debido a que actualmente los sistemas son más grandes y heterogéneos, la evaluación después de construido el sistema se convierte en algo más complejo. En el artículo *"Towards a quantitative assessment of security in software architectures"* [43] propone una metodología que arroja un valor cuantitativo sobre el nivel de seguridad que proporcionan los Patrones de Seguridad a determinado requerimiento y sobre las amenazas de seguridad más relevantes desde la fase de diseño sin importar la tecnología a utilizar en la implementación.

Antes de aplicar la metodología que proponen como solución en este trabajo, se realiza una relación entre requerimientos de seguridad y los Patrones de Seguridad mediante el uso de los objetivos de seguridad como intermediarios, debido a que proveen una abstracción conceptual de los requisitos. A partir de esta relación se comienza con el árbol de requisitos que se va detallando con la metodología planteada.

3.2.2. Descripción de la metodología

Esta metodología se divide en 4 partes [43]:

1. **Mapeo de amenazas con los objetivos de seguridad**. Haciendo uso de la metodología STRIDE de Microsoft, se seleccionan las amenazas que estén relacionadas con el modelado del software. Cada amenaza es organizada en árboles de amenaza y descompuesto a lo más en tres niveles.

2. **Clasificación de las amenazas de acuerdo a su severidad**. Dado que cada amenaza tiene un grado de severidad diferente, se recurre a una clasificación otorgándoles pesos a cada amenaza para diferenciarlos. Cada peso estará determinado por el nivel de riesgo definido en la DREAD de Microsoft.

3. **Determinación de la protección ante una amenaza**. Para determinar el nivel de protección que otorga un patrón de seguridad ante una amenaza, se asocian las amenazas a los objetivos de seguridad a los que el patrón contribuye.

4. **Cálculo de la cobertura de seguridad**. El cálculo se realiza por rama en el árbol de amenazas. Las hojas del árbol representarán el valor de protección que otorgan los patrones de seguridad para un requisito

Para incorporar los datos obtenidos de la metodología a los objetivos principales del sistema, a cada requisito se le asigna un peso de acuerdo al impacto de una falla en éste (perdidas monetarias) y el cálculo de la cobertura de seguridad de dicha rama.

La parte experimental para la evaluación de esta metodología se baso en realizar dos sistemas con los mismos requisitos, con una estrategia diferente para la selección de los Patrones

de Seguridad. El primero se enfocó en seleccionar un conjunto de Patrones de Seguridad que cubriera lo mínimo pero suficiente los requisitos; el segundo se enfocó en proporcionar la mejor solución de seguridad sin importar el costo de implementación.

3.2.3. Conclusiones del trabajo

La metodología propuesta es aplicada a un alto nivel de abstracción del diseño de software para encontrar posibles errores lo más rápido posible. Tanto el uso de árboles de objetivos de seguridad y amenazas dan un panorama debido a que las amenazas están en constante cambio. Se hace un énfasis en que los niveles de seguridad para los requerimientos fueron asignados de manera empírica por la experiencia de los autores.

3.2.4. Semejanzas

Este trabajo relacionado se asemeja en el presente trabajo de tesis en:

- Hace una evaluación cuantitativa
- Utiliza metodologías probadas para relacionar los requisitos de seguridad con los patrones de seguridad (STRIDE)
- Marca una secuencia para la definición de los patrones

3.2.5. Diferencias

- No utiliza la métrica directamente en la evaluación del patrón de seguridad
- Requiere la evaluación de un experto para elegir el peso de las amenazas

3.3. Uso de patrones de seguridad en combinación con métricas de seguridad

3.3.1. Introducción

Uno de los problemas analizados en la evaluación de los Patrones de Seguridad es la correcta selección de métricas para la medición de seguridad y su interpretación. En el artículo titulado *"Using security patterns to combine security metrics"* [11], se propone un método que al evaluar la correcta selección de los Patrones de Seguridad sobre un sistema se proporciona un indicador sí estos consiguen resolver un objetivo de seguridad.

3.3.2. Descripción de la metodología

La metodología consiste en 3 pasos [11]:

1. **Definición de Patrones de Seguridad a partir de los objetivos**
   Esta metodología considera que existen requisitos de seguridad, los cuales deben ser extrapolados a uno o más objetivos de seguridad. Un vez que se tienen especificados los objetivos, se buscan los Patrones de Seguridad que contribuirán al cumplimiento de cada objetivo.

2. **Selección de métricas**
   El proceso de selección de métricas va implícito en la selección del Patrón de Seguridad. Cabe resaltar que los resultados de las métricas son relevantes para los objetivos de seguridad. Los autores proponen el uso de gráficas de dependencias, las cuales facilitan la selección de métricas y dichas gráficas son construidas en la etapa de diseño. Para cada requerimiento de seguridad se define una gráfica de dependencia. Cada gráfica consiste en tres capas:

   - Objetivos de alto nivel. Aquí se identifica la relación entre diferentes objetivos de seguridad.

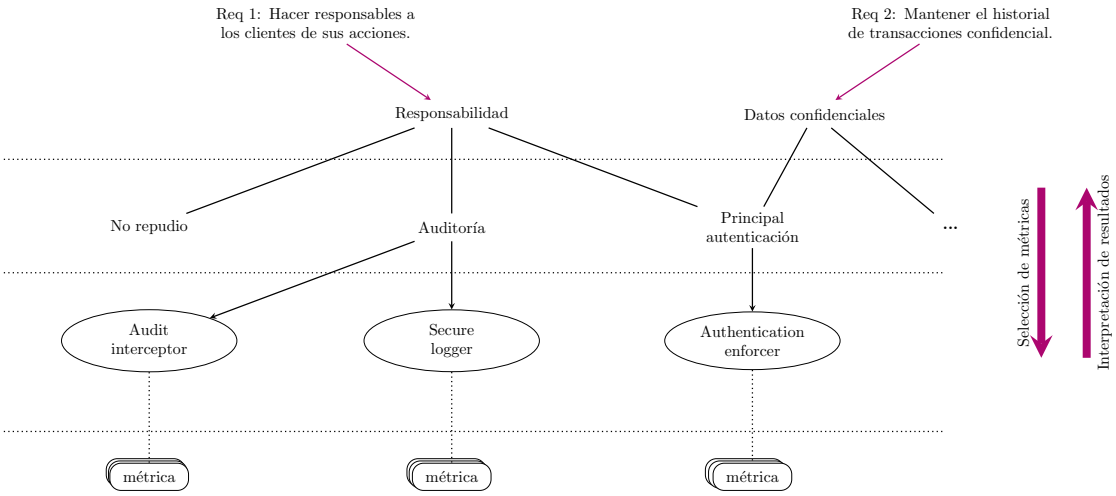

Figura 3.2. *Gráfica de dependencias obtenida de [11].*

- Objetivo de seguridad resuelto por un patrón. Uno o más Patrones de Seguridad pueden colaborar para resolver un objetivo de seguridad. En esta capa, se describe si existe esa relación o no.

- Métricas de Patrones de Seguridad. En esta última capa, son agregadas las métricas a los patrones que se están evaluando.

3. **Interpretación de resultados**

   Los resultados obtenidos de las métricas son interpretados en el contexto del Patrón de Seguridad a los que están asociados. Con ellos, se puede comprobar si el Patrón de Seguridad está siendo correctamente implementado. Si un resultado no es el deseado, se puede recurrir a la gráfica de dependencia para localizar qué Patrón de Seguridad no está siendo bien aplicado y corregirlo desde la fase de diseño. Un ejemplo de una gráfica de dependencias se muestra en la Figura 3.2, donde a los Patrones de Seguridad son relacionados con las métricas correspondientes; también se tiene que más de un patrón pueden resolver una característica de seguridad como *Audit Interceptor* y *Secure Logger* la Auditoría.

3.3.3. Conclusiones del trabajo

La solución en este trabajo pretende hacer una integración fácil de las métricas y su asociación con los Patrones de Seguridad, dicha asociación permite obtener un estado del nivel de seguridad del sistema a través de sus objetivos de seguridad. En particular, la solución toma en cuenta las métricas sobre lo que debería hacer el sistema sin tratar de detectar ataques específicos.

3.3.4. Semejanzas

Este trabajo relacionado se asemeja en el presente trabajo de tesis en:

- Se basan en patrones de seguridad para determinar el nivel de seguridad de un sistema
- Usa métricas para determinar el correcto funcionamiento de un Patrón de Seguridad
- Hace el análisis en la fase de diseño

3.3.5. Diferencias

- Utiliza métricas ya establecidas por cada Patrón de Seguridad y evalúa cada uno.
- La metodología sirve para identificar si hay posibles errores en los Patrones de Seguridad e identificar que objetivo de seguridad es el que no se está cumpliendo.

3.4. Resumen

En este capítulo se presenta el resumen de tres trabajos relacionados con la evaluación de los Patrones de Seguridad. En el primer trabajo se habla de una metodología para evaluar la seguridad de los patrones en todo el sistema y no de manera individual. La metodología se divide en cuatro fases que son: 1) identificación de amenazas, 2) selección de patrones de mal uso, 3) selección de patrones de seguridad y 4) evaluación de los sistemas. El principal

objetivo de este trabajo es hacer una evaluación a un sistema contemplando la evaluación de todos los Patrones de Seguridad seleccionados y no de uno a uno.

El segundo trabajo hace una evaluación de los Patrones de Seguridad dependiendo de los objetivos de seguridad y la severidad de las amenazas. En particular este trabajo presenta una metodología que otorga un valor de seguridad del sistema y se divide en cuatro fases que son: 1) mapeo de amenazas con los objetivos de seguridad, 2) clasificación de las amenazas de acuerdo a su severidad, 3) determinación de la protección ante la amenaza y 4) el cálculo de la cobertura de seguridad.

Por último, el tercer trabajo presenta una metodología que permite elegir los Patrones de Seguridad con respecto a los objetivos de seguridad y las métricas que evaluarán a los patrones. La metodología se divide en tres fases que son: 1) definición de los Patrones de Seguridad a partir de los objetivos de seguridad, 2) selección de métricas y 3) interpretación de resultados. Este trabajo tiene como objetivo integrar las métricas a la evaluación de un sistema que está utilizando los Patrones de Seguridad.

Capítulo 4

Evaluación de seguridad al implementar Patrones de Seguridad

El objetivo principal de este capítulo es describir un método que permita evaluar la seguridad de un sistema al implementar Patrones de Seguridad en el diseño del mismo. En la primera sección se describe a grandes rasgos los elementos necesarios para realizar la evaluación.

En las secciones posteriores se describen a detalle cada una de las etapas para realizar la evaluación propuesta.

4.1. Descripción del método de evaluación

En la Figura 4.1 se muestra el diagrama a bloques que representa las etapas necesarias para realizar la evaluación propuesta. En las subsecciones siguientes se describen a grandes rasgos cada una de ellas, siendo la primera etapa los previos requeridos y las tres etapas subsecuentes en las que se enfoca el desarrollo de este trabajo.

1. **Previos requeridos**

   a) *Requisito de seguridad.* Documento que incluye una necesidad de seguridad para el sistema a desarrollar.

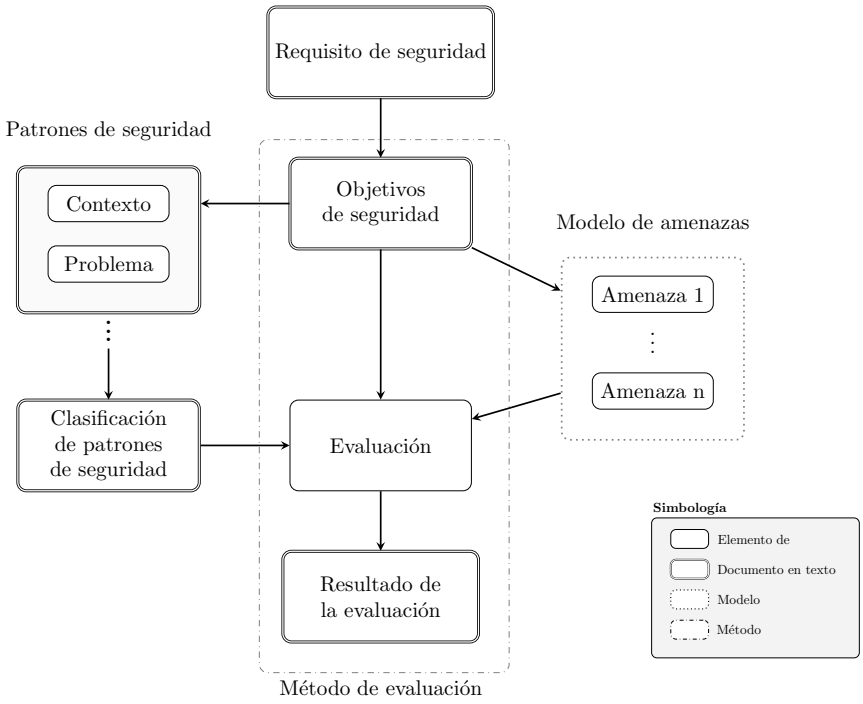

Figura 4.1. *Diagrama a bloques.*

b) *Patrones de seguridad*. Selección de Patrones de Seguridad que mitiguen las amenazas hacia los objetivos de seguridad identificados.

c) *Modelo de amenazas*. Conjunto de amenazas que atentan contra los objetivos de seguridad identificados.

2. **Objetivos de seguridad**. Identificación de los objetivos de seguridad que van relacionados con el requisito de seguridad.

3. **Método de evaluación**. Definición de criterios utilizando los datos recolectados de las etapas dos a cuatro.

4. **Resultado de la evaluación**. Aplicación del método de evaluación para obtención de un resultado que indique el nivel de seguridad que los Patrones de Seguridad otorgan al sistema.

4.2. Previos requeridos

4.2.1. Requisito de seguridad

Para realizar el diseño de un software que incluya seguridad, es necesario contar con al menos un requisito de seguridad. El requisito de seguridad se debe recolectar al mismo tiempo que se han recolectado los requisitos funcionales y no funcionales del sistema a desarrollar.

Dado que los requisitos de seguridad varian con respecto al proyecto que se está diseñando, el presente trabajo considera los requisitos de seguridad mínimos que contempla el NIST en el FIPS 200 mencionados en la Sección 2.1, la Tabla 4.1 muestra un ejemplo de un requisito de seguridad basado en dicho listado.

Requerimiento ID:	**Categoría: Seguridad**
Subcategorías	Autenticación, Credenciales, Contraseñas, Hashing
Nombre	Seguridad de credenciales
Requerimiento	El sistema debe almacenar la información utilizada para la autenticación de manera segura, utilizando algoritmos criptográficos públicos y aceptados.
Caso de uso	Almacenamiento de contraseñas
Fundamento	La información de autenticación debe ser almacenada de manera que un tercero sin autorización no pueda obtenerla fácilmente.
Prioridad	Crítica
Restricciones	N/A
Comentarios	Utilizar datos aleatorios (*salting*) por usuario es recomendado para el almacenamiento de los hash de las contraseñas para proveer un nivel de seguridad mayor
Número de caso de prueba	-

Tabla 4.1. *Ejemplo: Descripción de requerimiento de registro para seguridad de credenciales [22]*

Para fines de este trabajo, se propone la clasificación mostrada en la Tabla 4.2. Donde se utilizan los requisitos mínimos definidos en [26] y asignando a cada uno la categoría que le corresponde de [1] con la nomenclatura mostrada a continuación:

1. SPA *Seguridad con prioridad alta*
2. SP *Seguridad persistente*
3. CI *Calidad de la información*
4. CA *Control de acceso*

5. ST *Seguridad técnica*

Requisito	**Categoría**	**Objetivo de seguridad**
Control de Acceso	CA	Confidencialidad
Conocimiento y Entrenamiento	ST	No aplica
Auditoria y Gestión de roles	CI / CA	Integridad / Confidencialidad
Certificación, Acreditación y Evaluaciones de seguridad	SP	Integridad
Administración de configuraciones	SP	Integridad
Planeación ante contingencias	SP	Integridad
Identificación y Autenticación	CA	Confidencialidad
Responsable ante incidentes	ST	No aplica
Mantenimiento	ST	No aplica
Protección de medios de comunicación	SPA	Disponibilidad
Protección de elementos físicos y entorno de trabajo	ST	No aplica
Personal de seguridad	ST	No aplica
Evaluaciones de riesgo	SPA	Disponibilidad
Adquisición de sistemas y servicios	ST	No aplica
Protección de sistemas y comunicaciones	SPA	Disponibilidad
Sistemas e Integridad de la información	CI	Integridad

Tabla 4.2. *Clasificación de requisitos de seguridad*

Con los resultados de la Tabla 4.2, dado un requisito de seguridad se define la clasificación a la que pertenece, obteniendo con esto el objetivo de seguridad que abarca y que se requiere para la etapa mostrada en la Sección 4.3.

4.2.2. Patrones de seguridad

Para fines del presente trabajo se utiliza la clasificación mostrada en la Tabla 2.1 en el punto de objetivos de seguridad con las modificaciones mostradas a continuación en la Tabla 4.3.

Subcategorías	**Objetivo de seguridad**
Responsabilidad	Confidencialidad
Autenticación	
Identificación	
No repudio	
Control de acceso	Integridad
Transmisión de datos segura	Disponibilidad

Tabla 4.3. *Clasificación de patrones de seguridad*

Ejemplo

Un resumen del Patrón de Seguridad **Autorización** se muestra en la Tabla 4.4:

Característica	Descripción
Descripción	El patrón **Autorización** describe quién está autorizado para acceder a recursos específicos del sistema, dentro de un ambiente que requiere acceso controlado. El modelo indica, por cada sujeto activo, a cuales recursos tiene acceso y que puede hacer con ellos.
Contexto	Un ambiente computacional que tiene recursos valiosos para los usuarios u organización.
Problema	Se necesita una forma de controlar el acceso a los recursos, si no cualquier entidad (usuario, proceso) puede acceder a cualquier recurso y originar problemas de confidencialidad e integridad. ¿Cómo se puede describir quién está autorizado para acceder a recursos específicos en el sistema? La solución a este problema debe resolver las siguientes fuerzas: **Independencia**. La estructura de control de recursos debe ser independiente del tipo de recursos y debe aplicar para todos ellos. **Flexibilidad**. La estructura de control de recursos debe ser lo suficientemente flexible para acomodar diferentes tipos de usuarios y recursos. **Capacidad de cambio**. Debe ser fácil modificar los derechos de entidades activas en respuesta a cambios en sus funciones o responsabilidades. **Seguridad**. La estructura de control de recursos debe ser segura apesar de la manipulación.
Implementación	Una organización de acuerdo con sus políticas, debe definir todos los acesos que se requieren para los recursos. La política más común es *need-to-know*, en la que entidades activas reciben derechos de acuerdo a sus necesidades.El patrón *autorización* está descrito de manera abstracta y algunas implementaciones son posibles: las dos más comunes son *lista de control de acceso* y *capacidades*. La lista de control de acceso indica quienes tienen acceso a los objetos protegidos, mientras que las capacidades son asignadas a procesos para definir la ejecución de los derechos. Los tipos de accesos pueden estar orientados a aplicación.
Usos conocidos	Este patrón define los tipos más básicos de reglas de autorización, se pueden crear modelos más complejos de control de acceso. Está basado en el concepto de matriz de acceso, un modelo fundamental de seguridad. Es el sistema básico de control de acceso para los más comerciales sistemas operativos y bases de datos, como UNIX, Windows, Oracle entre otros.

Tabla 4.4. *Resumen del Patrón de Seguridad Autorización [6]*

4.2.3. Modelo de Amenazas

Los modelos de amenazas son una forma ya establecida de hacer un análisis de las posibles amenazas que puede sufrir un sistema conociendo los objetivos de seguridad establecidos en él. Son un conjunto de amenazas que ayudan a identificar desde la fase de diseño posibles vulnerabilidades del sistema.

En el presente trabajo, el modelo de amenazas se utiliza para conseguir identificar contra qué exactamente están protegiendo al sistema de información los Patrones de Seguridad. El modelo seleccionado es el STRIDE que se basa en técnicas de generación de información (por su definición en inglés *elicitation techniques*), una de las ventajas de este modelo es que dichas técnicas permiten que quienes lo utilizan (estén o no familiarizados con el modelo) sepan como utilizar la información proporcionada y así descubrir las amenazas.

Como se menciona en el Capítulo 2.6 el acrónimo STRIDE proviene de las palabras en inglés ***S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service y **E**levation of privilege*, donde cada una de las amenazas que contempla es el contrario de algunas propiedades de un sistema como autenticación, integridad, no repudio, confidencialidad, disponibilidad y autorización.

Para el presente trabajo, al modelo de amenazas STRIDE se le agrega una clasificación con los objetivos de seguridad que cada amenaza afecta directamente. Esta modificación se realiza con el fin de incluir dichas amenazas a la evaluación propuesta. La información que proporciona STRIDE con las modificaciones realizadas se muestra en la Tabla 4.5.

Amenaza	**Propiedad violada**	**Definición de amenaza**	**Víctimas típicas**	**Objetivo de seguridad**
Suplantación	Autenticación	Pretender ser algo o alguien diferente	Procesos Entidades externas Personas	Confidencialidad
Modificación	Integridad	Modificar algo en: disco, memoria o red	Almacenamiento de datos Flujo de datos Procesos	Integridad
Repudio	No repudio	Alegar que no se es responsable por alguna acción	Procesos	Confidencialidad
Información expuesta	Confidencialidad	Proveer información a alguien no autorizado de verla	Procesos Datos Almacenamiento Flujos de datos	Confidencialidad
Denegación de servicio	Disponibilidad	Consumir recursos necesarios para proveer el servicio	Procesos Fatos Almacenamiento Flujos de datos	Disponibilidad
Elevación de privilegios	Autorización	Permitir que alguien no autorizado realice alguna actividad	Procesos	Integridad

Tabla 4.5. *Desglose de amenazas del modelo STRIDE*

4.3. Objetivos de seguridad

Partiendo de los objetivos de seguridad (Integridad, Confidencialidad y Disponibilidad) se hace una relación entre la clasificación de los Patrones de Seguridad y las respectivas amenazas mostradas por STRIDE, haciendo el llenado de la Tabla 4.6.

Dado el requisito de seguridad, se deben identificar los Patrones de Seguridad que contribuyen con la solución al requisito.

	Integridad			Confidencialidad		Disponibilidad
	Suplantación	Repudio	Información expuesta	Modificación	Elevación de privilegios	Denegación de servicio
Autenticación						
Responsabilidad						
Identificación						
No repudio						
Control de acceso						
Transmisión de datos segura						

Tabla 4.6. *Relación patrones-amenaza de cada objetivo de seguridad*

Ejemplo

Si se tiene el requisito de seguridad mostrado en la Tabla 4.1, los Patrones de Seguridad que tanto en su contexto como en el problema contribuyen en la solución del mismo son *Credential* [34] y *Credential tokenizer* [36]. El primero se enfoca en el correcto almacenamiento de la información referente a la autenticación y autorización de un usuario y el segundo provee mecanismos para encapsular un token seguro.

Como se menciona en el Capítulo 2, los patrones no se contraponen, por lo tanto, considerar estos patrones es factible. Una vez identificados todos los patrones, se procede a realizar el llenado de la Tabla 4.9.

El llenado se realiza con marcas (✓) en cada una de las categorías, si el Patrón de Seguridad en su solución involucra otro objetivo de seguridad se coloca una marca a menos de que exista un patrón de seguridad que ya esté solucionando dicho objetivo de seguridad.

	Integridad			Confidencialidad		Disponibilidad
	Suplantación	Repudio	Información expuesta	Modificación	Elevación de privilegios	Denegación de servicio
Autenticación			✓			
Responsabilidad			✓			
Identificación						
No repudio						
Control de acceso					✓	
Transmisión de datos segura						

Tabla 4.7. *Ejemplo: Registro para seguridad en credenciales*

La Tabla 4.9 tiene la función de proporcionar un panorama general de cómo se está comportando cada requisito de seguridad en el negocio de la empresa y con la información de cada requisito se procede a la siguiente fase de la evaluación mostrada en la Sección 4.4.

4.4. Método de evaluación

El método de evaluación propuesto, pretende que la seguridad inmersa en el diseño de un sistema de información sea evaluada y entregar un parámetro que indique el nivel de seguridad de éste.

Para el análisis, se considera que existe al menos un requisito de seguridad. Cada requisito debe estar adecuadamente clasificado, identificando el objetivo de seguridad atiende. En caso de existir una ambigüedad en la clasificación se debe replantear el requisito.

La clasificación de los requisitos de seguridad se realiza considerando que los objetivos de seguridad son independientes, es decir, no hay un requisito de seguridad que atienda a más de un objetivo de seguridad y no hay ataques que atenten contra más de un objetivo de seguridad.

Una vez que se tienen los requisitos de seguridad del sistema con la clasificación correspondiente, se desarrolla la parte de los ataques a los que se está expuesto el sistema. Como lo visto en la sección 4.2.3 se define para cada objetivo de seguridad las amenazas a las que está expuesto, las cuales para el método de evaluación son un conjunto de ataques.

Debido a que existe un gran número de ataques, el método de evaluación solo contempla los ataques más conocidos como parámetro base los cuales están clasificados en el modelo de amenazas. En caso de existir un requisito de seguridad donde se conozcan los ataques que intenta evitar y sobre los cuales existan estadísticas, se debe replantear el diseño del diagrama para incluirlos en el grupo de amenazas.

Posteriormente, conociendo ya los requisitos de seguridad del sistema se realiza una búsqueda en un catálogo de Patrones de Seguridad de los patrones que ayuden a mitigar los ataques a los que se está expuesto. Se conoce que dado a la cantidad de amenazas no existe un número suficiente de Patrones de Seguridad que cubran todas, por lo tanto, hay requisitos que no son atendidos por ningún Patrón de Seguridad.

Teniendo el diagrama completo con los requisitos, las amenazas y los patrones, se procede a realizar la evaluación de la seguridad del diseño del sistema.

Como primer paso, se obtiene el impacto de los requisitos sobre cada objetivo de seguridad. El impacto que cada objetivo de seguridad tiene en el diseño del sistema se obtiene como:

$$OS = \frac{\sum_i Req_i(OS)}{N}$$

Donde OS es el objetivo de seguridad que se está evaluando, $Req(OS)$ es el requisito que atiende a dicho objetivo de seguridad y N es el total de requisitos de seguridad del sistema.

Como paso dos, se debe encontrar el peso que tienen las amenazas sobre ese objetivo de seguridad, el cual está representado como w_{OS}. Para este paso se cuenta con tres fases:

1. Con los resultados de la búsqueda de Patrones de Seguridad, se relaciona cada uno al ataque que mitigan. En caso de que si exista un patrón se asigna un valor de $v_p = 0$ que indica que existe una mitigación del ataque[1], si no existe al menos un patrón que mitigue el ataque se asigna un valor de $v_p = 1$ indicando que dicho ataque persiste.

2. Se debe contar con la probabilidad de que ocurran los ataques contemplados para el

[1]Este valor no indica que el ataque desaparece.

sistema que se está diseñando[2]. Cada ataque cuenta con una probabilidad de que ocurra representada como $P(atq)$.

Esta fase depende de la anterior. Si existe al menos un Patrón de Seguridad ligado a un ataque dentro del diagrama, se multiplica el valor asignado a ese patrón por la probabilidad de que ocurra el ataque.

3. Por último, se calcula la probabilidad de que ocurra una amenaza al sistema, es decir, que exista la posibilidad de que se genere un ataque. Esta probabilidad se ve definida por:

$$P(amenaza) = P(atq_1) + P(atq_2) + ... + P(atq_M)$$

Donde, la probabilidad $P(amenaza)$ es la suma de todas las probabilidades de ataques definidos en el diagrama. Considerando que los ataques son independientes uno de otro de que ocurran.

Para obtener los pesos de las amenazas que atentan contra un objetivo de seguridad, se suman las probabilidades de las amenazas correspondientes.

- $w_I = P(S) + P(R) + P(I)$
- $w_C = P(M) + P(E)$
- $w_D = P(D)$

Como último paso de la evaluación, se obtiene el total de la seguridad del sistema. El total de la seguridad en el sistema ss está definida como :

$$ss = w_I \cdot I + w_C \cdot C + w_D \cdot D$$

Donde, cada evaluación de los objetivos de seguridad independiente es multiplicada por el peso de las amenazas que atentan contra él. La seguridad del diseño del sistema esta definido por la suma de estas evaluaciones.

[2]La probabilidad de que exista cada ataque es considerada basada en estadísticas de ataques a sistemas ocurridos en años pasados, pensando que en el tiempo se siguen comportando de la misma forma para la aplicación del método de evaluación propuesto [28].

En el caso de que no exista ningún requerimiento que atienda a un objetivo de seguridad, el valor de dicho objetivo no es contemplado. Por lo tanto, el peso de la amenaza del objetivo pasa directamente a la ecuación de la seguridad en el sistema. Por ejemplo, si no existe ningún requisito que atienda la Integridad, la ecuación de ss se representa como:

$$ss = w_I \cdot I + w_C \cdot C + w_D \cdot D$$

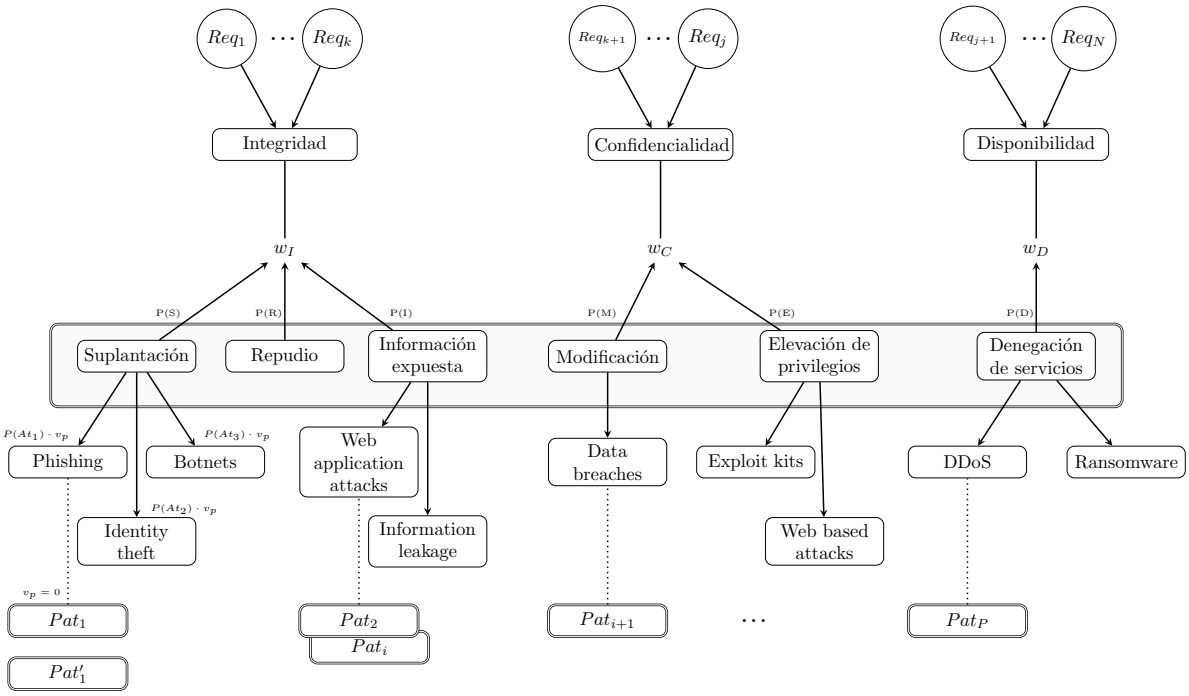

Figura 4.2. *Diagrama general de la evaluación del diseño de un sistema.*

Ejemplo

Supongamos que se tiene el requerimiento mostrado en la Tabla 4.8 el cual impacta en el objetivo de seguridad de *Integridad*.

Un sistema que no contemple seguridad en contraseñas, está expuesto a amenazas relacionadas con *Información expuesta*, dentro de los cuales se encuentran los siguientes ataques:

- Ataques de diccionario
- Ataque de espionaje de teclado

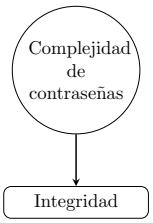

Figura 4.3. *Selección de objetivo de seguridad correspondiente al requerimiento.*

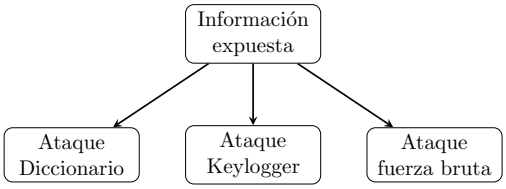

Figura 4.4. *Identificación de la amenaza y ataques correspondientes.*

- Ataque de fuerza bruta

Una vez identificado el objetivo de seguridad que se está evaluando, se procede a llenar la tabla de los Patrones de Seguridad que mitigan las amenazas hacia ese objetivo de seguridad.

Para el ejemplo que se está planteando, se tienen los siguientes patrones de seguridad:

1. Password design and use :

   - Contexto: Se debe seleccionar un mecanismo de contraseñas para autenticar usuarios en un segmento de un sistema de información. La persona que aplique este patrón entiende los requerimientos de identificación y autenticación
   - Problema: ¿Cómo se puede crear, administrar y usar contraseñas de manera que sean accesibles para los usuarios pero difíciles para impostores?

Requerimiento ID:	**Categoría: Seguridad**
Subcategorías	Autenticación, Credenciales, Login
Nombre	Complejidad de contraseñas
Descripción	Verificar que la aplicación tiene las características administrativas necesarias para soportar requerimientos de complejidad de contraseñas para longitud mínima, caracteres alfabéticos y numéricos o especiales. Colocar requerimientos de complejidad y validar que se cumplan para diferentes tipos de usuarios.
Comentarios	Cuando un requerimiento de complejidad cambia, el nuevo requerimiento se debe cumplir automaticamente durante el siguiente ciclo de cambio de contraseña.

Tabla 4.8. *Ejemplo: Descripción de requerimiento de complejidad de contraseñas [22]*

2. Password pattern :

   - Contexto: No tiene mucho sentido tener un esquema complicado de contraseñas, pero se debe garantizar el acceso al sistema y a todos dentro de la red. Además se requiere elegir las contraseñas sobre todos los enfoques de seguridad.
   - Problema: ¿Cómo tener un esquema de contraseñas práctico y al mismo tiempo conseguir la seguridad necesaria?

En particular estos dos patrones de seguridad son similares y no agregan un valor extra a la seguridad del sistema el implementar ambos.

	Integridad			Confidencialidad		Disponibilidad
	Suplantación	Repudio	Información expuesta	Modificación	Elevación de privilegios	Denegación de servicio
Autenticación			✓			
Responsabilidad						
Identificación			✓			
No repudio						
Control de acceso						
Transmisión de datos segura						

Tabla 4.9. *Ejemplo: Registro para seguridad en credenciales*

La solución de los patrones de seguridad mostrados, no cubren todos los ataques derivados de la amenaza que se ha identificado.

Una vez identificados todos lo patrones a utilizar se coloca la información en el diagrama general del sistema para tener un panorama visual de lo que está sucediendo con el diseño y la evaluación del mismo.

Una vez obtenido el diagrama del sistema, se procede con los pasos de la evaluación.

Paso 1: Impacto de los requisitos de seguridad en los objetivos de seguridad. Debido a que los requisitos de seguridad de confidencialidad y disponibilidad no cuentan con requisitos de seguridad, el valor del peso de las amenazas pasan directamente a la ecuación de ss.

1. $Integridad = \frac{Req_1}{1}$

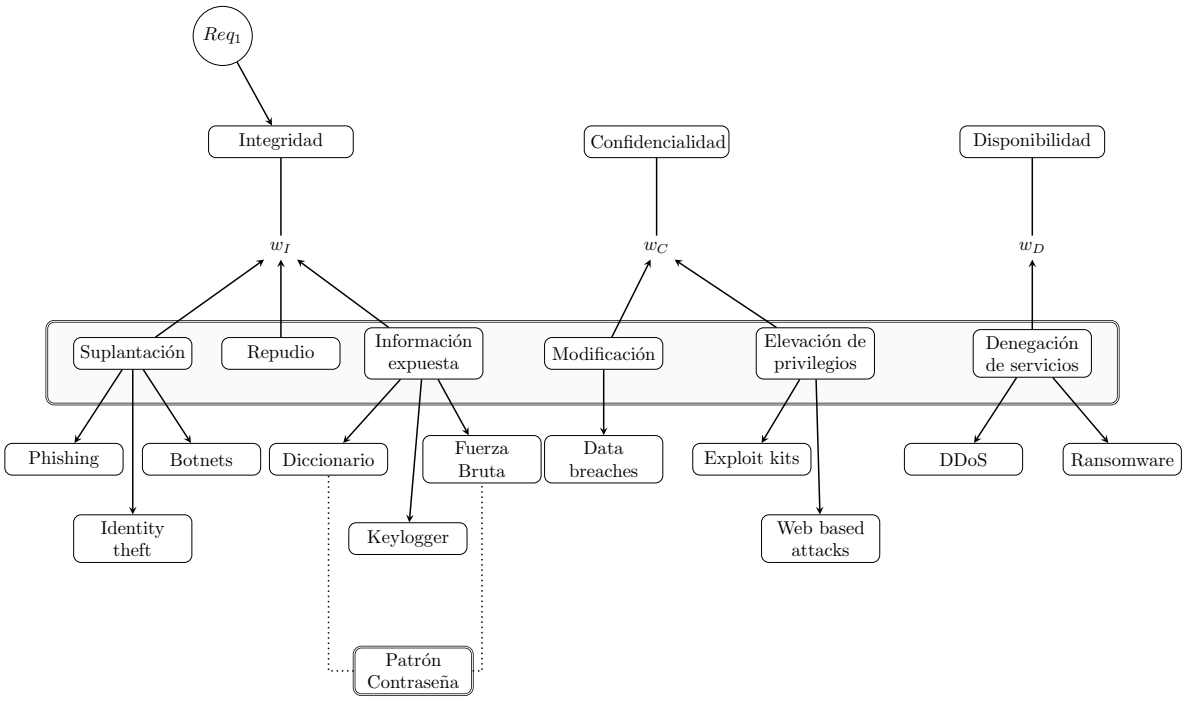

Figura 4.5. *Diagrama del sistema ejemplo.*

2. Confidencialidad, sin requisitos

3. Disponibilidad , sin requisitos

Paso 2: Peso de las amenazas sobre cada objetivo de seguridad.

- Fase 1:
  - Ataque diccionario: $v_p = 0$
  - Ataque Keylogger: $v_p = 1$
  - Ataque fuerza bruta: $v_p = 0$
- Fase 2:
  - Phishing: P(at1) = 0.0882
  - Identity theft: P(at2) = 0.1196
  - Botnets: P(at3) = 0.0063
  - Diccionario: P(at4) = 0.1155

- Keylogger: P(at5) = 0.0288
- Fuerza bruta: P(at6) = 0.0481
- Data breaches: P(at7) = 0.2941
- Exploit kits: P(at8) = 0.064
- Web based attacks: P(at9) = 0.1271
- DDoS: P(at10) = 0.0357
- Ransomeware: P(at11) = 0.0787

- Fase 3:
  - Phishing: $P(at1) \cdot 1$
  - Identity theft:$P(at2) \cdot 1$
  - Botnets: $P(at3) \cdot 1$
  - Diccionario: $P(at4) \cdot 0$
  - Keylogger: $P(at5) \cdot 1$
  - Fuerza bruta: $P(at6) \cdot 0$
  - Data breaches: $P(at7) \cdot 1$
  - Exploit kits: $P(at8) \cdot 1$
  - Web based attacks: $P(at9) \cdot 1$
  - DDoS: $P(at10) \cdot 1$
  - Ransomeware: $P(at11) \cdot 1$

  La probabilidad de amenaza queda definida como:

  $P(S) = 0{,}0882 + 0{,}1196 + 0{,}0063$

  $P(R) = 0$

  $P(I) = 0{,}0288$

  $P(M) = 0{,}2941$

  $P(E) = 0{,}064 + 0{,}1271$

$P(D) = 0{,}0357 + 0{,}0787$

Obteniendo como resultado:

- $w_I = 0{,}2141 + 0 + 0{,}0288 = 0{,}2429$
- $w_C = 0{,}2941 + 0{,}1911 = 0{,}4852$
- $w_D = 0{,}1144$

Como paso 3, se realiza la suma de la evaluación de los objetivos de seguridad.

$$\begin{aligned} ss &= 0{,}2429 \cdot I + 0{,}4852 + 0{,}1144 \\ &= 0{,}2429 \cdot 1 + 0{,}4852 + 0{,}1144 \\ &= 0{,}8425 \end{aligned}$$

4.5. Interpretación del resultado de la evaluación

A partir de la finalización del último paso de la sección 4.4, en esta sección se explica la interpretación que debe darse al valor numérico denominado *ss*.

Como primer punto el *ss* debe encontrarse en el rango de 0 a 1, esto por las probabilidades utilizadas en las amenazas posibles al sistema.

Dado el ejemplo mostrado en la sección anterior, se observa en la Figura 4.6 que el nivel de seguridad del sistema es bajo, dado que el valor *ss* está más cerca del valor de 1.

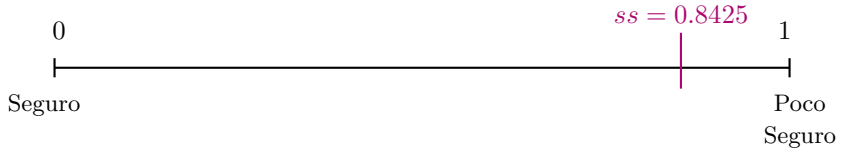

Figura 4.6. *Indicador de nivel de seguridad en el sistema*

El valor de seguridad del sistema *ss*, al encontrarse cercano al **0** (cero) indica que el sistema está completamente seguro ante cualquier amenaza, caso contrario de que si el valor *ss* está cercano al **1** (uno) indica que el sistema es propenso a cualquier amenaza.

En la Figura 4.7 se muestra una representación de 3 casos en los que el valor ss puede tener una interpretación diferente. Cabe mencionar que en las interpretaciones también influye el peso que tengan los requisitos de seguridad para el cliente.

- Cuando el valor $0 < ss \leq 0{,}3$: Al encontrarse dentro de este rango, la interpretación que puede darse es que al menos para cierta cantidad de amenazas el sistema se encuentra protegido. En particular, dentro de este rango el valor de ss no es igual a **0** debido a que ningún sistema está completamente seguro ante las amenazas existentes o nuevas.

- Cuando el valor $0{,}3 < ss \leq 0{,}7$: Si el valor ss se encuentra dentro de este rango, se puede considerar que el sistema está protegido pero la posibilidad de que exista un ataque es mayor.

- Cuando el valor $0{,}7 < ss \leq 1$: En el caso de que ss se encuentre en este rango, el sistema es muy propenso a ataques por lo que se debería replantear nuevos requisitos de seguridad para intentar proteger al sistema. Cabe resaltar que dentro de este rango el valor de ss puede estar muy cerca de **1**, si es este el caso, el sistema es muy vulnerable a ataques.

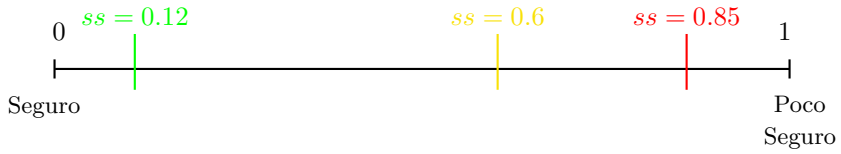

Figura 4.7. *Comparación del indicador de nivel de seguridad.*

4.6. Resumen

En este capítulo se muestran las etapas del método de evaluación propuesto. Primero, se presenta la parte de los previos requeridos para el método que son los requisitos de seguridad, los Patrones de Seguridad y el modelo de amenazas. Una vez teniendo los requisitos de seguridad, se hace una búsqueda de los Patrones de Seguridad que los atienden.

Se describen los pasos del método propuesto en los cuales, se obtiene el impacto de cada objetivo de seguridad, el peso de las amenazas sobre cada objetivo de seguridad y el resultado de la evaluación. Como complemento se presenta un ejemplo.

Capítulo 5

Caso de uso del método propuesto

Bibliografía

[1] Aceituno, V. (2017). Open information security managment maturity model (o-ism3). Technical Report 2.0, The Open Group.

[2] Atzeni, A. and Lioy, A. (2006). Why to adopt a security metic? a brief survey.

[3] Bazavan, I. V. and Lim, I. (2007). *Information Security Cost Management*. Auerbach publications.

[4] Bennett, D. (1947). *Designing hard software The essential tasks*. Manning Publications Co.

[5] Brotby, W. K. and Hinson, G. (2013). *Pragmatic security metrics: Applying metametrics to information security*. 978-1-4398-8153-8. CRC Press, Boca Raton, FL.

[6] Fernandez, E. B. (2013). *Security Patterns in practice: Designing secure architectures using software patterns*. Wiley.

[7] Fernandez, E. B. and Washizaki, H. (2010). Measuring the level of security introduced by security patterns. *International Conference on Availability, Reliability and Security*, pages 565–568.

[8] Frigault, M. and Wang, L. (2008). Measuring network security using bayesian network-based attack graphs. *Annual IEEE International computer Software and Applications Conference*, pages 698 – 703.

[9] Gupta, B., Agrawal, D., and Yamaguchi, S. (2016). *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. Advances in Information Security, Privacy, and Ethics. IGI Global.

[10] Halkidis, S. T., Chatzigeorgiou, A., and Stephanides, G. (2006). A qualitative analysis of software security patterns. *ELSEVIER*, (25):379–392.

[11] Heyman, T., Scandariato, R., Huygens, C., and Joosen, W. (2008). Using security patterns to combine security metrics. *Third International Conference on Availability, Reliability and Security.*

[12] IEEE (2014). *SWEBOK*. IEEE.

[13] Jacobs, S. (2015). *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance*. IEEE Press Series on Information and Communication Networks Security. Wiley.

[14] Jahankhani, H., W, D. L., Me, G., and Leonhardt, F. (2010). *Handbook of electronic security and digital forensics*. World Scientific.

[15] Jansen, W. (2009). Directions in security metrics research. In *Computer Security*. National Institute of Standards and Technology.

[16] Jouini, M., Rabai, L. B. A., and Aissa, A. B. (2014). Classification of security threats in information systems. *5th International Conference on Ambient Systems, Networks and Technologies*, pages 489–496.

[17] Kienzle, D. M., Elder, M. C., Tyree, D., and Edwards-hewitt, J. (2006). Security patterns repository, version 1.0.

[18] Kim, D. and Solomon, M. G. (2018). *Fundamentals of Information System Security*. Information Systems Security and Assurance Series. Jones and Bartlett Learning, third edition edition.

[19] Konrad, B. H. C. S., Campbell, L. A., and Wassermann, R. (2003). Using security patterns to model and analyze security requirements. *IEEE Workshop on Requirements for High Assurance Systems.*

[20] Landoll, D. J. (2017). *Information Security Policies, Procedures, and Standars A Practitioner's Reference*. CRC Press.

[21] Meland, P. H. and Jensen, J. (2008). Secure software design in practice. *IEEE*.

[22] Merkow, M. S. and Raghavan, L. (2012). *Secure and Resilient Software : Requirements, Test Cases and Testing Methods*. CRC Press.

[23] Mjolsnes, S. F. (2012). *A Multidisciplinary Introduction to Information Security*. Discrete Mathematics and its Applications. CRC Press.

[24] Nombela, J. J. (1997). *Seguridad informática*. Paraninfo.

[25] of Standards, N. I. and Technology (2004). *Standards for Security Categorization of Federal Information and Information Systems*. NIST.

[26] of Standards, N. I. and Technology (2006). *Minimum Security Requirements for Federal Information and Information Systems*. Number FIPS Publication 200. NIST.

[27] Ortiz, R., Garzás, J., and Fernández, E. (2011). Analysis of application of security patterns to build secure systems. *CAiSE*, pages 652–659.

[28] Passeri, P. January - september 2018 cyber attack statistics.

[29] Peltier, T. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. CRC Press.

[30] Ponde, P., Shirwaikar, S., and Kreiner, C. (2016). An analytical study of security patterns. *EuroPLoP*, page 26.

[31] Russel, D., Sr, G. T. G., and Lehtinen, R. (1991). *Computer Security Basics*. O'Reilly Media, second edition edition.

[32] Saarela, M. (2016). Measuring software security from the design of software. Master's thesis, University of Turku.

[33] Scandariato, R., Joosen, W., Yskout, K., and Heyman, T. (2006). A system of security patterns. *Report CW 469*.

[34] Schumacher, M., Fernandez, E. B., Hybertson, D., Buschmann, F., and Sommerland, P. (2006). *Security Patterns: Integrating security and systems Engineering*. Wiley.

[35] Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice*. Prentice Hall.

[36] Steel, C., Nagappan, R., and Lai, R. (2005). *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management*. Core Series. Prentice Hall PTR.

[37] Urbina, G. B. (2016). *Introducción a la Seguridad informática*. Grupo editorial Patria, primera edición edition.

[38] Varadharajan, V. (2011). Measuring security. *IEEE COMPUTER AND RELIABILITY SOCIETIES*, pages 60–65.

[39] von Helmholtz, H. L. F. (1887). *Zählen und Messen erkenntnisstheoretisch betrachtet*. Verlag nicht ermittelbar.

[40] Weik, M. H. (2001). *system design*, pages 1717–1717. Springer US, Boston, MA.

[41] Whitman, M. E. and Mattord, H. J. (2012). *Principles of Information Security*. Course Technology, cuarta edición edition.

[42] Wylder, J. (2003). *Strategic information security*. Auerbach publications.

[43] Yautsiukhin, A., Scandariato, R., Heyman, T., Massacci, F., and Joosen, W. Towards a quantitative assessment of security in software architectures.

[44] Zalewski, J., Drager, S., McKeever, W., and Kornecki, A. J. (2014). Measuring security: A challenge for the generation. *Federated Conference on Computer Science and Information Systems*, 3:131–140.