UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

CREACIÓN DE UNA GUÍA DE ASEGURAMIENTO DE LA INFORMACIÓN PARA APLICACIONES DE SOFTWARE EN EL SISTEMA NACIONAL DE CERTIFICACIÓN DIGITAL EN INTERNET.

Trabajo final de investigación aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Computación e Informática para optar al grado y título de Maestría Profesional en Computación e Informática

ANDRÉS GONZÁLEZ HERRERA

Ciudad Universitaria Rodrigo Facio, Costa Rica

2021

Dedicatoria

A Dios, que siempre me ha bendecido.

A mi esposa, hija y familia que siempre me han apoyado incondicionalmente.

Agradecimientos

Primeramente, debo agradecer a Dios por darle la posibilidad de presentar este trabajo.

También quiero agradecer al Dr. Ricardo Villalón, por su apoyo y paciencia durante todo el desarrollo de este trabajo. Su gran vocación, así como la disposición de colaborar y generar nuevo conocimiento para el país, son un ejemplo de la excelencia que distingue a la UCR.

De igual forma, le debo mi agradecimiento a las personas que han estado presentes y que han colaborado para que este trabajo sea una realidad.

A Miguel Carballo, por brindarme el espacio para desarrollar un trabajo en un tema tan relevante para el país como lo es la Firma Digital.

A mis compañeros del BCCR, Gabriel Lara y Luis Charpentier, que siempre tuvieron paciencia y disposición de colaborar con su conocimiento.

A la Dra. Gabriela Barrantes y el Msc. Alexander Rodríguez por sus aportes y colaboración en el desarrollo del proyecto.

A la UCR y todos los profesores de la universidad, por sus enseñanzas y gran ejemplo, que han sido pilares de mi carrera profesional.

A mi familia, por su apoyo incondicional y porque son ese impulso que me motiva a conseguir mis metas.

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Computación e Informática de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Computación e informática

ADRIAN LARA PETITDEMANGE (FIRMA)
PERSONA FISICA, CPF-01-1225-0679.
Fecha declarada: 23/09/2021 07:49:47 PM
Esta representación visual no es fuente
de confianza. Valide siempre la firma.

Dr. Adrián Lara Petitdemange
Representante del Decano
Sistema de Estudios de Posgrado

RICARDO VILLALON FONSECA (FIRMA)
Firmado digitalmente por RICARDO VILLALON FONSECA (FIRMA)
Fecha: 2021.09.20 13:16:25 -06'00'

Dr. Ricardo Villalón Fonseca
Profesor Guía

ELENA GABRIELA BARRANTES SLIESARIEVA (FIRMA)
PERSONA FISICA, CPF-01-0866-0165.
Fecha declarada: 22/09/2021 11:57:16 AM
Esta representación visual no es fuente
de confianza. Valide siempre la firma.

Dra. Gabriela Barrantes Sliesarieva
Lectora

ALEXANDER RODRIGUEZ CARBALLO (FIRMA)
Firmado digitalmente por ALEXANDER RODRIGUEZ CARBALLO (FIRMA)
Fecha: 2021.09.20 11:48:05 -06'00'

M.Sc. Alexander Rodríguez Carballo
Lector

GABRIELA MARIN RAVENTOS (FIRMA)
Firmado digitalmente por GABRIELA MARIN RAVENTOS (FIRMA)
Fecha: 2021.09.23 19:39:09 -06'00'

Dra. Gabriela Marín Raventós
Directora del Programa de Posgrado
en Computación e Informática

ANDRES GONZALEZ HERRERA (FIRMA)
Firmado digitalmente por ANDRES GONZALEZ HERRERA (FIRMA)
Fecha: 2021.09.20 11:21:09 -06'00'

Andrés González Herrera
Sustentante

Índice de contenido

Resumen

En Costa Rica, la ley de Protección de la Persona frente al tratamiento de sus datos personales establece la responsabilidad de asegurar los datos a quien sea responsable de almacenarlos. Esta obligatoriedad en la ley provoca que incluso instituciones como el BCCR deban desarrollar plataformas sumamente seguras, especialmente si se habla de sistemas tan críticos como la Firma Digital.

El BCCR cuenta con una herramienta que permite firmar digitalmente a través de una aplicación de escritorio y se ha avanzado en la definición de una nueva herramienta para hacerlo desde un dispositivo móvil. Por esto, se requiere de una guía de aseguramiento que contemple los nuevos escenarios, que incluyen tanto el acceso a través de internet y dispositivos móviles, como el acceso desde la aplicación de escritorio usada actualmente. En consecuencia, se identificó la necesidad de verificar que la plataforma implementa correctamente los servicios de seguridad correspondientes y las buenas prácticas de implementación a nivel de código fuente.

El objetivo general de la presente investigación fue desarrollar una guía de aseguramiento de la información para una aplicación de software que utilice los servicios de firma digital del Banco Central de Costa Rica. Para conseguirlo, se abordó la seguridad desde un enfoque multidimensional de la ciberseguridad, basado en un proceso sistemático y controlado, a través del cual se valoraron 72 riesgos, se definieron 45 políticas de seguridad, y se establecieron 24 objetivos de control.

Como resultado, se propuso una guía de implementación que podría funcionar como herramienta para evaluar el cumplimiento de los requisitos de seguridad propuestos.

Abstract

In Costa Rica, the Law on the Protection of Persons Regarding the Processing of their Personal Data establishes the responsibility of protect the data to whoever is responsible for storing them. This obligation in the law means that the institutions such as the BCCR must develop highly secure platforms, especially when talking about systems as critical as the Digital Signature.

The BCCR has a tool that allows digitally sign through a desktop application and a new tool to do so from a mobile device. For this reason, an assurance guide is required that contemplates the new scenarios, which include both access through the internet and mobile devices, as well as access from the desktop application currently used. Consequently, the need to verify that the platform correctly implements the security services and the best coding practices was identified.

The main objective of this research was to develop an information assurance guide for a software application that uses the digital signature services of the "Banco Central de Costa Rica". To achieve this, security was approached from a multidimensional cybersecurity approach, based on a systematic and controlled process, through which 72 risks were assessed, 45 security policies were defined, and 24 control objectives were established.

As a result, an implementation guide was proposed that works as a tool to assess compliance with the proposed security requirements.

Lista de tablas

Lista de figuras

Lista de gráficos

Lista de ecuaciones

Lista de abreviaturas

API *Application Program Interface.*

CA Autoridad Certificadora**.**

CAdES CMS *Advanced Electronic Signature*.

CA SINPE Autoridad Certificadora del Sistema Nacional de Pagos Electrónicos.

CITIC Centro de Investigaciones en Tecnologías de la Información y Comunicación.

CMS *Cryptographic Message Syntax.*

COBIT *Control Objectives for Information and Related Technology*.

BCCR Banco Central de Costa Rica.

DCFD Dirección de Certificadores de Firma Digital.

DCS Dispositivo Criptográfico Seguro**.**

ECCI Escuela de Ciencias de la Computación e Informática.

HSM *Hardware Security Module*.

IEC *International Electrotechnical Commission***.**

ISO *International Organization for Standardization*.

LAN *Local Area Network.*

MICITT Ministerio de Ciencia, Tecnología y Telecomunicaciones.

MVP *Minimum Viable Product.*

NIST *National Institute of Standards and Technology*.

PAdES PDF *Advanced Electronic Signature*.

PDF *Portable Document Format*.

PDF 1.7 PDF *version 1.7*.

PKCS#7 *Public Key Criptography Standard 7*.

RA Autoridad de Registro.

RAM *Random Access Memory*.

RMIAS *Reference Model for Information Assurance and Security*. xix

FVA Firmador, validador y autenticador del BCCR

PE Sistema Nacional de Pagos Electrónicos.

SNCD Sistema Nacional de Certificación Digital.

SQL *Structured Query Language*.

TLS *Transport Layer Security*.

TSA Autoridad de Estampado de Tiempo.

UCR Universidad de Costa Rica.

USB *Universal Serial Bus*.

XAdES XML *Advanced Electronic Signature*.

XML *Extensible Markup Language*.

WYSIWYS *What You See Is What You Sign*.

XMLDSig XML *Digital Signature*.

PKI *Public Key Infrastructure*

UNIVERSIDAD DE COSTA RICA

SEP Sistema de Estudios de Posgrado

Autorización para digitalización y comunicación pública de Trabajos Finales de Graduación del Sistema de Estudios de Posgrado en el Repositorio Institucional de la Universidad de Costa Rica.

Yo, Andrés González Herrera, con cédula de identidad 207110059, en mi condición de autor del TFG titulado CREACIÓN DE UNA GUÍA DE ASEGURAMIENTO DE LA INFORMACIÓN PARA APLICACIONES DE SOFTWARE EN EL SISTEMA NACIONAL DE CERTIFICACIÓN DIGITAL EN INTERNET

Autorizo a la Universidad de Costa Rica para digitalizar y hacer divulgación pública de forma gratuita de dicho TFG a través del Repositorio Institucional u otro medio electrónico, para ser puesto a disposición del público según lo que establezca el Sistema de Estudios de Posgrado. **SI** [X] **NO** *[ ]

***En caso de la negativa favor indicar el tiempo de restricción: _____ año (s).**

Este Trabajo Final de Graduación será publicado en formato PDF, o en el formato que en el momento se establezca, de tal forma que el acceso al mismo sea libre, con el fin de permitir la consulta e impresión, pero no su modificación.

Manifiesto que mi Trabajo Final de Graduación fue debidamente subido al sistema digital Kerwá y su contenido corresponde al documento original que sirvió para la obtención de mi título, y que su información no infringe ni violenta ningún derecho a terceros. El TFG además cuenta con el visto bueno de mi Director (a) de Tesis o Tutor (a) y cumplió con lo establecido en la revisión del Formato por parte del Sistema de Estudios de Posgrado.

INFORMACIÓN DEL ESTUDIANTE:

Nombre Completo: Andrés González Herrera.

Número de Carné: B12908 Número de cédula: 207110059.

Correo Electrónico: andres.gonzalezherrera@ucr.ac.cr.

Fecha: 21/08/2021. Número de teléfono: 89436601.

Nombre del Director (a) de Tesis o Tutor (a): Dr. Ricardo Villalón Fonseca.

ANDRES GONZALEZ HERRERA (FIRMA)

Firmado digitalmente por ANDRES GONZALEZ HERRERA (FIRMA)
Fecha: 2021.09.20 11:22:00 -06'00'

FIRMA ESTUDIANTE

Nota: El presente documento constituye una declaración jurada, cuyos alcances aseguran a la Universidad, que su contenido sea tomado como cierto. Su importancia radica en que permite abreviar procedimientos administrativos, y al mismo tiempo genera una responsabilidad legal para que quien declare contrario a la verdad de lo que manifiesta, puede como consecuencia, enfrentar un proceso penal por delito de perjurio, tipificado en el artículo 318 de nuestro Código Penal. Lo anterior implica que el estudiante se vea forzado a realizar su mayor esfuerzo para que no sólo incluya información veraz en la Licencia de Publicación, sino que también realice diligentemente la gestión de subir el documento correcto en la plataforma digital Kerwá.

1 Introducción

El Índice Global de Ciberseguridad es una muestra de los esfuerzos que realizan los distintos países para contar con herramientas que protejan los datos de los usuarios que navegan a través de Internet; en él se pretende dar una medida del desarrollo de cada Estado nación en temas de ciberseguridad, con el fin de que se intensifiquen esfuerzos para proteger la información (UIT, 2018b). Particularmente, Costa Rica se ubica en el puesto 115 del ranking global donde participan 175 países, lo que indica que aún queda mucho camino por recorrer y mejorar en dichos temas. A pesar de esto, se puede notar esfuerzos importantes como la creación de leyes y reglamentos que fomentan la protección de los datos de las personas.

Un ejemplo de dichos esfuerzos es la ley de Protección de la Persona frente al tratamiento de sus datos personales, aprobada en 2011, donde se establece la responsabilidad de asegurar los datos a quien sea responsables de almacenarlos:

ARTÍCULO 10.- Seguridad de los datos. *El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.*

Esta obligatoriedad en la ley provoca que incluso instituciones como el BCCR deban implementar las medidas necesarias para el aseguramiento de sus datos; por lo que toma mucha relevancia para la institución, las medidas que se puedan adoptar en sus sistemas; siendo uno de los más críticos, la firma digital, que ha sido incluida en el BCCR debido a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Gobierno de Costa Rica, 2006).

Debido a que en dicha ley el BCCR figura como encargado de implementar, custodiar y operar la raíz del SNCD (Víquez y Montes, 2013); esta institución ha tenido que realizar esfuerzos para desarrollar plataformas seguras donde se soporte la demanda de los distintos usuarios en el país.

Hoy en día, el BCCR cuenta con una herramienta que permite firmar digitalmente a través de una aplicación de escritorio y se ha avanzado en la definición de una herramienta para hacerlo desde un dispositivo móvil (Banco Central de Costa Rica, 2017). Por esto, se requiere de una guía de aseguramiento que contemple los nuevos escenarios, que incluyen tanto el acceso a través de internet y dispositivos móviles, como el acceso desde la aplicación de escritorio usada actualmente.

En esta investigación se utiliza un enfoque sistemático para crear una guía para el aseguramiento de la información de las aplicaciones en el contexto planteado. Por lo que la estructura del trabajo responde a un proceso de aseguramiento de aplicaciones, analizando primero los diferentes escenarios y componentes tecnológicos involucrados para luego establecer riesgos y derivar de ellos las políticas y controles necesarios para garantizar en algún grado la seguridad de la información. Como resultado, se propone una guía que se espera sirva de instrumento para evaluar el cumplimiento de los requerimientos de seguridad en los distintos escenarios de uso de las herramientas de firma digital del BCCR.

1.1 Antecedentes

Dada la operación de la firma digital en el país, se han creado numerosas aplicaciones que la utilizan, siendo partícipes de ello instituciones como el mismo Banco Central, el Poder Judicial, el Ministerio de Hacienda, el Tribunal Supremo de Elecciones, el Banco de Costa Rica y el Instituto Nacional de Seguros (Víquez y Montes, 2013). Esto junto con el aumento en el acceso al Internet (UIT, 2018a), han llevado a que el Banco Central

exponga sus soluciones para proveer la firma digital en distintos medios, como por ejemplo los dispositivos móviles.

Dado esto, toma relevancia el análisis de los principales escenarios de firma digital que afronta el Banco Central en la actualidad y en un futuro cercano, como lo son el acceso a través de aplicaciones de software de escritorio y aplicaciones de dispositivos móviles (M. Carballo, comunicación personal, 11 de junio de 2019). En la figura 1 se muestra a grandes rasgos las interacciones esperadas por el Banco Central con sus servicios de Firma Digital.

Para solventar dichos escenarios, en el Banco Central se han hecho grandes esfuerzos y también ha contado con colaboración de instituciones como la Universidad de Costa Rica. Estas iniciativas han generado diversos análisis e incluso guías como la de Mora (2017) que hoy continúa aportando al debido aseguramiento de los sistemas de Firma digital.

Sin embargo, cabe destacar que anteriormente y en la actualidad la comunicación con el firmador se ha venido haciendo a través de enlaces privados, por lo que, al interactuar en Internet por medio de redes no controladas y posiblemente inseguras, el Banco enfrentará escenarios muy distintos a los ya evaluados. Esto implica para el banco asegurar, no solo el no repudio, sino también la integridad, la confidencialidad y la disponibilidad, entre otros (Carballo, 2019).

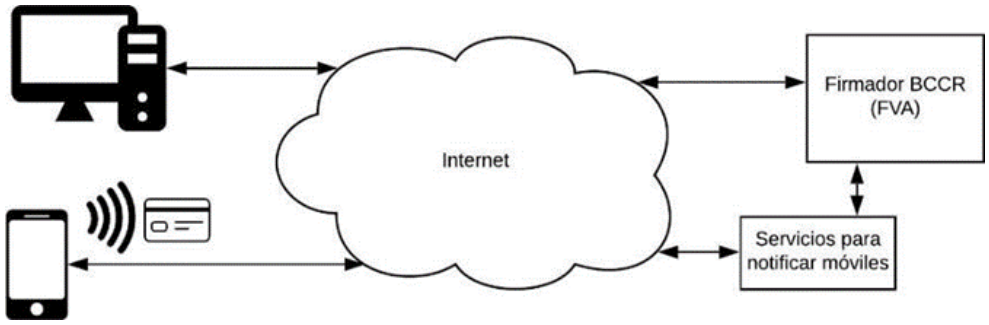

Figura 1Diagrama de interacciones con el Firmador BCCR. Fuente: Elaboración propia

1.2 Descripción del problema

Actualmente se dispone de un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software (Mora, 2017); sin embargo, el Banco Central carece de una guía puntual para el aseguramiento de los escenarios previstos en los que se accedería a través de Internet los servicios del Firmador BCCR, tomando en cuenta que los accesos serán por medio de los distintos clientes de escritorio y móviles a través de redes inseguras.

Dado que tradicionalmente se han accedido estos servicios por medio de redes internas y controladas, este cambio supone una nueva forma de acceder al Firmador BCCR. Las redes inseguras y los diferentes riesgos que se asumen al utilizar el internet generan nuevas necesidades en el tema de seguridad para el Banco Central, por lo que es de mucha importancia para la institución poder contar con un análisis de los escenarios y una guía para su aseguramiento.

1.3 Justificación

Con este trabajo se pretende generar un aporte en el correcto aseguramiento de la información que se manipula a través de los distintos medios que el Firmador BCCR expone a sus clientes, identificando hallazgos y riegos que eventualmente podrían ser traducidos a medidas o mejoras con el fin de satisfacer las disposiciones técnicas y legales definidas en el SNCD.

Los objetivos propuestos en el trabajo permitirán obtener los insumos requeridos para proponer una guía de aseguramiento, donde se incluyan las diferentes políticas y controles de acuerdo con el contexto actual de la institución.

Además, el Banco Central de Costa Rica se beneficiará al contar con una herramienta para asegurar la información en las distintas aplicaciones que accedan al Firmador BCCR, ya sea usando la funcionalidad provista para aplicaciones de escritorio o la funcionalidad

para dispositivo móviles; de modo que se cumpla con la serie de medidas dispuestas para protección de los usuarios de la firma digital en el país.

Esto le permitirá al Banco Central evaluar las herramientas que accedan a los servicios de Firma Digital y determinar si cumplen con las políticas previstas, o eventualmente proponer mejoras para garantizar la seguridad de la información. Esto representa también un beneficio directo a los usuarios de Firma Digital en el país, pues en alguna medida garantiza que las aplicaciones con las que realizan sus firmas cuentan con un grado de aseguramiento aceptado por una entidad como el BCCR y evaluado de una forma metodológica.

Finalmente, este trabajo genera un aporte tecnológico tanto para el BCCR como para el país, debido a que presenta una herramienta que podrá ser aplicada en los escenarios más recientes de uso de la Firma Digital y permitirá asegurar el cumplimiento de las normas y políticas establecidas para proteger la información de los usuarios en el SNCD.

1.4 Objetivos

El objetivo principal de esta investigación fue desarrollar una guía de aseguramiento de la información para una aplicación de software que utilice los servicios de firma digital del Banco Central de Costa Rica. Para conseguirlo, se plantearon los siguientes objetivos específicos:

1. Analizar y delimitar los escenarios en que una aplicación de software utilizaría los medios provistos por el BCCR en Internet para acceder a la firma digital.
2. Identificar y valorar los riesgos de seguridad presentes en los escenarios analizados.
3. Definir políticas y controles de seguridad que permitan minimizar los riesgos identificados.
4. Proponer una guía para el aseguramiento para aplicaciones de software que usen firma digital por medio del Firmador del BCCR en Internet.

1.5 Descripción del resto del documento

Las secciones restantes del documento se organizan de la siguiente forma. En el capítulo 2 se presenta el marco teórico que incluye temas relacionados con firma digital, aseguramiento de la información, ciberseguridad y modelos de seguridad, que son requeridos para la comprensión del trabajo realizado. Seguidamente en el capítulo 3 se detalla la metodología utilizada para alcanzar los objetivos propuestos. Posterior a esto, el capítulo 4 describe el análisis y la representación tanto del sistema como de la seguridad. En el capítulo 5 se muestran los resultados del proceso de identificación y valoración de riesgos. Siguiendo en el Capítulo 6 con un resumen de las políticas de seguridad definidas y los objetivos de control establecidos. El Capítulo 7 propone una guía de aseguramiento para aplicaciones de software que usen firma digital en el contexto evaluado en este trabajo. Por último, el Capítulo 8 presenta las conclusiones obtenidas a partir de la investigación, donde se evidencia el cumplimiento de los objetivos planteados, así como las recomendaciones y consideraciones que podrían colaborar en la realización del trabajo futuro.

2 Marco teórico

En este capítulo se describen los conceptos teóricos necesarios para el correcto entendimiento del presente documento. La primera parte incluye la explicación de los principales fundamentos de la seguridad informática que son necesarios para entender el proceso a seguir durante el trabajo. Se continúa con la descripción de conceptos básicos relacionados con las aplicaciones móviles, que permitirán contextualizar la firma móvil que se pretende analizar en esta investigación. Finalmente se realiza un acercamiento al funcionamiento de la firma digital y otros aspectos relevantes para su análisis, como por ejemplo criptografía, documentos electrónicos, funcionamiento de firma digital, infraestructura de firma digital en Costa Rica, entre otros.

2.1 Fundamentos de seguridad

Los sistemas de información están compuestos por aplicaciones, servicios, activos de tecnología u otros componentes de manejo de información (Instituto de Normas Técnicas de Costa Rica, 2014). Todos estos componentes tienen una gran cantidad de interacciones en distintos contextos sociales y organizacionales con el fin de automatizar tareas específicas (Boell & Dubravka, 2015).

Para realizar dichas tareas, los sistemas utilizan la información que se ha suministrado a través del usuario u otro sistema. Por lo tanto, se vuelve necesario tomar medidas para administrar de la mejor forma posible la información, es decir, asumir un esquema de seguridad que permita mantener la información y el propio sistema en un estado correcto.

Es en este punto que se vuelve relevante el concepto de seguridad de la información, entendido como un conjunto de acciones que protegen y defienden la información y los sistemas velando por establecer los distintos servicios de seguridad como por ejemplo la integridad, disponibilidad, autenticación, confidencialidad, no repudio, entre otros. Tomando en cuenta que se debe contar con la capacidad de detección, protección y restauración de los sistemas (Maconachy, Schou, Ragsdale, & Welch, 2001).

Sin embargo, dada la constante evolución de las tecnologías de la información y los nuevos retos que esto representa; se vuelve importante el análisis de la seguridad desde diferentes dimensiones organizativas, económicas, sociales, políticas y humanas (Goodall, Lutters, & Komlodi, 2009). Esta característica multidimensional es lo que da origen a la ciberseguridad, entendida como la organización y la recopilación de recursos, procesos y estructuras utilizados para proteger los sistemas (Craigen, Diakun-Thibault, & Purse, 2014).

A continuación, se presentan los conceptos fundamentales de seguridad de la información y la ciberseguridad con el fin de contextualizar el presente trabajo.

2.1.1 Ciberespacio

Al mencionar la ciberseguridad, es común encontrar en la literatura referencias a la protección y defensa del ciberespacio (CNSS, 2015), por lo que es importante ubicar el concepto de ciberespacio. Algunos autores como Deibert y Rohozinski (2010) lo definen como un ecosistema dinámico, evolutivo y multinivel; compuesto por infraestructura física, software, regulaciones, ideas, innovaciones e interacciones influenciadas por una población de contribuyentes.

Esta definición sin duda refleja la multidimensionalidad de la ciberseguridad y la necesidad de abordar en este trabajo todas las aristas posibles en los escenarios por asegurar mediante un proceso sistemático y controlado.

2.1.2 Amenazas

Se considera una amenaza a un evento que de ocurrir podría impactar en forma negativa la organización (Racciatti, 2012). La fuente de las amenazas podrían ser ataques cibernéticos o físicos hostiles; errores humanos de omisión, fallas de los recursos controlados por la organización (por ejemplo, hardware, software) y desastres naturales o provocados por el hombre, accidentes y fallas más allá del control de la organización. (National Institute of Standards and Technology, 2012).

Existen distintas clases de amenazas, por ejemplo, la divulgación o acceso no autorizado a la información; el engaño o aceptación de datos falsos; la interrupción de la correcta operación; y la usurpación o control no autorizado de alguna parte de un sistema (Bishop, 2002). Estas cuatro clases abarcan muchas de las amenazas más comunes.

Hay que destacar que la amenaza es potencial, es decir, que podría existir sin llegar a materializarse. Las acciones que hacen que una amenaza se materialice se denominan ataques, y quienes las ejecutan o provocan que sean ejecutadas, se llaman atacantes (Bishop, 2002).

2.1.3 Ciberataque

Un ataque es el conjunto de acciones que hacen que una amenaza se materialice. Ahora bien, si se trata del ámbito de ciberseguridad, podemos entender que un ciberataque es una explotación de una amenaza en el ciberespacio. Esta explotación podría tener como fin el acceder a información no autorizada o segura, espiar, deshabilitar redes y robar datos o dinero (Uma & Padmavathi, 2013).

2.1.4 Vulnerabilidad

Una vulnerabilidad es una debilidad que hace posible materializar una amenaza, es decir, que podría permitir que un atacante cause un daño en el sistema o en los distintos componentes y entidades relacionadas (OWASP, 2020). Una vulnerabilidad podría ser provocada, por ejemplo, debido a errores u omisiones en el diseño, la implementación, los controles internos e incluso en los mecanismos de seguridad (National Institute of Standards and Technology, 2012).

2.1.5 Riesgo

Un riesgo a menudo es definido como un peligro y las consecuencias que pueden ocurrir como resultado de un proceso en curso o futuro. (Febri, 2013). Para cuantificarlo,

es posible definirlo en función de la probabilidad de que una fuente de amenaza explote una vulnerabilidad, y el impacto negativo que pueda provocar en la organización. (National Institute of Standards and Technology, 2012).

Gracias a la posibilidad de cuantificar el riesgo, es posible priorizar cuales deben ser mitigados, dependiendo de su costo y beneficio. Con esto se invierten los esfuerzos según un criterio justificado evitando, por ejemplo, implementar soluciones costosas para ataques pocos probables y con impactos leves a la organización (Bishop, 2002).

2.1.6 Políticas y controles de seguridad

Según Bishop (2004), una política de seguridad se entiende como la definición de lo que es permitido en un sistema de información. Para establecer este criterio, las políticas de seguridad categorizan los estados de un sistema en seguros e inseguros y establecen el contexto en el que se puede definir que un sistema de información es seguro.

Las políticas pueden ser muchas según sean los requerimientos de seguridad de la organización, por ejemplo, en un sistema podría requerirse políticas de integridad, de disponibilidad, de confidencialidad, entre muchas otras. La forma en que se hace cumplir una política ya sea una herramienta, método o procedimiento, es lo que se define como control de seguridad. (Bishop, 2002)

2.1.7 Objetivos de control

Para determinar si una política de seguridad se está cumpliendo, es habitual verificar que los controles implementados sean eficaces. Para lograr esto, es que existe el concepto de objetivo de control.

Mora (2017) incluye en su trabajo una definición ampliada del concepto donde menciona que un objetivo de control "es la definición genérica de los requerimientos de seguridad mínimos que un control de seguridad debe satisfacer para considerarse aceptable, y que excluye detalles de implementación, tales como lenguajes de programación, algoritmos, sistemas operativos, etcétera". Esta forma de entenderlo

permite definir los objetivos de control de una manera adaptable a distintos escenarios, por lo que resulta de mucha utilidad en este trabajo, puesto que permite enfocarse en los elementos más relevantes sin verse afectado por detalles de implementación, salvo cuando representan aspectos esenciales en los objetivos de seguridad definidos.

2.1.8 Servicios de seguridad

Los servicios de seguridad son unos de los aspectos fundamentales en los que se basa la seguridad informática (Bishop, 2002). Autores como (Villalón, Solano, & Marín, 2014) los describen como el conjunto de información, propiedades o requerimientos que se busca satisfacer cuando se está aplicando seguridad.

En la literatura inicialmente se consideraban tres servicios primordiales: confidencialidad, integridad y disponibilidad (McCumber, 1991). Sin embargo, con el paso del tiempo han surgido otros elementos que hoy en día se toman en cuenta para asegurar los datos. Por ejemplo, en publicaciones más recientes se han incluido los servicios de la autenticación y el no repudio (Maconachy, Schou, Ragsdale, & Welch, 2001), que representan aspectos muy importantes en la seguridad de la información, especialmente cuando se trata de firmas digitales.

A continuación, se presenta una descripción de cada uno de estos servicios mencionados, dado que serán de utilidad en el presente trabajo:

Integridad

McCumber (1991) menciona que la integridad identifica qué tan cerca está la información de la realidad, lo que implica que la información debería cumplir con las propiedades de exactitud, relevancia y completitud. También se menciona que la integridad está relacionada con la prevención de un cambio indebido o no autorizado de los datos (Bishop, 2002).

Confidencialidad

La confidencialidad es la característica que garantiza que la información no se divulga a personas, procesos o dispositivos que no han sido autorizados (Maconachy, Schou, Ragsdale, & Welch, 2001). Para lograr esto, algunos autores como Bishop (2002) consideran importante el uso de mecanismos de control de acceso a la información, como por ejemplo la criptografía, que vuelve la información incomprensible para quien no esté autorizado.

Disponibilidad

Esta propiedad busca asegurar que la información esté disponible para los usuarios autorizados cada vez que ellos la necesiten o la soliciten (McCumber, 1991).

No repudio

El no repudio es la característica que permite que un remitente no pueda negarse a aceptar que envió o modificó alguna información. (Buchmann, Evangelos, & Wiesmaier, 2014). Para lograrlo se busca que el remitente de los datos adjunte una prueba indicando que él fue el responsable de enviar la información y el destinatario recibirá también dicha prueba para estar seguro de que el remitente es quien realmente dice ser (Maconachy, Schou, Ragsdale, & Welch, 2001).

Autenticación

La autenticación es el servicio de seguridad que verifica si una persona, entidad o sitio web es quien dice ser. Por ejemplo, la autenticación en el contexto de las aplicaciones web se realiza normalmente mediante el envío de un nombre de usuario y uno o más elementos de información privada que solo un usuario determinado debe conocer. Modelos de seguridad informática. (OWASP, 2020)

2.1.9 Modelos de seguridad informática

La seguridad de la información no es una tarea fácil, debido a esto, a través de la historia se han creado algunos modelos que buscan administrar de una mejor forma la

seguridad. Dichos modelos de seguridad son herramientas para hacer cumplir políticas de seguridad de la información utilizando métodos formales o informales. (Villalón, Solano, & Marín, 2014). Para el desarrollo de este trabajo se han adoptado características de los modelos que se describen a continuación.

Modelo de McCumber

En 1991, McCumber publicó su modelo de cubo, como se aprecia en la Figura 2, está compuesto por tres dimensiones. En una dimensión se ubican las características básicas de la seguridad de la información; a saber: confidencialidad, integridad y disponibilidad. En otra dimensión coloca los estados en los que puede estar la información; ya sea en transmisión, almacenada o en procesamiento. Finalmente, en la tercera dimensión menciona las medidas de seguridad útiles para el aseguramiento, donde podemos distinguir la tecnología, las políticas y prácticas y la educación, entrenamiento y conciencia.

La tecnología se refiere a cualquier dispositivo físico o técnica implementada que ayude en el aseguramiento de las características críticas de la información en cualquiera de los tres estados mencionados previamente. Las políticas y prácticas son el "qué" y el "cómo" se quiere asegurar. La educación, entrenamiento y conciencia, son habilidades que deben tener los usuarios para complementar el resto del sistema de seguridad (McCumber, 1991).

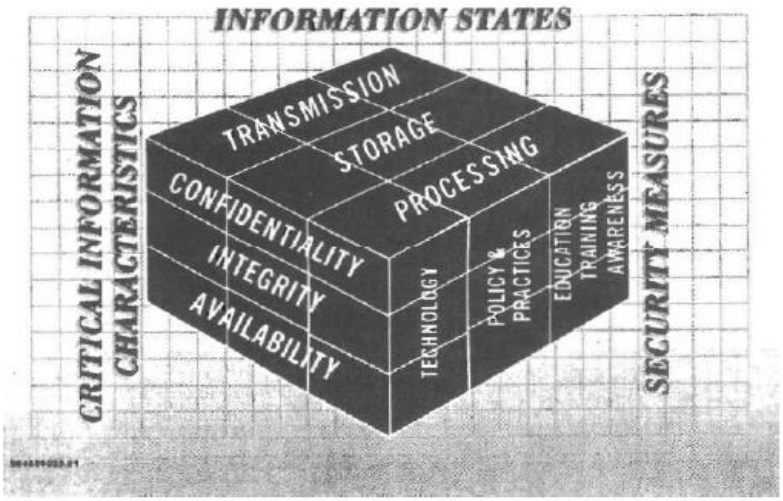

Figura 2 Modelo Original de McCumber. Fuente: (McCumber, 1991)

Modelo de Maconachy

El modelo de McCumber también constituyó una base para otros modelos que han surgido haciendo referencia al original, por ejemplo, el modelo de Maconachy. En este modelo, que mantiene los mismos principios, se agregan dos servicios de seguridad adicionales: la autenticación y el no repudio.

Además, se incluye una cuarta dimensión que representa al tiempo, dándole gran importancia como un agente de cambio que impacta a las demás dimensiones. Es decir que cuando hay cambios a través del tiempo en una dimensión, es posible que se requieran modificaciones en otras dimensiones para mantener el sistema en un estado seguro. (Maconachy, Schou, Ragsdale, & Welch, 2001)

En la Figura 3 se muestra el diseño del modelo de seguridad, donde se pueden notar los cambios y las similitudes.

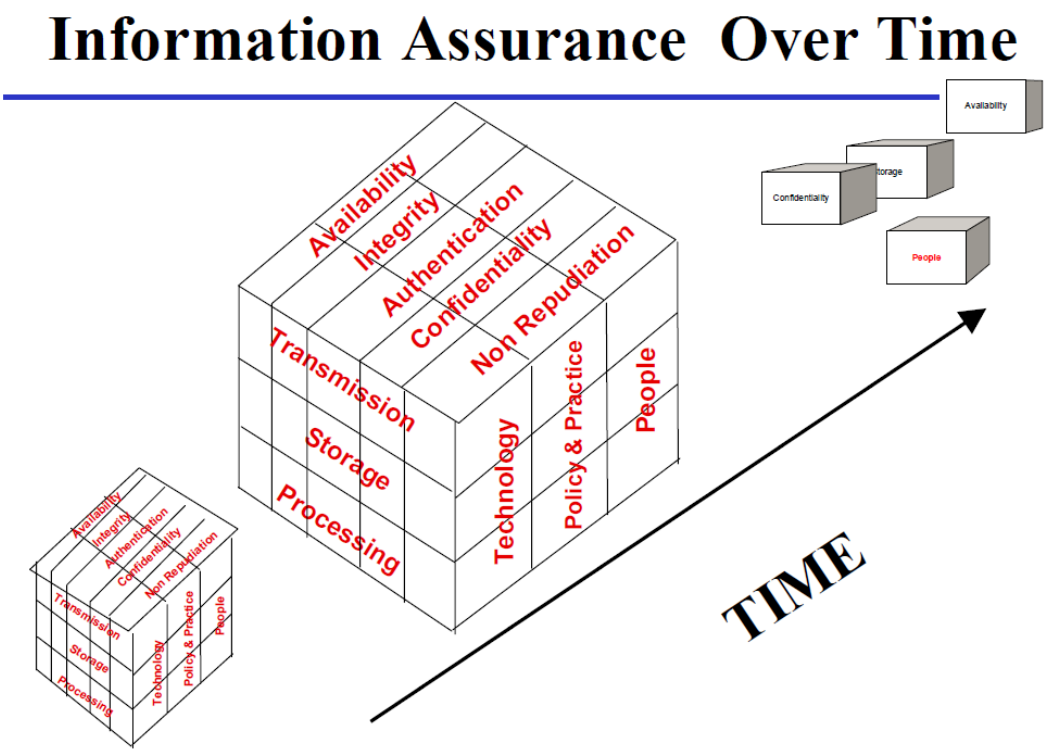

Figura 3 Modelo de Maconachy. Fuente: (Maconachy, Schou, Ragsdale, & Welch, 2001)

Modelo Infosec-Tree

El Infosec-Tree es un modelo que utiliza un patrón jerárquico del todo y las partes. En este modelo, un sistema tecnológico se descompone en los elementos que lo integran, utilizando un árbol. (Villalón, Solano, & Marín, 2014)

La raíz de ese árbol simboliza la totalidad del sistema. Los niveles más altos son las partes más grandes del sistema y conforme se avanza a niveles más bajos, se encuentran las partes más pequeñas. (Villalón, Solano, & Marín, 2014) Los nodos de este árbol pueden representar cualquier elemento del sistema, ya sea hardware o software, componentes físicos o lógicos, reales o virtuales, o bien una mezcla de todos ellos, siempre y cuando se respete el enfoque del todo y las partes. (Villalón, Solano, & Marín, 2014)

Para representar requerimientos de seguridad se utilizan las triadas, que tienen la siguiente forma: {Momento de seguridad, Estado de la información, Servicio de seguridad}. Y para representar nodos que se comunican, se utilizan los diagramas de flujos de información, donde las conexiones también son representadas mediante triadas, que en este caso se llaman triadas de puntos de conexión. (Villalón, Solano, & Marín, 2014)

Este modelo mantiene un enfoque ordenado y permite cubrir los elementos del sistema de una forma sistemática, lo cual es de suma importancia para este trabajo, especialmente en lo relacionado con la representación del sistema mediante el árbol del todo y las partes y los diagramas de flujo.

2.1.10 Estándares de seguridad informática

Como base para el desarrollo de este trabajo, también se tomaron características de algunos estándares relacionados con la seguridad informática. A continuación, se presenta una descripción de cada uno de ellos.

NIST 800-30 revisión 1, guía para conducir evaluaciones de riesgo

Como indica el NIST (2012), los sistemas de información están sujetos a graves amenazas que pueden tener efectos adversos en las operaciones y activos organizacionales, individuos y otras organizaciones, mediante la explotación de vulnerabilidades conocidas y desconocidas. Para mitigar esto, recalcan la importancia que tienen las evaluaciones de riesgo a nivel organizacional.

Las evaluaciones de riesgo son utilizadas para identificar, estimar y priorizar riesgos que pueden afectar a los individuos, las operaciones y los recursos de la organización (National Institute of Standards and Technology, 2012).

En su publicación, el NIST establece una serie de pasos recomendados para guiar una evaluación de riesgo. A continuación, se presenta en resumen los pasos que han sido ilustrados en la Figura 4.

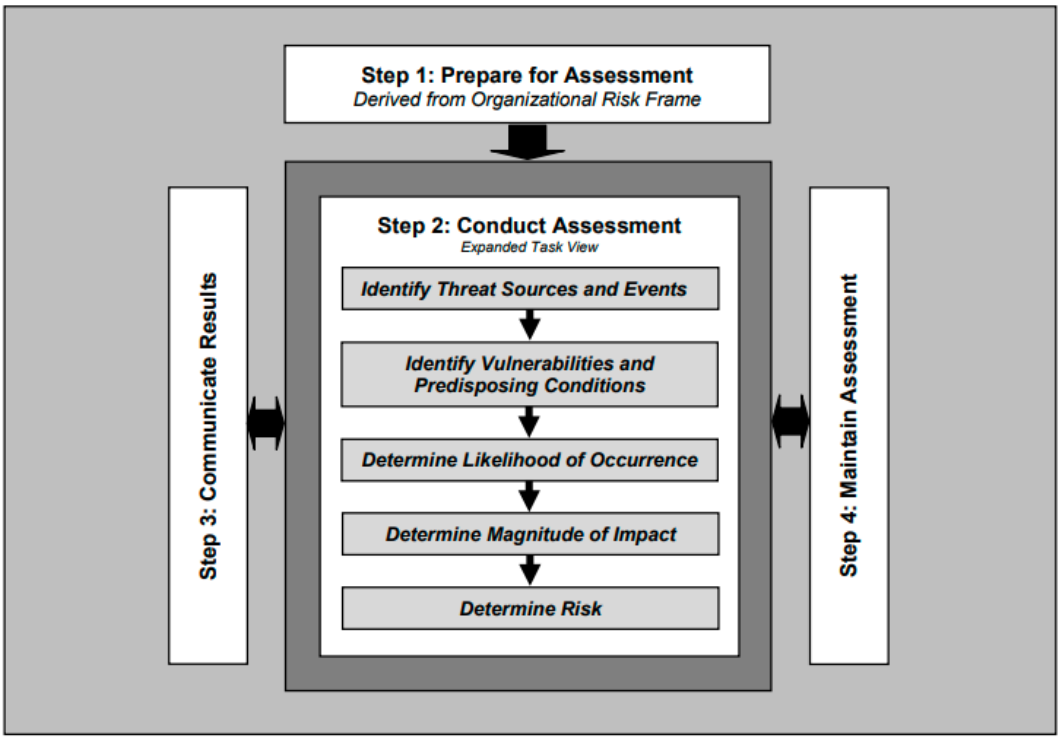

Figura 4 Proceso para la evaluación de riesgos. Fuente: (National Institute of Standards and Technology, 2012)

1. Preparar la evaluación

Con el objetivo de definir el contexto del proceso de evaluación de riesgos, se deben llevar a cabo las siguientes tareas.

- Identificar el propósito de la evaluación.
- Identificar el alcance de la evaluación.
- Identificar las suposiciones y las limitaciones asociadas con la evaluación.
- Identificar las fuentes usadas como entradas de información para la evaluación.
- Identificar el modelo de riesgo y los enfoques analíticos a ser usados durante la evaluación.

2. **Conducir la evaluación**

En esta etapa el objetivo es producir una lista de riesgos en la seguridad de la información que pueden ser priorizados según su nivel de riesgo y utilizados para la toma de decisiones. Para lograrlo se tienen las siguientes tareas:

- Identificar fuentes de amenazas que son relevantes para la organización.
- Identificar eventos que podrían ser producidos por esas amenazas.
- Identificar vulnerabilidades dentro de la organización que podrían ser explotadas por fuentes de amenazas a través de eventos específicos, y las condiciones que podrían favorecer una explotación exitosa.
- Determinar la probabilidad de que las fuentes de amenazas identificadas puedan producir eventos de amenazas, y de que esos eventos sean exitosos.
- Determinar el impacto que afecta a la organización como resultado de la explotación de vulnerabilidades por las fuentes de amenazas.
- Determinar el riesgo en la seguridad de la información, como una combinación de la probabilidad y el impacto descritos.

3. **Comunicar y compartir los resultados**

En esta fase se comparten los resultados y la información del proceso de evaluación. El objetivo es garantizar que las personas encargadas de la toma de decisiones en la organización tienen información suficiente acerca de los riesgos, para tomar las decisiones al respecto. Esta etapa se logra mediante las siguientes tareas:

- Comunicar los resultados de la evaluación de los riesgos.
- Compartir la información obtenida a partir de la evaluación.

4. **Mantener la evaluación**

Esta fase trata de mantener actualizado el conocimiento de los riesgos en los que se puede incurrir, ante eventuales cambios. Las tareas que indican para completar esta fase son las siguientes:

- Monitorear factores de riesgo identificados durante las evaluaciones de forma continua, y comprender los cambios que se produzcan en los mismos.
- Actualizar los componentes de las evaluaciones de riesgo, reflejando las actividades de monitoreo realizadas.

Esta guía es de vital importancia para este trabajo, debido a que será utilizada como base para la definición y evaluación de los riesgos presentes en los sistemas analizados; brindando de esta forma una base para la definición de políticas y controles de seguridad.

NIST 800-163 revisión 1, comprobación de la seguridad de las aplicaciones móviles

En el marco de los ambientes móviles, el NIST (2019) también emite criterios y recomendaciones para el aseguramiento. En esta guía, los autores mencionan que es importante mantener un proceso de evaluación de riesgos tal como se hace con los demás sistemas. Además, añaden a la fase de preparación de la evaluación un concepto muy importante, como lo es el nivel de tolerancia al riesgo (National Institute of Standards and Technology, 2019).

El nivel de tolerancia al riesgo es el nivel, o grado de incertidumbre, que es aceptable para una organización. Un nivel de tolerancia al riesgo definido identifica el grado en que una organización debe estar protegida. (National Institute of Standards and Technology, 2019)

Al definir el nivel de tolerancia al riesgo se debe tener en cuenta los siguientes factores:

- Cumplimiento de las normas, recomendaciones y mejores prácticas de seguridad
- Riesgos de privacidad
- Amenazas de seguridad
- Datos y valor de los activos

- Industria y presión competitiva
- Preferencias de gestión.

En este trabajo es importante tener claro cuál es el nivel de tolerancia que se maneja para las aplicaciones analizadas, en especial si se considera que esto tendría un impacto en la definición y selección de los riesgos identificados.

2.2 Dispositivos móviles

Hoy en día, los dispositivos móviles son un elemento común en la vida diaria de las personas. El uso masivo de estos dispositivos, tanto en el ámbito personal como en el laboral, ha provocado que las organizaciones consideren seriamente los potenciales problemas de seguridad que los afectan. (Pacheco & Piazza, 2007)

Para poder contextualizar los escenarios de análisis que se plantean en este trabajo, se definen brevemente algunos de los conceptos a los que se hace referencia.

2.2.1 Dispositivo móvil

En la actualidad muchos aparatos como teléfonos, cámaras, computadoras portátiles, entre otros, son considerados dispositivos móviles. Según la W3C (Nkeze, Pearce, & Womer, 2007) son todos aquellos aparatos portátiles, con los que se puede acceder a la web y están diseñados para ser usados en movimiento. Inclusive autores como Morillo (2010) van un poco más allá y mencionan que para categorizar a un dispositivo como móvil se deben cumplir las siguientes características esenciales.

- Movilidad.
- Tamaño reducido
- Comunicación inalámbrica
- Interacción con las personas
- Capacidad de procesamiento
- Conexión permanente o intermitente a una red

- Uso de memoria (RAM, tarjetas MicroSD, Flash, entre otros)
- Normalmente se asocian al uso individual, tanto en posesión como en operación

2.2.2 Notificaciones "*push*"

Una notificación en el contexto móvil es un mensaje que aparece en el dispositivo del usuario. Las notificaciones "*push"* son aquellas que se pueden activar localmente mediante una aplicación, o se pueden enviar desde un servidor al usuario incluso cuando la aplicación no se está ejecutando. (Google, 2020)

2.2.3 NFC

NFC por sus siglas en inglés que significa Near Field Communication, es un conjunto de tecnologías inalámbricas de corto alcance, que generalmente requieren una distancia de 4 cm o menos para iniciar una conexión. Con esta tecnología es posible compartir cargas de datos entre distintos dispositivos. (Google, 2020)

2.3 Criptografía

En el ámbito de la ciberseguridad, se puede definir la criptografía como el estudio de técnicas matemáticas para proteger información, cálculos y sistemas digitales de ataques adversarios. (Katz & Lindell, 2014).

Es importante recalcar que la criptografía no es el único mecanismo para proveer seguridad de la información, sino más bien, son un conjunto de técnicas y procedimientos matemáticos con el objetivo principal de permitir a los usuarios comunicarse de forma segura a través de un canal inseguro. (Menezes, van Oorschot, & Vanstone, 1997)

El componente fundamental de la criptografía es el sistema criptográfico. Existen varios tipos de sistemas, por un lado, están los que usan la misma llave para cifrar y descifrar; por otra parte, están los sistemas de criptografía asimétrica o llave pública que

utilizan un par de llaves que están relacionadas matemáticamente. En estos últimos la llave pública se usa para cifrar mensajes y la privada para descifrarlos. (Bishop, 2002)

En la criptografía de llave pública se establece una diferencia entre las llaves de cifrado y las de descifrado. Una de estas llaves es de conocimiento público, mientras que la otra es solamente de conocimiento del dueño. Cuando se desea enviar un mensaje secreto, lo que se hace es cifrar dicha información con la llave pública del destinatario y enviarlo. Cuando el destinatario lo recibe, lo descifra haciendo uso de su llave privada (Bishop, 2002).

Bishop (2002) hace énfasis en que para que este sistema funcione correctamente se deben cumplir las siguientes tres premisas:

- Debe ser computacionalmente fácil cifrar y descifrar un mensaje, dada la llave correcta.
- Debe ser computacionalmente imposible descubrir la llave privada a raíz de la llave pública.
- Debe ser computacionalmente imposible descubrir la llave privada a raíz de un ataque.

2.4 Firma digital

La conservación y organización de documentos siempre han sido temas de especial interés en distintos campos. Aunado a esto, el surgimiento de las tecnologías de la información y la aparición de los documentos electrónicos han traído consigo una serie de nuevos desafíos. (Aguilar, Barquero, Chavarría, Fernández, & Solano, 2011)

El uso extendido y continuamente creciente de los documentos electrónicos ha provocado que surjan nuevas necesidades, como el poder vincularlos con su autor, tal como se hace con la firma manuscrita en los documentos tradicionales. (Aguilar, Barquero, Chavarría, Fernández, & Solano, 2011)

Para lograr esto, inicialmente surge el concepto de la firma electrónica, que consiste en un conjunto de datos que se adjunta o asocia a otro conjunto de datos y que es capaz de identificar al firmante. Como menciona Aguilar et al. (2011), este concepto no ha sido introducido en la legislación costarricense debido a que usualmente no constituye un mecanismo equivalente a la firma manuscrita. (Aguilar, Barquero, Chavarría, Fernández, & Solano, 2011)

Esto se puede ejemplificar si se piensa en un documento al que se adjunta una imagen escaneada de la firma manuscrita, que cumple con la definición al ser un conjunto de datos que se asocia al documento y que identifica al firmante. Pero en este caso, dado que ese tipo de archivos podría ser copiado, alterado o borrado con relativa facilidad, no se puede considerar que es un mecanismo equivalente a la firma manuscrita.

Para resolver este inconveniente, existe el concepto de firma digital, que es un subconjunto de las firmas electrónicas, en el cual, haciendo uso de criptografía asimétrica y los certificados digitales, se logran resolver las deficiencias de las firmas electrónicas para vincular jurídicamente al autor. (Mora, 2017)

El Gobierno de Costa Rica (2005) define la firma digital como conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permite verificar su integridad, así como identificar de forma unívoca y vincular jurídicamente al autor con el documento. Además, en la Ley N° 8454 se les otorga a los mecanismos de firma digital que cumplan con ciertos requerimientos técnicos y legales, el mismo peso probatorio que la firma manuscrita (Gobierno de Costa Rica, 2005)

2.4.1 Funcionamiento de la firma digital

En este trabajo se analizan distintos escenarios de firma digital sin hacer énfasis en los procesos internos de creación y verificación de la firma. Sin embargo, es igualmente importante entender su funcionamiento para la identificación de riesgos y el

establecimiento de políticas y controles. Es por esto que en esta sección se brinda una descripción muy simplificada de dichos procesos.

El proceso de creación de una firma digital comienza calculando un resumen del documento electrónico que se requiere firmar. Para esto se utiliza una función hash resistente a colisiones y de una sola vía. Seguidamente a partir de la llave privada del firmante, se cifra el resumen obtenido. Ese resumen cifrado del documento constituye la firma digital. (Aguilar, Barquero, Chavarría, Fernández, & Solano, 2011)

El proceso de verificación de la validez de la firma digital consiste en tomar la fima y descifrarla mediante la llave pública del firmante, lo que produce un resumen, que corresponde al documento original. Posteriormente, se calcula de nuevo un resumen del documento electrónico original, y se compara con el resumen obtenido en el primer paso. Si ambos son iguales, la firma se considera válida. (Aguilar, Barquero, Chavarría, Fernández, & Solano, 2011)

Cabe destacar que estos procesos han sido presentados de una forma general, pero que existen múltiples factores que podrían agregar complejidad y que no están explicados en este trabajo, debido a que no se considera requerido para el entendimiento y análisis del problema a resolver.

2.4.2 Firma en dispositivos móviles

El ritmo de la tecnología en la actualidad y el avance vertiginoso de los dispositivos móviles han hecho que se vuelva importante llevar la firma electrónica al campo de la movilidad. (Alcaraz, 2019)

Cada día las capacidades de los dispositivos móviles se parecen mucho a las que podríamos tener en una computadora de escritorio y, por lo tanto, la ejecución de aplicaciones en una u otra plataforma no resultan tan diferentes ante la perspectiva del usuario. Autores como Alcaraz (2019), inclusive mencionan que, en estos casos, los

procesos de firma apenas se deberían diferenciar en la limitación de la pantalla y la dificultad de conexión con elementos externos como lectores de tarjetas criptográficas.

Ante esto, han surgido una serie de modelos para la aplicación de la firma digital en dispositivos móviles. A continuación, se describen brevemente algunos de los principales escenarios de la firma digital móvil, que permiten contextualizar el presente trabajo.

Claves criptográficas en SIM

Para poder implementar la firma digital con teléfonos móviles, algunos operadores de telefonía móvil han desarrollado plataformas de firma que utilizan tarjetas SIM con capacidades criptográficas, para generar y almacenar en ellas claves y certificados digitales. Gracias a esto, les es posible realizar firmas de documentos y transacciones utilizando un teléfono móvil como dispositivo de firma.

Figura 5 Diagrama de firma digital usando tarjeta SIM. Fuente: (Alcaraz 2019)

Como se muestra en la Figura 5, para realizar firmas desde un teléfono móvil es necesario contar con una tarjeta SIM criptográfica con soporte de firma electrónica y un

certificado emitido por una autoridad de certificación que tenga conexión con la plataforma del operador de telefonía móvil del cliente. (Alcaraz, 2019)

Claves criptográficas en microSD

El hecho de que la mayoría de los dispositivos móviles ya utilizan el hardware de tarjetas microSD, ha motivado a que se desarrollen tarjetas de memoria que permiten disponer de la funcionalidad de dispositivos criptográficos. (Alcaraz, 2019)

En este escenario la memoria y el controlador criptográfico pueden ser accedidos independientemente del terminal en que se usen y las claves criptográficas pueden ser generadas directamente en la tarjeta microSD sin que tengan que dejar el sistema original, y por tanto son menos expuestas a riesgos de intercepción o manipulación. (Alcaraz, 2019)

Lector de tarjetas criptográficas

Dado la posibilidad de incorporar dispositivos con conectividad al móvil, es factible crear firmas digitales de la misma forma que se haría en una computadora de escritorio: haciendo uso de un software específico y de un lector de tarjetas criptográficas. (Alcaraz, 2019)

Firma mediante NFC

Otra posibilidad para la incorporación de la firma en los dispositivos móviles se encuentra en el uso de tarjetas compatibles con la tecnología de NFC, mediante la cual no se requiere de otro dispositivo adicional (Alcaraz, 2019).

En este escenario, es requerido contar con tarjetas que incluyan la capacidad de almacenar los certificados digitales y comunicarse mediante NFC.

Firma en el lado del servidor

En este modelo, se propicia la creación de la firma mediante el uso de claves centralizadas alojadas en “la nube”. Esto difiere significativamente del modelo de claves

alojadas en dispositivos (Tarjeta criptográfica, SIM, SDCard etc.), y hace posible desarrollar software de firma para dispositivos sin la necesidad de disponer de un dispositivo criptográfico. (Alcaraz, 2019)

En este escenario, generalmente se almacenan las claves y eventualmente se generan las firmas, en un Módulo de Seguridad por Hardware (HSM), ya que estos dispositivos pueden tener conectividad y aportar funcionalidad criptográfica de clave pública de alto rendimiento que se efectúa dentro del propio hardware (Alcaraz, 2019).

3 Metodología

En este capítulo se describen detalladamente las etapas y procedimientos que se llevarán a cabo para cumplir con los objetivos definidos en esta investigación.

Cabe destacar que la metodología utilizada en este trabajo ha sido elaborada con base en las propuestas que surgen del contexto del proyecto de investigación B9095 "Creación de una herramienta sistémica y con apoyo automático parcial para el aseguramiento de la información en sistemas de computadores, software y redes", inscrito en la Vicerrectoría de Investigación de la UCR.

En dicha metodología se busca primeramente definir claramente el sistema y generar una base para preparar el análisis de la seguridad. Esto se realiza mediante el análisis de los escenarios de firma digital que estarán sujetos al proceso de aseguramiento, la construcción de la representación del sistema y la definición de los objetivos de seguridad de alto nivel que delimitan y a su vez guían el desarrollo del trabajo

La siguiente etapa, consiste en propagar los objetivos de seguridad dentro del sistema. Además, se identifican las relaciones y las cadenas de seguridad entre los componentes del sistema que servirán como insumos para tareas como la identificación y valoración de riesgos, la definición de políticas y controles de seguridad y eventualmente la creación de una guía de implementación que permita evaluar las políticas definidas. En la Figura 6 se resumen los pasos de la metodología.

Cabe destacar que cada artefacto que se va generando en las distintas etapas, requiere de un ciclo de diseño con su respectivo proceso de evaluación. Por ejemplo, en la etapa de definición de los objetivos, se debe realizar la respectiva evaluación para garantizar que dichos objetivos están acordes a la solución propuesta y son los esperados tanto para el desarrollo del trabajo como para el BCCR.

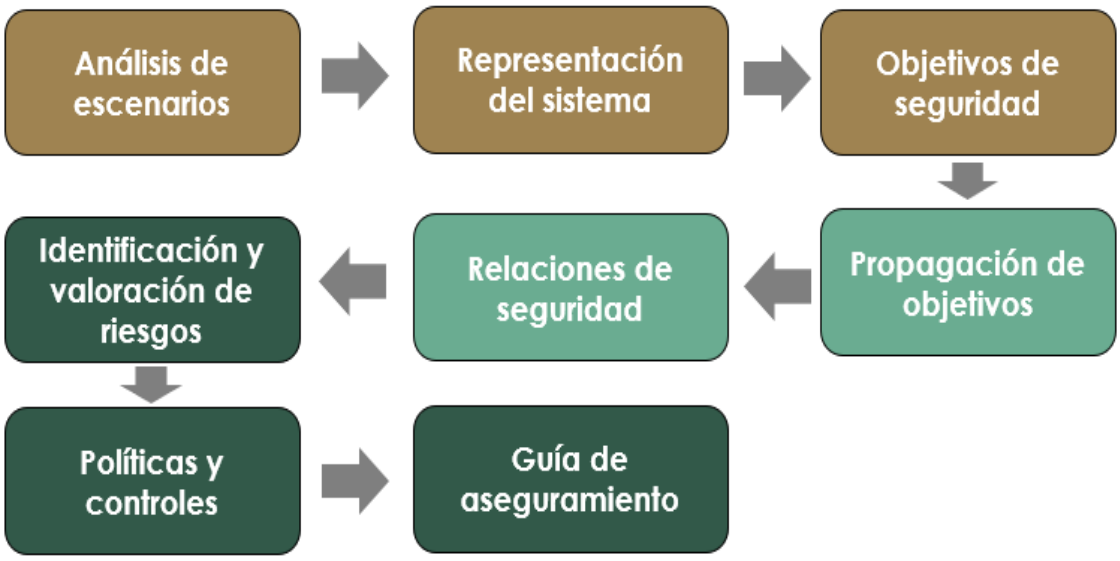

Figura 6. Etapas de la metodología para abordar los objetivos del trabajo.

Fuente: Elaboración propia.

3.1 Análisis de escenarios

En esta sección se presenta la metodología seguida para el debido análisis y selección de escenarios de la firma digital sobre el contexto de este trabajo. Es esta etapa se llevaron a cabo dos actividades: la recopilación de los escenarios del sistema y la selección de los que serían incluidos dentro del alcance de la investigación.

Para lograr recopilar los escenarios del sistema, fue necesario hacer una revisión de los documentos que describen la funcionalidad del sistema y también de las distintas normas, estándares y leyes que aplican en este contexto.

La selección de las fuentes pertinentes fue realizada en base a lo recopilado en reuniones con los expertos del Área de Seguridad de la División de Servicios Tecnológicos del BCCR y el análisis de trabajos previos relacionados, leyes y normas establecidas en el país.

Una vez recopilados los escenarios, se procedió a seleccionar los que serían incluidos en el trabajo. Esto se logró a partir de reuniones con los expertos, en donde de acuerdo con las preocupaciones y necesidades de la organización, se delimitó una lista de los escenarios más importantes y se descartaron los que ya han sido cubiertos por otros trabajos de investigación o que estuvieran fuera del alcance de esta investigación.

3.2 Construcción de la representación del sistema

A partir de los escenarios seleccionados para el análisis, se debe establecer una representación del sistema que permita la aplicación de las siguientes etapas del proceso. Esto se logra por medio de dos pasos, a saber, la construcción de un árbol del todo y las partes y la elaboración de los diagramas de interacción. Cabe destacar que ambos artefactos serán validados mediante reuniones y análisis con expertos del BCCR.

3.2.1 Árbol del todo y las partes

Este elemento, permite describir la organización estructural del sistema y funciona como punto de partida para conocer cuales componentes serán protegidos. Para construir el árbol del todo y las partes se comienza con la definición de un nodo raíz o primer nivel, que será la representación de todo el sistema, en este caso, el sistema de firma digital del BCCR. Luego para el segundo nivel, se descompone el sistema en partes grandes o independientes, como en este caso, el componente de firma digital móvil y el de firma digital de escritorio. A partir de esto, se continúa con los siguientes niveles seleccionando algunos (o todos) los componentes y describiéndolos como las sub partes hasta llegar al nivel de detalle deseado.

Es importante destacar que el árbol resultante puede no ser equilibrado debido a que no todos los nodos se descomponen siempre al mismo nivel de granularidad. En el caso particular de este trabajo, se consideró un nivel de granularidad diferente en algunos componentes, con el fin de ajustarse al alcance acordado con los especialistas del BCCR. Esto tiene impacto en el proceso y el nivel de detalle para el resultado final.

3.2.2 Diagramas de interacción

Los diagramas se construyen a partir de las interacciones internas y externas que se presentan entre los componentes del sistema; siendo cada nodo un componente y cada arista una interacción. En el caso de las interacciones externas, solamente los componentes sobre los que se tiene autonomía serán parte del proceso de aseguramiento, siendo estos generalmente el lado interno de la interacción.

La composición de estos diagramas puede ser tan sencilla como todas las interacciones directas para un solo componente o tan complejo como las interacciones presentes en un caso de uso, donde habría diferentes niveles de granularidad, y describe una secuencia de interacciones para un escenario funcional del sistema.

Para la elaboración de los diagramas de este trabajo se fraccionaron las relaciones por afinidad de los componentes y por funcionalidad. Dando como resultado diagramas en los que existen relaciones con componentes internos y externos. Los componentes externos al BCCR fueron excluidos del proceso de aseguramiento y solamente se tomarán en cuenta acciones para los componentes que están bajo el control de la organización.

Una vez que se dispone de estos diagramas, además del árbol del todo y las partes, es posible continuar con la definición y propagación de los objetivos.

3.3 Definición de los objetivos de seguridad de alto nivel

Como parte de una metodología para desarrollar un proceso de aseguramiento, es importante identificar los objetivos de seguridad que se pretenden alcanzar y que, a su vez, delimitan el trabajo a realizar. Dichos objetivos, es común que sean establecidos a partir de una revisión de las políticas de alto nivel y objetivos generales de la organización.

Para la elaboración de este trabajo, se procederá primero con la definición de los objetivos a ser analizados. Para esto se evaluaron las necesidades y la naturaleza de los sistemas del BCCR.

En esta etapa fue posible establecer tres objetivos de seguridad que serán la guía para el análisis de este trabajo; a saber: integridad, confidencialidad y autenticación. Cabe mencionar que se descartó el objetivo de preservación del no repudio, debido a que se encuentra cubierto por trabajos previos (Mora, 2017).

A continuación, se describe brevemente cada uno de los objetivos que serán tomados en cuenta, y la razón por la cual son relevantes para el desarrollo de esta investigación.

3.3.1 Integridad

Debido a que el BCCR provee al usuario de software cliente para la realización de la firma digital, es importante para la organización asegurar que tanto la información como el mismo software preservan su integridad en los distintos procesos en los que interactúan. Esto en el contexto de los canales del Firmador BCCR, significa que tanto el software instalado en el dispositivo del usuario, como la información que es enviada y recibida, debe mantenerse tal como es esperado, sin alteraciones ni destrucciones, durante el proceso de la firma digital. Por ejemplo, si el usuario envía un documento firmado al sistema, se espera que este llegue a su destino con la misma información que fue creado. Pero si por el contrario el documento es alterado o eliminado por un tercero en el transcurso de los procesos de firma, entonces se estaría comprometiendo la integridad de la información.

Es importante destacar que el software que se brinda al cliente también está expuesto a este tipo de situaciones, donde un atacante podría intentar comprometer la integridad del mismo con el objetivo de explotar alguna vulnerabilidad. Por ejemplo, si se piensa en un escenario donde es posible crear una copia del Firmador e incluir código malicioso, un atacante podría generar miles de copias e intentar generar afectación en el sistema por medios como denegación de servicios, entre otros. En este trabajo, gracias al abordaje iterativo de los componentes y los objetivos de seguridad, es posible detectar dichas relaciones y posibles riesgos asociados.

3.3.2 Confidencialidad

Un objetivo de seguridad que se vuelve relevante cuando existe la posibilidad de manipular información sensible, es la confidencialidad. Esta investigación, debe tomar en cuenta que mucha de la información manipulada por el sistema de Firma Digital es de uso confidencial, por lo que se debe analizar los escenarios con el fin de garantizar en cierto grado que los datos del sistema sólo son visualizados por las personas autorizadas para tal fin.

Un ejemplo claro de estas situaciones es un escenario en el que un usuario no autorizado acceda a la información contenida en un documento que otra persona está firmando en su propio dispositivo. Por lo que será necesario el abordaje de este objetivo de seguridad en todo el proceso de análisis.

3.3.3 Autenticación

Otro de los temas que es de suma importancia para el BCCR, es la identificación del suscriptor que realiza una firma digital. Para tales efectos, es necesario conocer que quien realiza una acción en el sistema es realmente quien dice ser. Esto incluye tanto al usuario como al mismo sistema. Para lograrlo se procede con la incorporación del objetivo de autenticación, donde se revisan los distintos escenarios con el fin de analizar la verificación de la identidad de cada sujeto o componente en el sistema, durante todo el proceso de la firma digital.

3.4 Definición y propagación de los objetivos de seguridad directos

Los objetivos de seguridad deben ser derivados de las políticas y objetivos de la organización, en un análisis que se apoya en la representación del sistema. Cada uno de los objetivos debe especificar claramente tres partes: lo que se quiere asegurar, en qué parte del sistema y cuándo es requerido.

Es posible definir objetivos de seguridad directos para cualquier componente del sistema, incluso para todo el sistema y pueden establecerse iterativamente para un conjunto específico de componentes presentes en el árbol del todo y las partes.

Cabe destacar, que los objetivos directos también pueden ser propagados sistemáticamente al iterar sobre los elementos del árbol del todo y las partes. Esto se logra aplicando los objetivos a componentes más específicos.

En este trabajo, se aplicó la propagación de los objetivos de seguridad dados por la organización, generando una serie de objetivos de seguridad directos, que a su vez generarán otros objetivos a partir de las relaciones entre componentes del sistema. Dichos objetivos requieren ser validados para verificar que estén completos y acorde a lo definido con los expertos del BCCR.

3.5 Identificación de las relaciones de seguridad

Una relación de seguridad es una relación entre un par de componentes basado en sus requerimientos de seguridad. En ellas, se identifica un primer componente que tiene un objetivo de seguridad directo, y un segundo componente donde además se puede definir un objetivo de seguridad indirecto. Este segundo objetivo, representa una meta complementaria para alcanzar una solución integral de seguridad.

Las relaciones de seguridad se establecen a partir de la naturaleza de la seguridad, donde se tiene que toda relación deriva de una fuente de requerimientos de seguridad; como lo son el aislamiento, la interacción y la representación.

Por esta razón, se pueden definir relaciones estructurales cuando un componente se comporta como un aislador parcial o total de otro, respecto a los demás componentes del sistema, relaciones de interacción cuando dos componentes interactúan de cualquier forma y relaciones de representación cuando un componente actúa como representación de otro.

Para este trabajo, se identificaron las relaciones de seguridad de los tres tipos, derivando en nuevos objetivos de seguridad indirectos. Este proceso se aplicó de forma

iterativa y se logró al identificar las relaciones estructurales para cada nodo en el árbol del todo y las partes, las relaciones de interacción para cada arista en los diagramas de interacción, e incluyendo relaciones de representación entre componentes del sistema de firma digital. Este proceso se realizó hasta que se llegó a un determinado nivel de detalle, definido previamente mediante el análisis previo con los expertos del Banco Central.

Cabe destacar que esta manera iterativa de abordar la seguridad genera una serie de cadenas de seguridad compuestas por los componentes que se quieren asegurar y los objetivos de seguridad requeridos, evidenciando como la solución se torna integral y constituye un proceso completo de seguridad del sistema.

3.6 Identificación y valoración de riesgos

En la siguiente sección se presenta la metodología utilizada para identificar y valorar los riesgos. Es importante mencionar que, gracias al establecimiento previo de las cadenas de seguridad y los respectivos objetivos directos e indirectos, fue posible identificar y caracterizar los componentes relevantes y que deben ser asegurados. En las siguientes secciones se describen los pasos para identificar y valorar dichos riesgos.

3.6.1 Selección de fuentes de vulnerabilidad

A partir del enfoque sistemático que llevó a la propagación de objetivos, es posible identificar los componentes más relevantes y que además deben ser asegurados. En este trabajo, esto permite enfocarse en las vulnerabilidades y amenazas relacionadas con dichos elementos del sistema y a partir de ello realizar un análisis de riesgos, y posteriormente, definir políticas de seguridad de la información y establecer objetivos de control.

Debido al abordaje de este proyecto, donde no se cuenta con detalle técnico de las implementaciones y tecnologías utilizadas para la firma móvil, no se procedió a identificar vulnerabilidades específicas relacionadas con tecnologías particulares en dichos

escenarios. Sin embargo, sí se identificaron las fuentes de vulnerabilidades que podrían generar alguna afectación en los componentes por asegurar en el sistema.

La selección de fuentes de vulnerabilidad **¡Error! No se encuentra el origen de la referencia.** mantiene un enfoque similar al realizado por (Mora, 2017) donde se resumen y categorizan las fuentes de vulnerabilidades seleccionadas para desarrollar el proceso de identificación y valoración de riesgos, las cuales fueron obtenidas a partir de listas disponibles al público como (OWASP, 2016), (SANS, 2020), (CVE, 2020) y (OWASP, 2020), que mantienen relación con los componentes y objetivos de seguridad seleccionados en este análisis.

Categoría	Fuente de vulnerabilidad
Infraestructura	• Equipos desactualizados • Configuraciones de equipos incorrectas o incompletas.
Software de escritorio y móvil	• Software de terceros • Defectos en el software • Especificación incompleta o incorrecta para el desarrollo de software. • Errores de configuración • Errores en el diseño • Excesiva complejidad del software • Software infectado o dañado
Tecnología y herramientas	• Sistemas operativos • Navegadores • Plataformas o entornos de ejecución del software • Frameworks de aplicación
Canales de comunicación	• Protocolos • Comunicaciones sin protección

Categoría	Fuente de vulnerabilidad
	• Puertos abiertos • Permisos innecesarios a los componentes
Gestión y mantenimiento	• Errores del sistema no resueltos • Mala configuración de los sistemas • Errores en gestión de los problemas e incidentes • Ausencia de actualizaciones de seguridad • Privilegios excesivos para los usuarios

Tabla 1 Resumen de fuentes de vulnerabilidades

3.6.2 Selección de fuentes de amenazas

En esta etapa se identificaron las fuentes de amenazas que podrían poner en riesgo al sistema analizado. Para lograrlo se mantiene un enfoque similar al que menciona Mora (2017) basado en la guía del NIST (2012). En este caso se tomaron en consideración al igual que en el trabajo de Mora (2017) las fuentes de amenazas originadas por adversarios, que son individuos, grupos, organizaciones o estados que buscan explotar la dependencia que una organización tiene en determinados recursos tecnológicos (National Institute of Standards and Technology, 2012) .

En la Tabla 2 se muestran algunos ejemplos de fuentes de amenazas consideradas.

Tabla 2 Ejemplos de fuentes de amenazas. Fuente: NIST (2012).

Categoría	Sub categoría	Fuentes de amenazas
Adversarios	Individuos	• Intrusos • Personal interno • Personal de confianza • Personal con privilegios
	Grupos	• Ad Hoc • Previamente establecidos

Categoría	Sub categoría	Fuentes de amenazas
	Organizaciones	• Competidores • Proveedores • Socios • Clientes

3.6.3 Identificación de riesgos

La siguiente etapa consiste en la identificación de los riesgos en los componentes que se requieren asegurar. Para lograrlo, se relacionan las fuentes de amenazas y las vulnerabilidades. En este punto las fuentes de amenazas que se deben considerar como aceptables son las que tengan el potencial de explotar al menos una fuente de vulnerabilidad identificada (National Institute of Standards and Technology, 2012).

Por ejemplo, una fuente de amenaza aceptable sería un adversario que lleva a cabo una modificación indebida en el tráfico de red para presentar información falsa al usuario. Esto porque está explotando una fuente de vulnerabilidad como lo son las comunicaciones desprotegidas.

Este paso se aplica para cada objetivo de seguridad directo o indirecto que haya sido derivado mediante los pasos anteriores. Esto permite canalizar los esfuerzos en los puntos del sistema que son más importantes dados los objetivos que fueron debidamente propagados en el sistema.

3.6.4 Determinación de la probabilidad del riesgo

Una vez que se tienen los riesgos identificados, el siguiente paso consiste en asignarles una probabilidad de que ocurran, con el objetivo de usarla como insumo para calcular su grado de severidad.

En esta investigación, se utilizará la metodología que expone Mora (2017) en su trabajo. En ella menciona que la probabilidad de que un riesgo se materialice es una estimación aproximada de qué tan factible es que una vulnerabilidad sea descubierta y explotada por un atacante. Además, indica que según OWASP (2015) no es necesario ser excesivamente preciso en esa estimación, ya que en la práctica por lo general es suficiente identificar si la probabilidad es baja, media o alta.

El proceso que expone Mora (2017) inicia categorizando las fuentes de amenazas por nivel de habilidad, recompensa recibida y recursos tecnológicos requeridos por el atacante para realizar el ataque. Seguidamente se caracterizan las vulnerabilidades por facilidad de descubrimiento y facilidad de explotación. La Tabla 3 y la Tabla 4 detallan estos factores.

Adicionalmente, los factores se acompañan de una escala de valores que va de cero a nueve, la cual permite asignar un valor a cada factor de acuerdo con criterios cuantitativos previamente definidos. Esto según explica el mismo autor, tiene como objetivo minimizar las subjetividades en el momento de estimar.

Tabla 3 Factores característicos de las fuentes de amenazas generadas por adversarios para determinar la probabilidad del riesgo. Fuente: (Mora,2017)

Identificador	Factor	Escala de valores
H	**Nivel de habilidad** ¿Qué nivel técnico es requerido por la fuente de amenaza para encontrar la vulnerabilidad y explotarla?	• Requiere un nivel mínimo de habilidades técnicas = 9 • Requiere un nivel básico de habilidades técnicas = 7 • Requiere un nivel intermedio de habilidades técnicas = 5 • Requiere un nivel avanzado de habilidades técnicas = 3 • Requiere un nivel experto de habilidades técnicas = 1

Identificador	Factor	Escala de valores
		• Requiere un nivel omnisciente de habilidades técnicas = 0
Ro	**Recompensa** ¿Cuál es la magnitud del incentivo que recibe la fuente de amenaza para encontrar la vulnerabilidad y explotarla?	• La recompensa es muy grande = 9 • La recompensa es grande = 7 • La recompensa es moderada = 5 • La recompensa es pequeña = 3 • La recompensa es insignificante = 1 • No hay recompensa = 0
Ru	**Recursos necesarios** ¿Cuál es la cantidad de recursos tecnológicos en espacio y tiempo que necesita la fuente de amenaza para encontrar la vulnerabilidad y explotarla?	• Requiere recursos mínimos = 9 • Requiere pocos recursos = 7 • Requiere algunos recursos = 5 • Requiere bastantes recursos = 3 • Requiere muchos recursos = 1 • Requiere acceso total a recursos = 0

Tabla 4. Factores característicos de las fuentes de vulnerabilidades para determinar la probabilidad del riesgo. Fuente: (Mora, 2017)

Identificador	Factor	Escala de valores
D	**Facilidad de descubrimiento** ¿Qué tan fácil es descubrir la vulnerabilidad para una fuente de amenaza?	• Inmediata = 9 • Fácil = 7 • Moderada = 5 • Difícil = 3 • Muy difícil = 1 • Imposible = 0
E	**Facilidad de ser explotada** ¿Qué tan fácil es explotar la vulnerabilidad para una fuente de amenaza?	• Inmediata = 9 • Fácil = 7 • Moderada = 5 • Difícil = 3 • Muy difícil = 1 • Imposible = 0

Una vez que se asigna un valor a cada factor, se puede determinar la probabilidad de ocurrencia del riesgo. Para lograr esto, el autor menciona dos formas posibles, pero en este trabajo solamente se contemplará una debido a que los resultados obtenidos por Mora (2017) muestran que ambas formas no distan mucho entre sí. Dicho esto, la probabilidad se determina a partir de un promedio de los valores asignados a cada factor. Es decir que consiste en sumar esos valores y luego dividir el resultado entre la cantidad de factores, tal como se muestra en la Ecuación 1, para luego utilizar el resultado como referencia para seleccionar un valor de una escala cuantitativa tal como se muestra en la Tabla 5.

Ecuación 1 Promedio de los valores asignados a cada factor para estimar la probabilidad del riesgo. Fuente: (Mora,2017)

$$\boldsymbol{Promedio} = \frac{\boldsymbol{H} + \boldsymbol{Ro} + \boldsymbol{Ru} + \boldsymbol{D} + \boldsymbol{E}}{\mathbf{5}}$$

Tabla 5 Escala cuantitativa para el cálculo de la probabilidad del riesgo. Fuente: (Mora, 2017)

Rango del promedio calculado	Probabilidad
0 a < 1	Muy baja
1 a < 3	Baja
3 a < 5	Media
5 a < 7	Alta
7 a 9	Muy alta

3.6.5 Determinación del impacto

El impacto, como indica Mora (2017), puede ser entendido como una estimación del nivel de los efectos adversos que se producirían en la aplicación y en el negocio tras un ataque exitoso. Según OWASP (2015), en la estimación del impacto de un riesgo, se debe considerar tanto el impacto técnico, que afecta a la aplicación, los datos que usa y las funciones que provee, como el impacto en el negocio, que afecta a la organización que hace uso del software.

Para definir el impacto de un riesgo, se procede de manera similar a lo que se indicó para la probabilidad, por lo que se definen una serie de factores como la interrupción de la actividad del negocio, la pérdida económica y la pérdida de reputación. Además, se incluye un factor más que corresponde a la interrupción de alguno de los servicios de seguridad relevantes para la organización. La Tabla 6 muestra el detalle de dichos factores y sus respectivas escalas de valores.

Una vez definidos los factores, se obtiene el promedio de los valores asignados a cada uno como se muestra en la Ecuación 2 y luego se utiliza dicho promedio para seleccionar un valor dentro de una escala cuantitativa que se ilustra en la Tabla 7.

Ecuación 2 Promedio de los valores asignados a cada factor para estimar el impacto del riesgo. Fuente:(Mora,2017)

$$Promedio = \frac{C + A + E + R}{4}$$

Tabla 6 Factores característicos para la determinación del impacto del riesgo. Fuente: (Mora,2017)

Identificador	Factor	Escala de valores
C	**Consecuencias de la interrupción de un servicio de seguridad de la información** ¿Cuál es el nivel de las consecuencias de la interrupción de un servicio de seguridad información como resultado del ataque?	• Las consecuencias son muy altas = 9 • Las consecuencias son altas = 7 • Las consecuencias son moderadas = 5 • Las consecuencias son leves = 3 • Las consecuencias son muy leves = 1 • No hay consecuencias = 0
A	**Interrupción de la actividad del negocio** ¿Cuál es el grado de interrupción de la correcta prestación de servicios de firma digital por parte del SNCD	• La interrupción es muy alta = 9 • La interrupción es alta = 7 • La interrupción es moderada = 5 • La interrupción es leve = 3 • La interrupción es insignificante = 1 • No hay interrupción = 0

Identificador	Factor	Escala de valores
	como resultado del ataque?	
E	**Pérdida económica** ¿Cuál es el nivel de pérdida económica dentro del SNCD como resultado del ataque?	• Las pérdidas económicas son incalculables = 9 • Las pérdidas económicas son altas = 7 • Las pérdidas económicas son moderadas = 5 • Las pérdidas económicas son bajas = 3 • Las pérdidas económicas son insignificantes = 1 • No hay pérdidas económicas = 0
R	**Pérdida de reputación** ¿Cuál es el nivel de afectación de la buena imagen del SNCD como resultado del ataque?	• La pérdida de reputación es irreversible = 9 • La pérdida de reputación es alta = 7 • La pérdida de reputación es moderada = 5 • La pérdida de reputación es baja = 3 • La pérdida de reputación es insignificante = 1 • No hay pérdida de reputación = 0

Tabla 7 Escala cuantitativa para el cálculo del impacto del riesgo. Fuente: (Mora,2017)

Rango del promedio calculado	Impacto
0 a < 1	Muy bajo
1 a < 3	Bajo
3 a < 5	Medio
5 a < 7	Alto
7 a 9	Muy alto

3.6.6 Determinación del nivel de severidad

El último paso de la valoración de riesgos es la asignación de un nivel de severidad, de acuerdo con la probabilidad y el impacto estimados. Esto se hace mediante la matriz de la Tabla 8, donde corresponde a la celda en la que se intersecan la probabilidad y el

impacto previamente obtenidos. Por ejemplo, si la probabilidad se estimó como alta y el impacto se estimó como medio, al riesgo se le asignó un nivel de severidad alto.

Tabla 8 Niveles de severidad del riesgo. Fuente: (Mora, 2017)

		Probabilidad				
		Muy baja	**Baja**	**Media**	**Alta**	**Muy alta**
Impacto	**Muy bajo**	Muy bajo	Muy bajo	Bajo	Bajo	Medio
	Bajo	Muy bajo	Bajo	Bajo	Medio	**Alto**
	Medio	Bajo	Bajo	Medio	**Alto**	**Alto**
	Alto	Bajo	Medio	**Alto**	**Alto**	**Muy alto**
	Muy alto	Medio	**Alto**	**Alto**	**Muy alto**	**Muy alto**

3.7 Definición de políticas y objetivos de control de seguridad

Para definir de forma apropiada las políticas que mitigan los riesgos identificados, se llevaron a cabo tres actividades, a saber: selección de los riesgos a ser mitigados, definición de las políticas de seguridad de la información y definición de los objetivos de control. A continuación, se detalla cada una de las actividades.

3.7.1 Selección de los riesgos a ser mitigados

Para la selección de riesgos a mitigar, se estableció que se mitigarían los riesgos cuya severidad fuera valorada como media, alta o muy alta; y se descartaron los que tuvieran otro nivel de severidad.

3.7.2 Definición de las políticas de seguridad de la información

La definición de las políticas se realizó de manera iterativa en todos los riesgos que fueron seleccionados para mitigar. En cada una de ellas se estableció en lenguaje natural los requisitos de seguridad necesarios para mitigar uno o varios riesgos.

3.7.3 Definición de objetivos de control

Para definir los objetivos de control, fue necesario analizar los requisitos de seguridad que dictan las políticas definidas y con base en ello, redactar los requisitos que debe cumplir un control de seguridad para ser considerado como efectivo a la hora de hacer cumplir la política que lo origina. Sobre este aspecto es importante recalcar que no se establecieron controles puntuales debido al nivel de granularidad en los componentes del sistema y el hecho de que el sistema presenta cierto grado de generalidad al estar aún en desarrollo.

3.8 Elaboración de una guía de implementación

En esta sección se pretende describir el proceso que se sigue para crear la guía de implementación para asegurar aplicaciones de software que usen firma digital por medio de los distintos medios de acceso a la firma digital del BCCR en Internet.

Para alcanzar dicho objetivo se redactó un documento que funciona como un instrumento para evaluar el cumplimiento de las políticas de seguridad definidas en este trabajo, a través de los objetivos de control establecidos. El documento está compuesto por las siguientes secciones:

- Introducción.
- Descripción de la guía de implementación.
- Lista de políticas de seguridad que serán evaluadas.
- Lista de objetivos de control que permiten evaluar el cumplimiento de las políticas de seguridad.
- Lista de observaciones finales.
- Tabla con el resumen de la evaluación.

4 Identificación de escenarios, representación del sistema y seguridad

Este capítulo describe los resultados del análisis aplicado a los escenarios de firma digital, donde se logró construir una representación del sistema y luego propagar una serie de objetivos a lo largo de los componentes. Según lo planteado en la metodología, el capítulo inicia con un resumen de los escenarios de firma digital que fueron considerados, luego se presentan los componentes que han sido seleccionados y su respectiva representación por medio del "árbol del todo y las partes" y los diagramas de interacción. Finalmente se presentan de forma resumida los resultados de propagar los objetivos en los componentes del sistema, así como las relaciones de seguridad que fueron identificadas en el proceso.

4.1 Identificación de escenarios

Para poder analizar el sistema completo de Firma Digital del BCCR, fue necesario distinguir por una parte los escenarios de firma en los dispositivos móviles y por otra los de firma en equipos de escritorio, desde la perspectiva del usuario final.

Se hace énfasis en describir los componentes y los comportamientos que están involucrados en el proceso; ya que estos constituyen los insumos necesarios para, posteriormente, definir la representación del sistema. Cabe destacar que ambos escenarios comparten algunos componentes de información, por lo que estos se presentan como parte de cada escenario y posteriormente se unifican para su respectivo análisis. En las siguientes secciones se presenta el desarrollo de los escenarios indicados.

4.1.1 Firma digital en dispositivos móviles

El proceso de firma digital desde los dispositivos móviles, que se desarrolla en este trabajo, se divide en dos etapas. La primera etapa consiste en la solicitud de una firma al usuario y la segunda corresponde al proceso de realización de la firma desde el dispositivo móvil del usuario.

Como se muestra en la Figura 7, la primera etapa, que corresponde a la solicitud de la firma al usuario, comienza cuando se le solicita firmar desde algún portal (1). En este punto la entidad respectiva solicita al servicio Firmador Validador y Autenticador del BCCR (FVA) que se realice el proceso de firma enviándole la solicitud de una nueva firma (2). Una vez que el FVA recibe la solicitud, se verifica si el usuario está registrado en el sistema con un dispositivo móvil y que además no se encuentre activo en ese momento desde el firmador de escritorio (3). Si el usuario solamente está activo desde su dispositivo móvil, el FVA procede a solicitar, a través de los servicios expuestos para firma móvil, que se notifique al usuario la existencia de una solicitud de firma pendiente (4). Para lograr notificar al usuario, los servicios para firma móvil utilizan el componente "*Notification Hub*" de Microsoft Azure, que se encarga de dirigir la notificación al dispositivo móvil del usuario mediante las plataformas del respectivo sistema operativo (5) y finalmente la notificación es mostrada al usuario en pantalla (6).

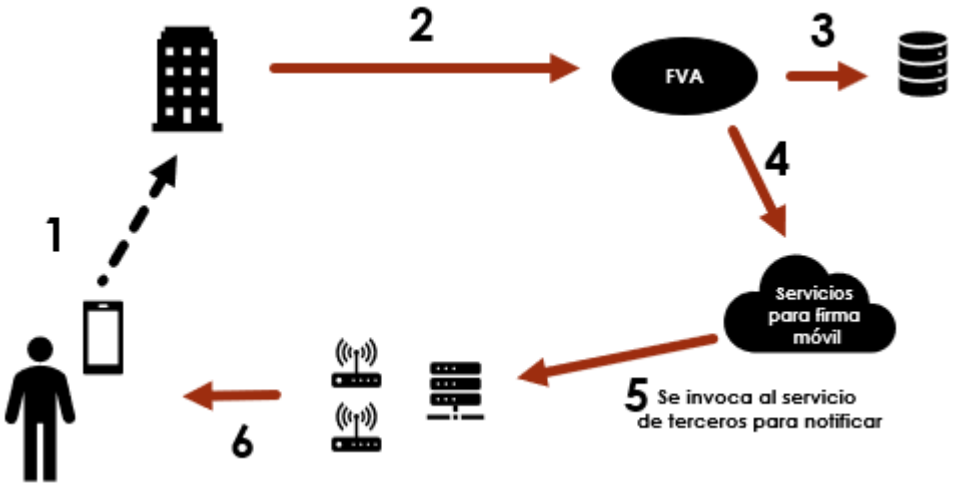

Figura 7 Diagrama del flujo de solicitud de firma al usuario. Fuente: Elaboración propia

Con respecto a la segunda etapa donde se realiza la firma, en la Figura 8 se puede ver que el proceso inicia cuando el suscriptor ha recibido una notificación de firma y procede a aceptarla (1), para activar la aplicación de Firma Móvil y que ésta a su vez solicite la información de la solicitud vigente de firma a los servicios expuestos para la firma móvil

(2). Una vez que la aplicación obtiene la respuesta y cuenta con dicha información, se le solicita al usuario sus credenciales de firma (incluyendo el acercamiento de la tarjeta con NFC) y se envían al BCCR junto con los datos de la solicitud de firma (3). Finalmente, el FVA procesa la firma digital (4) y se encarga de notificar a la entidad sobre el resultado de la firma (5).

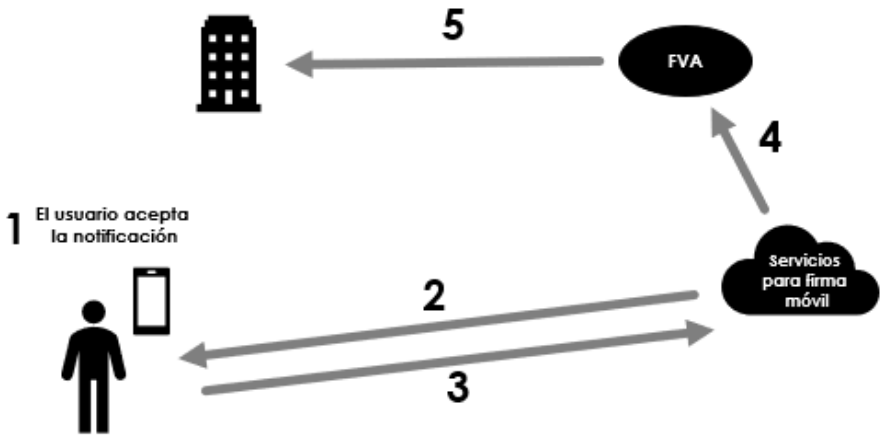

Figura 8 Diagrama del flujo de realización de la firma en móviles. Fuente: Elaboración propia

A partir de estos procesos y su respectivo análisis en detalle, se desprenden una serie de componentes que se presentan en la Tabla 9 y la Tabla 10 .

Tabla 9 Componentes del escenario de firma móvil. Fuente: Elaboración propia

Componente	Detalle
Equipo donde se solicita la firma	Compuesto a su vez por otros componentes como lo son el Navegador, el Sistema Operativo, las aplicaciones y eventualmente el Firmador de escritorio del BCCR
Web Service notificador de la entidad	Este componente pertenece a la infraestructura de la entidad y es el punto al cual se dirigen las notificaciones de los resultados de las firmas procesadas por FVA.
Servicio de Firma Digital invocado por la entidad	Este servicio se encuentra en infraestructura BCCR y es el responsable de recibir las solicitudes de firma, entre otros provenientes de la entidad.
Servicios internos de firma digital	Estos son los servicios que gestan el proceso interno de la firma. Incluye componentes como el propio servicio del FVA y la Base de Datos del FVA.
Servicios expuestos para Firma móvil	Este componente engloba los servicios que se ponen a disposición para ser consumidos por la aplicación de Firma móvil.
Equipos móviles	Este componente representa la agrupación de los elementos con que dispone el suscriptor para operar la firma móvil, tales como los equipos Android, los equipos IOS y la tarjeta de Firma Digital con NFC.

Tabla 10 Componentes de información del escenario de Firma móvil. Fuente: Elaboración propia

Componente	Detalle
Solicitud de nueva firma desde la entidad	Incluye datos como Identificador del suscriptor, el documento a firmar y su resumen, el algoritmo utilizado, el hash del documento, la fecha de referencia, el hash del resumen del documento y la entidad origen.
Datos del usuario registrado	Incluye los datos del usuario, incluyendo entre los más destacados relevantes para localizar al suscriptor y enviarle la notificación.
Datos de la solicitud de firma	Incluye elementos como el resumen del documento, el nombre de la entidad, el límite de tiempo para procesar la firma, el hash a firmar del resumen, el identificador de la solicitud, logo de la entidad, hash a firmar del documento y el tipo de firma requerido.
Credenciales	Son los datos del usuario con los que se accede a la firma. Incluye el código verificador y el PIN de su tarjeta con NFC.
Respuesta de firma	En la respuesta de la firma se incluyen datos como el hash firmado del documento, el hash firmado del resumen, el código de verificación, un código de error y el identificador de la solicitud procesada.
Notificación a la entidad	En este componente se incluyen el indicador de éxito, un código de error, el documento firmado y el hash del documento firmado.

4.1.2 Firma digital de escritorio

El proceso de firma digital desde un dispositivo de escritorio comienza cuando desde una computadora o algún otro dispositivo se requiere una firma digital (1). En ese punto la entidad realiza dos tareas, primero solicita al FVA una nueva firma (2) y luego le muestra al usuario el código de verificación y el resumen del documento que se firmará (3). Una vez que FVA recibe la solicitud, procede a enviar una solicitud al cliente estándar o Firmador BCCR (4,5). El firmador de escritorio realiza la firma y envía los datos al FVA (6) para que este se encargue de notificar a la entidad del resultado de dicha firma (7,8).

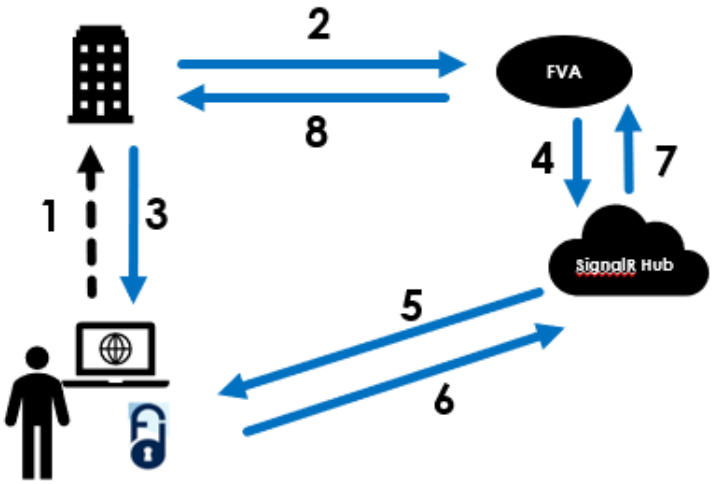

Figura 9 Diagrama con el flujo de firma desde una computadora. Fuente: Elaboración propia

Como se puede notar con la descripción de los procesos, los componentes de información involucrados en este escenario son los mismos que se tienen en los escenarios de firma móvil. Pero se incluyen otros componentes que se detallan en la Tabla 11.

Tabla 11 Componentes del escenario de firma de escritorio. Fuente: Elaboración propia

Componente	Detalle
Equipo donde se solicita la firma	Compuesto a su vez por otros componentes como lo son el Navegador, el Sistema Operativo, las aplicaciones y el Firmador de escritorio del BCCR
Web service notificador de la entidad	Este componente pertenece a la infraestructura de la entidad y es el punto al cual se dirigen las notificaciones de los resultados de las firmas procesadas por FVA.
Servicio de firma digital invocado por la entidad	Este servicio se encuentra en infraestructura BCCR y es el responsable de recibir las solicitudes de firma, entre otros provenientes de la entidad.
SignalR Hub	Este componente establece la comunicación constante con cliente firmador de escritorio.
Servicio FVA	Servicio encargado del procesamiento de la firma.
Base de datos de FVA	Base de datos con la información del proceso de firma digital.

4.2 Representación del sistema

Una vez que se han identificado los componentes y se ha realizado el debido análisis del sistema, el siguiente paso corresponde a elaborar la representación de componentes del sistema. En esta sección se presentan los resultados de la representación del sistema mediante las herramientas del "árbol del todo y las partes" y los diagramas de interacción. Cabe destacar que en este proceso se excluyeron los componentes que están fuera del alcance del trabajo o que, por distintas razones, se considera que están fuera del campo de acción del BCCR para establecer controles de seguridad, como, por ejemplo; los servicios

de Microsoft Azure y Google que son utilizados en la aplicación para el manejo de las notificaciones en los dispositivos móviles, entre otros.

4.2.1 Representación de componentes - árbol del todo y las partes

Como resultado de modelar los componentes del sistema, se obtuvo un árbol donde la raíz es el sistema de Firma digital y los demás niveles son sus respectivas descripciones en subcomponentes. Además, a cada componente se le asignó un identificador numérico para poder referenciarlo en etapas posteriores del trabajo.

Como lo muestra la Figura 10, en un primer nivel se establecieron los dos escenarios de firma digital que se han mencionado en este trabajo más el componente que engloba toda la información del sistema.

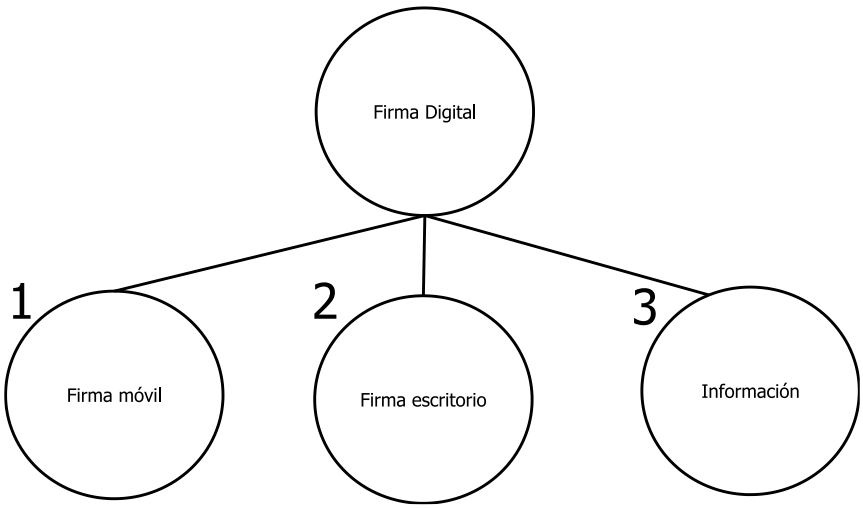

Figura 10 Primer nivel del Árbol del todo y las partes. Fuente: Elaboración propia

Luego se continuó con la descomposición de cada uno de esos elementos, iniciando con el nodo de Firma Móvil y dando como resultado el subárbol de la Figura 11.

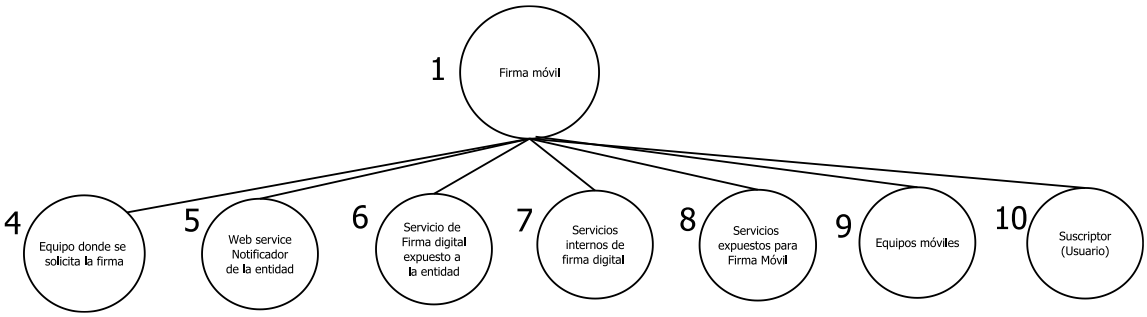

Figura 11 Sub árbol de Firma móvil. Fuente: Elaboración propia

Posteriormente este proceso se repitió con cada nodo del árbol, generando la jerarquía ilustrada en la Figura 12 para el Equipo donde se solicita la firma, el subárbol de la Figura 13 con los subcomponentes de los servicios internos de firma digital, y finalmente el sub árbol de los componentes de los equipos móviles que se refleja en la Figura 14.

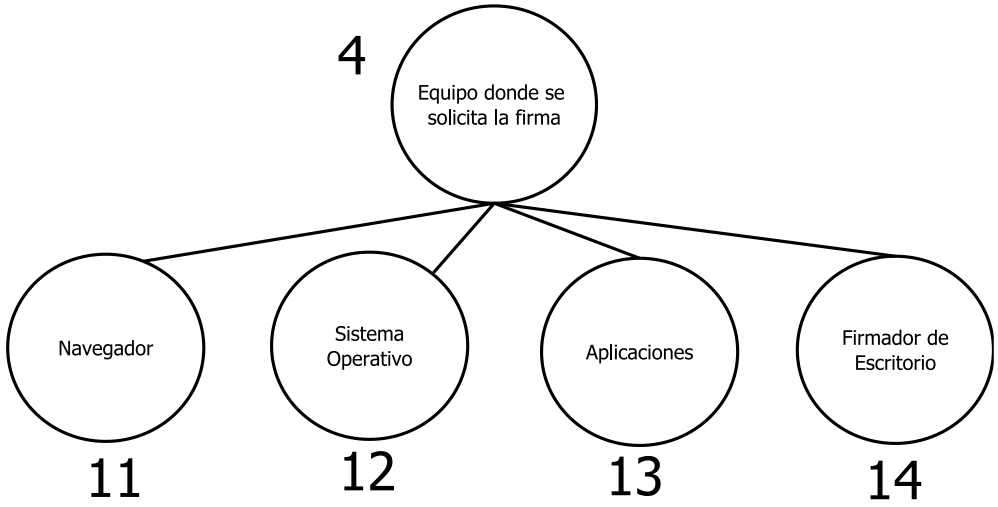

Figura 12 Sub árbol del equipo donde se solicita la firma. Fuente: Elaboración propia

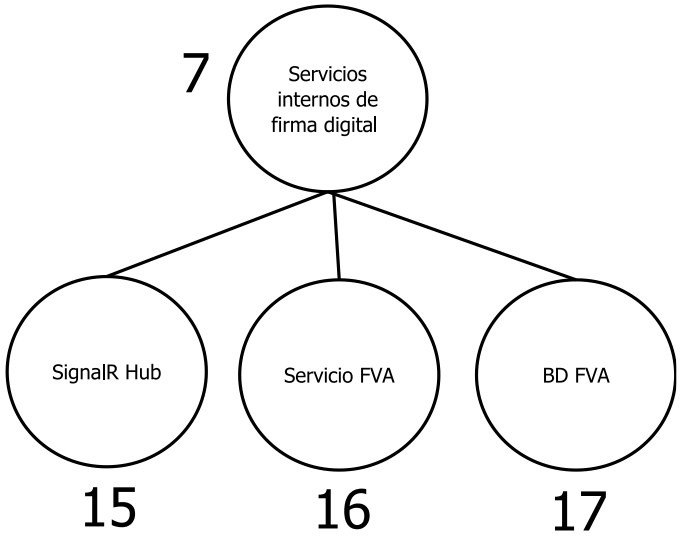

Figura 13 Sub árbol de los componentes de Servicios internos de firma digital. Fuente: Elaboración propia

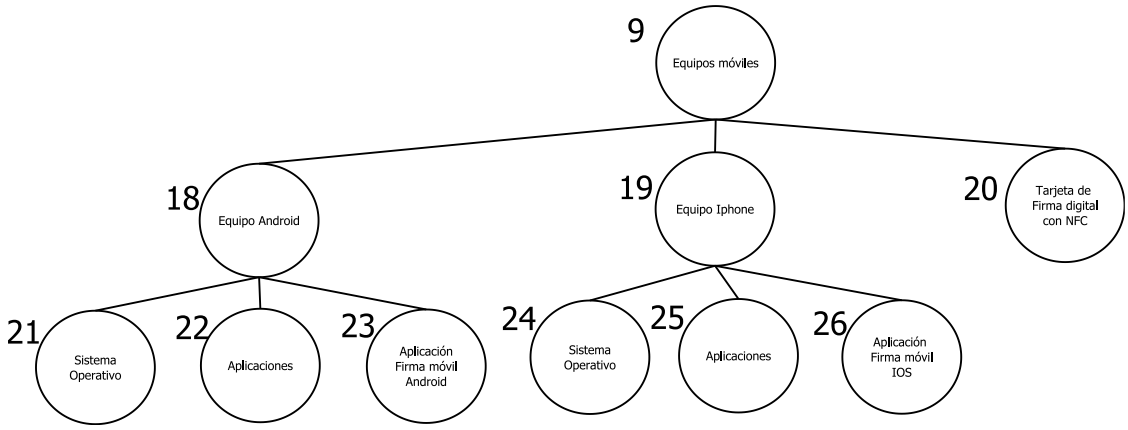

Figura 14 Sub árbol de los componentes de Equipos Móviles. Fuente: Elaboración propia

Este mismo proceso se realizó para el nodo de Firma de escritorio representado en la Figura 15y el nodo de Información que se incluye en la Figura 16.

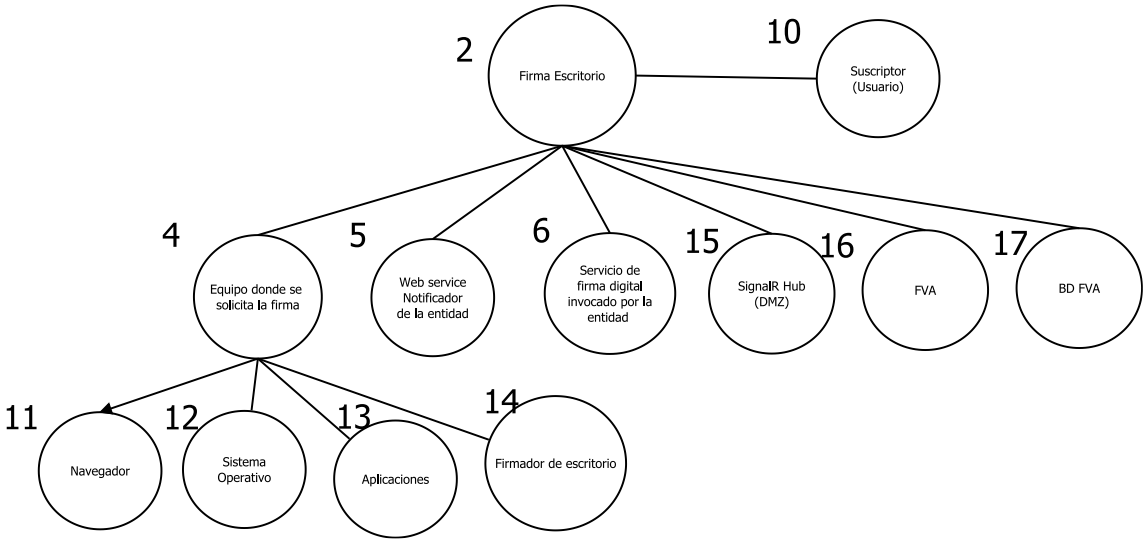

Figura 15 Sub árbol de Firma escritorio. Fuente: Elaboración propia

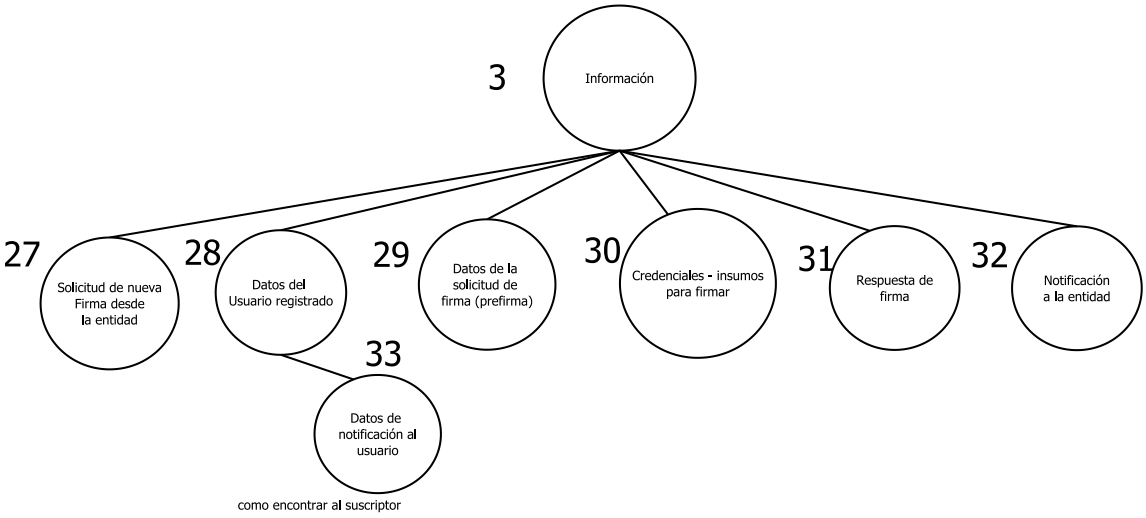

Figura 16 Sub árbol de Información. Fuente: Elaboración propia

4.2.2 Diagramas de interacción

El segundo insumo que se requiere para establecer las relaciones de seguridad en etapas posteriores, son los diagramas de interacción. En esta sección se describe el enfoque utilizado para elaborarlos y se presentan, a manera de ejemplo, algunos de los diagramas utilizados durante el desarrollo del trabajo.[1]

Para elaborar los diagramas de interacción se utilizó un enfoque que permitiera cubrir todas o la mayor parte de las interacciones que se presentan en el sistema. El mismo consiste en primero definir, para cada componente del sistema, sus interacciones directas; formando una especie de estrella y posteriormente definir un diagrama de interacción por cada flujo o escenario del sistema.

A manera de ejemplo, en la Figura 17 y la Figura 18 se muestran las interacciones directas identificadas en el escenario de firma de escritorio para los componentes “Equipo donde se solicita la firma” y “Firmador BCCR” respectivamente. Estas interacciones se lograron a partir del análisis de documentación como casos de uso, guías, presentaciones y otros elementos brindados por el BCCR.

[1] El detalle de los diagramas de interacción se puede encontrar en el Apéndice F: Diagramas de interacción.

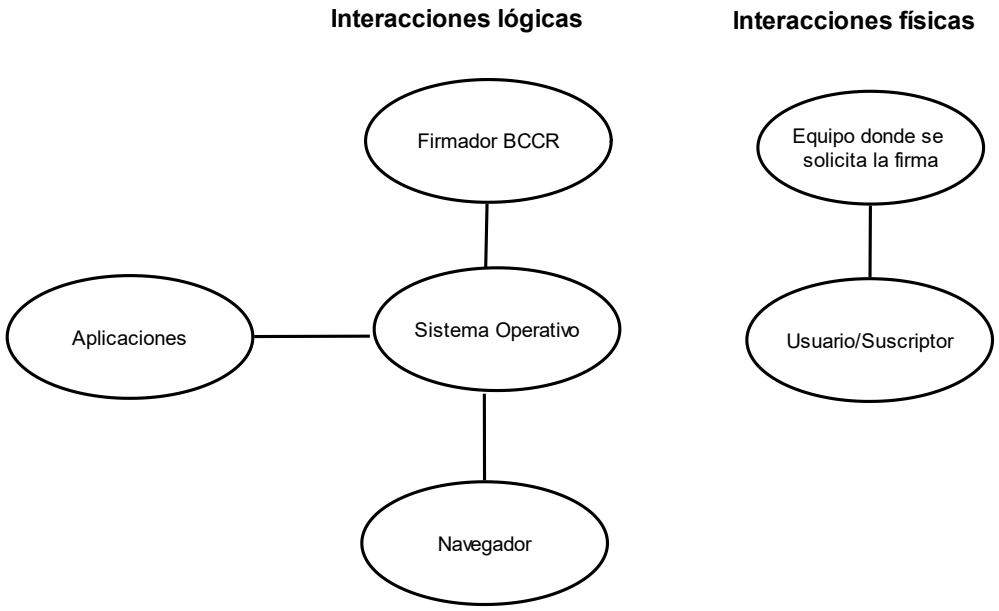

Figura 17 Interacciones tipo estrella para el Equipo donde se solicita la firma.
Fuente: Elaboración propia

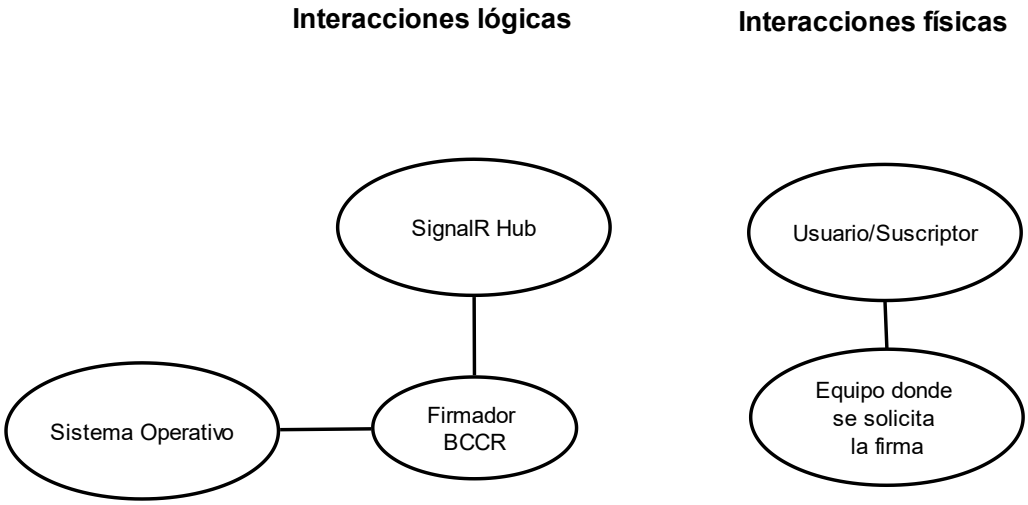

Figura 18 Interacciones tipo estrella para el Firmador BCCR.
Fuente: Elaboración propia

De la misma forma, se establecieron diagramas con las interacciones directas para los componentes del escenario de firma móvil, como se puede ver por ejemplo en la Figura 19 para el componente de "Aplicación de firma móvil Android".

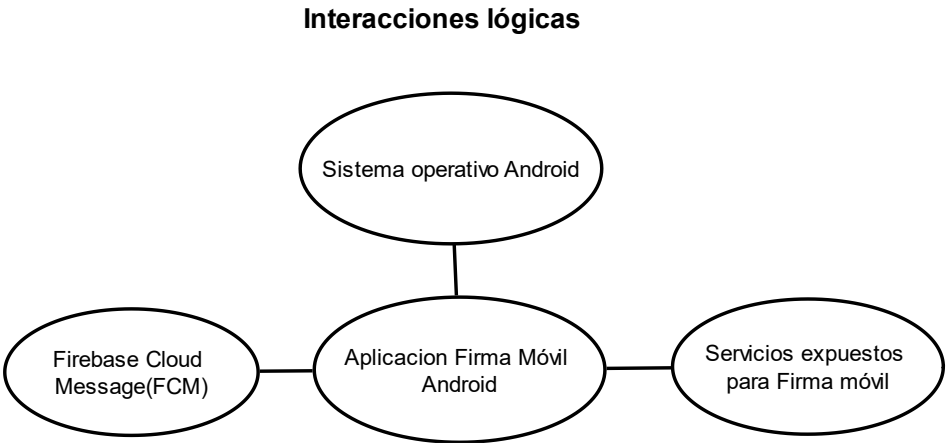

Figura 19 Interacciones tipo estrella en Aplicación Firma Móvil Android.
Fuente: Elaboración propia

Una vez que se iteró sobre todos los componentes definiendo sus interacciones directas, se procedió a identificar tanto las relaciones directas como las indirectas mediante diagramas de interacción que representan los flujos presentados en los escenarios bajo análisis. Por ejemplo, uno de los flujos analizados corresponde al proceso de solicitud de una nueva firma desde dispositivos móviles, donde se obtuvo el diagrama que se muestra en la Figura 20.

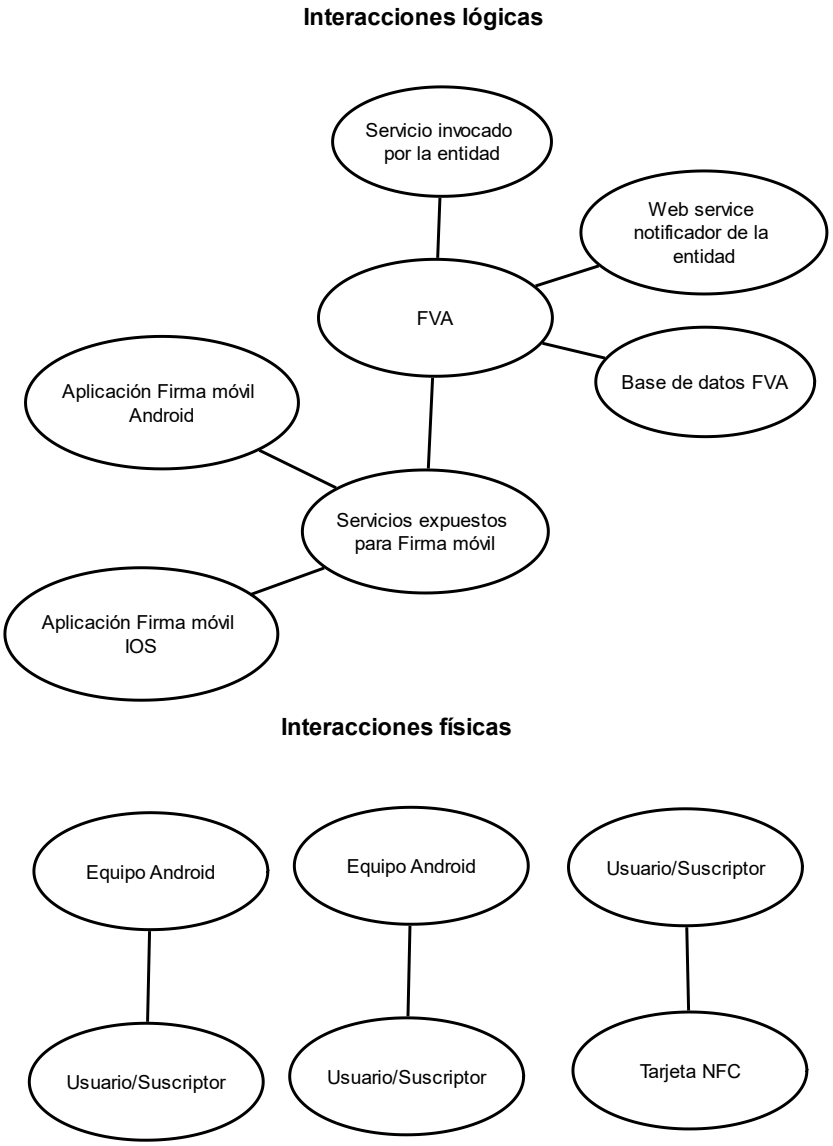

Figura 20 Diagrama de interacciones para flujo de solicitar firma móvil. Fuente: Elaboración propia

Este proceso también se realizó en los flujos del escenario de firma de escritorio, donde a manera de ejemplo se puede ver en la Figura 21 las interacciones generadas para el flujo de solicitud de una nueva firma mediante el Firmador BCCR.

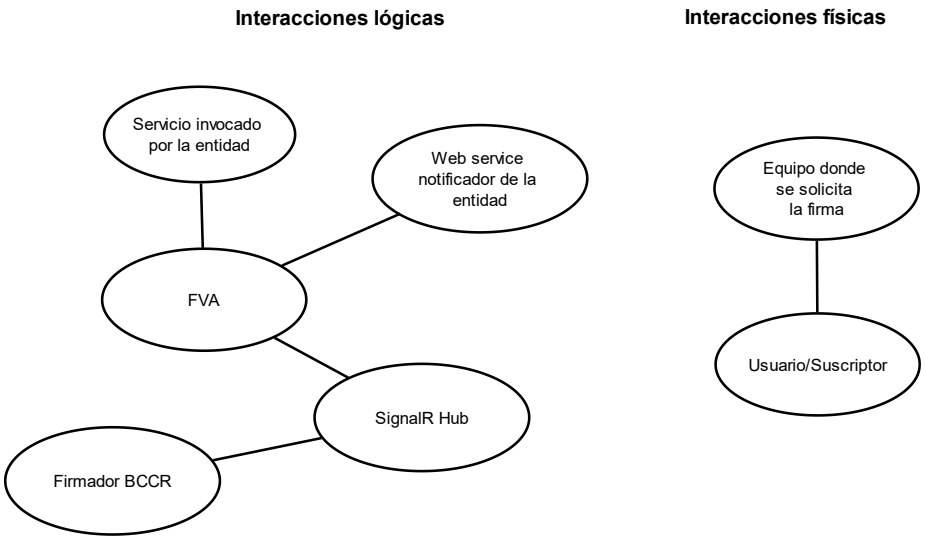

Figura 21 Diagrama de interacciones para flujo de solicitar firma de escritorio. Fuente: Elaboración propia

Al finalizar esta etapa de construcción de la representación, se consiguieron los insumos necesarios para proceder a propagar los objetivos a través de los componentes del sistema.

4.3 Definición y propagación de los objetivos de seguridad

En esta sección se detallan los resultados del proceso de definición y propagación de objetivos de seguridad. Este proceso se logra a través de iterar sobre el árbol del todo y las partes para aplicar los objetivos definidos en partes más específicas del sistema.

En la Tabla 12 se presentan los objetivos iniciales que fueron definidos en alto nivel para el sistema por analizar. A cada objetivo de seguridad se le asignó un identificador para poder relacionarlo en etapas posteriores del trabajo.

Tabla 12 Objetivos de seguridad de alto nivel. Fuente: Elaboración propia

Identificador	Servicio de seguridad	Dónde	Cuándo
1	Integridad	En la información y el software cliente	En el proceso de firma digital
2	Autenticación	En los individuos y el software cliente	En el proceso de firma digital
3	Confidencialidad	En los canales de comunicación	Se realiza comunicación con el sistema de Firma Digital

Dichos objetivos fueron descompuestos en objetivos directos para los componentes del sistema. Para ello, fue necesario primero establecer una relación, como se muestra en la Tabla 13, entre el "Dónde" del objetivo de negocio y los componentes a los que hace referencia; con el objetivo de luego poder aplicarlos de manera iterativa en las jerarquías de componentes representadas en el árbol del todo y las partes. La Tabla 14 presenta los objetivos directos que fueron derivados luego de la respectiva propagación.

Tabla 13 Correlación entre elementos de los objetivos de negocio y los componentes del sistema. Fuente: Elaboración propia

Elemento en el objetivo de negocio	Componentes a los que hace referencia	Identificador del componente
Software cliente	Firmador de escritorio	14
	Firmador Android	23
	Firmador IOS	26
Individuos	Suscriptor	10
Canales	Servicios expuestos para Firma Móvil	8
	Hub de Firma (SignalR Hub)	15
	Web service notificador de la entidad	5
	Servicio invocado por la entidad	6
Información	Solicitud de nueva firma desde la entidad	27
	Datos del usuario registrado	28
	Datos de notificación al usuario	33
	Datos de la solicitud de firma escritorio	29
	Credenciales/insumos para firmar	30
	Respuesta de la firma	31
	Notificación a la entidad	32
	Datos de notificación al usuario	33

Tabla 14 Objetivos directos. Fuente: Elaboración propia

Identificador	Objetivo directo	Justificación
OD[3][1]	Se requiere Integridad en Componentes de información durante el proceso de firma digital	Objetivo directo por objetivo de negocio 1
OD[27][1]	Se requiere Integridad en Solicitud de nueva firma desde la entidad durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[28][1]	Se requiere Integridad en Datos del usuario registrado durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[29][1]	Se requiere Integridad en Datos de la solicitud de firma (prefirma) durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[30][1]	Se requiere Integridad en Credenciales - insumos para firmar durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[31][1]	Se requiere Integridad en Respuesta de la firma durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[32][1]	Se requiere Integridad en Notificación a la entidad durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[33][1]	Se requiere Integridad en Datos de notificación al usuario durante el proceso de firma digital	Objetivo grupal OD[3][1] propagado
OD[14][1]	Se requiere Integridad en Firmador de escritorio durante el proceso de firma digital	Objetivo directo por objetivo de negocio 1
OD[23][1]	Se requiere Integridad en Aplicación Firma Móvil ANDROID durante el proceso de firma digital	Objetivo directo por objetivo de negocio 1
OD[26][1]	Se requiere Integridad en Aplicación Firma Móvil IOS durante el proceso de firma digital	Objetivo directo por objetivo de negocio 1
OD[10][2]	Se requiere Autenticación en Suscriptor durante el proceso de firma digital	Objetivo directo por objetivo de negocio 2
OD[14][2]	Se requiere Autenticación en Firmador de escritorio durante el proceso de firma digital	Objetivo directo por objetivo de negocio 2
OD[23][2]	Se requiere Autenticación en Aplicación Firma Móvil ANDROID durante el proceso de firma digital	Objetivo directo por objetivo de negocio 2
OD[26][2]	Se requiere Autenticación en Aplicación Firma Móvil IOS durante el proceso de firma digital	Objetivo directo por objetivo de negocio 2
OD[8][3]	Se requiere Confidencialidad en Servicios expuestos para Firma Móvil durante el proceso de firma digital	Objetivo directo por objetivo de negocio 3
OD[15][3]	Se requiere Confidencialidad en SignalR Hub durante el proceso de firma digital	Objetivo directo por objetivo de negocio 3
OD[5][3]	Se requiere Confidencialidad en Web service notificador entidad durante el proceso de firma digital	Objetivo directo por objetivo de negocio 3
OD[6][3]	Se requiere Confidencialidad en Servicio de firma expuesto a la entidad durante el proceso de firma digital	Objetivo directo por objetivo de negocio 3

A partir de la lista de objetivos directos y la representación del sistema, es posible comenzar a establecer relaciones de seguridad que derivan en nuevos objetivos indirectos a tomar en cuenta.

4.4 Relaciones de seguridad

El propósito de esta sección es presentar y caracterizar a grandes rasgos la lista de objetivos de seguridad obtenidos a partir de las relaciones de seguridad identificadas en el sistema de Firma Digital. Esta lista será el insumo principal para determinar los riesgos en su respectiva valoración.

Para identificar relaciones de seguridad, se procedió analizando primero todas las relaciones estructurales presentes en el árbol del todo y las partes, luego todas las relaciones de interacción para cada elemento de los diagramas de interacción y finalmente identificando las relaciones de representación.

Este proceso se realizó de manera iterativa, evaluando también los componentes que presentaban algún objetivo indirecto, hasta que se llegó a un grado aceptable debido al nivel de detalle del sistema analizado.

En resumen, partiendo de una base de 3 objetivos de negocio, que suponían 19 objetivos directos, fue necesario identificar y analizar 136 relaciones de seguridad que derivaron en los 25 objetivos indirectos que se presentan en la Tabla 15.

Tabla 15 Objetivos indirectos. Fuente: Elaboración propia

Identificador	Objetivo indirecto
OI[4][1]	Se requiere Integridad en Equipo donde se solicita la firma durante el proceso de firma digital
OI[12][1]	Se requiere Integridad en Sistema Operativo durante el proceso de firma digital
OI[18][1]	Se requiere Integridad en Equipo Android durante el proceso de firma digital
OI[21][1]	Se requiere Integridad en Sistema Operativo Android durante el proceso de firma digital
OI[19][1]	Se requiere Integridad en Equipo Iphone durante el proceso de firma digital
OI[24][1]	Se requiere Integridad en Sistema Operativo IOS durante el proceso de firma digital
OI[15][1]	Se requiere Integridad en SignalR Hub durante el proceso de firma digital
OI[11][1]	Se requiere Integridad en Navegador durante el proceso de firma digital
OI[8][1]	Se requiere Integridad en Servicios expuestos para Firma Móvil durante el proceso de firma digital
OI[16][1]	Se requiere Integridad en Servicio FVA durante el proceso de firma digital
OI[5][1]	Se requiere Integridad en Web service notificador entidad durante el proceso de firma digital
OI[6][1]	Se requiere Integridad en Servicio de firma expuesto a la entidad durante el proceso de firma digital
OI[17][1]	Se requiere Integridad en BD FVA durante el proceso de firma digital
OI[20][1]	Se requiere Integridad en Tarjeta de firma digital con NFC durante el proceso de firma digital
OI[15][2]	Se requiere Autenticación en SignalR Hub durante el proceso de firma digital
OI[8][2]	Se requiere Autenticación en Servicios expuestos para Firma Móvil durante el proceso de firma digital
OI[16][2]	Se requiere Autenticación en Servicio FVA durante el proceso de firma digital
OI[5][2]	Se requiere Autenticación en Web service notificador entidad durante el proceso de firma digital
OI[6][2]	Se requiere Autenticación en Servicio de firma expuesto a la entidad durante el proceso de firma digital
OI[20][2]	Se requiere Autenticación en Tarjeta de firma digital con NFC durante el proceso de firma digital
OI[16][3]	Se requiere Confidencialidad en Servicio FVA durante el proceso de firma digital
OI[23][3]	Se requiere Confidencialidad en Aplicación Firma Móvil ANDROID durante el proceso de firma digital
OI[26][3]	Se requiere Confidencialidad en Aplicación Firma Móvil IOS durante el proceso de firma digital
OI[18][2]	Se requiere Autenticación en Equipo Android durante el proceso de firma digital
OI[19][2]	Se requiere Autenticación en Equipo Iphone durante el proceso de firma digital

Cabe destacar que la evaluación de dichas relaciones ejemplifica de buena manera el carácter integral de la solución propuesta al problema de seguridad. Esto porque se logró constatar que, mediante la formación de cadenas de seguridad, es posible conocer cuáles objetivos indirectos son necesarios para atender un objetivo directo. En el Gráfico 1 se puede observar como un mayor porcentaje de los objetivos fueron derivados a partir de relaciones de seguridad, es decir, que estos objetivos de seguridad no estaban contemplados inicialmente, y su inclusión mejora la seguridad del sistema al complementar los objetivos de seguridad directos.

Dichas cadenas pueden ser tan sencillas como la que se presenta en la Figura 22, donde puede verse que, debido a una relación de seguridad existente, se vuelve necesario asegurar la integridad también en el "Equipo donde se solicita la firma" para de esta forma cubrir dicho servicio de seguridad en el "Firmador de escritorio"; o un poco más complejas como la mostrada en la Figura 23 donde para asegurar el "Servicio FVA" se requieren de incluir más objetivos de seguridad indirectos que cubran los componentes que mantienen algún tipo de relación con el primero.

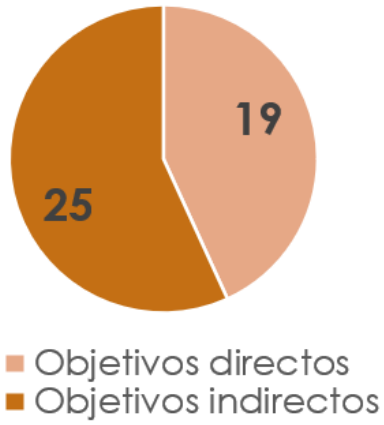

Gráfico 1 Objetivos por tipo. Fuente: Elaboración propia

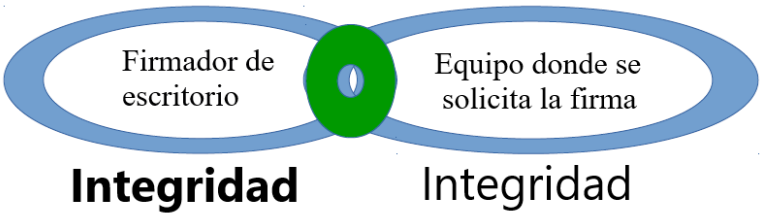

Figura 22 Cadena de seguridad sencilla con dos eslabones

Figura 23 Cadena de seguridad con múltiples objetivos indirectos

Otro aspecto interesante al analizar las relaciones de seguridad es su naturaleza. En el Gráfico 2 se aprecia la cantidad de objetivos indirectos categorizados por el tipo de relación del que fueron derivados. Esto nos muestra como la gran mayoría de relaciones presentes en el sistema son por alguna interacción entre componentes de software, y a su vez estas interacciones generaron una buena cantidad de objetivos de seguridad que complementan los objetivos definidos en primera instancia por el negocio. Estos datos también concuerdan con el tipo de componentes presentes en la representación del sistema, donde es posible deducir que al haber una gran mayoría de componentes digitales

o de software, se presentarían más interacciones que relaciones de aislamiento o de representación.

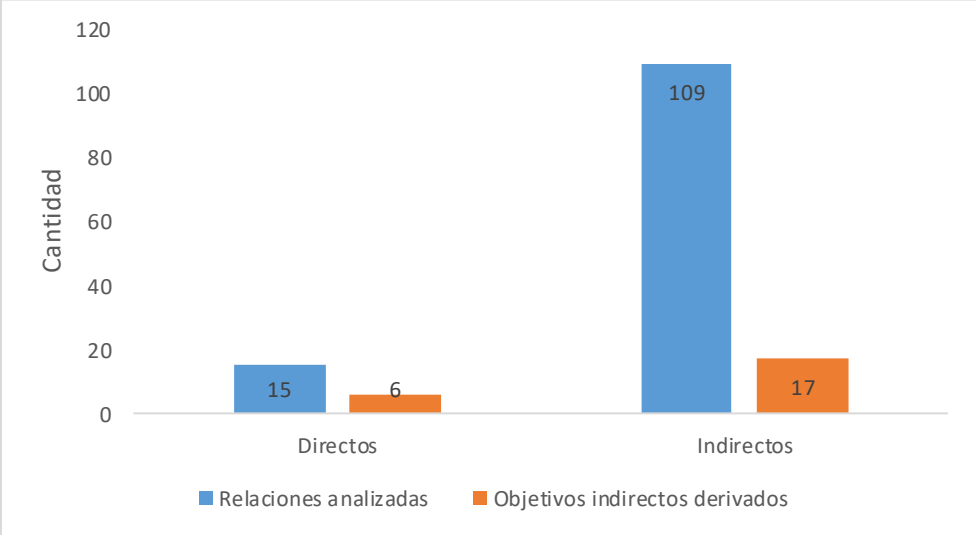

Gráfico 2 Objetivos de seguridad por tipo de relación. Fuente: Elaboración propia

5 Análisis de riesgos

En este capítulo se presentan los resultados obtenidos durante la identificación y valoración de los riesgos presentes en cada uno de los escenarios de firma digital

analizados. El capítulo inicia con algunas consideraciones generales que se tomaron previo al análisis y que delimitan el trabajo realizado. Después, se describe brevemente como los objetivos directos e indirectos funcionan como insumos para el debido análisis de riesgo y finalmente se concluye con un resumen del proceso de identificación y valoración de riesgos.

5.1 Consideraciones generales

5.1.1 Restricciones

Dada la naturaleza del sistema y de la firma digital, hay situaciones o escenarios en los que los servicios de seguridad pueden verse afectados indirectamente por circunstancias que están fuera del ámbito de la seguridad de la información. Un ejemplo de esto puede ser una persona que solicita el acceso a un determinado portal por medio de la aplicación de firma móvil, pero que lo hace bajo amenazas de un tercero que quiere suplantarlo para conseguir algún tipo de información a la que no está autorizado. Esto constituye una violación a la confidencialidad y sin embargo la persona está siguiendo el proceso correcto de la firma móvil, por lo que podría en algún futuro argumentar que lo hizo en contra de su voluntad.

Por esa razón es importante mencionar que en este análisis no fueron considerados aquellos riesgos que no están relacionados directamente con la seguridad del sistema, como, por ejemplo, amenazas, extorsión y coacción a personas, entre otros.

5.1.2 Limitaciones

En cuanto a las limitaciones, cabe destacar que el presente trabajo se enfoca en la prevención e identificación de incidentes que comprometan la seguridad del sistema analizado, por tanto, el análisis de riesgos se enfoca en la prevención y detección, dejando de lado la respuesta ante un eventual problema de seguridad, así como su corrección.

También se debe aclarar que este análisis se basa en la información y el nivel de detalle que se tiene de previo del sistema en cuestión, considerando que algunos

componentes no han sido detallados o descompuestos en otros más específicos. Esto responde a temas de confidencialidad y de trabajos previos que han abordado la seguridad en dichos componentes. Un ejemplo de esto se puede ver con el componente "Servicio FVA" que ha sido objeto de análisis en otros trabajos como (Mora, 2017) y que por tanto no es de suma relevancia su detalle, sino más bien el comportamiento que tiene con el sistema completo y sus entradas y salidas.

Finalmente, existe una limitante más que corresponde a la existencia de componentes externos sobre los cuales la organización no tiene un control total. Por esta razón, como se ha descrito en la metodología, estos componentes no se consideran individualmente ni generan relaciones u objetivos de seguridad indirectos. Un ejemplo de esto son las tecnologías utilizadas para hacer llegar las notificaciones a los teléfonos celulares, que constituyen una solución de un proveedor externo sobre el que no se tiene control o detalle de su implementación interna.

5.1.3 Verdades base

Bishop (2002) aclara que un aspecto importante en la seguridad es la confianza y la claridad de las verdades base sobre las que se apoya el análisis. Pues si estas son incorrectas, se destruyen toda la estructura que se haya trabajado sobre ellas. Por esa razón es importante analizar y enumerar los principales enunciados que se tomarán como verdaderos, con el fin de evitar que suposiciones aparentemente correctas lleven a conclusiones erróneas.

Las siguiente son algunas de las verdades base más relevantes que se asumieron correctas, y que conducen el proceso de aseguramiento de la información:

- Los componentes como el Servicio FVA que no ha sido detallado para su análisis se asume correctamente implementado y solo se considera su interacción con otros componentes como un factor de riesgo.
- Los certificados digitales identifican de forma unívoca a los usuarios finales.

- Los componentes externos al sistema y que pertenecen a infraestructuras de proveedores se consideran correctos y solo se incluye en el análisis sus puntos de conexión con el sistema.
- Los dispositivos criptográficos seguros utilizados en los escenarios del sistema han sido previamente estudiados y aceptados dentro del SNCD, por lo que no se consideran un riesgo para la seguridad de la información.
- Las actualizaciones del software complementario como por ejemplo sistemas operativos, navegadores , entre otros se asumen íntegras y correctas.
- Los componentes de hardware requeridos para ejecutar las aplicaciones, tales como computadoras, routers, firewalls, entre otros, se asumen correctamente fabricados y conectados.

5.2 Resumen de la identificación y valoración de riesgos

En esta sección se presenta un resumen de la valoración de los riesgos identificados. Dicha valoración se realizó con base en el cálculo de promedios de las ecuaciones 1 y 2, presentadas en las secciones 3.6.4 y 3.6.5 respectivamente. En total, se valoraron 72 riesgos, que se caracterizan a continuación.

5.2.1 Riesgos agrupados por nivel de severidad

El Gráfico 3 muestra la cantidad de riesgos valorados, agrupados por nivel de severidad. En total, de los 72 riesgos, se eligieron 52 para mitigarse, dado que esos riesgos se determinaron con nivel de severidad medio, alto o muy alto.

Por ejemplo, riesgos como el número 21: *"Defectos en el software del componente Firmador BCCR permiten que la aplicación genere resúmenes a partir del uso de algoritmos hash inseguros"* tienen un nivel de severidad muy alto, y por lo tanto debió ser mitigado, mientras que otros como el riesgo 43: "*Errores de configuración en el componente "Equipo Android" permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos"* tienen un riesgo bajo y por tanto no se incluyen acciones para su mitigación.

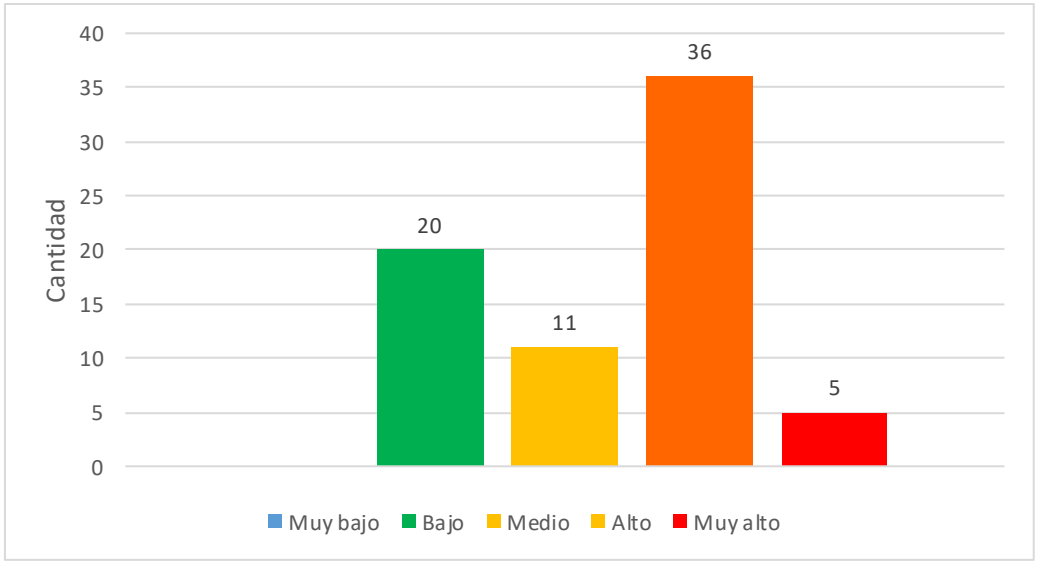

Gráfico 3 Cantidad de riesgos por nivel de severidad. Fuente: Elaboración propia

6 Definición de políticas de seguridad y objetivos de control

En este capítulo se pretende caracterizar y describir las políticas de seguridad que se han determinado para mitigar los riesgos presentes en los escenarios analizados, así como los objetivos de control que velan por su cumplimiento.

A nivel general fue posible determinar 45 políticas, que se encuentran listadas en el APÉNDICE D: Políticas de Seguridad Definidas, con lo que se logró cubrir todos los riesgos que fueron valorados con severidad media, alta o muy alta. Esto permite que se logre un grado de seguridad aceptable según los criterios establecidos al inicio de este trabajo.

Cabe destacar que una parte de las políticas pertenecen al escenario de firma digital en dispositivos móviles, pero no han sido diferenciadas de las del escenario de firma de escritorio debido a que ambos comparten los mismos componentes y en muchos casos las políticas debían aplicarse por igual para ambos escenarios. Por ejemplo, la política donde se indica que debe protegerse la información de la solicitud de la firma mientras se transmite por la red, es algo que debe hacerse independientemente del escenario donde se presente.

En cuanto a los objetivos de control, fue posible identificar y enumerar 24 controles que aplican en su gran mayoría para todos los escenarios estudiados en este proyecto. Dichos objetivos de control se encuentran enumerados en el APÉNDICE E: Objetivos de control.

7 Guía de implementación

En las siguientes subsecciones se detalla la guía de implementación generada en este trabajo.

Para aplicar esta guía se deben seguir una serie de pasos, a saber:

1. Recorrer la lista de políticas de seguridad presentadas en la sección 7.1.2, hasta que ya no queden políticas sin evaluar.
2. Para cada política, determinar si ésta es aplicable en el contexto de la evaluación.
3. Si la política no se considera aplicable, debe indicarse y agregar una observación con la justificación.
4. Si la política es aplicable, se debe determinar si los controles de seguridad implementados para hacerla cumplir satisfacen los requisitos establecidos por los objetivos de control correspondientes. Los objetivos de control se encuentran en la sección 0.
5. Si algún control de seguridad implementado no satisface los requisitos establecidos por el objetivo de control correspondiente, se debe indicar que no hay cumplimiento de la política e incluir una observación con la justificación correspondiente.
6. Si todos los controles de seguridad satisfacen los requisitos de seguridad que dictan los objetivos de control, se indica que hay cumplimiento de la política.

7.1 Introducción

Dada la criticidad y la relevancia del sistema de Firma Digital en Costa Rica, es sumamente importante validar que las aplicaciones de software que acceden o interactúan con el sistema sean seguras y confiables. En esta guía de implementación se pretende brindar un instrumento que permita evaluar el cumplimiento de un conjunto políticas de seguridad definidas para este tipo de aplicaciones, a través de objetivos de control que

especifican requisitos mínimos que deben satisfacerse, con el fin de proteger la seguridad de la información.

7.1.1 Descripción de la guía de implementación

Esta guía puede ser utilizada para evaluar los escenarios de firma digital en dispositivos móviles y en equipos de escritorio. Los servicios de seguridad que se verifican son los siguientes:

- Integridad (I): entendido como la propiedad de la información que previene un cambio indebido o no autorizado de los datos.
- Autenticación (A): entendida como verificación de la identidad de un sujeto o un componente.
- Confidencialidad (C): como la propiedad que garantiza que la información no esté disponible ni se divulgue a personas o procesos no autorizados.

7.1.2 Lista de políticas de seguridad a evaluarse

En la Tabla 16 se presenta la lista de políticas que debe ser evaluada.[2]

[2] En esta sección se presenta solamente un resumen de las políticas, con el fin de ejemplificar la tabla y su debido formato. Para referirse a todas las políticas que deben ser incluidas se debe revisar el APÉNDICE D: Políticas de Seguridad Definidas

Tabla 16 Lista de políticas a evaluar en la guía de implementación

ID	Política	Objetivos de control	Cumplimiento			Observaciones
			Sí	No	NA	
1	Se debe proteger el software cliente instalado en las máquinas de los usuarios de manera que no sea fácilmente escanearle o analizado para encontrar vulnerabilidades.	4				
…	…	…				
…	…	…				
45	El software de los dispositivos móviles debe tener instaladas las actualizaciones más recientes de las aplicaciones cliente.	5, 9				

7.1.3 Lista de objetivos de control

En la Tabla 17 se presenta la lista de objetivos de control que deberán ser evaluados.[3]

Tabla 17 Lista de objetivos de control para la guía de implementación

ID	Objetivo de control	Políticas
1	Se deben validar los datos que ingresan al sistema digitados por el usuario, verificando que cada entrada cumple al menos con los siguientes requisitos: Cuando la entrada es texto • Los caracteres introducidos deben ser válidos, según el conjunto de caracteres permitido correspondiente. • La longitud de los caracteres introducidos debe estar dentro de los límites mínimos y máximos correspondientes. • Si la entrada requiere un formato específico (como una fecha, una dirección de correo electrónico, un número telefónico, etcétera), los caracteres introducidos deben cumplir con ese formato. • Si la entrada se utiliza como argumento en una operación de creación, lectura, actualización o borrado de registros en una base de datos, se debe hacer a través de sentencias parametrizadas (prepared statements), y no mediante la concatenación de hileras de caracteres. • Si la entrada debe mostrarse al usuario posteriormente, durante su interacción con el sistema, deben aplicarse las reglas de escape correspondientes según el o los lenguajes utilizados. Cuando la entrada es un archivo • El archivo debe tener un formato permitido. • El formato del archivo debe ser correcto. • El tamaño del archivo no debe exceder un tamaño máximo permitido. • El archivo no debe almacenar contenido malicioso, como virus, malware, etcétera.	5, 6, 7, 8, 22, 23

[3] Al igual que en las políticas, en esta sección se incluye un resumen que ejemplifica el contenido de la tabla, pero para el detalle de los objetivos revisar el APÉNDICE E: Objetivos de control.

ID	Objetivo de control	Políticas
	• Si el archivo se almacenará en el sistema de archivos de un servidor, su nombre o ubicación no debe ser igual al de algún archivo de configuración según el tipo de servidor. Por ejemplo, .htaccess en Apache, o Web.conf en IIS, entre otros.	
…	…	…
24	La visualización del documento electrónico debe utilizar un método que cumpla con el principio WYSIWYS	43

7.1.4 Lista de observaciones finales

En la Tabla 18 se brinda una sección para indicar cualquier observación que se considere pertinente. Al agregar una observación se recomienda hacer referencia a la política de seguridad de donde surge dicha observación.

Tabla 18 Observaciones finales de la evaluación

No	Observación

7.1.5 Tabla con el resumen de la evaluación

En la Tabla 19 se muestra el resumen de la evaluación que será de utilidad para tener un panorama del estado de la revisión, además de identificar con mayor facilidad el grado de cumplimiento de la guía en general.

Tabla 19 Resumen de la evaluación

Política	Cumplimiento	
	Sí	No
1		
…		
…		
45		

8 Conclusiones, recomendaciones y trabajo futuro

A continuación, se presentan las conclusiones y los principales hallazgos de este trabajo. Adicionalmente, se propone una serie de recomendaciones que surgen a partir de los resultados, y se mencionan posibles oportunidades de trabajo futuro.

8.1.1 Conclusiones

Aporte del trabajo

Este trabajo ha permitido generar una serie de requisitos de seguridad que buscan una solución más segura y robusta de las aplicaciones de Firma Digital analizadas. Con esto, se pretende dar una referencia al incluir requisitos de seguridad en la construcción de los productos respectivos o eventualmente proveer un instrumento de evaluación al momento de dar mantenimiento a las aplicaciones existentes.

Enfoque integral basado en las cadenas de seguridad

Uno de los puntos más importantes de este trabajo es el enfoque seguido para lograr abarcar la seguridad del sistema. Dada la metodología planteada se logró generar una representación bastante fiable del sistema como se planteó en el objetivo específico número 1, y además que todos los riesgos identificados correspondan al menos a un objetivo de seguridad del sistema, cumpliendo así con lo planteado en el objetivo específico número 2. Dichos objetivos fueron obtenidos a partir de objetivos iniciales y las relaciones que existen entre los distintos componentes. Esto representa un enfoque integral debido a la existencia de cadenas de seguridad; es decir, de las necesidades de aplicar objetivos de seguridad en otros componentes para cubrir los objetivos en los componentes iniciales.

Por ejemplo, en un principio se definió que se debía asegurar la integridad en el componente “Servicio FVA”, pero gracias al análisis que presenta el modelo aplicado, se puede notar que este componente se relaciona con otros componentes y esto conlleva el debido análisis de cada uno de ellos. Una vez que se analizan se determina que para asegurar la integridad en el Servicio FVA es necesario también asegurarla en otros componentes como los servicios expuestos a las entidades, la base de datos de FVA, entre otros. Este proceso se repite de nuevo en cada componente que se suma a la lista de objetivos de seguridad y se van creando de esta forma cadenas donde un servicio de seguridad en un componente está directamente relacionado con un objetivo de seguridad en otro componente.

Este enfoque hace que, al identificar los riesgos en cada componente de la lista final obtenida, se ataca el problema desde un enfoque integral, valorando cada interacción del sistema y la posibilidad de que un riesgo de un componente pueda afectar a otro.

Además, se logró identificar políticas para cada riesgo del sistema, de manera que estos puedan ser minimizados y dar un grado de seguridad al sistema cubriendo lo propuesto en el objetivo específico número 3.

Guía de aseguramiento

Otro aspecto para resaltar es que, a partir de los escenarios analizados, los riesgos, las políticas y los objetivos de control, fue posible definir una guía de implementación que recopila una serie de requisitos de seguridad que buscan una solución más segura y robusta de las aplicaciones de Firma Digital analizadas. Esta guía puede servir como referencia al incluir requisitos de seguridad en la construcción de los productos respectivos o como un instrumento de evaluación al momento de dar mantenimiento a las aplicaciones existentes.

Un aspecto importante de esta guía es que presenta el resultado final en un formato que la gente conoce, pero además si se ocupara corregir o modificar algún aspecto, se tiene una estructura en el proceso que lo permite, además, con esta guía cumplimos el objetivo específico número 4.

8.1.2 Recomendaciones

Dado que el sistema analizado en este trabajo se encuentra en constante cambio y evolución, es importante revisar con cierta frecuencia los requerimientos de seguridad que han sido definidos. Cabe destacar que el enfoque de la metodología seguida durante esta investigación permite realizar de manera relativamente rápida este tipo de actualizaciones.

También es recomendable la automatización de algunas etapas del proceso, debido a que esto podría generar un ahorro de tiempo principalmente en la construcción de la

representación del sistema, la identificación de relaciones y la propagación de objetivos. Además de contribuir a minimizar los errores humanos en los procesos que son más repetitivos y que involucran buena cantidad de información.

Otro aspecto importante es que, automatizando ciertas etapas, podría darse un enfoque mayor en algunos elementos claves, como la definición de los escenarios y los objetivos de seguridad, que finalmente son etapas que sustentan el proceso.

De igual forma es importante hacer énfasis en que durante el desarrollo del trabajo es primordial el involucramiento del cliente, principalmente durante las etapas más tempranas del proceso, porque gracias a su colaboración es posible dar forma y validar los distintos productos del trabajo. Esto implica constantes revisiones y análisis en conjunto para generar un producto de utilidad.

8.1.3 Trabajo futuro

La aplicación de la guía de aseguramiento en el sistema es algo que podría aportar significativamente a este trabajo y al mejoramiento del propio sistema. Este sería un trabajo pendiente luego de esta investigación. Además, también sería importante aumentar el nivel de detalle descrito en la representación del sistema con el fin de atacar más puntualmente los requerimientos de seguridad de cada elemento del sistema.

Finalmente, el proceso para la identificación de objetivos de seguridad y determinación de riesgos que se siguió tiende a volverse un poco complejo al realizarse de forma manual. Esto es algo que se puede mejorar mucho si pudiera realizarse de forma automatizada. Por lo tanto, se sugiere desarrollar herramientas de software que faciliten la ejecución de procesos seguidos y que sirvan como una opción más rápida y efectiva.

9 Bibliografía

Aguilar, C., Barquero, A., Chavarría, D., Fernández, M., & Solano, K. (2011). *Propuesta para estandarizar el formato de los documentos electrónicos firmados digitalmente en Costa Rica*. Costa Rica: Instituto Tecnológico de Costa Rica.

Alcaraz, D. (2019). *Firma Electrónica en dispositivos móviles.* España: Universidad autónoma de Barcelona. Recuperado el 2 de 9 de 2020, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/62847/6/dmalcarazTFM0116memoria.pdf

Bishop, M. (2002). *The art and science of computer security.* Boston: Addison Wesley.

Boell, S., & Dubravka, C.-K. (2015). *What is an Information System?* Recuperado el 15 de 05 de 2020, de 48th Hawaii International Conference on System Sciences: https://www.computer.org/csdl/proceedings-article/hicss/2015/7367e959/12OmNB7LvzT

Buchmann, J., Evangelos, K., & Wiesmaier, A. (2014). *Introduction to Public Key Infrastructures*. Springer.

CNSS. (2015). *Committee on National Security Systems Glossary*. Recuperado el 20 de 05 de 2020, de https://www.cnss.gov/CNSS/issuances/Instructions.cfm

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*, 13-21. Recuperado el 20 de 01 de 2020, de https://timreview.ca/article/835

CVE. (2020). *Vulnerabilities by types*. Recuperado el 07 de 01 de 2020, de http://www.cvedetails.com/vulnerabilities-by-types.php

Deibert, R., & Rohozinski, R. (2010). Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy, 21*(4), 43-57. Recuperado el 15 de 01 de 2020, de https://muse.jhu.edu/article/398730

Dierks, T., & Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. Obtenido de The Internet Engineering Task Force: https://www.ietf.org/rfc/rfc5246.txt

Febri, M. (2013). *OWASP*. Recuperado el 20 de 01 de 2020, de Introduction and implementation OWASP Risk Rating Management: https://owasp.org/www-pdf-archive/Riskratingmanagement-170615172835.pdf

Gobierno de Costa Rica. (2005). *Ley de certificados, firmas digitales y documentos electrónicos No. 8454.* Costa Rica: Diario Oficial La Gaceta.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People,, 22*, 92-108. Recuperado el 02 de 04 de 2020, de https://www.emerald.com/insight/content/doi/10.1108/09593840910962186/full/html

Google. (2020). *Developers Android*. Obtenido de Near field communication overview: https://developer.android.com/guide/topics/connectivity/nfc

Google. (2020). *Introduction to Push Notifications*. Recuperado el 10 de 07 de 2020, de https://developers.google.com/web/ilt/pwa/introduction-to-push-notifications

Housley, R. (2004). *The Internet Engineering Task Force.* Recuperado el 10 de 12 de 2020, de https://www.ietf.org/rfc/rfc3852.txt

Instituto de Normas Técnicas de Costa Rica. (2014). *Norma INTE/ISO 27000:2014 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.* San José, Costa Rica.

Kaliski, B. (1998). *Cryptographic Message Syntax Version 1.5*. Recuperado el 01 de 01 de 2021, de The Internet Engineering Task Force: https://www.ietf.org/rfc/rfc2315.txt

Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography*. CRC Press.

Longley, D., & Shain, M. (1989). *Dictionary of standards concepts and terms*. Macmillan Publishers Ltd.

Maconachy, W., Schou, C., Ragsdale, D., & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security (*, 306-310.

McCumber, J. (1991). *Information Systems Security: a comprehensive model.* Washinton, DC.

Menezes, A., van Oorschot, P., & Vanstone, S. (1997). *Handbook of Applied Cryptography.* CRC Press.

Microsoft. (2002). *Microsoft Computer Dictionary*. Microsoft Press.

Mora, A. (2017). *Definición de un proceso de aseguramiento de la información para los componentes tecnológicos, que utilizan certificados y firma digital en una aplicación de software dentro del Sistema Nacional de Certificación Digital.* San José, Costa Rica.: Universidad de Costa Rica.

Morillo, J. (2010). *Introducción a los dispositivos móviles.* España: Universidad de Oberta de Catalunya.

National Institute of Standards and Technology. (2012). *SP 800-30. Guide for Conducting Risk Assessments.* Gaithersburg,.

National Institute of Standards and Technology. (2019). *SP 800-163Vetting the Security of Mobile Applications.* Gaithersburg.

Nkeze, E., Pearce, J., & Womer, M. (2007). *W3C*. Recuperado el 02 de 10 de 2020, de Device description landscape 1.0: http://www.w3.org/TR/dd-landscape

OWASP. (3 de 9 de 2015). *OWASP Risk Rating Methodology*. Obtenido de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

OWASP. (2016). *OWASP Periodic Table of Vulnerabilities*. Recuperado el 06 de 07 de 2020, de https://wiki.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities

OWASP. (2020). *OWASP mobile top 10*. Recuperado el 23 de 06 de 2020, de https://owasp.org/www-project-mobile-top-10/

OWASP. (10 de 12 de 2020). *OWASP.ORG*. Obtenido de Authentication Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

OWASP. (2020). *Vulnerabilities*. Obtenido de https://owasp.org/www-community/vulnerabilities/

Pacheco, S., & Piazza, C. (2007). *Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las*. Argentina: UNIVERSIDAD NACIONAL DE LA PLATA. Recuperado el 20 de 01 de 2020, de http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

Racciatti, H. (2012). Modelado de Amenazas. *OWASP*. Recuperado el 14 de 02 de 2020, de https://owasp.org/www-pdf-archive//HRacciatti_ModeladodeAmenazas.pdf

SANS. (2020). *SANS Top 25 software errors*. Recuperado el 15 de 05 de 2020, de https://www.sans.org/top25-software-errors

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security, 15*(5), 390-396. Recuperado el 14 de 01 de 2020, de http://ijns.femto.com.tw/

Villalón, R., Solano, B., & Marín, G. (2014). Infosec-Tree Model: An Applied, In-depth, and Structured Information Security Model for Computer and Network Systems. *Journal of Internet Technology and Secured Transactions (JITST)*, 300-310.

W3C. (2008). *XML Signature Syntax and Processing (Second Edition).* Obtenido de https://www.w3.org/TR/xmldsig-core/

10 Apéndices

10.1 APÉNDICE A: Riesgos identificados

El presente apéndice muestra todos los riesgos identificados después de aplicar la metodología propuesta. La Tabla 20 muestra la lista de los riesgos identificados para cada uno de los objetivos de seguridad directos o indirectos obtenidos para el sistema.

Tabla 20 Riesgos identificados a partir de las relaciones de seguridad

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
1	Comunicaciones desprotegidas	Atacante malintencionado	OD[27][1]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el documento electrónico que será firmado o los demás datos de la solicitud de firma, mientras se transmite desde su ubicación original hacia el componente "Servicio de firma digital invocado por la entidad".
2	Defectos en el software	Usuario	OD[27][1]	Defectos en el componente "Servicio de firma digital invocado por la entidad" permiten que la aplicación acepte del usuario documentos electrónicos cuyos formatos no son soportados o son incorrectos.
3	Defectos en el software	Atacante malintencionado	OD[27][1]	Defectos en el componente "Servicio de firma digital invocado por la entidad" permiten que la aplicación acepte de un atacante malintencionado documentos electrónicos que contienen código oculto o malicioso.
4	Comunicaciones desprotegidas	Atacante malintencionado	OD[28][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos del usuario registrado, mientras se transmiten desde el componente "Dispositivo móvil" hacia el componente "Servicios expuestos para firma móvil".
5	Defectos en el software	Atacante malintencionado	OD[28][1] OD[8][3]	Defectos en el componente "Servicios expuestos para firma móvil" permiten que la aplicación acepte de un atacante malintencionado datos del usuario registrado con información incorrecta o maliciosa.
6	Comunicaciones desprotegidas	Atacante malintencionado	OD[29][1] OD[15][3] OI[15][1]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
				firma, mientras se transmiten desde el componente "Servicio FVA" hacia el componente "SignalR Hub".
7	Comunicaciones desprotegidas	Atacante malintencionado	OD[29][1] OD[15][3] OI[15][1]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de firma, mientras se transmiten desde el componente "SignalR Hub" hacia el componente "Firmador BCCR".
8	Defectos en el software	Atacante malintencionado	OD[29][1] OI[15][1]	Defectos en el software del SignalR Hub podrían permitir a un atacante modificar los datos que se envían al componente "Firmador BCCR"
9	Comunicaciones desprotegidas	Atacante malintencionado	OD[29][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de firma, mientras se transmiten desde el componente "Servicios expuestos para firma móvil" hacia el componente "Aplicación Firma móvil Android".
10	Comunicaciones desprotegidas	Atacante malintencionado	OD[29][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de firma, mientras se transmiten desde el componente "Servicios expuestos para firma móvil" hacia el componente "Aplicación Firma móvil IOS".
11	Comunicaciones desprotegidas	Atacante malintencionado	OD[30][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de los credenciales o insumos para firmar, mientras se transmiten desde el componente "Aplicación firma móvil Android" hacia el componente "Servicios expuestos para Firma móvil".
12	Comunicaciones desprotegidas	Atacante malintencionado	OD[30][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de los credenciales o insumos para firmar, mientras se transmiten

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
				desde el componente “Aplicación firma móvil IOS” hacia el componente “Servicios expuestos para Firma móvil”.
13	Comunicaciones desprotegidas	Atacante malintencionado	OD[30][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de los credenciales o insumos para firmar, mientras se transmiten desde el componente “Servicios expuestos para Firma móvil” hacia el componente “Servicio FVA”.
14	Comunicaciones desprotegidas	Atacante malintencionado	OD[31][1] OD[15][3] OI[15][1]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente “Firmador BCCR” hacia el componente “SignalR Hub”.
15	Comunicaciones desprotegidas	Atacante malintencionado	OD[31][1] OD[15][3] OI[15][1]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente “SignalR Hub” hacia el componente “Servicio FVA”.
16	Comunicaciones desprotegidas	Atacante malintencionado	OD[31][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente “Aplicación firma móvil Android” hacia el componente “Servicios expuestos para firma móvil”.
17	Comunicaciones desprotegidas	Atacante malintencionado	OD[31][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente “Aplicación firma móvil IOS” hacia el componente “Servicios expuestos para firma móvil”.

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
18	Comunicaciones desprotegidas	Atacante malintencionado	OD[32][1] OD[5][3] OI[5][1]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente "Servicio FVA" hacia el componente "Web service notificador de la entidad".
19	Comunicaciones desprotegidas	Atacante malintencionado	OD[33][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de notificación al usuario, mientras se transmiten desde el componente "Servicio FVA" hacia el componente "Servicios expuestos para firma móvil".
20	Comunicaciones desprotegidas	Atacante malintencionado	OD[33][1] OD[8][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de notificación al usuario, mientras se transmiten desde el componente "Servicios expuestos para firma móvil" hacia el componente "Dispositivo móvil".
21	Defectos en el software	Usuario	OD[14][1]	Defectos en el software del componente "Firmador BCCR" permiten que la aplicación genere resúmenes a partir del uso de algoritmos hash inseguros
22	Defectos en el software	Usuario	OD[14][1]	Defectos en el componente "Firmador BCCR" permiten que la aplicación acepte del usuario certificados digitales inválidos.
23	Defectos en el software	Usuario	OD[14][1]	Defectos en el componente de "Firmador BCCR" permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
24	Defectos en el software	Usuario	OD[14][1]	Defectos en el componente de “Firmador BCCR” permiten que la aplicación acepte del usuario datos con código oculto o malicioso.
25	Defectos en el software	Usuario	OD[23][1]	Defectos en el software del componente “Aplicación firma móvil Android” permiten que la aplicación genere resúmenes a partir del uso de algoritmos hash inseguros
26	Defectos en el software	Usuario	OD[23][1]	Defectos en el componente “Aplicación firma móvil Android” permiten que la aplicación acepte del usuario certificados digitales inválidos.
27	Defectos en el software	Usuario	OD[23][1]	Defectos en el componente de “Aplicación firma móvil Android” permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.
28	Defectos en el software	Usuario	OD[23][1]	Defectos en el componente de “Aplicación firma móvil Android” permiten que la aplicación acepte del usuario datos con código oculto o malicioso.
29	Defectos en el software	Usuario	OD[26][1]	Defectos en el software del componente “Aplicación firma móvil IOS” permiten que la aplicación genere resúmenes a partir del uso de algoritmos hash inseguros
30	Defectos en el software	Usuario	OD[26][1]	Defectos en el componente “Aplicación firma móvil IOS” permiten que la aplicación acepte del usuario certificados digitales inválidos.
31	Defectos en el software	Usuario	OD[26][1]	Defectos en el componente de “Aplicación firma móvil IOS” permiten que la aplicación acepte del usuario

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
				certificados digitales que no están almacenados en un dispositivo criptográfico seguro.
32	Defectos en el software	Usuario	OD[26][1]	Defectos en el componente de "Aplicación firma móvil IOS" permiten que la aplicación acepte del usuario datos con código oculto o malicioso.
33	Defectos en el software	Usuario	OD[10][2]	Defectos en el componente de "Firmador BCCR" podrían permitir que el usuario acceda a firmar un documento sin utilizar credenciales.
34	Defectos en el software	Usuario	OD[10][2]	Defectos en el componente de "Aplicación firma móvil Android" podrían permitir que el usuario acceda a firmar un documento sin utilizar credenciales.
35	Defectos en el software	Usuario	OD[10][2]	Defectos en el componente de "Aplicación firma móvil IOS" podrían permitir que el usuario acceda a firmar un documento sin utilizar credenciales.
36	Defectos en el software	Atacante malintencionado	OD[8][3]	Defectos en el componente "Servicios expuestos para firma móvil" permiten que la aplicación revele datos sin autorización.
37	Defectos en el software	Atacante malintencionado	OD[15][3]	Defectos en el software del SignalR Hub podrían permitir a un atacante acceder a los datos que se envían al componente "Firmador BCCR" de uno o varios usuarios.
38	Defectos en el software	Atacante malintencionado	OD[5][3]	Defectos en el software del Web Service notificador de la entidad podrían permitir a un atacante acceder a los datos que se envían a la entidad desde el componente "Servicio FVA".

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
39	Defectos en el software	Atacante malintencionado	OD[6][3]	Defectos en el software del "Servicio de firma expuesto a la entidad" podrían permitir a un atacante acceder a los datos que se envían al componente "Servicio FVA".
40	Errores de configuración	Atacante malintencionado	OI[4][1]	Errores de configuración en el componente "Equipo donde se solicita la firma" permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.
41	Errores de configuración	Atacante malintencionado	OI[4][1]	Errores de configuración en el componente "Equipo donde se solicita la firma" permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.
42	Software desactualizado	Atacante malintencionado	OI[12][1]	La falta de actualizaciones en el sistema operativo permite a un atacante malintencionado instalar software malicioso en la máquina donde se ejecuta algún componente de la aplicación.
43	Errores de configuración	Atacante malintencionado	OI[18][1]	Errores de configuración en el componente "Equipo Android" permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.
44	Errores de configuración	Atacante malintencionado	OI[18][1]	Errores de configuración en el componente "Equipo Android" permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.
45	Software desactualizado	Atacante malintencionado	OI[21][1]	La falta de actualizaciones en el "Sistema operativo Android" permite a un atacante malintencionado instalar software malicioso en el dispositivo donde se ejecuta la aplicación de firma móvil.

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
46	Errores de configuración	Atacante malintencionado	OI[19][1]	Errores de configuración en el componente “Equipo IOS” permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.
47	Errores de configuración	Atacante malintencionado	OI[19][1]	Errores de configuración en el componente “Equipo IOS” permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.
48	Software desactualizado	Atacante malintencionado	OI[24][1]	La falta de actualizaciones en el “Sistema operativo IOS” permite a un atacante malintencionado instalar software malicioso en el dispositivo donde se ejecuta la aplicación de firma móvil.
49	Defectos en el software	Atacante malintencionado	OI[15][1]	Defectos en el software del “SignalR Hub” podrían permitir a un atacante modificar a los datos que se envían al componente “Firmador BCCR” de uno o varios usuarios.
50	Errores de configuración	Atacante malintencionado	OI[15][1]	Errores de configuración en el componente “SignalR Hub” podrían permitir al usuario modificar datos de la aplicación mediante técnicas como falsificación de solicitudes entre sitios.
51	Defectos en el software	Atacante malintencionado	OD[15][3]	Defectos en el software “SignalR Hub” podrían permitir al usuario acceder a información confidencial explotando un mal manejo de las excepciones.
52	Software desactualizado	Atacante malintencionado	OI[11][1]	La falta de actualizaciones en el navegador de internet permite a un atacante malintencionado instalar software malicioso en la máquina donde se ejecuta algún componente de la aplicación.

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
53	Defectos en el software	Atacante malintencionado	OI[8][1]	Defectos de software en el componente “Servicios expuestos para firma móvil” permiten al atacante alterar los datos que se envían al “Servicio FVA”.
54	Errores de configuración	Atacante malintencionado	OI[16][1]	Errores de configuración de la(s) máquina(s) donde la aplicación está instalada permite la divulgación de stack traces u otro tipo de información, que permite que algún atacante malintencionado obtenga datos suficientes para realizar un ataque exitoso.
55	Defectos en el software	Atacante malintencionado	OI[16][1]	Defectos de software en el componente “Servicio FVA” permiten al atacante alterar los datos que se envían a los demás componentes del sistema.
56	Comunicaciones desprotegidas	Atacante malintencionado	OI[16][1] OI[16][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos mientras se transmiten desde el “Servicio FVA” hacia el resto del sistema
57	Defectos de software	Atacante malintencionado	OI[5][1]	Defectos de software en el componente “Web service notificador de la entidad” podrían permitirle al atacante acceder a los datos que se envían a la entidad y eventualmente modificarlos.
58	Defectos de software	Atacante malintencionado	OI[6][1]	Defectos de software en el componente “Servicio de firma expuesto a la entidad” podrían permitirle al atacante acceder a los datos que se envían desde la entidad y eventualmente modificarlos.
59	Defectos del software	Atacante malintencionado	OI[17][1]	Defectos en el componente “BD FVA” permiten a un atacante malintencionado modificar el contenido del documento electrónico mientras éste se encuentra almacenado dicho componente.

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
60	Comunicaciones desprotegidas	Atacante malintencionado	OI[17][1]	Comunicaciones desprotegidas permiten al atacante modificar los datos de la "Solicitud de nueva firma desde la entidad" mientras se transmiten al componente "BD FVA"
61	Comunicaciones desprotegidas	Atacante malintencionado	OI[20][1]	Comunicaciones desprotegidas permiten al atacante modificar los datos mientras se transmiten desde el componente "Tarjeta de firma digital con NFC" al componente "Aplicación firma móvil Android"
62	Comunicaciones desprotegidas	Atacante malintencionado	OI[20][1]	Comunicaciones desprotegidas permiten al atacante modificar los datos mientras se transmiten desde el componente "Tarjeta de firma digital con NFC" al componente "Aplicación firma móvil IOS"
62	Defectos en el hardware	Usuario	OI[20][1] OI[20][2]	Defectos en el componente "Tarjeta de firma digital con NFC" permiten que la aplicación genere datos cifrados mediante el uso de algoritmos de cifrado inseguros.
63	Defectos en el software	Atacante malintencionado	OI[15][2]	Defectos en el software del SignalR Hub podrían permitir a un atacante acceder a datos de otros usuarios sin estar autorizados para ello.
64	Defectos en el software	Atacante malintencionado	OI[8][2]	Defectos de software en el componente "Servicios expuestos para firma móvil" permiten al atacante acceder a datos de otros usuarios sin estar autorizados para ello.
65	Defectos en el software	Atacante malintencionado	OI[16][2]	Defectos de software en el componente "Servicio FVA" permiten al atacante acceder a datos de otros usuarios sin estar autorizados para ello.
66	Errores de configuración	Atacante malintencionado	OI[5][2]	Errores de configuración en el componente "Web service notificador de la entidad" permiten al atacante acceder sin autorización a la información enviada desde el "Servicio FVA"

ID	Fuente de vulnerabilidad	Fuente de amenaza	Objetivos relacionado	Descripción del riesgo
67	Errores de configuración	Atacante malintencionado	OI[6][2]	Errores de configuración en el componente "Servicio de firma expuesto a la entidad" permiten al atacante acceder sin autorización a la información enviada desde el "Servicio FVA"
68	Comunicaciones desprotegidas	Atacante malintencionado	OI[16][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado revelar datos que se transmiten hacia el componente "Servicio FVA"
69	Comunicaciones desprotegidas	Atacante malintencionado	OI[23][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado revelar datos que se transmiten hacia el componente "Aplicación firma móvil Android"
70	Comunicaciones desprotegidas	Atacante malintencionado	OI[26][3]	Comunicaciones desprotegidas permiten a un atacante malintencionado revelar datos que se transmiten hacia el componente "Aplicación firma móvil IOS"
71	Errores de configuración	Atacante malintencionado	OI[18][2]	Errores de configuración en el componente "Equipo Android" podrían permitir al atacante el acceso a datos como "Datos de notificación al usuario" sin tener autorización para ello.
72	Errores de configuración	Atacante malintencionado	OI[19][2]	Errores de configuración en el componente "Equipo Android" podrían permitir al atacante el acceso a datos como "Datos de notificación al usuario" sin tener autorización para ello.

10.2 APÉNDICE B: Detalle de la valoración de los riesgos identificados

En este apéndice se presenta el detalle de la valoración de los riesgos identificados. A cada riesgo se procedió a asignarle los valores para cada factor incluido en las escalas previamente definidas en el capítulo de metodología y posteriormente se le determinó su impacto y nivel de severidad.

Tabla 21 Valoración de los riesgos identificados. Fuente: Elaboración propia.

ID	Descripción del riesgo	H	Ro	Ru	D	E	Probabilidad	C	A	E	R	Impacto	Severidad
1	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el documento electrónico que será firmado o los demás datos de la solicitud de firma, mientras se transmite desde su ubicación original hacia el componente "Servicio de firma digital invocado por la entidad".	3	9	5	3	3	**4.6**	9	9	7	7	**8**	**Alto**
2	Defectos en el componente "Servicio de firma digital invocado por la entidad" permiten que la aplicación acepte del usuario documentos electrónicos cuyos formatos no son	3	3	9	5	5	**5**	3	3	3	3	**3**	**Alto**

	soportados o son incorrectos.												
3	Defectos en el componente “Servicio de firma digital invocado por la entidad” permiten que la aplicación acepte de un atacante malintencionado documentos electrónicos que contienen código oculto o malicioso.	1	9	3	1	1	**3**	7	7	7	7	**7**	**Alto**
4	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos del usuario registrado, mientras se transmiten desde el componente “Dispositivo móvil” hacia el componente “Servicios expuestos para firma móvil”.	5	5	5	3	3	**4.2**	3	7	3	3	**4**	**Medio**
5	Defectos en el componente	1	5	3	1	1	**2.2**	5	5	5	5	**5**	**Medio**

	"Servicios expuestos para firma móvil" permiten que la aplicación acepte de un atacante malintencionado datos del usuario registrado con información incorrecta o maliciosa.												
6	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de firma, mientras se transmiten desde el componente "Servicio FVA" hacia el componente "SignalR Hub".	1	5	1	1	1	**1.8**	3	3	3	3	**3**	**Bajo**
7	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos	3	5	3	1	1	**2.6**	5	7	3	7	**5.5**	**Medio**

	de la solicitud de firma, mientras se transmiten desde el componente "SignalR Hub" hacia el componente "Firmador BCCR".												
8	Defectos en el software del SignalR Hub podrían permitir a un atacante modificar los datos que se envían al componente "Firmador BCCR"	1	5	3	1	1	**2.2**	7	5	3	7	**5.5**	**Medio**
9	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de firma, mientras se transmiten desde el componente "Servicios expuestos para firma móvil" hacia el componente "Aplicación Firma móvil Android".	3	5	5	3	3	**3.8**	7	5	3	7	**5.5**	**Alto**

10	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los datos de la solicitud de firma, mientras se transmiten desde el componente "Servicios expuestos para firma móvil" hacia el componente "Aplicación Firma móvil IOS".	3	5	5	3	3	**3.8**	7	5	3	7	**5.5**	**Alto**
11	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de los credenciales o insumos para firmar, mientras se transmiten desde el componente "Aplicación firma móvil Android" hacia el componente	3	9	5	1	1	**3.8**	7	3	5	5	**5**	**Alto**

	"Servicios expuestos para Firma móvil".												
12	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de los credenciales o insumos para firmar, mientras se transmiten desde el componente "Aplicación firma móvil IOS" hacia el componente "Servicios expuestos para Firma móvil".	3	9	5	3	3	**4.6**	7	3	5	5	**5**	**Alto**
13	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de los credenciales o insumos para firmar, mientras se transmiten desde el	1	9	1	1	1	**2.6**	7	7	7	7	**7**	**Alto**

	componente “Servicios expuestos para Firma móvil” hacia el componente “Servicio FVA”.												
14	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente “Firmador BCCR” hacia el componente “SignalR Hub”.	3	1	5	1	1	**2.2**	7	3	5	3	**4.5**	**Bajo**
15	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente	1	1	3	1	1	**1.4**	3	3	3	3	**3**	**Bajo**

	"SignalR Hub" hacia el componente "Servicio FVA".												
16	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente "Aplicación firma móvil Android" hacia el componente "Servicios expuestos para firma móvil".	3	1	5	3	1	**2.6**	5	7	3	7	**5.5**	**Medio**
17	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente	3	1	5	3	3	**3**	7	5	7	7	**6.5**	**Alto**

	"Aplicación firma móvil IOS" hacia el componente "Servicios expuestos para firma móvil".												
18	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de la respuesta de la firma, mientras se transmiten desde el componente "Servicio FVA" hacia el componente "Web service notificador de la entidad".	1	1	3	1	1	**1.4**	5	3	5	3	**4**	**Bajo**
19	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de notificación al usuario, mientras se	1	1	1	1	1	**1**	5	3	3	3	**3.5**	**Bajo**

	transmiten desde el componente “Servicio FVA” hacia el componente “Servicios expuestos para firma móvil”.												
20	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de notificación al usuario, mientras se transmiten desde el componente “Servicios expuestos para firma móvil” hacia el componente “Dispositivo móvil”.	3	1	5	1	3	**2.6**	5	5	3	3	**4**	**Bajo**
21	Defectos en el software del componente “Firmador BCCR” permiten que la aplicación genere resúmenes a partir del uso de	7	9	5	1	5	**5.4**	9	9	7	7	**8**	**Muy alto**

	algoritmos hash inseguros												
22	Defectos en el componente “Firmador BCCR” permiten que la aplicación acepte del usuario certificados digitales inválidos.	9	3	7	5	5	**5.8**	3	3	3	3	**3**	**Alto**
23	Defectos en el componente de “Firmador BCCR” permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.	9	3	7	3	5	**5.4**	3	3	3	3	**3**	**Alto**
24	Defectos en el componente de “Firmador BCCR” permiten que la aplicación acepte del usuario datos con código oculto o malicioso.	7	9	1	1	1	**3.8**	7	7	7	7	**7**	**Alto**

25	Defectos en el software del componente “Aplicación firma móvil Android” permiten que la aplicación genere resúmenes a partir del uso de algoritmos hash inseguros	9	3	7	1	9	**5.8**	9	9	7	7	**8**	**Muy alto**
26	Defectos en el componente “Aplicación firma móvil Android” permiten que la aplicación acepte del usuario certificados digitales inválidos.	9	3	7	5	5	**5.8**	3	3	3	3	**3**	**Alto**
27	Defectos en el componente de “Aplicación firma móvil Android” permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.	7	3	5	7	7	**5.8**	3	3	3	3	**3**	**Alto**

28	Defectos en el componente de "Aplicación firma móvil Android" permiten que la aplicación acepte del usuario datos con código oculto o malicioso.	7	9	3	5	5	**5.8**	7	7	7	7	**7**	**Muy alto**
29	Defectos en el software del componente "Aplicación firma móvil IOS" permiten que la aplicación genere resúmenes a partir del uso de algoritmos hash inseguros	9	3	3	1	9	**5**	9	9	7	7	**8**	**Muy alto**
30	Defectos en el componente "Aplicación firma móvil IOS" permiten que la aplicación acepte del usuario certificados digitales inválidos.	9	3	3	5	5	**5**	3	3	3	3	**3**	**Alto**

31	Defectos en el componente de “Aplicación firma móvil IOS” permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.	7	3	5	7	7	**5.8**	3	3	3	3	**3**	**Alto**
32	Defectos en el componente de “Aplicación firma móvil IOS” permiten que la aplicación acepte del usuario datos con código oculto o malicioso.	7	9	3	3	3	**5**	7	7	7	7	**7**	**Muy alto**
33	Defectos en el componente de “Firmador BCCR” podrían permitir que el usuario acceda a firmar un documento sin utilizar credenciales.	3	9	1	1	1	**3**	5	5	5	5	**5**	**Alto**

34	Defectos en el componente de "Aplicación firma móvil Android" podrían permitir que el usuario acceda a firmar un documento sin utilizar credenciales.	3	9	1	1	1	**3**	5	5	5	5	**5**	**Alto**
35	Defectos en el componente de "Aplicación firma móvil IOS" podrían permitir que el usuario acceda a firmar un documento sin utilizar credenciales.	3	9	1	1	1	**3**	5	5	5	5	**5**	**Alto**
36	Defectos en el componente "Servicios expuestos para firma móvil" permiten que la aplicación revele datos sin autorización.	1	9	3	1	1	**3**	7	5	7	7	**6.5**	**Alto**
37	Defectos en el software del SignalR Hub podrían permitir a un atacante acceder	1	5	5	1	1	**2.6**	5	5	5	5	**5**	**Medio**

	a los datos que se envían al componente "Firmador BCCR" de uno o varios usuarios.												
38	Defectos en el software del Web Service notificador de la entidad podrían permitir a un atacante acceder a los datos que se envían a la entidad desde el componente "Servicio FVA".	1	3	5	1	1	**2.2**	9	9	3	7	**7**	**Alto**
39	Defectos en el software del "Servicio de firma expuesto a la entidad" podrían permitir a un atacante acceder a los datos que se envían al componente "Servicio FVA".	1	5	5	1	1	**2.6**	9	9	3	7	**7**	**Alto**
40	Errores de configuración en el componente "Equipo	1	3	3	3	3	**2.6**	9	3	5	1	**4.5**	**Bajo**

	donde se solicita la firma" permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.												
41	Errores de configuración en el componente "Equipo donde se solicita la firma" permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.	1	3	3	3	3	**2.6**	9	3	5	1	**4.5**	**Bajo**
42	La falta de actualizaciones en el sistema operativo permite a un atacante malintencionado instalar software malicioso en la máquina donde se ejecuta algún componente de la aplicación.	1	3	3	1	5	**2.6**	9	3	5	1	**4.5**	**Bajo**

43	Errores de configuración en el componente “Equipo Android” permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.	1	7	3	1	1	**2.6**	9	3	5	1	**4.5**	**Bajo**
44	Errores de configuración en el componente “Equipo Android” permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.	1	5	3	1	1	**2.2**	9	3	5	1	**4.5**	**Bajo**
45	La falta de actualizaciones en el “Sistema operativo Android” permite a un atacante malintencionado instalar software malicioso en el dispositivo donde se	1	5	3	3	3	**3**	9	3	5	1	**4.5**	**Medio**

	ejecuta la aplicación de firma móvil.												
46	Errores de configuración en el componente “Equipo IOS” permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.	1	5	3	1	1	**2.2**	9	3	5	1	**4.5**	**Bajo**
47	Errores de configuración en el componente “Equipo IOS” permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.	1	5	3	1	1	**2.2**	9	3	5	1	**4.5**	**Bajo**
48	La falta de actualizaciones en el “Sistema operativo IOS” permite a un atacante malintencionado instalar software malicioso en el	1	5	3	1	1	**2.2**	9	3	5	1	**4.5**	**Bajo**

	dispositivo donde se ejecuta la aplicación de firma móvil.												
49	Defectos en el software del "SignalR Hub" podrían permitir a un atacante modificar a los datos que se envían al componente "Firmador BCCR" de uno o varios usuarios.	3	7	3	1	1	**3**	3	3	3	3	**3**	**Medio**
50	Errores de configuración en el componente "SignalR Hub" podrían permitir al usuario modificar datos de la aplicación mediante técnicas como falsificación de solicitudes entre sitios.	1	5	3	1	1	**2.2**	3	5	3	3	**3.5**	**Bajo**
51	Defectos en el software "SignalR Hub" podrían permitir al usuario	1	3	3	1	1	**1.8**	3	3	3	3	**3**	**Bajo**

	acceder a información confidencial explotando un mal manejo de las excepciones.												
52	La falta de actualizaciones en el navegador de internet permite a un atacante malintencionado instalar software malicioso en la máquina donde se ejecuta algún componente de la aplicación.	1	5	3	3	3	**3**	3	3	3	1	**2.5**	**Bajo**
53	Defectos de software en el componente "Servicios expuestos para firma móvil" permiten al atacante alterar los datos que se envían al "Servicio FVA".	1	5	3	1	1	**2.2**	9	9	9	9	**9**	**Alto**
54	Errores de configuración de la(s) máquina(s) donde la aplicación	3	3	3	1	3	**2.6**	3	3	3	7	**4**	**Bajo**

	está instalada permite la divulgación de stack traces u otro tipo de información, que permite que algún atacante malintencionado obtenga datos suficientes para realizar un ataque exitoso.												
55	Defectos de software en el componente "Servicio FVA" permiten al atacante alterar los datos que se envían a los demás componentes del sistema.	1	9	3	1	1	**3**	9	9	9	7	**8.5**	**Alto**
56	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos mientras se transmiten desde el "Servicio FVA"	1	9	3	1	1	**3**	9	9	9	8	**8.75**	**Alto**

	hacia el resto del sistema												
57	Defectos de software en el componente "Web service notificador de la entidad" podrían permitirle al atacante acceder a los datos que se envían a la entidad y eventualmente modificarlos.	1	3	3	1	3	**2.2**	3	5	3	7	**4.5**	**Bajo**
58	Defectos de software en el componente "Servicio de firma expuesto a la entidad" podrían permitirle al atacante acceder a los datos que se envían desde la entidad y eventualmente modificarlos.	1	9	3	1	3	**3.4**	5	5	5	7	**5.5**	**Alto**
59	Defectos en el componente "BD FVA" permiten a un atacante malintencionado modificar el	1	9	3	1	1	**3**	9	9	9	9	**9**	**Alto**

	contenido del documento electrónico mientras éste se encuentra almacenado dicho componente.												
60	Comunicaciones desprotegidas permiten al atacante modificar los datos de la "Solicitud de nueva firma desde la entidad" mientras se transmiten al componente "BD FVA"	1	3	3	1	1	**1.8**	9	9	9	9	**9**	**Alto**
61	Comunicaciones desprotegidas permiten al atacante modificar los datos mientras se transmiten desde el componente "Tarjeta de firma digital con NFC" al componente "Aplicación firma móvil Android"	5	9	5	3	3	**5**	9	3	3	3	**4.5**	**Alto**
62	Comunicaciones desprotegidas permiten al atacante	5	9	5	3	3	**5**	9	3	3	3	**4.5**	**Alto**

	modificar los datos mientras se transmiten desde el componente “Tarjeta de firma digital con NFC” al componente “Aplicación firma móvil IOS”												
62	Defectos en el componente “Tarjeta de firma digital con NFC” permiten que la aplicación genere datos cifrados mediante el uso de algoritmos de cifrado inseguros.	3	9	5	3	3	**4.6**	9	3	3	3	**4.5**	**Medio**
63	Defectos en el software del SignalR Hub podrían permitir a un atacante acceder a datos de otros usuarios sin estar autorizados para ello.	1	3	3	1	1	**1.8**	9	5	5	5	**6**	**Medio**
64	Defectos de software en el componente “Servicios expuestos para firma móvil” permiten al atacante	1	3	3	3	3	**2.6**	9	5	5	5	**6**	**Medio**

	acceder a datos de otros usuarios sin estar autorizados para ello.												
65	Defectos de software en el componente "Servicio FVA" permiten al atacante acceder a datos de otros usuarios sin estar autorizados para ello.	1	3	3	1	1	**1.8**	9	9	9	9	**9**	**Alto**
66	Errores de configuración en el componente "Web service notificador de la entidad" permiten al atacante acceder sin autorización a la información enviada desde el "Servicio FVA"	1	3	3	1	1	**1.8**	9	9	9	9	**9**	**Alto**
67	Errores de configuración en el componente "Servicio de firma expuesto a la entidad" permiten al atacante acceder sin	1	3	3	1	1	**1.8**	9	7	5	9	**7.5**	**Alto**

	autorización a la información enviada desde el "Servicio FVA"												
68	Comunicaciones desprotegidas permiten a un atacante malintencionado revelar datos que se transmiten hacia el componente "Servicio FVA"	1	3	3	1	1	**1.8**	9	5	5	9	**7**	**Alto**
69	Comunicaciones desprotegidas permiten a un atacante malintencionado revelar datos que se transmiten hacia el componente "Aplicación firma móvil Android"	3	3	5	3	3	**3.4**	9	3	3	5	**5**	**Alto**
70	Comunicaciones desprotegidas permiten a un atacante malintencionado revelar datos que se transmiten hacia el	3	3	5	3	3	**3.4**	9	3	3	5	**5**	**Alto**

	componente “Aplicación firma móvil IOS”												
71	Errores de configuración en el componente “Equipo Android” podrían permitir al atacante el acceso a datos como “Datos de notificación al usuario” sin tener autorización para ello.	1	3	3	1	1	**1.8**	5	3	3	3	**3.5**	**Bajo**
72	Errores de configuración en el componente “Equipo Android” podrían permitir al atacante el acceso a datos como “Datos de notificación al usuario” sin tener autorización para ello.	1	3	3	1	1	**1.8**	5	3	3	3	**3.5**	**Bajo**

10.3 APÉNDICE C: Terminología relevante en la definición de políticas de seguridad y objetivos de control

En esta sección se presenta la terminología necesaria para entender algunos elementos de la definición de políticas de seguridad y objetivos de control. Cuando en el Apéndice D: Políticas de Seguridad Definidas y en el Apéndice E: Objetivos de Control Establecidos se utilice uno de los siguientes conceptos, se debe interpretar con base en la definición o explicación utilizada en este apéndice.

APLICACIÓN: es cualquier programa informático diseñado para asistir en la ejecución de una tarea específica, como un procesador de texto, un software contable, un sistema de administración de inventarios, etc. (Microsoft, 2002)

BITÁCORA: en el contexto de la computación, es un registro de la secuencia de eventos o procesos ejecutados por una computadora. (Longley & Shain, 1989)

CACHÉ: es un tipo especial de memoria en la cual los valores de datos frecuentemente usados son almacenados para acceder a ellos con mayor rapidez (Microsoft, 2002). Las computadoras incorporan varios tipos diferentes de caché para funcionar con mayor eficiencia, entre los cuales se encuentran la caché del navegador de Internet, la caché del disco duro, la caché de la memoria y la caché del procesador.

CMS: es la abreviatura de "Sintaxis de Mensaje Criptográfico" , se refiere a un formato de documento electrónico que soporta firma digital y cifrado. CMS describe una sintaxis que se utiliza para firmar digitalmente, resumir, autenticar o cifrar contenido arbitrario de un mensaje. (Housley, 2004)

DRIVER: es un programa informático que permite a una computadora controlar dispositivos, como una impresora o una unidad de disco. (Microsoft, 2002)

FRAMEWORK: es una estructura de diseño básico reutilizable, que consta de clases abstractas y concretas, que ayuda en la construcción de aplicaciones. (Microsoft, 2002)

Malware: es un software creado y distribuido con propósitos maliciosos. (Microsoft, 2002)

Memoria local: es un tipo de memoria basada en semiconductores, que puede ser leída y escrita por la unidad de procesamiento central (CPU) u otros dispositivos de hardware.

Las posiciones de almacenamiento pueden ser accedidas en cualquier orden. (Microsoft, 2002)

PKCS#7: es la abreviatura de "Estándar de Criptografía de Llave Pública 7" (Public Key Criptography Standard 7 en inglés), un estándar criptográfico para el intercambio de certificados digitales en criptografía de llave pública. PKCS#7 especifica la sintaxis de los certificados digitales y otra información cifrada, específicamente, el método por el cual los datos se cifran y se firman digitalmente, así como los algoritmos implicados. (Kaliski, 1998)

PLUG-IN: es un software que le provee funcionalidad adicional a otro programa (Microsoft, 2002).

SENTENCIA PARAMETRIZADA: es un tipo de consulta SQL que puede personalizarse a través de marcadores de posición para definir los parámetros de la consulta. Las sentencias parametrizadas ofrecen dos beneficios principales: 1) contribuyen a mejorar el rendimiento de las aplicaciones, pues la consulta sólo necesita ser analizada una vez, pero se puede ejecutar varias veces con distintos parámetros; y 2) ayudan a prevenir ataques de inyección de SQL. (Mora, 2017)

SISTEMA: es cualquier conjunto de componentes que trabajan juntos para ejecutar una tarea. Por ejemplo, un sistema operativo, que está constituido por un grupo de programas y archivos de datos; o un motor de bases de datos, usado para procesar distintos tipos de información. (Microsoft, 2002)

320

SQL: es la abreviatura de "Lenguaje de Consultas Estructurado" (Structured Query Language en inglés), un lenguaje de base de datos utilizado en la consulta, actualización y gestión de bases de datos. (Microsoft, 2002)

TLS: es la abreviatura de "Seguridad de la Capa de Transporte" (Transport Layer Security en inglés), un protocolo que proporciona privacidad e integridad de los datos transmitidos entre dos aplicaciones que se comunican a través de una red. (Dierks & Rescorla, 2008)

VIRUS: es un programa malicioso que infecta archivos en una computadora, insertando en esos archivos copias de sí mismo. Las copias son normalmente ejecutadas cuando el archivo se carga en la memoria, permitiendo que el virus infecte otros archivos. (Microsoft, 2002)

WISYWIS: es la abreviatura de "Lo que Usted Ve Es Lo que Usted Firma" (what you see is what you sign en inglés), una propiedad deseable en los sistemas de firma digital. La propiedad WYSIWYS establece que la representación de bits de los documentos electrónicos debe ser visualizada consistentemente y según lo previsto para el firmante, por el sistema de firma digital. Cualquier violación de la propiedad WYSIWYS tiene el

potencial de imponer o quitar indebidamente la responsabilidad de personas u organizaciones que hacen uso de las firmas digitales. (Mora, 2017)

XMLDSig: es la abreviatura de "Firma Digital XML" (XML Digital Signature en inglés), una recomendación del World Wide Web Consortium (W3C) que especifica la sintaxis y las reglas de procesamiento para firmas digitales XML. XMLDSig provee los servicios de integridad y autenticación del emisor para datos de cualquier tipo, ya sea que estén dentro del XML que incluye la firma o en archivos separados. (W3C, 2008)

10.4 APÉNDICE D: Políticas de Seguridad Definidas

En esta sección se presentan las políticas de seguridad de la información que han sido definidas para mitigar los riesgos que han sido seleccionados por tener un nivel de severidad medio, alto o muy alto.

La lista de riesgos completa y su valoración se pueden consultar en el Apéndice A: Riesgos Identificados, y en el Apéndice B: Detalle de la Valoración de los Riesgos Identificados.

Tabla 22 Políticas de seguridad

ID	Política	Base lógica
1	Se debe proteger el software cliente instalado en las máquinas de los usuarios de manera que no sea fácilmente escanearle o analizado para encontrar vulnerabilidades.	Mitiga riesgos 5,25,32
2	Se debe verificar que el software cliente no contenga funcionalidad adicional o innecesaria.	Mitiga riesgos 5,25,32
3	Se debe validar que los datos de notificación al usuario no se entreguen a usuarios no autorizados.	Mitiga riesgos 19, 20, 36,55,56
4	Se debe validar que los datos del usuario registrado no se entreguen a usuarios no autorizados.	Mitiga riesgos 4, 5, 36,55,56
5	Se debe validar que los datos de la solicitud de firma no contienen código oculto o malicioso	Mitiga riesgos 3,8, 24, 28, 32,55,56
6	Se debe validar que la respuesta de la firma no contiene código oculto o malicioso	Mitiga riesgos 14,15,16,17,18
7	Se debe validar que los datos de notificación al usuario no contienen código oculto o malicioso	Mitiga riesgos 19, 20, 38,39, 53
8	Se debe validar que los datos del usuario registrado no contienen código oculto o malicioso	Mitiga riesgos 4, 5
9	Se debe proteger los datos de la solicitud de firma mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos 6, 7,8, 9, 10
10	Se debe proteger los datos del usuario registrado mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos 4, 5
11	Se debe proteger la respuesta de la firma mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos 14,15,16,17,18

ID	Política	Base lógica
12	Se debe proteger los datos de la solicitud de firma, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos 1, 6, 7,8, 9, 10
13	Se debe proteger los datos de la solicitud de firma, mientras se encuentra almacenado dentro algún componente de la aplicación, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgo 59
14	Se debe proteger los datos de notificación al usuario mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos 19, 20,
15	Se debe proteger la respuesta de la firma, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos 14,15,16,17,18, 39, 53
16	Se debe proteger los datos de notificación al usuario, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos 19, 20
17	Se debe proteger la respuesta de la firma, mientras se encuentra almacenado dentro algún componente de la aplicación, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgo 59
18	Se debe proteger los datos de notificación al usuario, mientras se encuentra almacenado dentro algún componente de la aplicación, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgo 59
19	Se debe validar que los datos para solicitar la firma en el cliente se envíen solamente a los usuarios previamente autenticados.	Mitiga riesgo 37, 49
20	Se debe validar que los datos de la solicitud de firma no se entreguen a usuarios no autorizados.	Mitiga riesgos 1, 6, 7,8, 9, 10,55,56
21	Se debe validar que la respuesta de la firma no se entregue a usuarios no autorizados.	Mitiga riesgos 14,15,16,17,18
22	Se debe validar que el formato del documento electrónico que se va a firmar está soportado por el SNCD y la aplicación, y que además es correcto.	Mitiga riesgo 2
23	Se debe validar que el documento electrónico que se va a firmar no contiene código oculto o malicioso.	Mitiga riesgos 3, 24, 28, 32

ID	Política	Base lógica
24	Se debe proteger el documento electrónico que se va a firmar, así como sus representaciones derivadas (documento electrónico formateado, resumen del documento electrónico, resumen cifrado del documento electrónico y documento electrónico firmado), mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos 1, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18,61,62,63
25	Se debe proteger el certificado digital que se utilizará en el proceso de firma, mientras se transmite por una red, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos 22, 23, 26,27, 30,31
26	Se debe proteger el resultado de la validación del certificado digital que se utilizará en el proceso de firma, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgos 22, 23, 26,27, 30,31
27	Se debe proteger el documento electrónico que se va a firmar, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgo 59
28	Se debe proteger el documento electrónico que se va a firmar, mientras se encuentra almacenado dentro algún componente de la aplicación, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos 1,2,3
29	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	Mitiga riesgos 42, 45, 48, 52
30	El acceso a la llave privada almacenada en el dispositivo criptográfico seguro, con el fin de ejecutar operaciones criptográficas, debe ser concedido únicamente a usuarios o procesos debidamente autenticados.	Mitiga riesgos 22, 26, 31
31	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de firma es válido.	Mitiga riesgos 22, 26, 30
32	Se debe validar que el certificado digital que se utilizará en el proceso de firma pertenece a la jerarquía nacional de certificadores registrados.	Mitiga riesgos 22, 26, 30
33	Se debe validar que el certificado digital que se utilizará en el proceso de firma es válido dentro del contexto de la sesión del usuario actualmente autenticado en la aplicación.	Mitiga riesgos 22, 26, 30
34	Se debe validar que el certificado digital que se utilizará en el proceso de firma se encuentra almacenado en un dispositivo criptográfico seguro.	Mitiga riesgos 23, 27, 31

ID	Política	Base lógica
35	Se debe validar el uso correcto del certificado que se utilizará en el proceso de firma.	Mitiga riesgos 22,23,26,27,30,31
36	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no sean reveladas al usuario, ni asequibles local o remotamente por un tercero no autorizado.	Mitiga riesgos 11,12,13, 61,62,63
37	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no puedan ser obtenidas utilizando mecanismos de fuerza bruta.	Mitiga riesgo 33,34,35
38	Se debe validar que el documento electrónico firmado resultante no se entregue a usuarios no autorizados.	Mitiga riesgo 65, 66, 67
39	Se debe validar que el acceso a recursos del sistema en el que se ejecuta la aplicación esté dado únicamente a usuarios o procesos autorizados.	Mitiga riesgo 36, 40,41,43, 46
40	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	Mitiga riesgo 54 , 51,52
41	El resumen del documento electrónico que se va a firmar debe calcularse utilizando algoritmos *hash* seguros.	Mitiga riesgos 21, 25,29
42	Se debe validar que el certificado digital que se utilizará en el proceso de firma se encuentra vigente al momento de crear la firma digital.	Mitiga riesgo 22, 26, 30
43	Antes de iniciar con el proceso de firma digital, se debe mostrar al usuario una representación del documento electrónico que se va a firmar, cuyo contenido nunca cambie, independientemente del dispositivo en que se visualice.	Ley de certificados, firmas digitales y documentos electrónicos N° 8454 (artículo 10)
44	Las direcciones requeridas para validar las rutas de certificación de los certificados digitales deben extraerse directamente del certificado, y de ninguna manera deben estar contenidas en el código fuente, archivos de texto, base de datos o cualquier otro tipo de almacenamiento.	Mitiga riesgos 22, 26, 30
45	El *software* de los dispositivos móviles debe tener instaladas las actualizaciones más recientes de las aplicaciones cliente.	Mitiga riesgos 28,32

10.5 APÉNDICE E: Objetivos de control

A continuación, se presentan los objetivos de control que se han establecido en base al cumplimiento de las políticas descritas para el sistema en análisis.

Tabla 23 Objetivos de control

ID	Objetivo de control	Fundamento
1	Se deben validar los datos que ingresan al sistema digitados por el usuario, verificando que cada entrada cumple al menos con los siguientes requisitos: *Cuando la entrada es texto* • Los caracteres introducidos deben ser válidos, según el conjunto de caracteres permitido correspondiente. • La longitud de los caracteres introducidos debe estar dentro de los límites mínimos y máximos correspondientes. • Si la entrada requiere un formato específico (como una fecha, una dirección de correo electrónico, un número telefónico, etcétera), los caracteres introducidos deben cumplir con ese formato. • Si la entrada se utiliza como argumento en una operación de creación, lectura, actualización o borrado de registros en una base de datos, se debe hacer a través de sentencias parametrizadas (*prepared statements*), y no mediante la concatenación de hileras de caracteres. • Si la entrada debe mostrarse al usuario posteriormente, durante su interacción con el sistema, deben aplicarse las reglas de escape correspondientes según el o los lenguajes utilizados. *Cuando la entrada es un archivo* • El archivo debe tener un formato permitido. • El formato del archivo debe ser correcto. • El tamaño del archivo no debe exceder un tamaño máximo permitido. • El archivo no debe almacenar contenido malicioso, como virus, *malware*, etcétera. • Si el archivo se almacenará en el sistema de archivos de un servidor, su nombre o ubicación no debe ser igual al de algún archivo de configuración según el tipo de servidor. Por ejemplo, *.htaccess* en Apache, o *Web.conf* en IIS, entre otros.	Permite evaluar políticas 5, 6, 7, 8, 22, 23

ID	Objetivo de control	Fundamento
2	Se debe validar por medio de revisiones de código que las aplicaciones móviles no contengan funcionalidades adicionales que no son necesarias, o que expone información relacionada con entornos de prueba, demostración o preparación. Estas no deben incluirse en una compilación de producción.	Permite evaluar política 2
3	Se debe ofuscar el código de las aplicaciones cliente que se entregan para correr en dispositivos del usuario.	Permite evaluar política 2
4	En las aplicaciones móviles se debe incluir funcionalidad para detectar en tiempo de ejecución si hay alguna modificación en el código que haya alterado su integridad. Para esto se debe: • Incluir en el código de la aplicación una verificación de "Checksum" o de "Hashing" del código mediante un algoritmo igual o superior a SHA-256.	Permite evaluar política 1
5	Se debe validar en cada petición proveniente de las aplicaciones móviles, que dicho dispositivo mantenga la última versión disponible en producción.	Permite evaluar política 45
6	Se debe validar que los formatos de documento firmado en formato simple corresponden a alguno de los formatos que se han establecido como válidos.	Permite evaluar políticas 22, 23
7	Los datos se deben transmitir por red utilizando algún protocolo que proporcione cifrado de datos, con una efectividad igual o superior a la ofrecida por TLS 1.0.	Permite evaluar políticas 9,10,11, 14, 24, 25, 26
8	Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, *malware* y cualquier otro tipo de *software* malicioso que facilite la modificación no autorizada de datos, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final* Se debe validar la existencia de un procedimiento periódico , para comprobar que las máquinas no están infectadas. Se debe registrar una bitácora por máquina cada vez que el procedimiento se ejecuta, en la que se almacene al menos la siguiente información: • Nombre del responsable de ejecutar el procedimiento. • Fecha y hora en la que se ejecuta el procedimiento. • Identificador de la máquina. • Herramienta utilizada para ejecutar el procedimiento.	Permite evaluar política 29

ID	Objetivo de control	Fundamento
	• Lista de archivos analizados. • Resultado del análisis. *Cuando algún componente de la aplicación se ejecuta en una máquina o dispositivo que está bajo control total o parcial del usuario final* Se debe incluir en la documentación al usuario final, recomendaciones e importancia de mantener la máquina libre de infecciones	
9	Se debe validar que el *software* complementario, requerido para ejecutar la aplicación, se encuentra actualizado en la máquina donde se ejecuta, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final* Se debe validar la existencia un procedimiento periódico, para comprobar que al menos el sistema operativo, los navegadores de Internet, los *frameworks*, los *plug-ins* y los *drivers* necesarios, están actualizados. *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final* Se debe incluir en la documentación al usuario final, recomendaciones e importancia de mantener la máquina libre de infecciones	Permite evaluar políticas 29, 45
10	Se debe implementar un mecanismo de autenticación en el dispositivo criptográfico seguro que conste al menos de un factor. Por ejemplo: un PIN, un usuario y una contraseña, un control biométrico, entre otros.	Permite evaluar políticas 30, 35, 36, 37,
11	Se debe validar que el perfil del certificado digital cumple con los requisitos establecidos en la sección 7.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013).	Permite evaluar política 31,42
12	Se debe validar la pertenencia del certificado digital a la jerarquía nacional de certificadores registrados .	Permite evaluar políticas 31, 32, 33, 34,42

ID	Objetivo de control	Fundamento
13	Se debe validar que existe una correcta asociación entre el usuario en la sesión actual y el certificado digital. Si dicha asociación no puede verificarse, el certificado no se considera válido.	Permite evaluar políticas 31, 32, 33, 34,42
14	Se debe garantizar que los certificados digitales utilizados se cargan desde los dispositivos criptográficos seguros conectados.	Permite evaluar políticas 30, 34
15	Se debe validar que el uso del certificado digital cumple con los requisitos establecidos en la sección 1.4.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013).	Permite evaluar políticas 30,31,32,33,34,42
16	La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro debe cumplir al menos con los siguientes requisitos: • Cuando las credenciales deban ser introducidas por el usuario, el campo de texto destinado para ese fin debe enmascarar todos los caracteres, sustituyéndolos por algún otro símbolo, por ejemplo, un asterisco (*). • Las credenciales no deben, bajo ninguna circunstancia, ser almacenadas en bitácoras, ni mostradas al usuario durante su interacción con la aplicación.	Permite evaluar políticas 36, 37
17	La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro, ante ataques de prueba y error, debe cumplir con al menos uno de los siguientes requisitos: • Implementar algún método de tipo desafío-respuesta, que permita determinar si quien trata de acceder al dispositivo criptográfico es humano o no, y deniegue el acceso cuando no lo es. • Bloquear el acceso al dispositivo criptográfico seguro durante un intervalo de tiempo, después de una cantidad predefinida de fallos en la autenticación	Permite evaluar política 37
18	La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro, ante el almacenamiento en caché, debe cumplir al menos con los siguientes requisitos:	Permite evaluar políticas 36, 37

ID	Objetivo de control	Fundamento
	Cuando el almacenamiento en caché está prohibido • La aplicación debe implementarse de manera tal que las credenciales no sean almacenadas en cualquier tipo de memoria caché. • Cuando aplique, se debe desactivar el almacenamiento en caché de las credenciales a nivel de navegador de Internet. • Cuando aplique, se debe desactivar el almacenamiento en caché de las credenciales a nivel de sistema operativo. *Cuando el almacenamiento en caché es requerido* • Antes de que las credenciales sean almacenadas en caché, se debe capturar la manifestación de la voluntad del usuario, lo que debe cumplir con los siguientes requisitos: o Se debe mostrar al usuario una llamada a la acción que describa clara y concisamente la operación que está por ejecutar. o Antes de que la operación mencionada anteriormente se ejecute, el usuario debe satisfacer al menos un método de tipo desafío-respuesta. • Durante el periodo en el cual se accede a las operaciones criptográficas del dispositivo criptográfico seguro, por medio de las credenciales almacenadas en caché, se deben generar bitácoras que almacenen al menos la siguiente información: o Datos que permitan identificar a la entidad actualmente autenticada. o La fecha y la hora del suceso. o El propósito de uso que justifique el almacenamiento en caché de las credenciales.	
19	Para que la entrega del documento electrónico firmado sea posible, se debe satisfacer al menos un control de autorización.	Permite evaluar políticas 22, 23, 24, 27,28, 38
20	Debe existir un contexto de encapsulamiento, en el que se definen al menos tres controles de autorización, los cuales deben satisfacerse antes de acceder a recursos del sistema.	Permite evaluar política 39, 3, 4, 12, 13, 15, 16, 17, 18, 19, 20, 21

ID	Objetivo de control	Fundamento
21	La prevención del despliegue de datos que revelan detalles acerca de la configuración e implementación del sistema debe cumplir al menos con los siguientes requisitos: • Ningún tipo de información sensible debe mostrarse a través de mensajes de error, incluyendo, pero no limitándose a: detalles del sistema, identificadores e información de cuentas. • Se debe usar manejadores de errores que no despliegan información de depuración, ni *stack traces*. • Se deben implementar mensajes de error genéricos, y usar pantallas de error personalizadas. • Cuando corresponda, la aplicación debe manejar los errores que ocurren dentro de esta, y no delegar esa función en la configuración del servidor. • La lógica de manejo de errores asociada a controles de seguridad debe denegar el acceso por defecto.	Permite evaluar políticas 40, 44
22	Se debe validar que los algoritmos de *hash* utilizados son seguros, y tienen una efectividad igual o superior a SHA-2, y rechazar los demás.	Permite evaluar política 41
23	La validación de la vigencia del certificado debe cumplir con los siguientes requisitos: • Se debe verificar que el certificado se encuentra activo, es decir, que no ha expirado ni ha sido revocado o suspendido. • Se debe evaluar la vigencia del certificado, y la vigencia de todos los certificados de las CA en la ruta de certificación a la que pertenece el certificado. • La información de revocación se debe obtener a partir de CRLs u OCSP, de acuerdo con el grado de tolerancia al riesgo.	Permite evaluar política 31, 34
24	La visualización del documento electrónico debe utilizar un método que cumpla con el principio WYSIWYS.	Permite evaluar política 43

ID	Objetivo de control	Fundamento

10.6 Apéndice F: Diagramas de interacción

A continuación, se presentan los diagramas de interacción que se obtuvieron a partir del análisis de los escenarios y los distintos componentes del sistema.

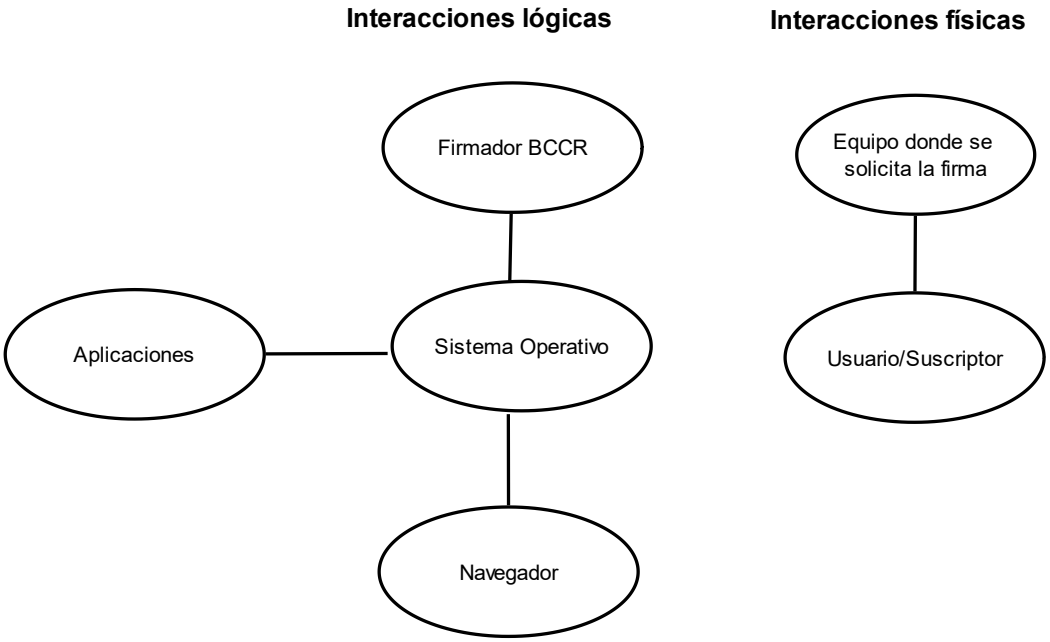

Figura 24 Diagrama componente Equipo donde se solicita la firma

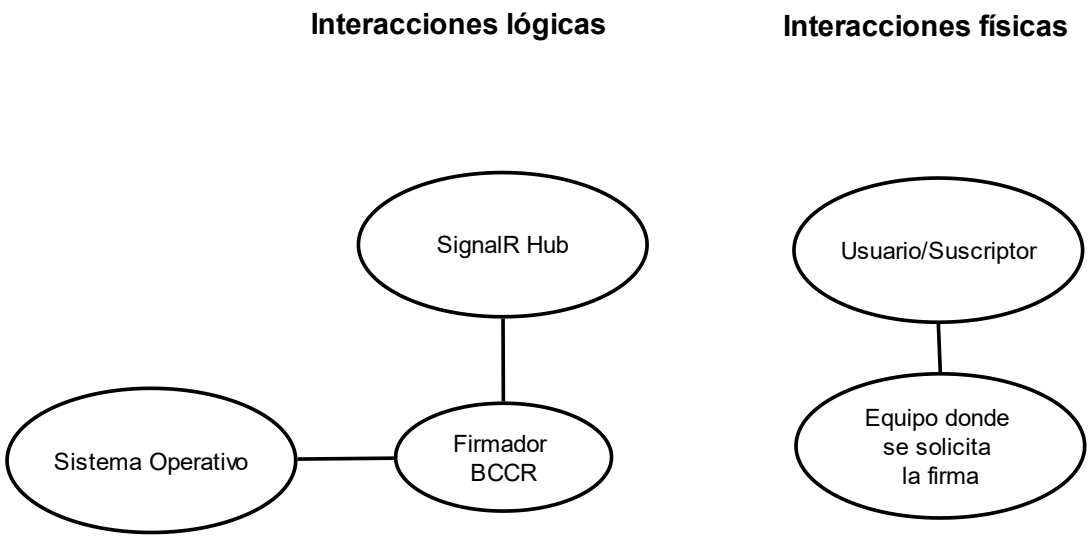

Figura 25 Diagrama componente Firmador BCCR

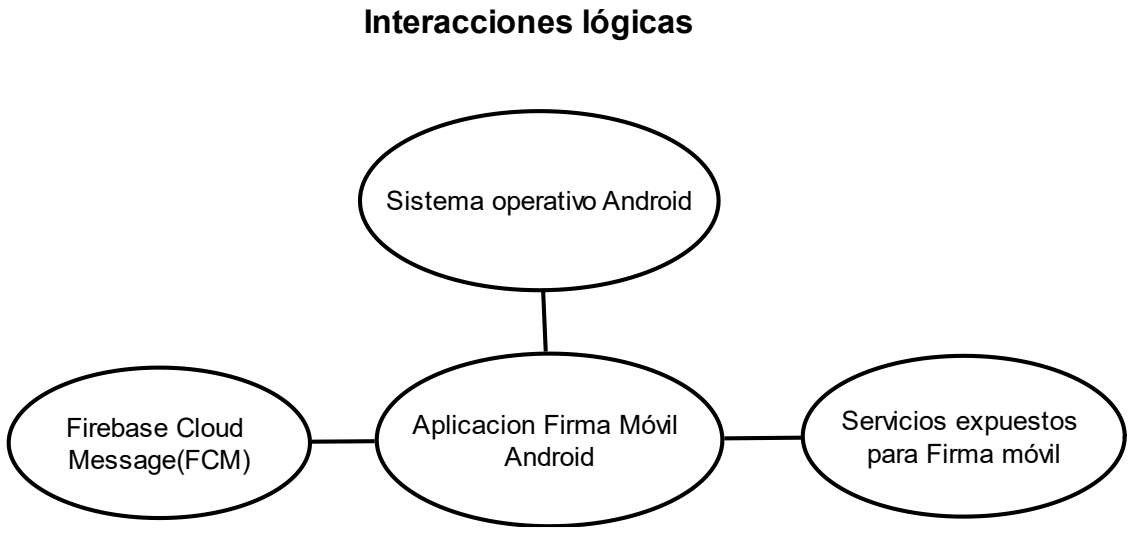

Figura 26 Diagrama componente Aplicación Firma Móvil

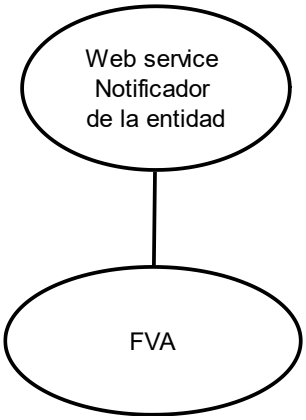

Figura 27 Diagrama componente Web Service notificador de la entidad

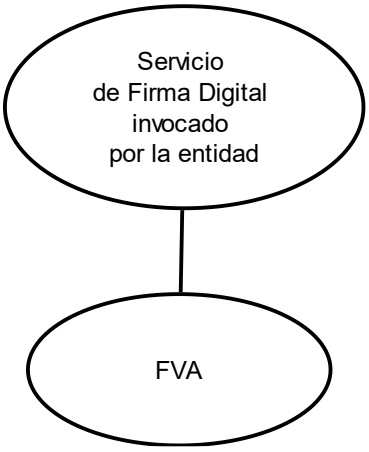

Figura 28 Diagrama componente Servicio de Firma Digital invocado por la entidad

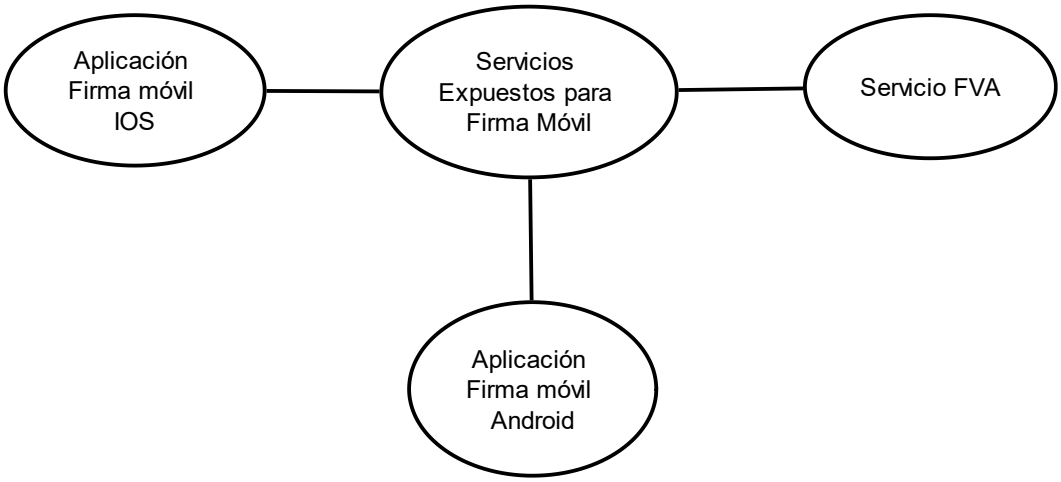

Figura 29 Diagrama componente Servicios expuestos para firma móvil

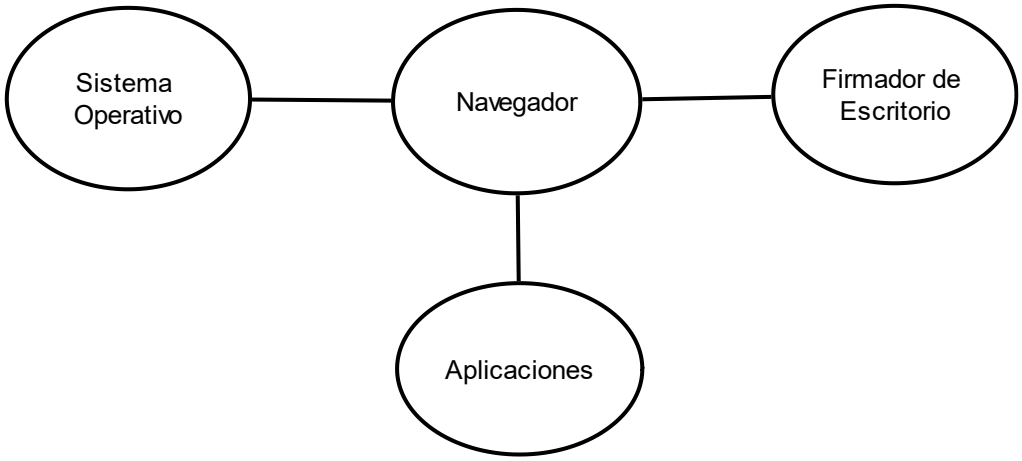

Figura 30 Diagrama componente Navegador

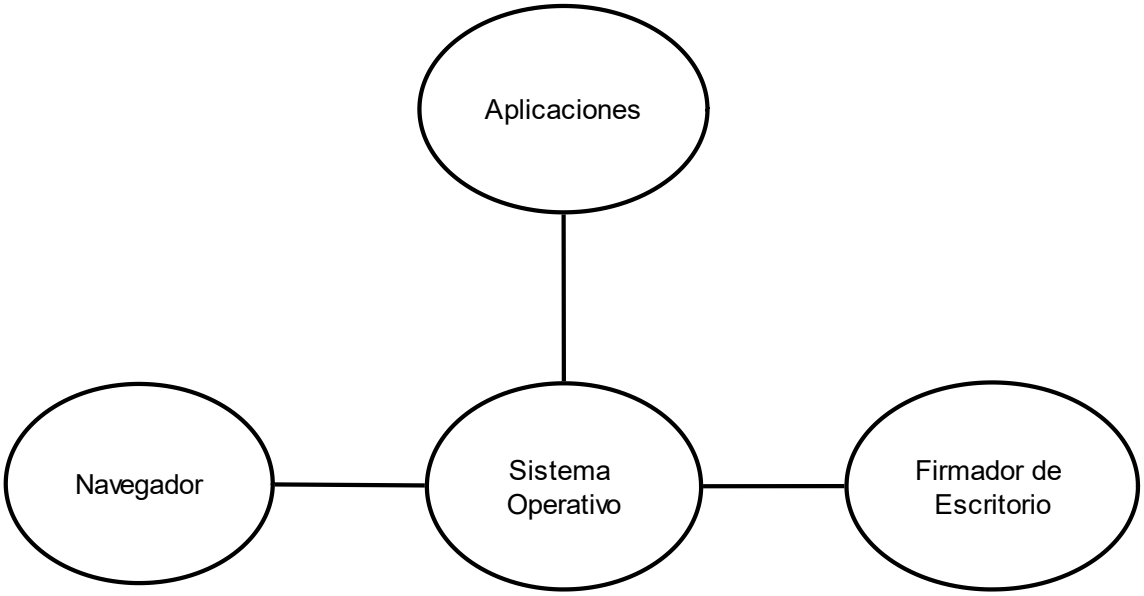

Figura 31 Diagrama componente Sistema Operativo

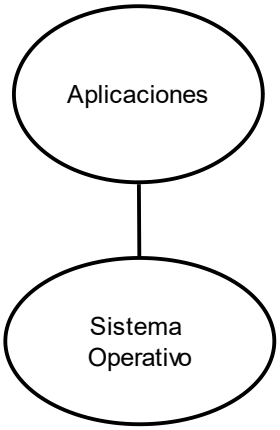

Figura 32 Diagrama componente Aplicaciones

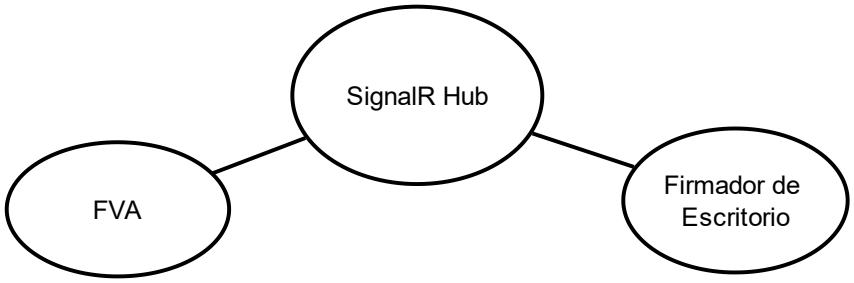

Figura 33 Diagrama componente SignalR Hub

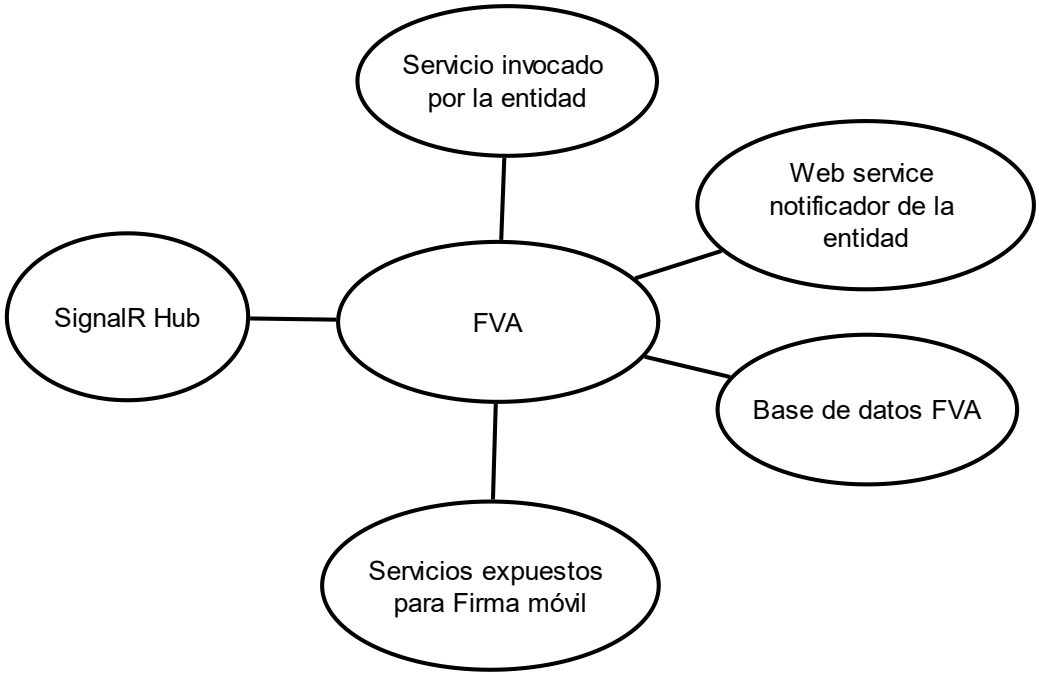

Figura 34 Diagrama componente FVA

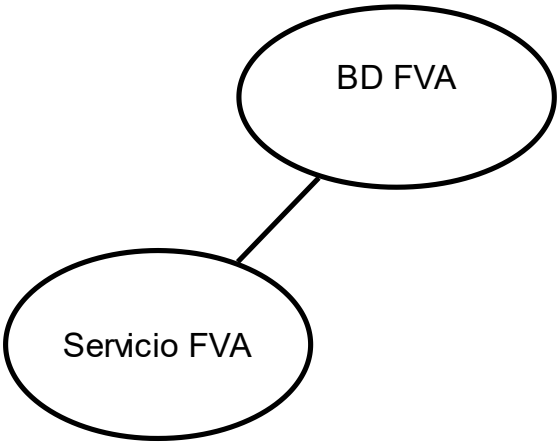

Figura 35 Diagrama componente BD FVA

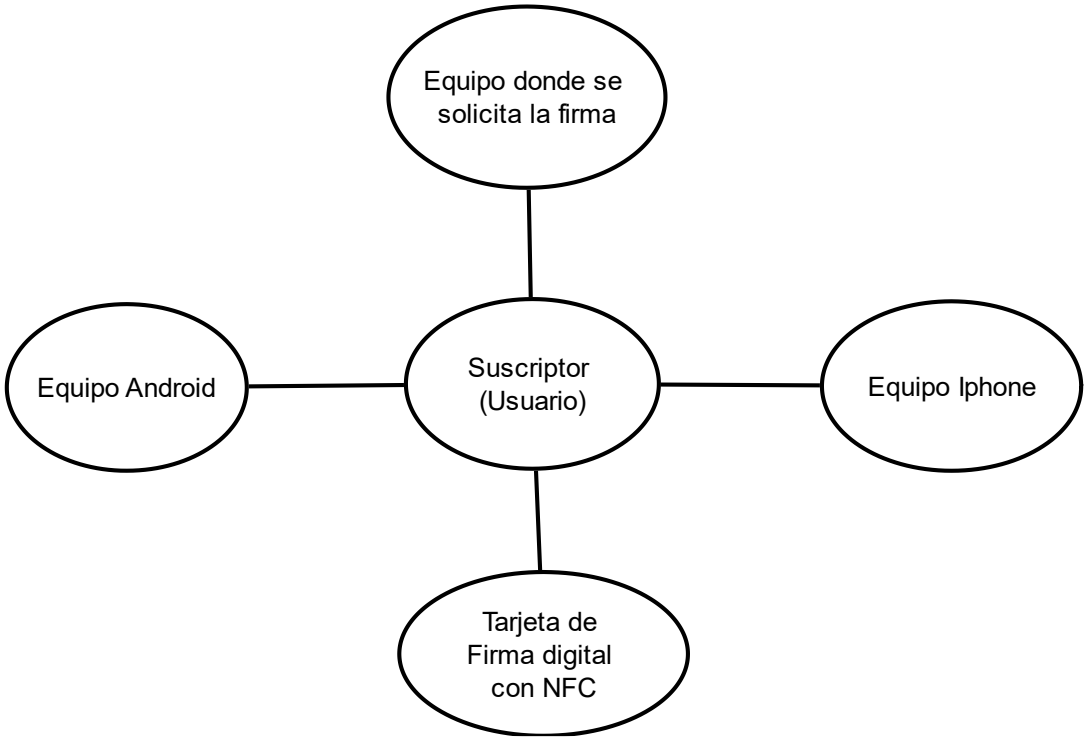

Figura 36 Diagrama componente Suscriptor

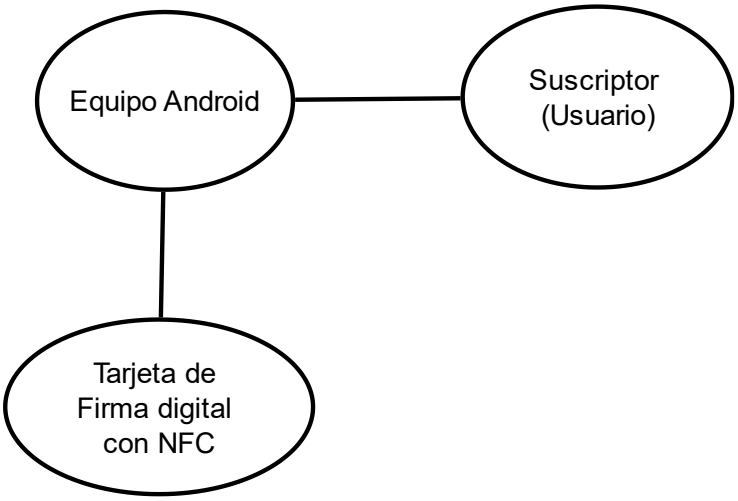

Figura 37 Diagrama componente Equipo Android

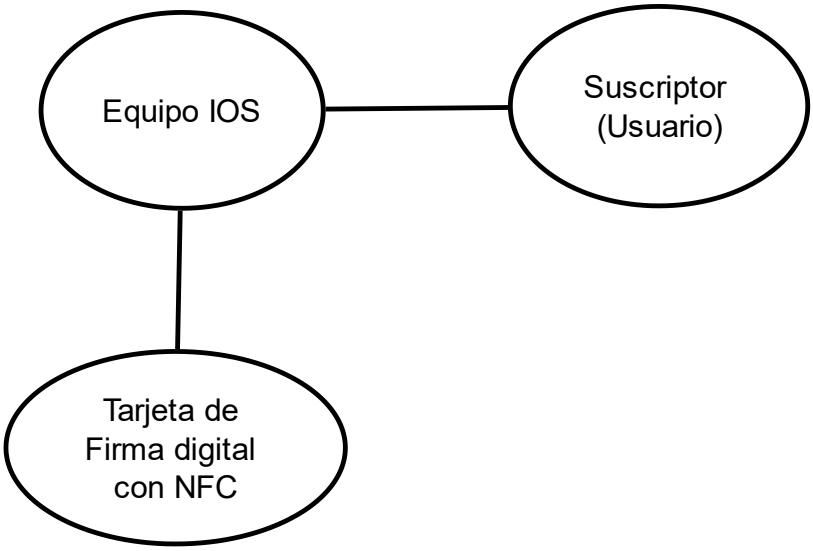

Figura 38 Diagrama componente Equipo IOS

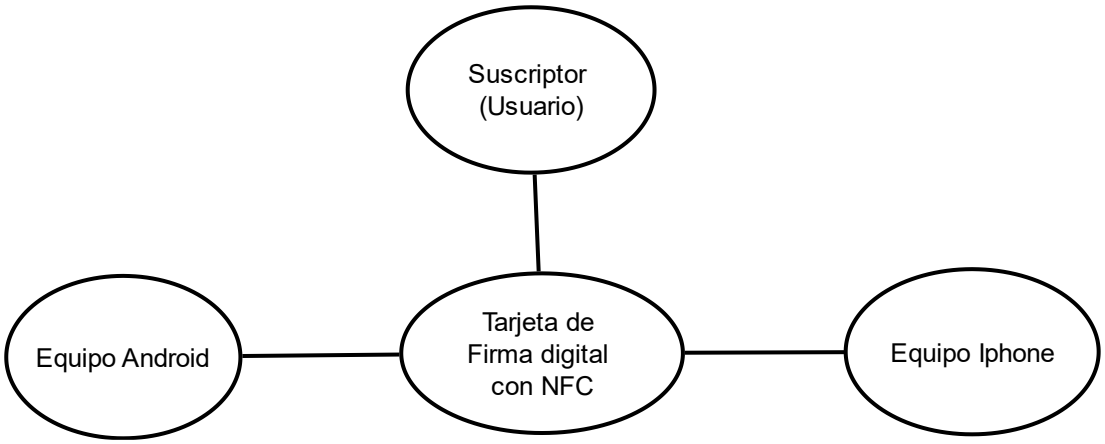

Figura 39 Diagrama componente Tarjeta NFC

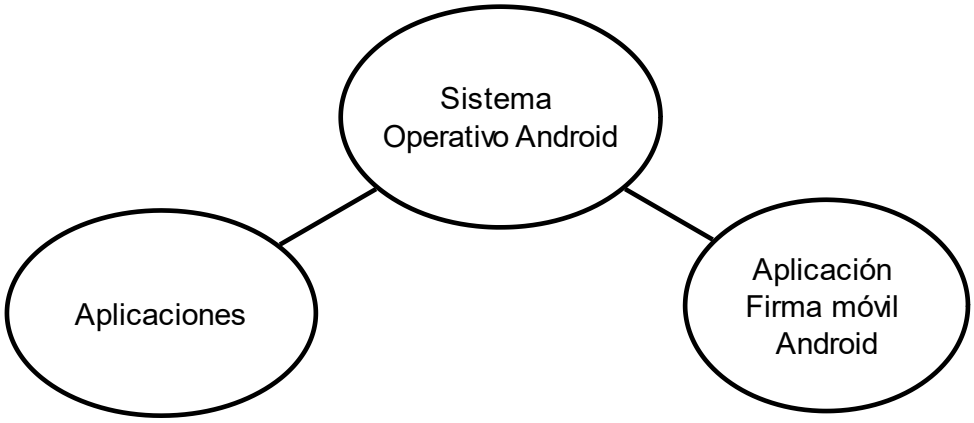

Figura 40 Diagrama componente Sistema Operativo Android

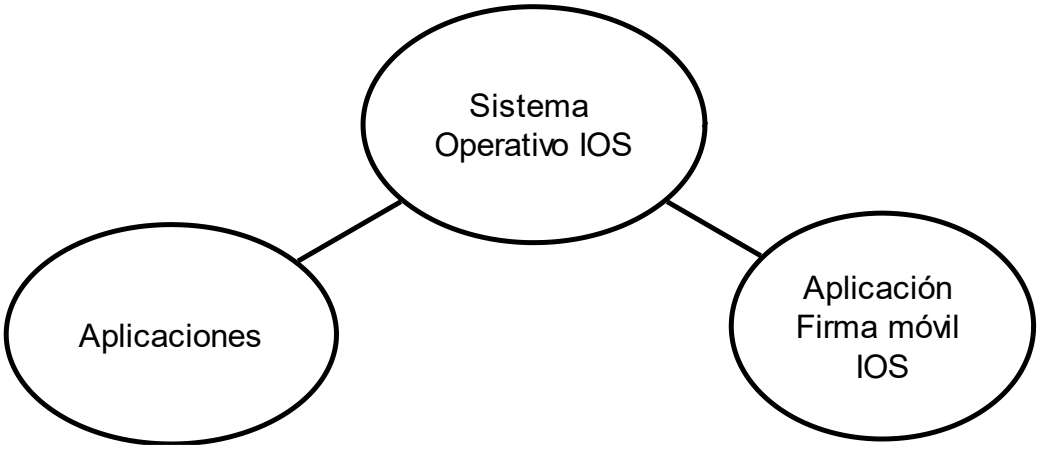

Figura 41 Diagrama componente Sistema Operativo IOS

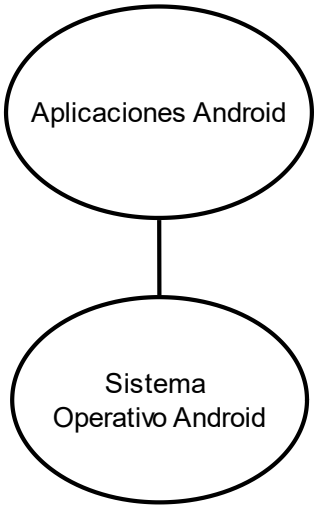

Figura 42 Diagrama componente Aplicaciones Android

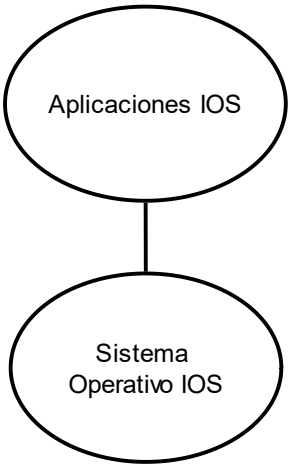

Figura 43 Diagrama componente Aplicaciones IOS

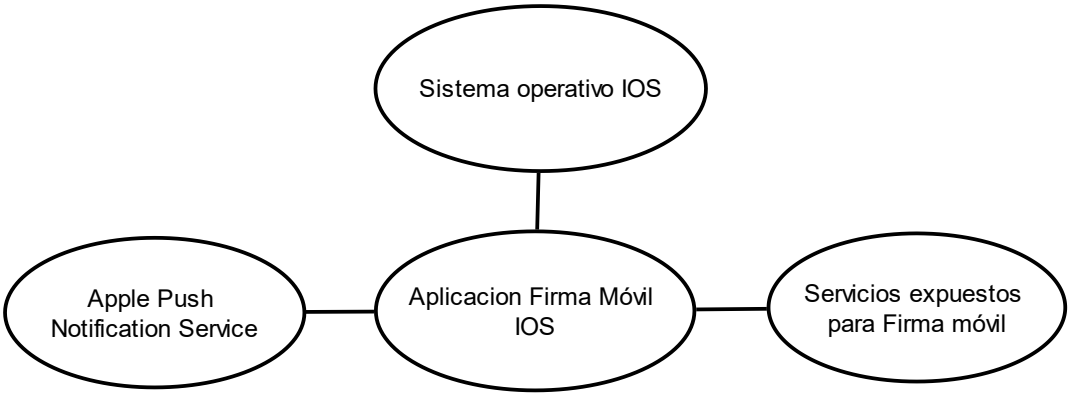

Figura 44 Diagrama componente Aplicación Firma Móvil IOS

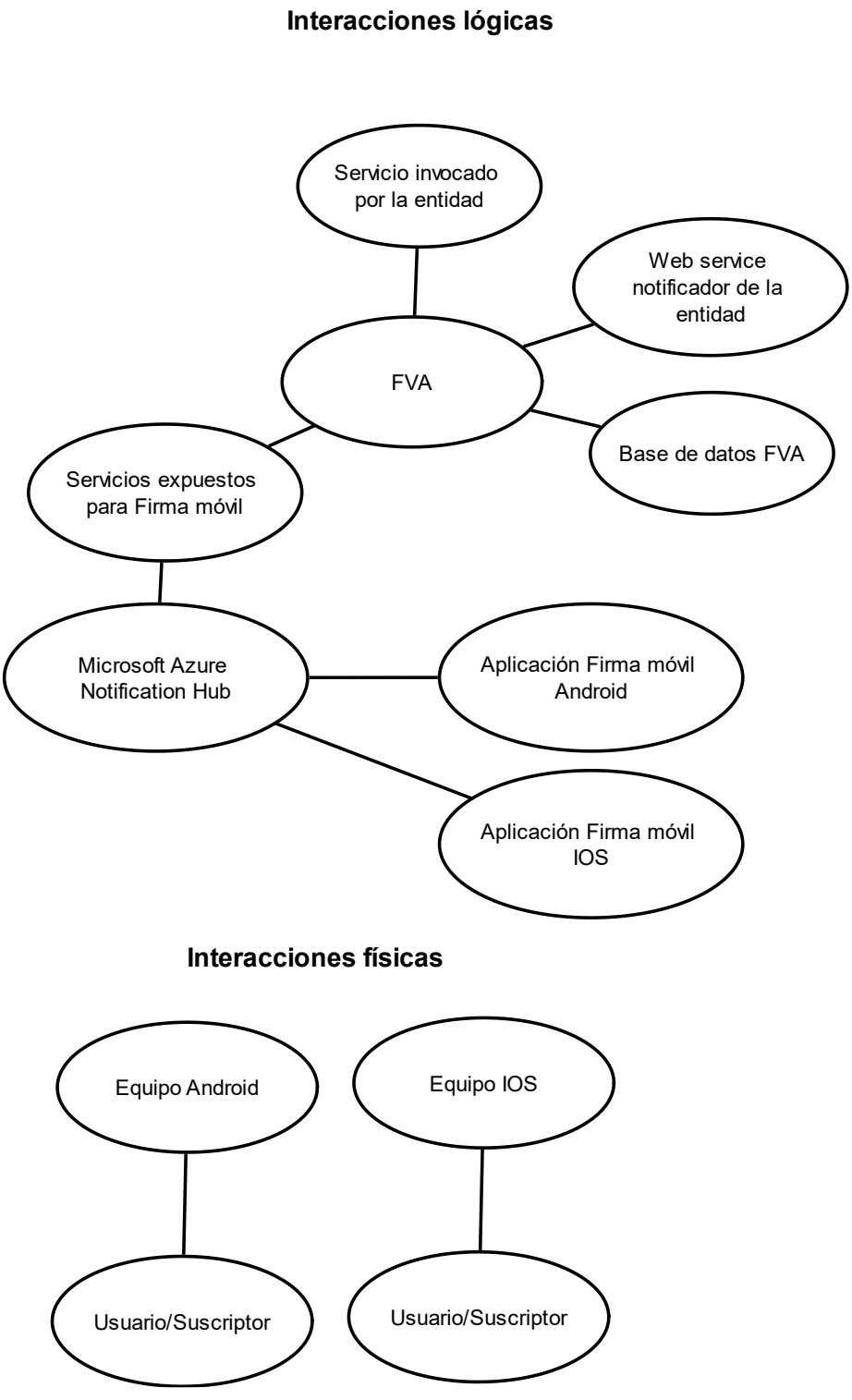

Figura 45 Diagrama de interacciones para flujo de notificación de solicitud de firma en móvil

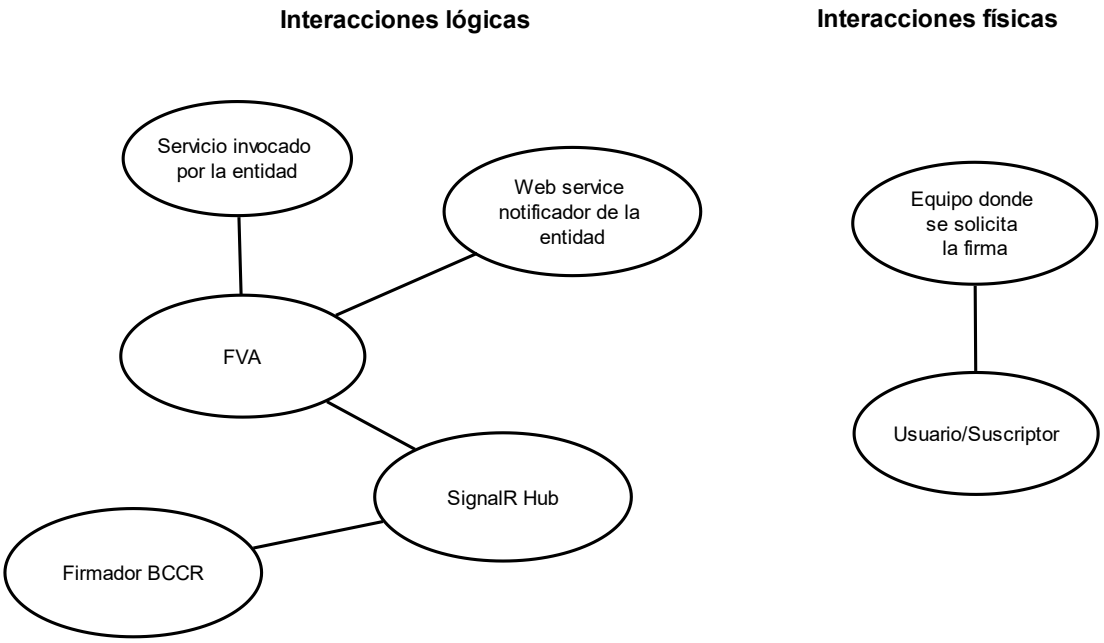

Figura 46 Diagrama de interacciones del flujo de solicitud de firma en escritorio

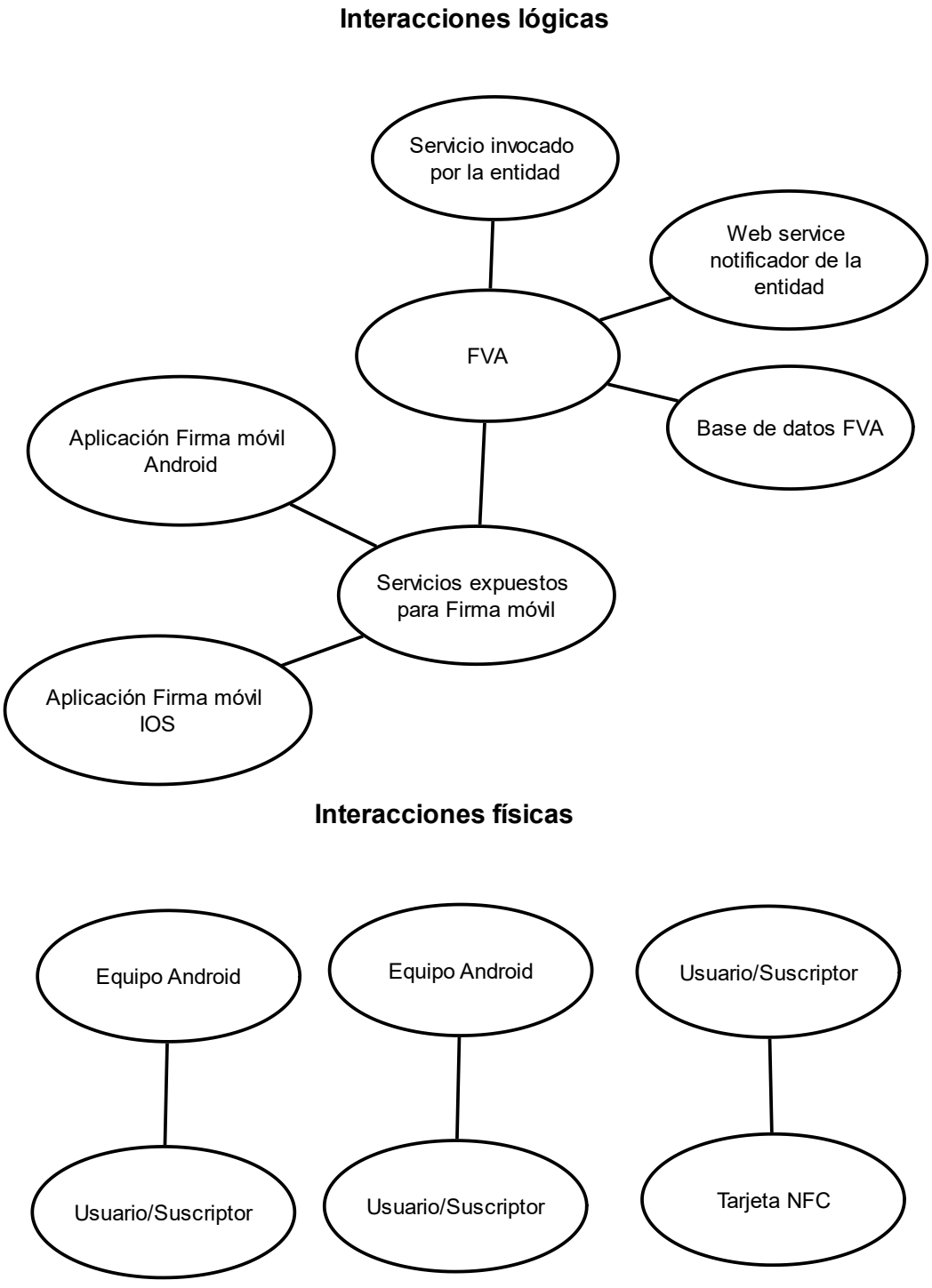

Figura 47 Diagrama de interacciones del flujo de solicitar firma en el móvil