UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

"Diseño de un Framework para la planificación de tareas preemptive en sistemas embebidos heterogéneos"

TESIS

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

PRESENTA:

José Antonio Ayala Barbosa

DIRECTOR DE TESIS:

Dr. Paul Erick Méndez Monroy

Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas

Ciudad Universitaria, CDMX a Septiembre 2020

Índice general

Índice de Figuras

Índice de Tablas

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 cuantitativas.

Los patrones de seguridad proporcionan una solución probada desde la fase de diseño ante un problema recurrente que coloca a un sistema en peligro de sufrir amenazas. Pero, ¿cómo evaluar la seguridad de un sistema? y ¿qué elementos son importantes para dicha evaluación?

En este trabajo, se define un método de evaluación de la seguridad sobre un sistema informático previamente construido usando patrones de seguridad. La evaluación propuesta contempla que la seguridad, además de mitigar amenazas, también requiere de satisfacer requisitos de seguridad y políticas de seguridad. Con esto, se pretende otorgar un valor para conocer el nivel de seguridad de dicho sistema.

Capítulo 1

Introducción

1.1. Contexto

AAAAAAaAAAAAA

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 [**?** **?** **?**].

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

Investigaciones recientes se enfocan en generar evaluaciones que indiquen cuán seguro es el sistema que se está desarrollando y corregir posibles vulnerabilidades durante las etapas del ciclo de vida de software. Los patrones de seguridad son una herramienta para diseñar sistemas más seguros [**?** **?** **?**].

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 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 [**?** **?** **?**].

Además de las cuestiones económicas que conlleva medir la seguridad de la información, existe la parte tecnológica en el desarrollo de los sistemas. Como dijo Lord Kelvin *"Si no puedes medirlo, no podrás mejorarlo"*. La existencia de evaluaciones en esta área también contribuye mejorar las tecnologías con las 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 durante la etapa de diseño 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 activo. Existe una gran variedad de patrones de seguridad como la colección mostrada en [**?**].

Se sabe que la seguridad es un tema subjetivo, tornando complejo 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) [**?**].

1.2. Problema

El problema abordado en esta tesis es evaluar la seguridad de un sistema ya creado, específicamente los sistemas que desde el diseño fueron construidos utilizando patrones de seguridad

como un conjunto.

La evaluación debe proporcionar un parámetro que ayude a los diseñadores y desarrolladores a mejorar los productos de software a los que se quiere proporcionar seguridad.

1.3. Hipótesis

La hipótesis del presente trabajo es:

> *Se puede evaluar la seguridad de un sistema de forma sistemática de tal manera que se proporcione una métrica la cual indique bajo cierto criterio si es seguro o no, si previamente se sabe que ha sido construido usando patrones de seguridad.*

1.4. Aproximación

Mediante el análisis de los elementos inherentes a un sistema como los diagramas UML, requisitos de seguridad y políticas de seguridad, el presente trabajo presenta un método para evaluar la seguridad de los sistemas de información que previamente han sido construidos con patrones de seguridad. Se realiza la evaluación de un sistema que consiste en aplicar el método presentado y se proporciona un valor que indica cuán seguro puede ser considerado.

1.5. Contribuciones

El objetivo principal del presente trabajo es proporcionar una evaluación que contribuya a definir un nivel de seguridad de un sistema que utiliza patrones de seguridad y considerar que los requisitos y políticas de seguridad también son una parte importante de la evaluación de seguridad de cualquier sistema. El análisis de un sistema utilizando esta evaluación apoyaría a diseñadores y desarrolladores en conocer cuál es la cobertura de amenazas, requisitos de seguridad y políticas de seguridad del sistema para aplicar acciones de ser necesario.

1.6. Estructura de la tesis

El presente trabajo se estructura en capítulos, los cuales se describen brevemente 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 detallada por qué 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 seguridad sobre sistemas.

Capítulo 3 **Trabajo relacionado**

En este capítulo, se describe el trabajo relacionado a las métricas asociadas con sistemas que usan 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 se presenta la propuesta de evaluación y cómo interpretar los resultados obtenidos.

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

En este capítulo se utiliza como ejemplo un sistema financiero básico sobre el cual se aplica el método planteado en el Capítulo 4.

Capítulo 6 **Conclusiones**

Luego de presentar el método de evaluación, se discuten y analizan los resultados obtenidos en la tesis. Además, se proponen trabajos futuros que den continuidad al trabajo presentado.

Capítulo 2

Antecedentes

El objetivo de este capítulo es introducir los conceptos de: 1) sistemas en tiempo real; 2) tipos de ejecución de tareas; 3) el algoritmo por defecto de los sistemas en tiempo real 4) sistemas embebidos heterogéneos; 5) arquitecturas de hardware y software de tarjetas gráficas; y 6) cómputo de propósito general en en unidades de procesamiento de gráficos.

2.1. Sistemas en tiempo real

Los sistemas en tiempo real son sistemas de cómputo cuyas tareas deben actuar dentro de limitaciones de tiempo precisas ante eventos en su entorno. Por lo que el comportamiento del sistema depende, no solo del resultado del cálculo, sino también del momento (tiempo) en que se produce [3].

2.1.1. Tipos de ejecución de tareas

Existen dos tipo de ejecución de tareas, las ***preemptive***, donde es necesario interrumpir temporalmente una tarea que está realizando un sistema de cómputo, para darle la oportunidad a otra con mayor prioridad, con el compromiso de reanudar la rezagada más adelante, y los ***non-preemptive*** donde se requiere que termine la tarea actual para que posteriormente inicie una con mayor prioridad.

2.1.2. Algoritmos de planificación

Earliest Deadline First (EDF) es un algoritmo óptimo de planificación para sistemas de tiempo real, y acepta tareas en modo preemptive. Es un algoritmo muy extendido en sistemas en tiempo real debido a su optimalidad teórica en el campo no-preemptive, pero al momento de implementarlo en un planificador preemptive, el resultado puede acarrear un exceso de ejecución si se toma el peor caso [5]. Por ello es necesario buscar alternativas de algoritmos que tengan un mejor desempeño en tareas específicas.

2.2. GPU

2.2.1. Arquitectura Pascal

2.2.2. GPGPU

El GPGPU (computo de proposito general en unidades de procesamiento de graficos) es utilizado para acelerar el procesamiento realizado tradicionalmente por la CPU unicamente, donde la GPU actua como un coprocesador que puede aumentar la velocidad del trabajo [6].

2.3. Sistemas embebidos

Un sistema embebido es un sistema de cómputo diseñado para realizar tareas dedicadas, donde el mayor retos es realizar tareas específicas donde la mayoría de ellas tengan requerimientos de tiempo real [2].

2.3.1. Sistemas embebidos heterogéneos

En los últimos años los sistemas embebidos han ido demandando nuevas características debido a su rápida adopción en el mercado. Con lo que surge el desarrollo de sistemas embebidos heterogéneos, donde está contemplado realizar una gran cantidad de cómputo pero con una gran eficiencia tanto energética como en espacio.

Actualmente la empresa NVIDIA tiene en su catálogo sistemas embebidos heterogéneos con un gran soporte y bibliotecas para el cómputo de alto rendimiento. Dichos sistemas cuentan con la arquitectura pascal de última generación [4], la cual permite compartir memoria entre CPU y GPU.

2.3.1.1. Jetson TX2

Debido a que la mayoría de las GPU en sistemas embebidos no son de naturaleza preemptive, es importante programar los recursos de GPU de manera eficiente en múltiples tareas [1] ya sea de planificación o memoria, lo que permite pensar en un framework que ayude a la administración de sus características.

2.4. 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 en diseño disminuye las posibilidades de una amenaza al sistema ya implementado.

Capítulo 3

Trabajo Relacionado

Este capítulo presenta los trabajos relacionados con el tema de esta tesis, se analizan 1) Evaluar el grado de seguridad de un sistema construido usando patrones de seguridad (*Evaluating the degree of security of a system built using security patterns*), 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*).

3.1. Evaluar el grado de seguridad de un sistema construido usando patrones de seguridad

Dentro de la variedad de métodos para construir sistemas seguros no se explica cómo evaluar la seguridad de los productos finales. A pesar de que la definición de seguridad no es del todo clara para los sistemas de información, existen pocas métricas aceptadas pero que son complicadas de aplicar. El artículo *"Evaluating the degree of security of a system built using security patterns"* [**?**] propone una métrica utilizando una aproximación de búsqueda de amenazas en sistemas que han sido construido utilizando patrones.

Tomando como definición de la seguridad de sistemas como la habilidad de proteger a los activos ante ataques internos o externos, el método define un listado de amenazas y verifica

cuales amenazas están siendo mitigadas por al menos un patrón de seguridad. La métrica consiste en la cantidad de amenazas que están atendidas por un patrón de seguridad.

Una amenaza T_i usa una secuencia de pasos de ataque T_{ik}, es decir, $T_i \rightarrow T_{i1}, T_{i2}, ..., T_{ij}$, para detener T_i es suficiente con detener alguna de los T_{ij}. Los patrones de seguridad describen qué ataques pueden detener, dado que el método propuesto por [**?**] contempla que el sistema ha sido previamente construido con patrones de seguridad, se sabe que hay un conjunto de pasos de ataque que están siendo mitigados. Contabilizando el número de amenazas mitigadas TN y conociendo el número total de amenazas identificadas T, la métrica de seguridad SC se define como $SC = \frac{TN}{T}$.

El proceso para evaluar la seguridad de un sistema consiste en:

- Enumerar las amenazas basándose en las metas del atacante (parte de la metodología de desarrollo).
- Elegir las amenazas de acuerdo a probabilidad o impacto de ocurrencia.
- Determinar SC con todas o las amenazas más importantes.

La obtención de las amenazas del sistema se deriva durante las etapas de obtención de requisitos y diseño del desarrollo de software, donde se analiza cada actividad dentro del diagrama de actividades de un caso de uso, observando cómo podría un atacante cumplir sus metas.

Se propone una manera de refinar la métrica SC utilizando la aproximación *Twin peaks*, que se refiere a una forma iterativa de construir arquitecturas de software. El método de enumeración de amenazas comienza por un modelo de seguridad conceptual donde los patrones de seguridad han sido agregados al modelo funcional (obtenido de los requisitos funcionales del sistema), entonces se analiza cada caso de uso para generar el diagrama de actividades que es el que revela las amenazas como metas del atacante e identifica los activos a proteger.

Utilizando *Twin peaks* se produce una nueva arquitectura en cada ciclo, es decir, cada ciclo contempla los mismos casos de uso pero a mayor detalle considerando nuevos elementos como se muestra en la Figura 3.1.

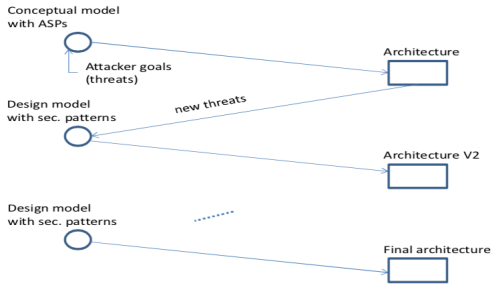


Figura 3.1. *Iteraciones Twin peaks obtenida de [?].*

La métrica propuesta realiza la enumeración de las amenazas como parte de la metodología de desarrollo del software donde cada ataque es descrito como un patrón de mal uso, pero no hay forma de mostrar que todos los patrones de mal uso relevantes para el sistema han sido considerados. Una ventaja es que, al identificar los patrones de seguridad aplicados al sistema se identifica a un gran número de patrones de mal uso mitigados.

La métrica presentada utiliza un método de enumeración de amenazas específico, no obstante puede aplicarse a sistemas que tengan una enumeración de amenazas obtenidas de métodos diferentes. Cabe resaltar que la enumeración solo contempla cierto número de amenazas dentro de las etapas del ciclo de vida del desarrollo del sistema o en las iteraciones de *Twin Peaks*.

3.2. Evaluación cuantitativa de la seguridad en arquitecturas de software

En el artículo *"Towards a quantitative assessment of security in software architectures"* [?] propone una aproximación para evaluar la seguridad en arquitecturas de software basadas en patrones. En particular, los patrones de seguridad se utilizan para medir que extensión de una arquitectura está protegida con respecto a las amenazas de seguridad más relevantes.

Esta metodología se divide en 4 partes [?]:

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 está 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

A cada arista del árbol de requerimientos se le asignan pesos, estos pesos reflejan el impacto a cada requisito de manera individual calificando la pérdida monetaria si es que el requisito de seguridad falla.

La parte experimental consiste en realizar dos sistemas utilizando el mismo conjunto de requisitos pero con una estrategia diferente para la selección de los patrones de seguridad en cada sistema. El primero se enfocó en seleccionar un conjunto de patrones de seguridad que cubriera lo mínimo pero suficiente los requisitos y el segundo se enfocó en proporcionar la mejor solución de seguridad sin importar el costo de implementación. La Figura 3.2 muestra la descomposición de los objetivos con patrones del ejemplo utilizado en este artículo.

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 los niveles de seguridad para los requerimientos, ya que fueron asignados de manera empírica por la experiencia de los autores, además de utilizar STRIDE como el conjunto de amenazas base de la evaluación.

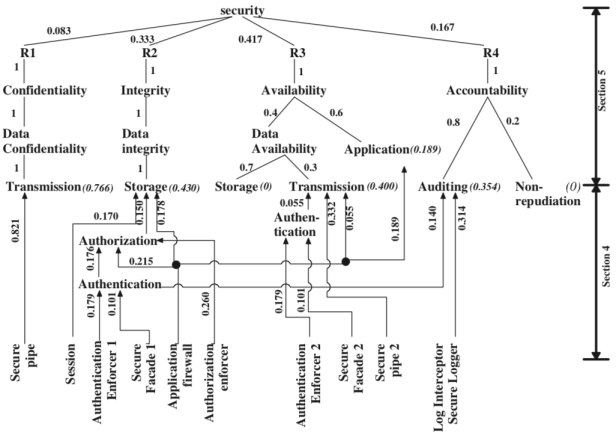


Figura 3.2. *Descomposición de objetivos con patrones obtenida de [?].*

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

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"* [**?**], se propone un método que al evaluar la correcta selección de los patrones de seguridad sobre un sistema se obtiene un indicador de si estos consiguen atender un objetivo de seguridad. La metodología consiste en 3 pasos [**?**]:

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.
- 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 comprueba 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. Un ejemplo de una gráfica de dependencias se muestra en la Figura 3.3, 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* a la Auditoría.

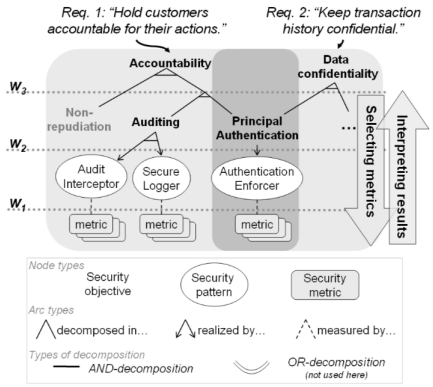


Figura 3.3. *Gráfica de dependencias obtenida de [?].*

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.

3.4. Resumen

En este capítulo se presenta el resumen de tres trabajos relacionados con la evaluación de los patrones de seguridad. El primer trabajo presenta una métrica de seguridad denominada SC la cual contabiliza el total de amenazas mitigadas por patrones de seguridad entre el total de amenazas. Una de las mejoras que propone es utilizar la aproximación *Twin peaks* que produce una nueva arquitectura en cada ciclo contemplando los mismos casos de uso pero a mayor detalle.

El segundo trabajo presenta una metodología que consiste en medir qué extensión de una arquitectura está protegida con respecto a las amenazas de seguridad más relevantes. La metodología consiste en cuatro partes: 1) mapeo de las amenazas con los objetivos de seguridad, 2) clasificación de las amenazas de acuerdo a su severidad, 3) determinación de la protección ante una amenaza y 4) 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 e 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 en sistemas implementados con patrones de seguridad

El objetivo principal de este capítulo es describir una extensión del método propuesto por [**?**] que permita evaluar la seguridad de un sistema que ha sido construido usando patrones de seguridad. En la primera sección se describe a grandes rasgos los elementos necesarios para realizar la evaluación. En las secciones posteriores se detalla cómo identificar las amenazas, la evaluación propuesta y la interpretación del resultado obtenido.

Cada sección es ejemplificada utilizando el caso de uso de un sistema financiero básico denominado *Auditoría de órdenes de comercio*.

4.1. Descripción general del método

En la Figura 4.1 se muestra el diagrama a bloques que representa los elementos de la evaluación propuesta. Se describen a grandes rasgos cada elemento, siendo los tres primeros bloques (requisitos de seguridad, patrones de seguridad y casos de uso) los elementos obtenidos del sistema a evaluar que denominaremos previos requeridos, el elemento de amenazas y por último los elementos evaluación de seguridad y resultado que son en los que se enfoca

el desarrollo de este trabajo.

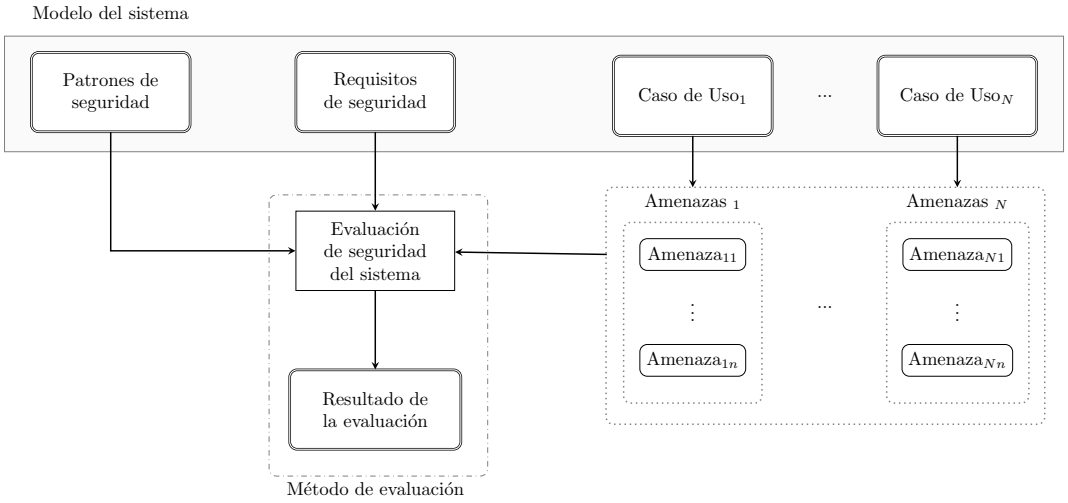


Figura 4.1. *Diagrama a bloques.*

Previos requeridos

Dado que el presente trabajo se enfoca en evaluar un sistema construido utilizando patrones de seguridad en el diseño, los previos requeridos son obtenidos tanto del modelo UML como de la documentación que exista sobre el sistema.

- **Requisitos de seguridad**. Se considera que el sistema tiene varios requisitos de seguridad, obtenidos de un listado de políticas de seguridad, políticas internas de la empresa o políticas gubernamentales.
  Cada requisito de seguridad tiene una prioridad diferente para la empresa, usando dos niveles:

  - **Baja**. Cubrir el requisito de seguridad es deseable.
  - **Alta**. Cubrir el requisito de seguridad es imprescindible.

  Por ejemplo, los requisitos de seguridad correspondientes a *Auditoría de órdenes de comercio* .

  - Req_1. Se debe tener registro de todos los inicios de sesión realizados por el auditor (*prioridad baja*).

- Req_2. Se deben registrar todas las acciones realizadas por el auditor (*prioridad alta*).
- Req_3. El auditor solo puede leer la información de ordenes (asignadas a él) (*prioridad alta*).

- **Casos de uso**. Los casos de uso definen las posibles interacciones de usuarios con el sistema e indican las actividades y la información que se está manipulando en el sistema que se ha desarrollado.

  La Tabla 4.1 muestra el resumen de la documentación correspondiente al caso de uso *Auditoría de órdenes de comercio*.

Tabla 4.1. *Resumen auditoría de órdenes de comercio*

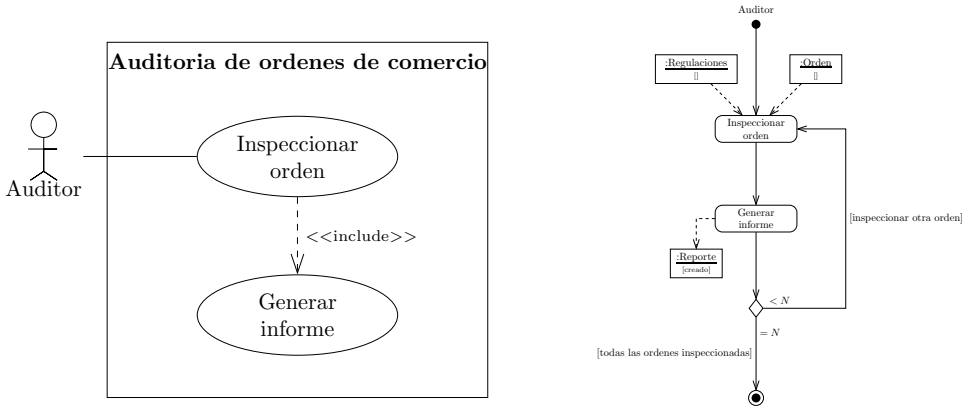
CU-5	**Auditoría de órdenes de comercio**	
Pre-condición	El auditor debe tener un listado de órdenes de comercio ya finalizadas.	
Descripción	El sistema debe comportarse como se describe en el siguiente caso de uso cuando el auditor solicite inspeccionar una orden.	
Secuencia normal	Paso	Acción
	1	El auditor solicita al sistema realizar la inspección de una orden de comercio.
	2	El auditor inspecciona la orden de comercio con respecto a las regulaciones gubernamentales y de la empresa.
	3	El auditor genera un informe tomando en cuenta el análisis realizado a la orden de comercio.
Post-condición	El auditor genera el informe de la orden de comercio.	
Excepciones	Paso	Acción
	4	El auditor de tener más ordenes de comercio asignadas a él repetirá los pasos del 1 al 3.
Comentarios	El auditor solo puede revisar las ordenes de comercio asignadas a él.	

  La Figura 4.2 muestra los diagramas correspondiente al caso de uso *Auditoría de órdenes de comercio*.

- **Patrones de seguridad**. Los patrones de seguridad son los que han sido implementados en el sistema y que provienen de algún catálogo pre-especificado.

  A continuación se indican los patrones correspondientes al caso de uso *Auditoría de órdenes de comercio*:

  - Pat_1: Role-based access control



(a) *Caso de uso* **(b)** *Diagrama de actividades*

Figura 4.2. *Caso de uso: Auditoría de ordenes de comercio*

- Pat_2: Authenticator
- Pat_3: Security logger and auditor

En este previo requerido se pueden encontrar de la misma manera patrones de regulación y roles[1].

Modelado de amenazas

Una vez que contamos con los previos requeridos, se procede a hacer el análisis de amenazas a las que está expuesto el sistema. Para este proceso, por cada caso de uso se obtiene el conjunto de amenazas.

Todas las amenazas obtenidas por cada caso de uso son consideradas para el presente trabajo como, el total de amenazas a las que está expuesto el sistema. Por ello es importante usar métodos de enumeración sistemáticos que garanticen la identificación de las amenazas importantes.

[1]Los patrones de regulación se encuentran en desarrollo, por lo que para ciertos sistemas deben escribirse patrones para completar los diagramas, es decir, hace falta contar con un catálogo de patrones de regulación como catálogo de patrones de seguridad.

Evaluación de seguridad del sistema

La evaluación de seguridad conjunta tanto los requisitos de seguridad (que son las metas de seguridad que se han planteado para el sistema) como las amenazas a las que está expuesto el sistema que se ha desarrollado. Dado que el sistema fue construido utilizando patrones de seguridad, estos mitigarán ciertas amenazas proporcionando un nivel de seguridad al mismo.

La evaluación contempla que no todas las amenazas tienen el mismo impacto en el sistema y por ello se puede prescindir de evitar las de menor impacto.

Resultado de la evaluación: métrica de seguridad

Una vez aplicado el método de evaluación al sistema, se obtiene un valor el cual indica qué tan seguro es el sistema ante las amenazas identificadas considerándolo como el resultado de la evaluación. Se da una interpretación a los diferentes posibles resultados, que van desde no hacer nada más a agregar nuevas defensas.

4.2. Modelado de amenazas

Para el método propuesto, se ha agregado una columna a la tabla creada en [**?**]. La columna **Impacto** define el impacto que tiene dicha amenaza en el sistema a criterio de la empresa, usando tres niveles:

- **Bajo**. La amenaza de existir genera un riesgo insignificante para la empresa.
- **Medio**. La amenaza tiene un impacto en la empresa pero no es crítica.
- **Alto**. La amenaza es considerada de alto impacto para la empresa y crítica.

Este nuevo criterio nos permite dar un peso diferente a las amenazas a las que está expuesto el sistema. Una determinada amenaza puede ser de mayor impacto para un sistema que para otro dependiendo de el contexto en el que se implemente; es decir, obtener la información de cuenta de un usuario de banco es diferente a obtener los tuits de un usuario en un foro.

Las amenazas son obtenidas por cada caso de uso del sistema, por lo tanto, en la columna # de la tabla se coloca como abreviatura T_{ca}, donde la **T** proviene de la palabra en inglés (*Threat*), **c** es el número de actividad analizada y **a** es el número de amenaza dentro de la actividad.

La Tabla 4.2 muestra la plantilla de actividades de mal uso con los datos requeridos del análisis de amenazas[2].

Tabla 4.2. *Plantilla de actividades de mal uso*

Actor	Actividad	#	Atri. seg.	Impacto	Origen ataque	Descripción	Activo

Se realiza el análisis de amenazas utilizando el método de [**?**] con las modificaciones descritas anteriormente para el caso de uso *Auditoría de órdenes de comercio* y utilizando el diagrama de actividades mostrado en la Figura 4.2b.

Para comenzar con la búsqueda de amenazas, existen tres posibles atacantes u origen de la amenaza (Interno autorizado, Interno no autorizado, Externo no autorizado) y por cada actividad se considera *"¿Qué mal uso se puede realizar en <actividad> por el <origen de amenaza> que compromete el <atributo de seguridad> del <dato a proteger>"* como se muestra a continuación:

- ¿Qué mal uso se puede realizar en *Inspeccionar Orden* por el *Auditor* que compromete la *Responsabilidad* sobre el *Informe* ?: Negar haber inspeccionado una orden.
- ¿Qué mal uso se puede realizar en *Inspeccionar Orden* por *Auditor* que compromete la *Confidencialidad* de la *Orden*? : Copiar la información de la orden para otros usos e inspeccionar órdenes no asignadas a él.
- ¿Qué mal uso se puede realizar después de haber *Inspeccionado todas las ordenes* por el *Auditor/Impostor* que compromete la *Responsabilidad* sobre el *Informe* ?: Enviar información a una persona externa a la empresa.

[2]Atri. seg. es la abreviatura dada a Atributo de Seguridad/Objetivo de Seguridad en el presente trabajo.

- ¿Qué mal uso se puede realizar en *Generar Informe* por el *Auditor/Impostor* que compromete la *Responsabilidad* del *Informe*? : Ignorar los requerimientos gubernamentales o de la empresa.
- ¿Qué mal uso se puede realizar en *Generar Informe* por el *Atacante externo* que compromete la *Confidencialidad* del *Informe*? : Leer la información del informe generado.

Con el análisis anterior se llena la tabla modificada de actividades de mal uso, identificando el impacto que tiene cada una en la empresa como se muestra en la Tabla 4.3, también se puede visualizar este análisis de una forma gráfica como se muestra en la Figura 4.3.

Tabla 4.3. *Resultado de amenazas Auditoría de órdenes de comercio*

Actor	Actividad	#	Atri. seg.	Impacto	Origen ataque	Descripción	Activo
Auditor	Inspeccionar Orden	T_{1_1}	R	Bajo	InA	Negar haber inspeccionado una orden de compra	Orden
		T_{1_2}	C	Alto	InA/InN	Copiar información de ordenes para otros usos	Orden
Auditor	Generar Informe	T_{2_1}	R	Alto	InA	Ignorar los reglamentos gubernamentales o de la empresa aplicables a una orden al generar un informe	Informe
		T_{2_2}	R	Alto	InA	Enviar información de los informes a una persona externa	Informe
		T_{2_3}	C	Medio	Ext	Leer información sobre los informes generados	Informe

4.3. Método de evaluación de seguridad

Paso 1: Se debe encontrar el peso de las amenazas mitigadas sobre el sistema, representado como w_{ame}. Para este paso se cuenta con tres fases:

a) Se relaciona cada patrón de seguridad con la amenaza que mitiga, si el patrón mitiga más de una amenaza debe replicarse en cada una. En caso de existir al menos un patrón se asigna un valor de $v_p = 1$ que indica que existe una mitigación de la amenaza[3], si no existe al menos un patrón que mitigue la amenaza se asigna un valor de $v_p = 0$ indicando que dicha amenaza persiste.

[3]Este valor no indica que la amenaza desaparece.

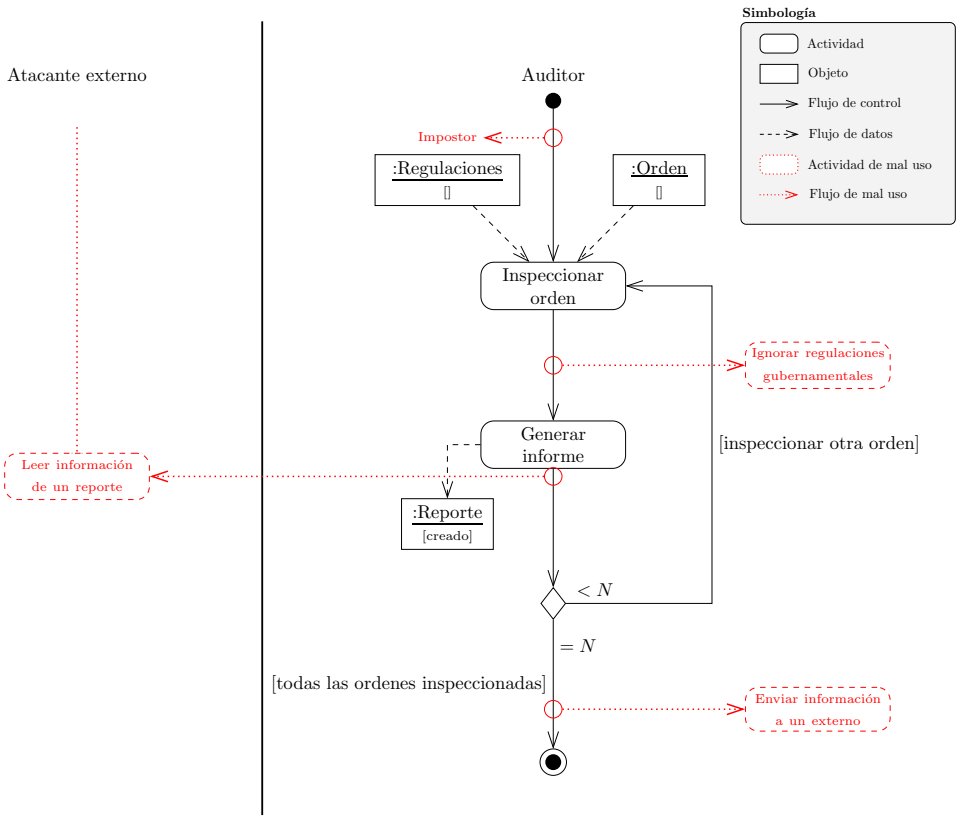


Figura 4.3. *Diagrama con actividades de mal uso*

b) Esta siguiente fase nos permite conocer el impacto de las amenazas sobre el sistema. Para esta fase a cada nivel de impacto se le asigna un valor: **Bajo=1**, **Medio=2**, **Alto=3**.

Cada amenaza tiene un valor de impacto en el sistema como:

$$\alpha = \frac{imp}{M}$$

Donde, α es el peso de la amenaza; imp es el impacto de la amenaza y M es el número total de amenazas identificadas.

c) Por último, para obtener los pesos de las amenazas mitigadas se utiliza:

$$w_{ame} = \frac{\sum_{i=1}^{M} \alpha_i \cdot v_{p_i}}{\sum_{i=1}^{M} \alpha_i} \qquad (0 \leq w_{ame} \leq 1)$$

Donde, w_{ame} es peso mitigado para el sistema, α_i es el peso de cada amenaza y v_{p_i} es el valor de patrón asignado a la amenaza α_i.

La Tabla 4.4 muestra la plantilla de impacto de amenazas con la información obtenida del paso anterior.

Tabla 4.4. *Plantilla de datos impacto de amenazas*

Amenaza	Patrón(es)	α	v_p	w_{ame}

Usando el caso de uso de *Auditoría de ordenes de comercio* y la información obtenida en la Tabla 4.3 se procede a llenar la tabla del impacto de amenazas como se muestra en la Tabla 4.5.

Tabla 4.5. *Impacto de las amenazas*

Amenaza	Patrón(es)	α	v_p	w_{ame}
T_{11}	Pat_3	$\frac{1}{5}$	1	$\frac{\frac{1}{5}\cdot 1+\frac{3}{5}\cdot 1+\frac{3}{5}\cdot 1+\frac{3}{5}\cdot 1+\frac{2}{5}\cdot 1}{\frac{12}{5}} = 1$
T_{12}	Pat_1	$\frac{3}{5}$	1	
T_{21}	Pat_3	$\frac{3}{5}$	1	
T_{22}	Pat_1	$\frac{3}{5}$	1	
T_{23}	Pat_2	$\frac{2}{5}$	1	

Paso 2: Se debe contar con el peso de los requerimientos de seguridad satisfechos en el sistema tanto por patrones de seguridad como patrones de regulación o roles, representado como w_{req}. Para esto se cuenta con las siguientes fases:

a) Se relaciona cada patrón de seguridad, patrón de regulación o rol con el requisito de seguridad que atiende, si el patrón o rol atiende más de un requisito de

seguridad debe replicarse en cada una. En caso de existir al menos un patrón se asigna un valor de $v_p = 1$ que indica que el requisito de seguridad es satisfecho, si no existe al menos un patrón se asigna un valor de $v_p = 0$ indicando que no ha sido atendido.

b) Conociendo la prioridad que tiene cada requisito de seguridad para la empresa se obtiene el peso de cada uno asignando un valor a cada prioridad: **Baja**=1,**Media**=2 **Alta**=3.

Cada requisito de seguridad tendrá una prioridad en el sistema como:

$$\mu = \frac{prio}{N}$$

Donde, μ es el importancia del requisito de seguridad en el sistema, *prio* es la prioridad y N es el número total de requisitos de seguridad proporcionados.

c) Por último, para obtener el peso de todos los requisitos de seguridad satisfechos se utiliza:

$$w_{req} = \frac{\sum_{j=1}^{N} \mu_j \cdot v_{p_j}}{\sum_{j=1}^{N} \mu_j} \qquad (0 \leq w_{req} \leq 1)$$

Donde w_{req} es peso de los requisitos de seguridad atendidos en el sistema, μ_j es la importancia de cada requisito de seguridad y v_{p_j} es el valor de patrón asignado al requisito o política μ_j.

La Tabla 4.6 muestra la plantilla de los requisitos de seguridad satisfechos con la información obtenida del paso anterior.

Tabla 4.6. *Plantilla de datos requisitos de seguridad satisfechos*

Requisito	Patrón(es)	μ	v_p	w_{req}

Usando el caso de uso de *Auditoría de ordenes de comercio* y la información sobre

los requisitos de seguridad se procede a llenar la tabla de requisitos de seguridad atendidos como se muestra en la Tabla 4.7.

Tabla 4.7. *Requisitos de seguridad satisfechos*

Requisito	Patrón(es)	μ	v_p	w_{req}
Req_1	Pat_3	$\frac{1}{4}$	1	$\frac{\frac{1}{4}\cdot 1+\frac{2}{4}\cdot 1+\frac{1}{4}\cdot 1+\frac{2}{4}\cdot 1}{\frac{6}{4}} = 1$
Req_2	Pat_3	$\frac{2}{4}$	1	
Req_3	Pat_1	$\frac{1}{4}$	1	
Req_4	Pat_1	$\frac{2}{4}$	1	

Paso 3: Se obtiene el total de la seguridad del sistema, definido como :

$$ss = w_{ame} \cdot w_{req}$$

Donde, w_{ame} son las amenazas mitigadas por los patrones de seguridad en el sistema y w_{req} son los requisitos de seguridad satisfechos por los patrones de seguridad identificados en el sistema. La multiplicación de ambos pesos indican el nivel de seguridad del sistema ss; es decir, definen una métrica que combina seguridad y políticas de la empresa.

El valor obtenido también puede ayudar a analizar la seguridad del sistemas y observar dónde es necesario hacer mejoras para incrementar la seguridad del mismo o identificar si existen elementos seguridad que hacen ineficiente al sistema de los cuales se puede prescindir sin perder seguridad.

4.4. Resultado de la evaluación

En esta sección se explica la interpretación que debe darse al valor numérico denominado ss obtenido en la sección anterior.

El valor de seguridad del sistema ss debe encontrarse en el rango de 0 a 1. Si se encuentra cercano al 1 (uno) indica que el sistema está completamente o casi seguro ante las amenazas

identificadas y se han satisfecho todos los requisitos de seguridad; en caso contrario, si el valor ss está cercano al 0 (cero) indica que el sistema es propenso a cualquier amenaza y que los requisitos de seguridad no están siendo satisfechos.

En la Figura 4.4 se muestra una representación de 3 casos en los que el valor ss puede tener una interpretación diferente.

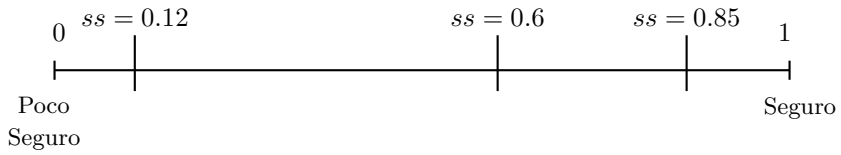


Figura 4.4. *Indicador del nivel de seguridad.*

- Cuando el valor $0.7 < ss \leq 1$: Al encontrarse dentro de este rango, la interpretación que se da es que al menos para cierta cantidad de amenazas el sistema se encuentra protegido y los requisitos de seguridad están siendo satisfechos. En particular, dentro de este rango el valor de ss al ser 1 indica que el sistema está protegido para las amenazas identificadas; pero pueden existir amenazas no identificadas.
- 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 una amenaza es mayor y que los requisitos de seguridad no están siendo satisfechos por completo.
- Cuando el valor $0 < ss \leq 0.3$: En el caso de que ss se encuentre en este rango, el sistema es muy propenso a amenazas. Cabe resaltar que dentro de este rango el valor de ss puede estar muy cerca de 0 pero no igual debido a que se considera que ha sido construido utilizando patrones de seguridad, si es este el caso, el sistema es vulnerable. La sugerencia en este caso es que el sistema debe reforzarse.

Con los datos obtenidos de la Tabla 4.5 y la Tabla 4.7 se puede obtener el valor ss del caso de uso *Auditoría de ordenes de comercio* dando como resultado:

$$ss = 1 \cdot 1 = 1$$

Del cual se puede interpretar que todas las amenazas identificadas están siendo mitigadas y todos los requisitos de seguridad están siendo satisfechos.

4.5. Resumen

En este capítulo se muestran las etapas del método de evaluación propuesto. Primero, se presenta la parte de los previos requeridos que son los requisitos de seguridad, los patrones de seguridad utilizados para construir el sistema y los casos de uso del sistema. Una vez teniendo los previos requeridos se obtiene el listado de amenazas, con el listado anterior se realiza el impacto de las amenazas y posteriormente se obtienen los requerimientos de seguridad atendidos por los patrones. Se muestra como realizar la evaluación y la interpretación del resultado obtenido. En cada etapa se presenta como ejemplo uno de los casos de uso de un sistema financiero básico.

Capítulo 5

Caso de estudio del método propuesto

En este capítulo se desarrolla la evaluación de seguridad de un sistema financiero utilizando el método propuesto en el capítulo anterior, el objetivo es mostrar cómo aplicar el método a un sistema para obtener el nivel de seguridad del mismo. En la primera sección se definen los previos requeridos, en la sección posterior se realiza el análisis de las amenazas y en las siguientes secciones se detalla la aplicación del método propuesto al ejemplo.

5.1. Previos requeridos

5.1.1. Requisitos de seguridad

Los requisitos de seguridad proporcionados son:

Req_1: Registrar todos los inicios de sesión realizados por el auditor. *prioridad=Baja*

Req_2: Registrar todas las acciones realizadas por el auditor, gerente, agente y cliente. *prioridad=Alta*

Req_3: El auditor solo puede leer la información de las ordenes (asignadas a él). *prioridad=Alta*

Req_4: El gerente solo puede abrir, cerrar y administrar cuentas (asignadas a él). *prioridad=Alta*

Req_5: El agente solo puede actualizar una cuenta hasta que se haya cerrado una orden de comercio. *prioridad=Alta*

Req_6: El gerente no puede modificar la información crediticia de un cliente. *prioridad=Alta*

Req_7: La información proporcionada por el cliente debe cifrarse antes de su transmisión al sistema. *prioridad=Media*

Req_8: La información sobre las cuentas debe estar cifrada en la base de datos. *prioridad=Alta*

Req_9: La información sobre las ordenes de comercio debe estar cifrada en la base de datos. *prioridad=Alta*

Req_{10}: Contar con un firewall con las reglas necesarias para evitar ataques DoS. *prioridad=Media*

Req_{11}: Las acciones sobre una cuenta deben estar previamente autorizadas por el cliente. *prioridad=Alta*

Las políticas de seguridad proporcionadas son:

Pol_1: Se debe monitorear, controlar y proteger las comunicaciones de la organización (i.e., la información transmitida y recibida por sistemas de información). *prioridad=Alta*

Pol_2: Se deben establecer, mantener e implementar planes para respuestas de emergencia, backups y recuperación de desastres a los sistemas de información. *prioridad=Alta*

Pol_3: Se debe identificar, reportar y corregir errores de información y de sistemas de información de manera oportuna. *prioridad=Media*

Pol_4: Se debe identificar a usuarios, procesos y dispositivos de los sistemas de información e identificar las identidades de cada uno. *prioridad=Alta*

Pol_5: Se debe crear, proteger y mantener los registros de las auditorías realizadas a los sistemas de información en caso de que exista alguna actividad inapropiada o no autorizada. Deben realizarse de forma periódica. *prioridad=Media*

5.1.2. Casos de uso

En la Figura 5.1 se muestra los casos de uso del sistema financiero a analizar. Cada caso de uso cuenta con su respectivo diagrama de actividades, mostrados a continuación:

CU_1: Abrir cuenta *Open Account*, diagrama de actividades mostrado en la Figura 5.2a

CU_2: Cerrar cuenta *Close Account*, diagrama de actividades mostrado en la Figura 5.2b

CU_3: Crear orden de comercio *Receive Trade Order*, diagrama de actividades mostrado en la Figura 5.3a

CU_4: Llevar a cabo orden de comercio *Perform Trade*, diagrama de actividades mostrado en la Figura 5.3a

CU_5: Auditoría de ordenes de comercio *Check Trade Info*, diagrama de actividades mostrado en la Figura 5.3b

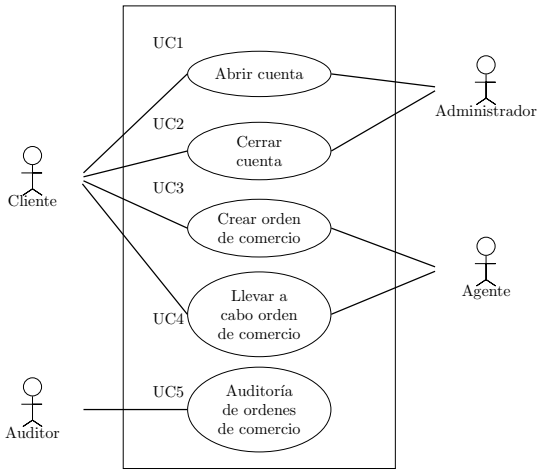


Figura 5.1. *Casos de uso del sistema financiero.*

5.1.3. Patrones de seguridad

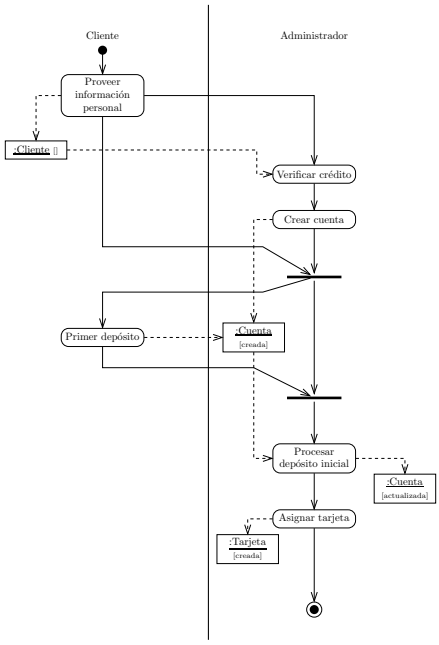
La información sobre los patrones de seguridad, patrones de regulación y roles son identificados en el diagrama de clases proporcionado del sistema se muestran de color en la Figura 5.4.

Los patrones de seguridad aplicados al sistema identificados son:

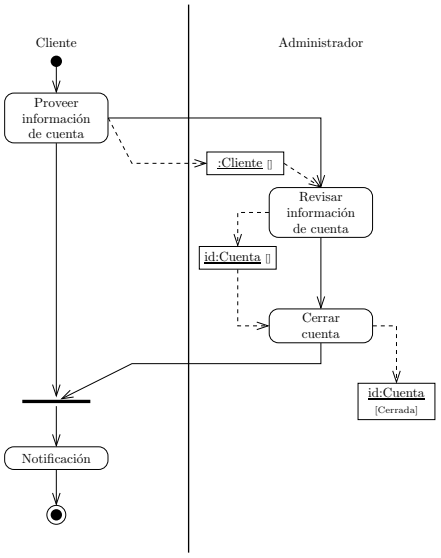
Pat_1: *Security logger and auditor*

Pat_2: *Role-based access control*

Pat_3: *Authenticator*

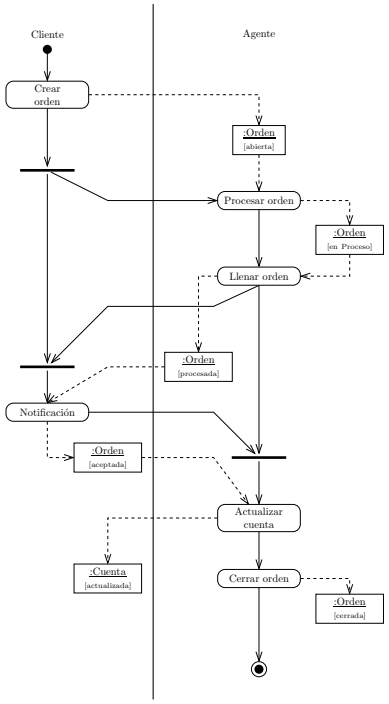


(a) *Abrir cuenta*

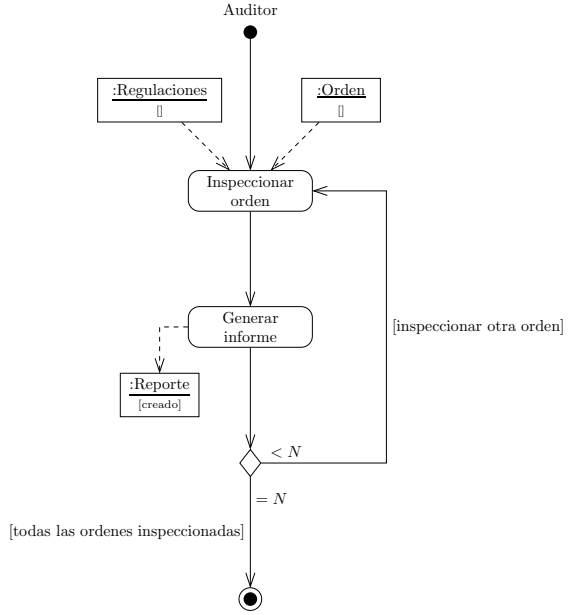


(b) *Cerrar cuenta*

Figura 5.2. *Diagramas de actividades parte 1*



(a) *Crear y llevar a cabo orden de comercio*



(b) *Auditoría de ordenes de comercio*

Figura 5.3. *Diagramas de actividades parte 2*

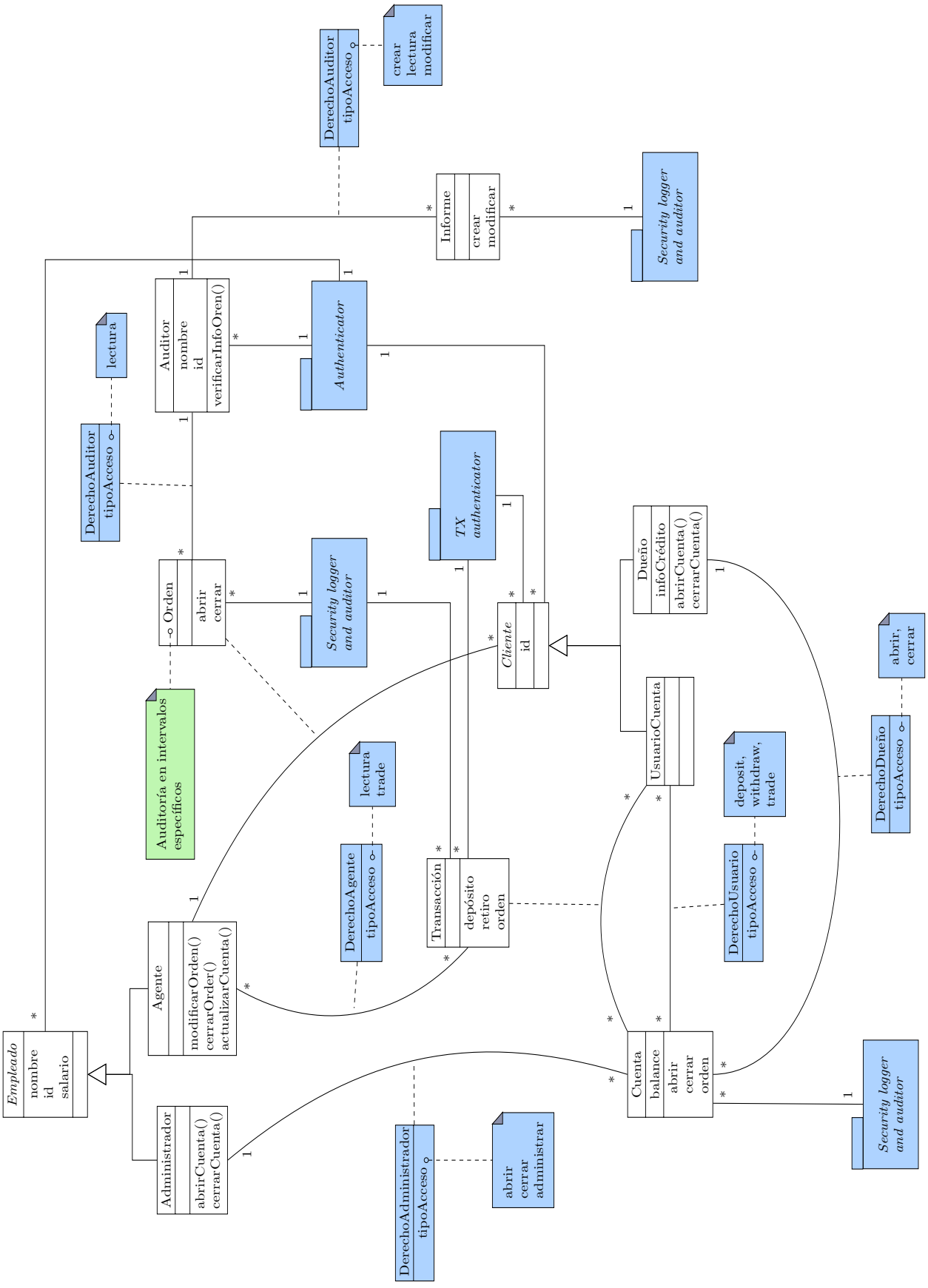


Figura 5.4. *Diagrama de clases de sistema financiero*

Pat_4: *TX Authentication*

Los patrones de regulación identificados en el sistema son:

Reg_1: Realizar auditorías en intervalos específicos.

5.2. Modelado de amenazas

El análisis de las amenazas sobre los diagramas de actividades se muestra el la Tabla 5.1. Los diagramas de actividades de mal uso donde se puede observar de manera gráfica el análisis realizado se muestra en las Figuras 5.5, 5.6, 5.7 y 5.8.

Tabla 5.1. *Resultado de amenazas*

Actor	Actividad	#	Atri Seg	Impacto	Origen ataque	Descripción	Activo
Abrir cuenta							
Cliente	Proveer información personal	T_{1_1}	R	Bajo	InA	Negar haber abierto una cuenta	Cuenta
		T_{1_2}	D	Bajo	Ext	Realizar multiples solicitudes de apertura de cuenta	-
		T_{1_3}	C	Alto	InN/Ext	Leer la información del cliente transmitida por la red	Cliente
		T_{1_4}	I	Bajo	InA	Provee información inválida (financiera, dirección, etc.)	Cliente
		T_{1_5}	I	Medio	InA	Provee información de otra persona (nombre, dirección, etc.)	Cliente
Gerente	Verificar historial crediticio	T_{2_1}	D	Bajo	InA	Negar haber modificado la información crediticia de un cliente	Cliente
		T_{2_2}	C	Alto	InA	Recolectar información personal del cliente para distribuirlo ilegalmente	Cliente
		T_{2_3}	C	Alto	InN/Ext	Leer la información del cliente transmitida por la red	Cliente
		T_{2_4}	C	Bajo	Ext	Recolectar información de manera ilegal	Cliente

Continúa en la siguiente página

Continúa desde la página previa

Actor	Actividad	#	Atri Seg	Impacto	Origen ataque	Descripción	Activo
		T_{2_5}	I	Alto	InA	Cambiar la información crediticia de un cliente	Cliente
Gerente	Crear cuenta	T_{3_1}	R	Bajo	InA	Negar haber creado una cuenta falsa	Cuenta
		T_{3_2}	C	Alto	InA	Recolectar información de cuentas para distribuirla ilegalmente	Cuenta
		T_{3_3}	C	Medio	InN/Ext	Leer la información de las cuentas	Cuenta
		T_{3_4}	I	Alto	InA	Crear una cuenta falsa	Cuenta
Cliente	Depósito inicial		-	-	-		-
Gerente	Expedir tarjeta	T_{5_1}	I	Alto	InA	Autorizar una tarjeta falsa	Tarjeta
Cliente	Transferir dinero	T_{6_1}	R	Medio	InA	Negar haber autorizado una transferencia	Cuenta
		T_{6_2}	D	Bajo	Ext	Inundar a la aplicación de solicitudes de transferencia	-
		T_{6_3}	C	Bajo	InN/Ext	Leer la información sobre las transferencias del cliente	Cuenta
		T_{6_4}	I	Alto	Ext	Transferir dinero entre cuentas de manera ilegal	Cuenta
Cerrar cuenta							
Cliente	Proveer información personal	T_{7_1}	R	Bajo	InA	Negar haber solicitado la cancelación de una cuenta	Cuenta
		T_{7_2}	R	Medio	InN/Ext	Proveer información falsa para solicitar una cancelación de cuenta	Cuenta
Gerente	Revisar cuenta	T_{8_1}	C	Alto	InN/Ext	Leer la información de la cuenta transmitida por la red	Cuenta
Gerente	Cerrar cuenta	T_{9_1}	I	Medio	InA	No cerrar adecuadamente una cuenta para usos ilegales	Cuenta
Crear y procesar orden de comercio							
Cliente	Crear orden	T_{10_1}	I	Medio	InA/Ext	Crear una orden de comercio con información falsa	Orden
		T_{10_2}	R	Bajo	InA	Negar haber creado una orden de comercio	Orden
		T_{10_3}	C	Alto	InN/Ext	Leer la información de una orden de comercio transmitida por la red	Orden
Agente	Procesar orden	T_{11_1}	I	Alto	InA	Modificar la información de una orden de comercio	Orden
		T_{11_2}	R	Alto	InA	Ignorar los reglamentos gubernamentales o de la empresa para procesar una orden	Orden
		T_{11_3}	R	Bajo	InN	Negar haber procesado una orden de comercio	Orden

Continúa en la siguiente página

Continúa desde la página previa

Actor	Actividad	#	Atri Seg	Impacto	Origen ataque	Descripción	Activo
Agente	Llevar a cabo orden de comercio	T_{12_1}	I	Alto	InA	Modificar la información de una orden de comercio	Orden
Cliente	Confirmación	-	-	-	-		-
Agente	Actualizar cuenta	T_{14_1}	I	Alto	InA/Ext	Transferir el dinero de una orden de comercio a una cuenta de manera ilegal	Cuenta
Agente	Cerrar orden	T_{15_1}	C	Medio	InA	Distribuir información de una orden de comercio de manera ilegal	Orden
		T_{15_2}	C	Medio	InN/Ext	Leer la información de una orden de comercio	Orden
Auditoría de ordenes de comercio							
Auditor	Inspeccionar orden	T_{16_1}	R	Bajo	InA	Negar haber inspeccionado una orden de comercio	Orden
		T_{16_2}	C	Alto	InA/InN	Copiar información de ordenes para otros usos	Orden
Auditor	Generar informe	T_{17_1}	R	Alto	InA	Ignorar los reglamentos gubernamentales o de la empresa aplicables a una orden al generar el informe	Informe
		T_{17_2}	R	Medio	InA/InN	Enviar la información de los informes a una persona externa	Informe
		T_{17_3}	C	Alto	Ext	Leer la información sobre los informes generados	Informe

5.3. Evaluación de seguridad del sistema

Paso 1: Encontrar el peso de las amenazas del sistema w_{ame} con la información contenida en la Tabla 5.2 plasmando la información como se muestra en la Tabla 5.2.

Paso 2: Encontrar el peso de los requerimientos de seguridad w_{req} con la información de los requisitos de seguridad y políticas de seguridad encontrados en los previos requeridos. Plasmando la información como se muestra en la Tabla 5.3

Paso 3: Obtener el valor de la seguridad del sistema con los valores obtenidos del paso anterior.

$$ss = 0.82 \cdot 0.54 = 0.44$$

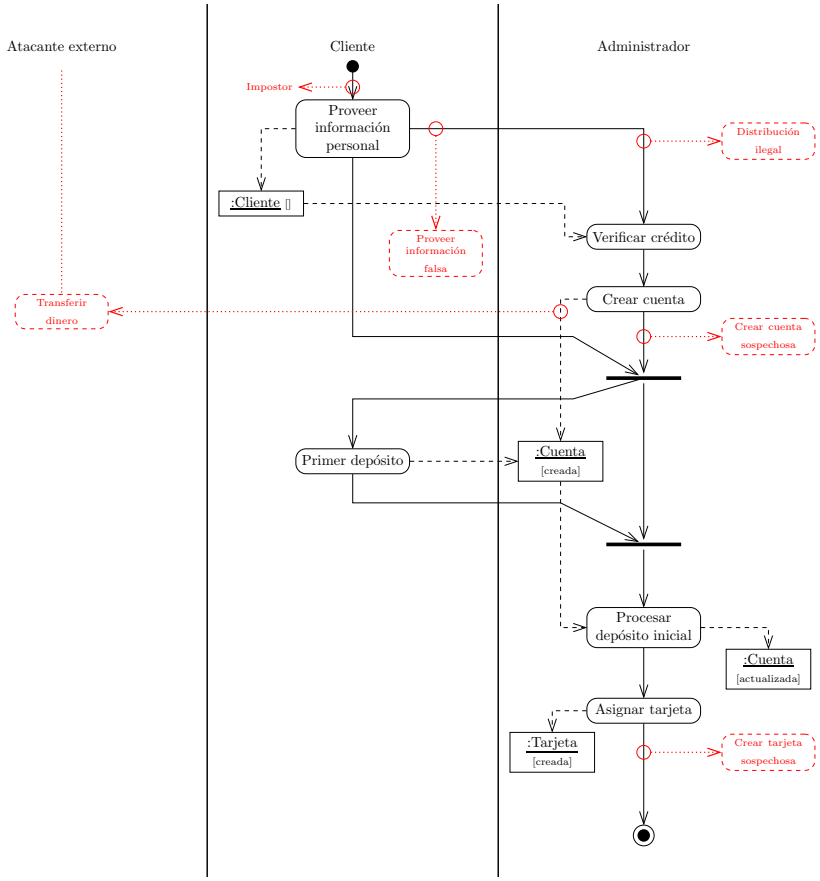


Figura 5.5. *Diagrama de actividades de mal uso en abrir cuenta*

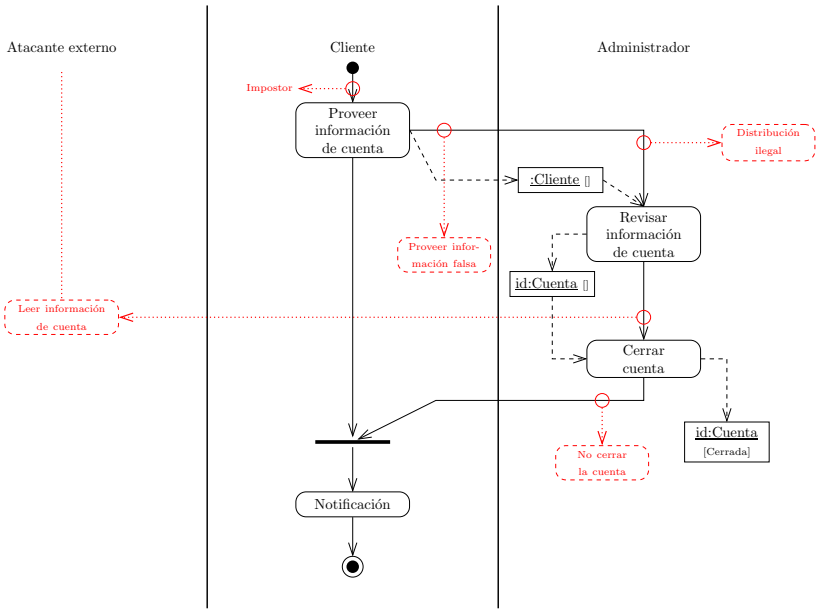


Figura 5.6. *Diagrama de actividades de mal uso en cerrar cuenta*

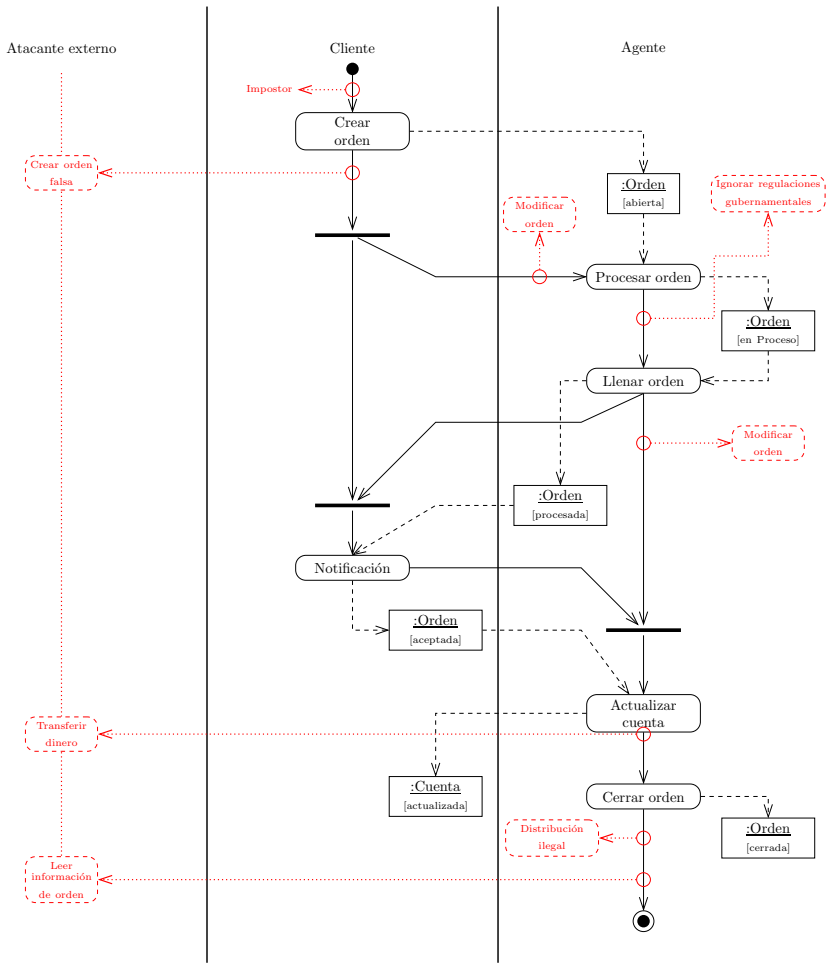


Figura 5.7. *Diagrama de actividades de mal uso en crear y llevar a cabo orden de comercio*

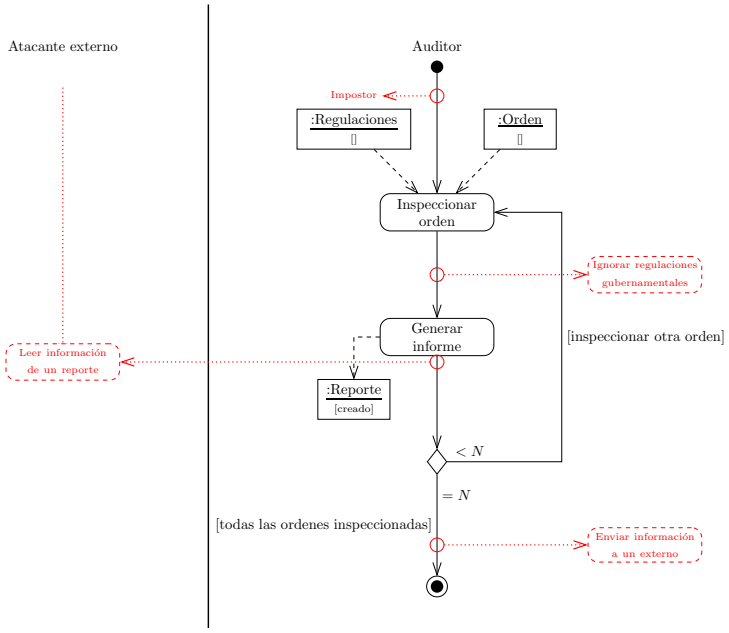


Figura 5.8. *Diagrama de actividades de mal uso en auditoría de ordenes de comercio*

Tabla 5.2. *Peso de las amenazas mitigadas*

Amenaza	Patrón(es)	α	v_p	w_{ame}	Amenaza	Patrón(es)	α	v_p	w_{ame}
T_{1_1}	Pat_1,Pat_2	$\frac{1}{37}$	1		T_{7_1}	Pat_2,Pat_3,Pat_4	$\frac{1}{37}$	1	
T_{1_2}		$\frac{1}{37}$	0		T_{7_2}	Pat_2	$\frac{2}{37}$	1	
T_{1_3}		$\frac{3}{37}$	0		T_{8_1}		$\frac{3}{37}$	0	
T_{1_4}	Pat_2	$\frac{1}{37}$	1		T_{9_1}	Pat_3	$\frac{2}{37}$	1	
T_{1_5}	Pat_2	$\frac{2}{37}$	1		T_{10_1}	Pat_2,Pat_3	$\frac{2}{37}$	1	
T_{2_1}	Pat_1,Pat_2	$\frac{1}{37}$	1		T_{10_2}	Pat_3	$\frac{1}{37}$	1	
T_{2_2}	Pat_1	$\frac{3}{37}$	1		T_{10_3}		$\frac{3}{37}$	0	
T_{2_3}		$\frac{3}{37}$	0		T_{11_1}	Pat_1	$\frac{3}{37}$	1	
T_{2_4}	Pat_2	$\frac{1}{37}$	1		T_{11_2}	Pat_2,Pat_3	$\frac{3}{37}$	1	
T_{2_5}	Pat_1	$\frac{3}{37}$	1		T_{11_3}	Pat_3	$\frac{1}{37}$	1	$\frac{\frac{67}{37}}{\frac{81}{37}} = \frac{61}{81} = 0.82$
T_{3_1}	Pat_2,Pat_3	$\frac{1}{37}$	1		T_{12_1}	Pat_1	$\frac{3}{37}$	1	
T_{3_2}	Pat_3	$\frac{3}{37}$	1		T_{14_1}	Pat_2,Pat_3,Pat_4	$\frac{3}{37}$	1	
T_{3_3}	Pat_2	$\frac{2}{37}$	1		T_{15_1}	Pat_1,Pat_2	$\frac{2}{37}$	1	
T_{3_4}	Pat_3	$\frac{3}{37}$	1		T_{15_2}	Pat_2	$\frac{2}{37}$	1	
T_{5_1}	Pat_3	$\frac{3}{37}$	1		T_{16_1}	Pat_3	$\frac{1}{37}$	1	
T_{6_1}	Pat_2,Pat_3,Pat_4	$\frac{2}{37}$	1		T_{16_2}	Pat_1	$\frac{3}{37}$	1	
T_{6_2}		$\frac{1}{37}$	0		T_{17_1}	Pat_3	$\frac{3}{37}$	1	
T_{6_3}	Pat_2	$\frac{1}{37}$	1		T_{17_2}	Pat_1	$\frac{2}{37}$	1	
T_{6_4}	Pat_4	$\frac{3}{37}$	1		T_{17_3}	Pat_2	$\frac{3}{37}$	1	

Tabla 5.3. *Peso de los requerimientos satisfechos*

Requisito	Patrón(es)	μ	v_p	w_{req}
Req_1	Pat_1	$\frac{1}{16}$	1	
Req_2	Pat_1	$\frac{3}{16}$	1	
Req_3	Pat_2	$\frac{3}{16}$	1	
Req_4	Pat_2	$\frac{3}{16}$	1	
Req_5		$\frac{3}{16}$	0	
Req_6	Pat_2	$\frac{3}{16}$	1	
Req_7		$\frac{2}{16}$	0	
Req_8		$\frac{3}{16}$	0	$\frac{\frac{23}{16}}{\frac{42}{16}} = \frac{23}{42} = 0.54$
Req_9		$\frac{3}{16}$	0	
Req_{10}		$\frac{2}{16}$	0	
Req_{11}	Pat_4	$\frac{3}{16}$	1	
Pol_1		$\frac{3}{16}$	0	
Pol_2		$\frac{3}{16}$	0	
Pol_3	Pat_2	$\frac{2}{16}$	1	
Pol_4	Pat_3	$\frac{3}{16}$	1	
Pol_5	Pat_2,Reg_1	$\frac{2}{16}$	1	

5.4. Resultado de la evaluación

Considerando el criterio mostrado en la sección 4.4, el valor obtenido $ss = 0.44$ indica que el sistema no se encuentra protegido ante todas las amenazas identificadas y los requisitos de seguridad y/o políticas de seguridad no están siendo satisfechas de manera adecuada.

Utilizando los valores w_{ame} y w_{req} se identifica la parte del sistema que requiere mejoras. Tomando los valores del ejemplo desarrollado se observa que la parte del sistema que requiere una revisión más exhaustiva por parte de los diseñadores del mismo es la implementación de patrones de seguridad para satisfacer los requisitos de seguridad y políticas de seguridad que se tienen contempladas.

5.5. Resumen

En este capítulo se presenta la evaluación de seguridad de un sistema financiero básico que ejemplifique el método propuesto en el Capítulo 4. En la primera sección se muestra

la información del sistema como diagramas UML, requisitos de seguridad y políticas de seguridad. Con la información obtenida de la primera sección, en las secciones posteriores se realiza el análisis de amenazas, la obtención del peso de las amenazas, la obtención del peso de los requisitos de seguridad y por último el resultado de la evaluación.

La métrica presentada en el presente trabajo muestra la evaluación de seguridad de un sistema que ha sido construido usando patrones de seguridad, analizando la aplicación del método con el ejemplo presentado en este capítulo se plantea la posibilidad de aplicar el método a sistemas que no han sido construidos desde su diseño con patrones de seguridad.

Capítulo 6

Conclusiones

Este capítulo presenta un resumen del trabajo propuesto, las conclusiones a partir de los resultados obtenidos en el Capítulo 5, las contribuciones del trabajo realizado y el trabajo futuro.

6.1. Resumen

De acuerdo a lo descrito en el presente trabajo, se da una solución al problema planteado en el Capítulo 1 a través de la evaluación mostrada en el Capítulo 4. A continuación se hace un análisis de los elementos utilizados para llegar a dicha solución.

Partiendo de la hipótesis presentada en el Capítulo 1:

> *Se puede evaluar la seguridad de un sistema de forma sistemática de tal manera que se proporcione una métrica la cual indique bajo cierto criterio si es seguro o no, si previamente se sabe que ha sido construido usando patrones de seguridad.*

Los elementos inherentes que componen un sistema nos indican qué es lo que realiza el sistema y qué necesita el sistema en cuestiones de seguridad. Utilizando estos elementos, en efecto, se puede realizar una evaluación sistemática independientemente de si el sistema es básico o robusto.

Realizando un análisis de dichos elementos inherentes de un sistema, se consigue identificar las amenazas y conociendo los patrones de seguridad que han sido utilizados en la construcción del sistema se puede definir cuáles de dichas amenazas están siendo mitigadas. Con esto, se define una métrica que indica ante que amenazas está protegido el sistema y cuales requisitos y políticas están siendo atendidas a través de los patrones de seguridad.

El resultado obtenido en el Capítulo 5 muestra que la hipótesis presentada sí es viable. En efecto, utilizando los elementos inherentes de un sistema se puede obtener una evaluación de la seguridad de manera sistemática e identificando cierto criterio se obtiene una métrica que indique si el sistema es seguro o no.

Este indicador le proporciona a los diseñadores y desarrolladores de un sistema un panorama de las amenazas que están y no siendo consideradas, los requisitos y políticas de seguridad que están y no siendo atendidas para que, en caso de ser necesario se apliquen soluciones.

6.2. Contribuciones

Las contribuciones del presente trabajo son:

- La evaluación de seguridad propuesta contempla además de las amenazas a las que un sistema está expuesto, los requisitos y políticas de seguridad.
- Se identifica de manera sistemática las amenazas de seguridad a las que está expuesto el sistema agregando un parámetro de impacto de cada una y se indica cuales de ellas están mitigadas por al menos un patrón de seguridad.
- Se indica cuales de los requisitos y políticas de seguridad están siendo atendidos por patrones de seguridad tomando en cuenta el parámetro de prioridad de cada uno.
- El valor **ss** muestra el nivel de seguridad del sistema con respecto a las amenazas mitigadas y los requisitos y políticas de seguridad atendidas. Pero además, las variables w_{ame} y w_{req} pueden ser utilizadas por los diseñadores para identificar en qué parte del sistema se tiene un menor nivel de seguridad.

- El método de evaluación propuesto puede ser aplicado en sistemas que no han sido construidos utilizando métodos orientados a objetos, puesto que aún es posible identificar los casos de uso.

6.3. Trabajo futuro

A continuación se muestran algunos temas de trabajos futuros:

- Evaluar la seguridad de un sistema sin que se conozca que previamente se han utilizado patrones de seguridad en su diseño, utilizando la aproximación de *security tactics* se puede identificar a través del código del sistema los patrones de seguridad que han sido implementados y posterior a esto poder utilizar la evaluación presentada.
- Se puede utilizar otra forma de enumeración de amenazas antes de pasar a la fase de identificación de los patrones que las mitigan, si es que se requiriera una manera particular de enumerarlas.
- La métrica presentada es aplicable para sistemas construidos con patrones de seguridad, una mejora para verificar su eficiencia es aplicarla a todas las etapas del ciclo de vida del sistema.

Anexos

Bibliografía

[1] Nvidia jetson tx2: High performance ai at the edge.

[2] Bertogna, M. and Baruah, S. (2010). Limited preemption edf scheduling of sporadic task systems. *IEEE Transactions on Industrial Informatics*, 6(4):579–591.

[3] Butazzo, G. C. (2011). *Hard real-time computing systems: predictable scheduling algorithms and applications*. Springer Science Business Media.

[4] Hartmann, C. and Margull, U. (2018). Gpuart - an application-based limited preemptive gpu real-time scheduler for embedded systems. *Journal of Systems Architecture*.

[5] Heath, S. (2003). *Embedded systems design*. EDN Series For Design Engineers.

[6] NVIDIA. Nvidia sobre la computación de gpu y la diferencia entre gpu y cpu.