

UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

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

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

ALEJANDRO MORA CASTRO

Ciudad Universitaria Rodrigo Facio, Costa Rica

2017

A Jessi, mi esposa.

Su amor incondicional opaca cualquier dificultad, e ilumina mi universo por completo.

Todo, absolutamente todo, es mejor cuando ella está a mi lado.

- Alejandro

AGRADECIMIENTOS

En general, gracias a Dios por todas las bendiciones que recibo diariamente. No sé qué hago para merecerlas, pero las recibo con total gratitud.

También le doy gracias a mi mamá, doña Grace, por haberme criado a partir de buenos ejemplos. Es, y siempre será, mi modelo a seguir en lo que a esfuerzo y superación respecta.

Por otra parte, la realización de este Trabajo Final de Investigación Aplicada contó con la colaboración de varios profesionales a los cuales quiero manifestar mi más sincero agradecimiento.

Primero, le agradezco a la Dirección de Certificadores de Firma Digital, representada por Alexander Barquero y Mario Álvarez, por el interés y apoyo mostrados en el desarrollo de este proyecto.

Adicionalmente, quiero dar las gracias a Miguel Carballo y a sus compañeros de la división de Seguridad Informática del Banco Central de Costa Rica, por el invaluable conocimiento compartido con mi persona a lo largo de todas las reuniones efectuadas.

Quiero brindar un agradecimiento especial al Dr. Ricardo Villalón, por la confianza depositada en mi persona para realizar este trabajo. Su dedicación y rigurosidad fueron fundamentales para concluir este proyecto de forma satisfactoria.

Finalmente, quiero agradecer a todos los profesores que tuve durante la maestría. Sus enseñanzas han sido un aporte valiosísimo a mi carrera profesional.

“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 por el grado y título de Maestría Profesional en Computación e Informática.”

Dra. Gabriela Barrantes Sliesarieva
Representante de la Decana
Sistema de Estudios de Posgrado

Dr. Ricardo Villalón Fonseca
Profesor Guía

Dr. Marcelo Jenkins Coronas
Lector

Dr. Vladimir Lara Villagrán
Director del Programa de Posgrado en Computación e Informática

Alejandro Mora Castro
Sustentante

ÍNDICE

Agradecimientos	iii
Resumen.....	x
Lista de Tablas	xi
Lista de Figuras.....	xiv
Lista de Gráficos.....	xvi
Lista de Ecuaciones.....	xvii
Lista de Abreviaturas	xviii
1. Introducción.....	1
1.1. Antecedentes	2
1.2. Descripción del Problema	3
1.3. Justificación	4
1.4. Objetivos	5
1.5. Organización del Documento.....	5
2. Marco Teórico	7
2.1. Aseguramiento de la Información.....	7
2.1.1. Conceptos Básicos de Seguridad de la Información	7
2.1.2. Modelos de Aseguramiento de la Información	11
2.2. Firma Digital.....	17
2.3. Criptografía	18
2.3.1. Cifrado simétrico.....	19
2.3.2. Cifrado Asimétrico.....	20
2.4. Documentos Electrónicos.....	22
2.5. Funciones Hash	23
2.6. Procesos de Creación y Verificación de una Firma Digital	24
2.7. Infraestructura de Llave Pública	25
2.7.1. Certificado Digital.....	25
2.7.2. Dispositivos Criptográficos Seguros.....	26
2.7.3. Usuarios Finales	26
2.7.4. Autoridades Certificadoras.....	27
2.7.5. Autoridades de Registro	27
2.7.6. Repositorios	27

2.7.7.	Rutas de Certificación	27
2.7.8.	Listas de Revocación de Certificados (CRL)	28
2.7.9.	Protocolo en Línea de Estado de Certificado (OCSP)	28
2.7.10.	Estampado de Tiempo.....	28
2.7.11.	PKI del SNCD de Costa Rica.....	29
2.8.	Tipos de Firma Digital	30
2.8.1.	Firma Digital Simple.....	31
2.8.2.	Firma Digital Avanzada	31
2.8.3.	Firma Digital Calificada.....	31
3.	Estado del Arte	33
3.1.	Francia.....	33
3.2.	España	34
3.3.	Brasil	36
3.4.	Alemania	38
3.5.	Unión Europea	39
3.6.	Bélgica	40
3.7.	Rusia.....	41
3.8.	Dinamarca	42
3.9.	Chile	42
3.10.	Colombia.....	43
3.11.	México	44
3.12.	Aplicabilidad de las Soluciones Identificadas.....	44
4.	Metodología.....	46
4.1.	Definición de Objetivos de Seguridad	46
4.2.	Análisis de Escenarios de Firma Digital	47
4.2.1.	Selección de Escenarios	47
4.2.2.	Definición del Producto Mínimo Viable Para Cada Escenario	48
4.3.	Identificación y Valoración de Riesgos	49
4.3.1.	Modelado del Sistema	49
4.3.2.	Selección de Fuentes de Vulnerabilidad	50
4.3.3.	Selección de Fuentes de Amenazas.....	51
4.3.4.	Identificación de Riesgos	52

4.3.5.	Determinación de la Probabilidad del Riesgo	54
4.3.6.	Determinación del Impacto del Riesgo	59
4.3.7.	Determinación del Nivel de Severidad del Riesgo.....	63
4.4.	Definición de Políticas de Seguridad de la Información.....	64
4.4.1.	Selección de los Riesgos a ser Mitigados.....	64
4.4.2.	Redacción de las Políticas de Seguridad de la Información.....	64
4.5.	Establecimiento de Objetivos de Control.....	65
4.6.	Elaboración de una Guía de implementación.....	65
5.	Análisis de Escenarios de Firma Digital	66
5.1.	Escenarios de Firma Digital Seleccionados	66
5.2.	Creación de Firma Digital y Sello Electrónico	67
5.2.1.	Producto Mínimo Viable Para la Creación de Firma Digital y Sello Electrónico....	67
5.2.2.	Caracterización de Componentes Para la Creación de Firma Digital y Sello Electrónico.....	68
5.2.3.	Diagrama de Flujos de Información Para la Creación de Firma Digital y Sello Electrónico.....	72
5.3.	Verificación de Firma Digital y Sello Electrónico.....	74
5.3.1.	Producto Mínimo Viable Para la Verificación de Firma Digital y Sello Electrónico74	
5.3.2.	Caracterización de Componentes Para la Verificación de Firma Digital y Sello Electrónico.....	75
5.3.3.	Diagrama de Flujos de Información Para la Verificación de Firma Digital y Sello Electrónico.....	79
5.4.	Conversión de una Firma Digital en Formato Simple a Formato Avanzado	81
5.4.1.	Producto Mínimo Viable Para la Conversión de una Firma Digital en Formato Simple a Formato Avanzado.....	81
5.4.2.	Caracterización de Componentes Para la Conversión de una Firma Digital en Formato Simple a Formato Avanzado	82
5.4.3.	Diagrama de Flujos de Información Para la Conversión de una Firma Digital en Formato Simple a Formato Avanzado	85
5.5.	Autenticación de Usuarios Mediante Certificados Digitales	87
5.5.1.	Producto Mínimo Viable Para la Autenticación de Usuarios Mediante Certificados Digitales	87
5.5.2.	Caracterización de Componentes Para la Autenticación de Usuarios Mediante Certificados Digitales	88

5.5.3. Diagrama de Fluxos de Información Para la Autenticación de Usuarios Mediante Certificados Digitales	91
6. Identificación y Valoración de Riesgos	93
6.1. Consideraciones Generales	93
6.1.1. Restricciones	93
6.1.2. Limitaciones.....	93
6.1.3. Verdades base	94
6.2. Infosec-tree de los Escenarios Analizados	96
6.3. Influencia del Ambiente de Ejecución de los Componentes Tecnológicos en la Valoración de Riesgos.....	97
6.4. Resumen de la Identificación y Valoración de Riesgos	99
7. Definición de Políticas de Seguridad de la Información y Establecimiento de Objetivos de Control	105
7.1. Definición de Políticas de Seguridad de la Información.....	105
7.2. Establecimiento de Objetivos de Control.....	108
8. Guía de Requerimientos Técnicos Para el Aseguramiento de la Información de los Componentes Tecnológicos que Utilizan Certificados y Firma Digital en Aplicaciones de Software Dentro del SNCD	110
8.1. Introducción	110
8.2. Descripción de la Guía de Implementación	110
8.2.1. Escenarios de Uso	110
8.2.2. Servicios de Seguridad de la Información.....	111
8.2.3. Pasos Para Aplicar la Guía de Implementación	111
8.3. Lista de Políticas de Seguridad de la Información a Ser Evaluadas	114
8.4. Lista de Objetivos de Control Para Evaluar el Cumplimiento de las Políticas de Seguridad de la Información.....	118
8.5. Lista de Observaciones de la Evaluación.....	125
8.6. Tabla Resumen de la Evaluación	126
9. Conclusiones, Recomendaciones y Trabajo Futuro	127
9.1. Conclusiones	127
9.2. Recomendaciones.....	128
9.3. Trabajo Futuro.....	129
10. Bibliografía	130
11. Apéndices.....	137

11.1.	Apéndice A: Riesgos Identificados	137
11.2.	Apéndice B: Detalle de la Valoración de los Riesgos Identificados.....	180
11.3.	Apéndice C: Resumen de La Valoración de Riesgos Utilizando un Procedimiento Alternativo.....	313
11.4.	Apéndice D: Terminología Relevante en la Definición de Políticas de Seguridad de la información y el Establecimiento de Objetivos de Control.....	316
11.5.	Apéndice E: Políticas de Seguridad de la Información Definidas	319
11.6.	Apéndice F: Objetivos de Control Establecidos	337

RESUMEN

El desarrollo de la firma digital en Costa Rica se ha incrementado a lo largo de la última década, ofreciendo a los ciudadanos múltiples beneficios a través de una infraestructura tecnológica y un marco jurídico robustos (MICITT, 2016). En nuestro país, el Sistema Nacional de Certificación Digital (SNCD) es el encargado de regir el uso de la firma digital y la generación de certificados digitales con relevancia jurídica a nivel nacional, por medio de un conjunto de disposiciones regulatorias, tales como la Ley 8454 (Gobierno de Costa Rica, 2005), que otorga validez legal a los documentos electrónicos firmados digitalmente. Para fomentar y masificar el uso de la firma digital en todo el país, el Gobierno de la República emitió la directriz 067-MICITT-H-MEIC (Gobierno de Costa Rica, 2014), en abril de 2014, con la cual estableció un lapso de tres años para que las instituciones del gobierno proveyeran servicios en línea a través de mecanismos de firma digital, como una alternativa equivalente a la firma manuscrita.

Aunque el uso de certificados y firma digital se ha incrementado en Costa Rica a lo largo de los últimos años (Víquez & Montes, 2013), el ámbito en el que se desarrollan aplicaciones de *software* que implementan firma digital no está regulado desde la perspectiva de la seguridad de la información. En consecuencia, se identificó una necesidad de establecer regulaciones a nivel nacional para garantizar que este tipo de aplicaciones de *software*: 1) cumplen con los requerimientos establecidos por el SNCD, 2) implementan correctamente los servicios de seguridad de la información correspondientes, y 3) utilizan las mejores prácticas de implementación a nivel de código fuente para el manejo seguro de los certificados digitales.

El objetivo general de la presente investigación, fue definir un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en una aplicación de *software* dentro del SNCD, con el fin de proponer requerimientos técnicos que permitan resolver el problema descrito. Para conseguirlo, se utilizó un enfoque sistemático, que soporta aplicaciones de software desarrolladas con diferentes tecnologías e infraestructuras, y a través del cual se valoraron 228 riesgos de la seguridad de la información, se definieron 103 políticas de seguridad, y se establecieron 26 objetivos de control para evaluar el cumplimiento de éstas.

Como resultado, se propuso una guía de implementación cuya finalidad es servir de herramienta para evaluar el cumplimiento de un conjunto de requisitos de seguridad de la información, definidos para aplicaciones de *software* que implementan firma digital dentro del SNCD.

LISTA DE TABLAS

Tabla 1. Ejemplos de amenazas por categoría. Fuente: Bishop (Bishop, 2002)	8
Tabla 2. Fuentes de vulnerabilidades seleccionadas, agrupadas por categoría. Fuente: Elaboración propia	50
Tabla 3. Ejemplos de fuentes de amenazas originadas por adversarios. Fuente: NIST (National Institute of Standards and Technology, 2012).	52
Tabla 4. Factores característicos de las fuentes de amenazas generadas por adversarios para determinar la probabilidad del riesgo. Fuente: Elaboración propia.	56
Tabla 5. Factores característicos de las fuentes de vulnerabilidades para determinar la probabilidad del riesgo. Fuente: Elaboración propia.....	57
Tabla 6. Escala cuantitativa para el cálculo de la probabilidad del riesgo. Fuente: Elaboración propia.	59
Tabla 7. Factores característicos para la determinación del impacto del riesgo. Fuente: Elaboración propia.	61
Tabla 8. Escala cuantitativa para el cálculo del impacto del riesgo. Fuente: Elaboración propia....	63
Tabla 9. Niveles de severidad del riesgo. Fuente: Elaboración propia.	64
Tabla 10. Descripción de los componentes propuestos para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.	69
Tabla 11. Descripción de los componentes propuestos para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia.	76
Tabla 12. Descripción de los componentes propuestos para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.	83
Tabla 13. Descripción de los componentes propuestos para la autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.	89
Tabla 14. Políticas de seguridad para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.	114
Tabla 15. Políticas de seguridad para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia.	115
Tabla 16. Políticas de seguridad para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.	116
Tabla 17. Políticas de seguridad para la autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.	117
Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.	118
Tabla 19. Espacio para anotar observaciones encontradas durante el proceso de evaluación. Fuente: Elaboración propia.	125
Tabla 20. Tabla desarrollada para mantener un resumen de la evaluación. Fuente: Elaboración propia.	126
Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.	138
Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.	150

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.....	159
Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.....	169
Tabla 25. Riesgos identificados en todos los escenarios. Fuente: Elaboración propia.....	179
Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia.....	181
Tabla 27. Políticas de integridad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.....	320
Tabla 28. Políticas de autenticación para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.....	321
Tabla 29. Políticas de confidencialidad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.....	322
Tabla 30. Políticas de no repudio para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.....	323
Tabla 31. Políticas de Integridad para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.....	324
Tabla 32. Políticas de autenticación para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.....	326
Tabla 33. Políticas de confidencialidad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.....	327
Tabla 34. Políticas de no repudio para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.....	327
Tabla 35. Políticas de integridad para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.....	328
Tabla 36. Políticas de autenticación para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.....	330
Tabla 37. Políticas de confidencialidad para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.....	330
Tabla 38. Políticas de no repudio para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.....	331
Tabla 39. Políticas de integridad para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.....	332
Tabla 40. Políticas de autenticación para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.....	333
Tabla 41. Políticas de confidencialidad para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.....	335
Tabla 42. Políticas de no repudio para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.....	336
Tabla 43. Objetivos de control para hacer cumplir las políticas de integridad definidas. Fuente: Elaboración propia.....	338
Tabla 44. Objetivos de control para hacer cumplir las políticas de autenticación definidas. Fuente: Elaboración propia.....	342

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente: Elaboración propia.....	344
Tabla 46. Objetivos de control para hacer cumplir las políticas de no repudio definidas. Fuente: Elaboración propia.....	350

LISTA DE FIGURAS

Figura 1. Modelo de aseguramiento de la información de Maconachy. Fuente: Elaboración propia:	12
Figura 2. Proceso de evaluación de riesgos propuesto por el NIST. Fuente: NIST (National Institute of Standards and Technology, 2012).	13
Figura 3. Infosec-tree para el aseguramiento de la información de una LAN con impresora compartida. Fuente: Elaboración propia.	15
Figura 4. Nodo de un infosec-tree. Fuente: Villalón, Solano & Marín (Villalón, Solano, & Marín, 2014).	16
Figura 5. Diagrama de flujos de información, generado a partir de un infosec-tree. Fuente: Elaboración propia.	17
Figura 6. Esquema de cifrado simétrico. Fuente: Elaboración propia.	20
Figura 7. Esquema de cifrado asimétrico utilizando la llave privada para cifrar. Fuente: Elaboración propia.	21
Figura 8. Jerarquía nacional de CAs para la emisión de certificados digitales. Fuente: MICITT (MICITT, 2016).	29
Figura 9. Diagrama resumen de los pasos de la metodología. Fuente: Elaboración propia.....	46
Figura 10. Ejemplo del proceso sistemático para la identificación de riesgos, usando el diagrama de flujos de información entre los componentes del sistema. Fuente: Elaboración propia.	53
Figura 11. Proceso para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.	67
Figura 12. Componentes propuestos para un módulo de creación de firma digital y sello electrónico. Fuente: Elaboración propia.	68
Figura 13. Diagrama de flujos de información de los componentes requeridos para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.	73
Figura 14. Proceso para la verificación de una firma digital. Fuente: Elaboración propia.	74
Figura 15. Componentes propuestos para un módulo de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.	75
Figura 16. Diagrama de flujos de información de los componentes requeridos para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia.	80
Figura 17. Proceso para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.	81
Figura 18. Componentes propuestos para un módulo de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.	82
Figura 19. Diagrama de flujos de información de los componentes requeridos para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.	86
Figura 20. Proceso para la autenticación de usuarios por medio de certificados digitales. Fuente: Elaboración propia.	87
Figura 21. Componentes propuestos para un módulo de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.	88
Figura 22. Diagrama de flujos de información de los componentes requeridos para la autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.	92

Figura 23. Infosec-tree propuesto para un sistema que implementa firma digital dentro del SNCD.	96
Fuente: Elaboración propia.....	96
Figura 24. Ejemplo de componentes centralizados y distribuidos. Fuente: Elaboración propia.....	98
Figura 25. Implementación del proceso de creación de firma digital utilizando una arquitectura centralizada y una cliente-servidor. Fuente: Elaboración propia.....	99
Figura 26. Diagrama de flujo para aplicar la guía de implementación. Fuente: Elaboración propia.	
.....	113

LISTA DE GRÁFICOS

Gráfico 1. Cantidad de riesgos valorados, agrupados por escenario. Fuente: Elaboración propia.	100
Gráfico 2. Cantidad de riesgos valorados, agrupados por ambiente de ejecución. Fuente: Elaboración propia.....	101
Gráfico 3. Cantidad de riesgos valorados, agrupados por nivel de severidad. Fuente: Elaboración propia	102
Gráfico 4. Cantidad de riesgos valorados, agrupados por escenario analizado y nivel de severidad. Fuente: Elaboración propia	103
Gráfico 5. Cantidad de riesgos valorados, agrupados por ambiente de ejecución y nivel de severidad. Fuente: Elaboración propia.....	104
Gráfico 6. Cantidad de políticas de seguridad de la información definidas, agrupadas por servicio de seguridad de la información. Fuente: Elaboración propia.....	106
Gráfico 7. Cantidad de políticas de seguridad de la información definidas, agrupadas por escenario analizado y servicio de seguridad de la información. Fuente: Elaboración propia.....	107
Gráfico 8. Cantidad de objetivos de control establecidos, agrupados por servicio de seguridad de la información. Fuente: Elaboración propia.....	108
Gráfico 9. Cantidad de riesgos valorados, agrupados por nivel de severidad, utilizando el procedimiento de valoración alternativo. Fuente: Elaboración propia.....	313
Gráfico 10. Cantidad de riesgos valorados, agrupados por escenario analizado y nivel de severidad, utilizando el procedimiento de valoración alternativo. Fuente: Elaboración propia.....	314
Gráfico 11. Cantidad de riesgos valorados, agrupados por ambiente de ejecución y nivel de severidad, utilizando el procedimiento de valoración alternativo. Fuente: Elaboración propia.	315

LISTA DE ECUACIONES

Ecuación 1. Promedio de los valores asignados a cada factor para estimar la probabilidad de riesgo. Fuente: Elaboración propia	57
Ecuación 2. Promedio de los valores asignados a cada factor para estimar la probabilidad de riesgo, utilizando variables dependientes. Fuente: Elaboración propia	58
Ecuación 3. Promedio de los valores asignados a cada factor para estimar el impacto de riesgo. Fuente: Elaboración propia	62
Ecuación 4. Promedio de los valores asignados a cada factor para estimar el impacto de riesgo, utilizando variables dependientes. Fuente: Elaboración propia	63

LISTA DE ABREVIATURAS

API	<i>Application Program Interface.</i>
CA	Autoridad Certificadora.
CAdES	<i>CMS Advanced Electronic Signature.</i>
CA SINPE	Autoridad Certificadora del Sistema Nacional de Pagos Electrónicos.
CITIC	Centro de Investigaciones en Tecnologías de la Información y Comunicación.
CMS	<i>Cryptographic Message Syntax.</i>
COBIT	<i>Control Objectives for Information and Related Technology.</i>
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	<i>Hardware Security Module.</i>
IEC	<i>International Electrotechnical Commission.</i>
ISO	<i>International Organization for Standardization.</i>
LAN	<i>Local Area Network.</i>
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones.
MVP	<i>Minimum Viable Product.</i>
NIST	<i>National Institute of Standards and Technology.</i>
PAdES	<i>PDF Advanced Electronic Signature.</i>
PDF	<i>Portable Document Format.</i>
PDF 1.7	<i>PDF version 1.7.</i>
PKCS#7	<i>Public Key Cryptography Standard 7.</i>
RA	Autoridad de Registro.
RAM	<i>Random Access Memory.</i>
RMIAS	<i>Reference Model for Information Assurance and Security.</i>

SINPE	Sistema Nacional de Pagos Electrónicos.
SNCD	Sistema Nacional de Certificación Digital.
SQL	<i>Structured Query Language.</i>
TLS	<i>Transport Layer Security.</i>
TSA	Autoridad de Estampado de Tiempo.
UCR	Universidad de Costa Rica.
USB	<i>Universal Serial Bus.</i>
XAdES	<i>XML Advanced Electronic Signature.</i>
XML	<i>Extensible Markup Language.</i>
WYSIWYS	<i>What You See Is What You Sign.</i>
XMLDSig	<i>XML Digital Signature.</i>

1. INTRODUCCIÓN

El desarrollo de la firma digital en Costa Rica se ha incrementado a lo largo de la última década. La firma digital ofrece a los ciudadanos múltiples beneficios, tales como la simplificación de trámites en instituciones públicas y privadas, la disminución del impacto ambiental al reducir el consumo de papel, y la garantía de seguridad y confianza, producto de una infraestructura tecnológica y un marco jurídico robustos (MICITT, 2016).

En Costa Rica, el Sistema Nacional de Certificación Digital (SNCD) es el encargado de regir el uso de la firma digital y la generación de certificados digitales con relevancia jurídica a nivel nacional, por medio de un conjunto de disposiciones regulatorias, tales como la Ley 8454 (Gobierno de Costa Rica, 2005), que otorga validez legal a los documentos electrónicos firmados digitalmente.

Con el fin de fomentar y masificar el uso de la firma digital en todo el país, el Gobierno de la República emitió la directriz 067-MICITT-H-MEIC (Gobierno de Costa Rica, 2014), en abril de 2014. Esta directriz ordena a las instituciones del gobierno que provean servicios en línea a través de mecanismos de firma digital, como una alternativa equivalente a la firma manuscrita, y establece un lapso de tres años para cumplir con el requerimiento.

A pesar de los esfuerzos mencionados, hay una carencia de regulaciones a nivel nacional para garantizar el aseguramiento de la información de las aplicaciones de *software* que implementan mecanismos de firma digital dentro del SNCD, y esto supone un riesgo para la confianza y el no repudio de dicho sistema.

La presente investigación utiliza un enfoque sistémico y sistemático para resolver el problema descrito. En ella se desarrolla un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de *software* dentro del SNCD. Como resultado, se propone una guía de implementación cuyo propósito es servir de instrumento para evaluar el cumplimiento de un conjunto de requisitos de seguridad de la información para este tipo de aplicaciones.

En las siguientes subsecciones se contextualiza el tema de investigación, y se describe la estructura de este documento.

1.1. ANTECEDENTES

En Costa Rica, el uso de certificados y firmas digitales está regulado por la Ley 8454 (Gobierno de Costa Rica, 2005), *Ley de Certificados, Firmas Digitales y Documentos Electrónicos*, aprobada en el año 2005. En ella se define el marco legal para el uso de certificados y firmas digitales como un mecanismo equivalente a la firma manuscrita, así como su validez y aplicabilidad a documentos electrónicos.

La Ley 8454 también regula a los actores que participan en el SNCD y crea la Dirección de Certificadores de Firma Digital (DCFD), un ente adscrito al Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), y encargado de proveer vía reglamento las regulaciones, requisitos y políticas de los distintos componentes del sistema. Asimismo, la DCFD cuenta con un Comité Asesor de Políticas, integrado por representantes del Banco Central de Costa Rica (BCCR), el Tribunal Supremo de Elecciones y el Registro Nacional, entre otros.

El *Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos* (Gobierno de Costa Rica, 2006) le confirió el grado de Autoridad Certificadora Raíz del SNCD a la DCDF, sin embargo, al no contar ésta con la infraestructura ni el recurso técnico necesario, se estableció un convenio de cooperación entre el MICITT y el BCCR, por lo que éste último se convirtió en el encargado de implementar, custodiar y operar la raíz del sistema. Posteriormente, el BCCR implementó la Autoridad Certificadora del Sistema Nacional de Pagos Electrónicos (SINPE), como una entidad subordinada de la Autoridad Certificadora Raíz, encargada de proveer certificados digitales a los usuarios del sistema financiero nacional con el fin de ofrecer transacciones electrónicas más seguras (Víquez & Montes, 2013).

Al existir oferta de certificados y firma digital, numerosas entidades nacionales comenzaron a desarrollar servicios que hacen uso de éstos. A enero de 2017, 54 entidades utilizan firma digital, para un total de 104 aplicaciones (MICITT, 2017). Algunos ejemplos son:

- El BCCR, que utiliza certificados digitales para la autenticación de usuarios en la aplicación Central Directo, utilizada para realizar inversiones directamente con dicha entidad, administrar cuentas de los clientes, negociar divisas entre participantes del mercado cambiario y realizar movimientos entre cuentas desde y hacia el BCCR;
- La Compañía Nacional de Fuerza y Luz, que utiliza certificados digitales para firmar digitalmente los reportes de calibración de sus equipos; y

- El Poder Judicial, que utiliza certificados digitales para que los médicos forenses firmen digitalmente los reportes de las autopsias que realizan (Aguilar, Barquero, Chavarría, Fernández, & Solano, 2011).

Sin embargo, no existe un lineamiento nacional que recopile buenas prácticas para guiar a las entidades que utilizan este tipo de aplicaciones. Esto evidencia una necesidad de estandarizar la manera en que se implementan los servicios apoyados por firma digital, con el fin de orientar los desarrollos hacia una misma dirección (Aguilar et al., 2011).

La seguridad de la información no escapa a la problemática descrita anteriormente, y es por ello que en marzo de 2015 la Escuela de Ciencias de la Computación e Informática (ECCI) inicia el proyecto de investigación 834-B5-181, titulado *Desarrollo de esquemas para certificar autoridades y aplicaciones de software en el Sistema Nacional de Certificación Digital (SNCD)*, inscrito ante la Vicerrectoría de Investigación de la Universidad de Costa Rica (UCR). El proyecto tiene dos objetivos fuertemente ligados al aseguramiento de la información de aplicaciones de *software* que implementan firma digital, los cuales son:

- Evaluar la aplicabilidad, dentro del SNCD, de soluciones existentes a nivel internacional para certificar aplicaciones de *software* que utilizan firma digital a nivel país.
- Diseñar un esquema con base en el estándar ISO 17067 para certificar, desde la perspectiva de la seguridad de la información, las aplicaciones de *software* que implementan mecanismos de firma digital dentro del SNCD.

1.2. DESCRIPCIÓN DEL PROBLEMA

Aunque el uso de certificados y firma digital se ha incrementado en Costa Rica a lo largo de los últimos años (Víquez & Montes, 2013), en un entorno como el actual, que no está regulado desde la perspectiva de la seguridad de la información para desarrollar este tipo de aplicaciones, aún existen retos técnicos que deben superarse. Por ejemplo, suponga una entidad que necesita ofrecer servicios para la creación de firmas digitales a sus clientes, y puede elegir una de varias soluciones disponibles, cada una de las cuales utiliza diferentes algoritmos para su implementación. Finalmente, la entidad elige una herramienta que, entre otras cosas, hace uso de funciones *hash* consideradas inseguras porque son susceptibles a colisiones. En ese escenario, existe una probabilidad de que documentos electrónicos diferentes, firmados digitalmente por un usuario, produzcan firmas digitales idénticas. Esas firmas serían repudiables, puesto que el usuario podría

argumentar que el documento electrónico que firmó no es el mismo que creyó estar firmando. Esta duda razonable pone en riesgo la confianza en la herramienta, en la entidad y en el SNCD. Si se comprometiera la confianza en el SNCD, no se podría contar con los beneficios que proporcionan las firmas digitales, ya que dejarían de ser una alternativa equivalente a las firmas manuscritas.

En consecuencia, existe una necesidad de establecer regulaciones a nivel nacional para garantizar que este tipo de aplicaciones de *software*:

- Cumplen con las leyes, reglamentos y políticas definidas por el SNCD.
- Implementan correctamente servicios de seguridad de la información tales como no repudio, integridad, autenticación y confidencialidad, que son fundamentales en este contexto.
- Utilizan las mejores prácticas de implementación a nivel de código fuente para el manejo seguro y eficiente de los certificados digitales.

En la presente investigación se desarrolla un proceso de aseguramiento de la información con el fin de proponer requerimientos técnicos que permiten resolver el problema descrito.

1.3. JUSTIFICACIÓN

El 25 de abril de 2014, el Gobierno de la República emitió la directriz 067-MICITT-H-MEIC, *Masificación de la implementación y el uso de la firma digital en el sector público costarricense*, publicada en el diario oficial La Gaceta y en la que decretó (Gobierno de Costa Rica, 2014):

“A partir de la publicación de esta directriz, todas las instituciones del sector público costarricense deberán tomar las medidas técnicas y financieras necesarias que le permitan disponer de los medios electrónicos para que los ciudadanos puedan obtener información, realizar consultas, formular solicitudes, manifestar consentimiento y compromiso, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos. Se busca con esta directriz hacer efectivo el derecho a exigir igualdad en el acceso por medios electrónicos a todos los servicios que se ofrecen por medios físicos, pudiendo las personas físicas utilizar en cualquier escenario la capacidad de firma digital certificada, ya sea para autenticarse o para firmar todos los trámites con la institución por vía electrónica.”

Con esta directriz, más de 300 entidades del sector público tendrán que adaptar todos sus servicios actuales para soportar certificados y firma digital (Barquero, 2014). Esto implica que una gran cantidad de aplicaciones deberían ser implementadas o mejoradas en el corto y mediano plazo.

A partir de los resultados generados en esta investigación, la DCFD cuenta con un criterio técnico adicional para definir un esquema de certificación de aplicaciones de *software* que utilizan certificados y firma digital dentro del SNCD. Esto tiene un impacto positivo por las siguientes razones:

- Se genera conocimiento sobre la adecuada implementación de aplicaciones de *software* que utilizan certificados y firma digital.
- Se proponen pautas a seguir en todas las aplicaciones de *software* que utilizan certificados y firma digital en Costa Rica, dentro del SNCD.
- Se promueve el uso masivo de certificados y firma digital a nivel nacional.
- Se coloca a la UCR como un actor relevante en la masificación del uso de certificados y firma digital en el país.

1.4. OBJETIVOS

El objetivo general de la presente investigación es definir un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en una aplicación de *software* dentro del SNCD. Para cumplir con este objetivo, se definieron los siguientes objetivos específicos:

1. Analizar los escenarios en los que una aplicación de *software* puede utilizar certificados y firma digital.
2. Identificar los riesgos de seguridad de la información existentes en los escenarios analizados.
3. Definir políticas de seguridad para mitigar los riesgos analizados.
4. Establecer controles de seguridad para hacer cumplir las políticas definidas.
5. Proponer una guía para la implementación de un proceso de aseguramiento de la información.

1.5. ORGANIZACIÓN DEL DOCUMENTO

Este documento se organiza de la siguiente manera. El Capítulo 2 presenta un marco teórico relacionado con aseguramiento de la información, firma digital, criptografía e infraestructuras de llave pública, requeridos para la comprensión del resto del documento. El Capítulo 3 detalla los

resultados de una revisión del estado del arte a nivel internacional, en materia de soluciones a nivel país para validar la seguridad de la información en aplicaciones que implementan firma digital. El Capítulo 4 describe la metodología utilizada a lo largo de la presente investigación para cumplir con los objetivos planteados. El Capítulo 5 revela el producto del análisis de escenarios de firma digital. El Capítulo 6 muestra los resultados del proceso de identificación y valoración de riesgos. El Capítulo 7 resume las políticas de seguridad de la información definidas y los objetivos de control establecidos. El Capítulo 8 enuncia una guía de implementación para aplicaciones que hacen uso de la firma digital. Por último, el Capítulo 9 expone las principales conclusiones obtenidas a partir de la investigación, así como una serie de recomendaciones y pautas a seguir para realizar trabajo futuro.

2. MARCO TEÓRICO

En el presente capítulo se exponen los fundamentos teóricos que sustentan el desarrollo de este proyecto. Inicia con una explicación de diferentes conceptos vinculados con el aseguramiento de la información. Continúa con una descripción de firma digital y otros aspectos relacionados, tales como criptografía, funciones *hash*, procesos de creación y verificación de firma digital, y documentos electrónicos. Adicionalmente, se exponen varios conceptos relevantes en el contexto de las infraestructuras de llave pública. Finalmente, se reseñan los tipos de firma digital que se encuentran en la literatura.

2.1. ASEGURAMIENTO DE LA INFORMACIÓN

Las tecnologías de la información y comunicación evolucionan constantemente, presentando con frecuencia nuevos retos. Uno de los desafíos más importantes es el aseguramiento de la información, que se define como el conjunto de operaciones que protegen y defienden la información y los sistemas de información, para asegurar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. Esto incluye proveer capacidades de protección, detección y reacción para restaurar los sistemas de información (Maconachy, Schou, Ragsdale, & Welch, 2001).

2.1.1. CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se exponen términos fundamentales dentro del contexto de la seguridad de la información.

AMENAZAS

Una amenaza es una violación potencial de la seguridad. Se dice potencial, porque no necesariamente debe ocurrir para ser considerada una amenaza. 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).

Shirey (1994) clasifica las amenazas en cuatro clases generales:

- Divulgación (disclosure): es el acceso no autorizado a la información.
- Engaño (deception): es la aceptación de datos falsos.
- Interrupción (disruption): es la interrupción o prevención de una correcta operación.
- Usurpación (usurpation): es el control no autorizado de alguna parte de un sistema.

La TABLA 1 muestra algunos ejemplos de amenazas comunes, y las categorías dentro de las cuales pueden clasificarse.

Tabla 1. Ejemplos de amenazas por categoría. Fuente: Bishop (Bishop, 2002).

Amenaza	Definición	Categoría
Intromisión (<i>snooping</i>)	Intercepción no autorizada de la información	Divulgación
Modificación o alteración (<i>Modification o alteration</i>)	Cambio no autorizado de la información	Engaño, interrupción, usurpación
Enmascaramiento (<i>Masquerading o spoofing</i>)	Suplantación de una identidad por otra	Engaño, usurpación
Repudio de origen (<i>repudiation of origin</i>)	Negación de que una entidad creó o envió algo, cuando sí lo hizo	Engaño
Negación de recibo (<i>denial of receipt</i>)	Negación de que una entidad recibió algún tipo de información, cuando sí lo hizo	Engaño
Demora (<i>delay</i>)	Inhibición temporal de un servicio	Usurpación, engaño
Negación de servicio (<i>denial of service</i>)	Inhibición a largo plazo de un servicio	Usurpación

Finalmente, se conoce como una fuente de amenaza a:

- El intento dirigido hacia la explotación deliberada de una vulnerabilidad; y
- Una situación que puede activar accidentalmente una vulnerabilidad (National Institute of Standards and Technology, 2012).

VULNERABILIDADES

Una vulnerabilidad es una debilidad que hace posible que una amenaza se materialice (Bishop, 2002). Las vulnerabilidades generalmente son defectos en procedimientos de seguridad, diseño, implementación, o controles internos de un sistema de información, y dan lugar a una violación de sus políticas de seguridad (National Institute of Standards and Technology, 2012).

RIESGOS

Un riesgo es una función de la probabilidad de que una fuente de amenaza explote una vulnerabilidad, y el impacto resultante de ese evento adverso sobre la organización (National Institute of Standards and Technology, 2012).

Esta función de probabilidad e impacto permite determinar la prioridad de los riesgos que deben ser atendidos, según una relación entre costo y beneficio. Si la ocurrencia de un ataque es poco probable, implementar protección contra él debe tener una prioridad menor que la que debe tener la implementación de protección contra un ataque más probable. Sin embargo, si el ataque poco probable tuviera gran impacto en la organización, y el ataque más probable tuviera un impacto mínimo, mayor esfuerzo debería ponerse en la implementación de protección contra el ataque poco probable (Bishop, 2002).

POLÍTICAS DE SEGURIDAD

Una política de seguridad es una declaración de lo que es y no es permitido en un sistema de información (Bishop, 2004). Las políticas de seguridad dividen los estados de un sistema en dos conjuntos: los seguros (o autorizados), y los inseguros (o no autorizados). Las políticas de seguridad también establecen el contexto en el que se puede definir un sistema de información seguro. Dependiendo de los requerimientos de seguridad de un sistema, pueden ser necesarias múltiples políticas, por ejemplo, políticas de integridad, políticas de confidencialidad, políticas de disponibilidad, etcétera (Bishop, 2002).

CONTROLES DE SEGURIDAD

Un control de seguridad es un método, herramienta o procedimiento que hace cumplir una política de seguridad (Bishop, 2004).

OBJETIVOS DE CONTROL

Utilizar controles de seguridad para verificar el cumplimiento de las políticas definidas en el proceso de aseguramiento de la información desarrollado en este trabajo es poco práctico. Primero, los controles de seguridad, por definición, están asociados al cómo implementar una solución en un contexto específico, mientras que este proceso de aseguramiento de la información debe ser adaptable a múltiples aplicaciones, implementadas utilizando diferentes arquitecturas e infraestructuras tecnológicas. Segundo, es muy complejo mantener una lista constantemente

actualizada de todos los controles de seguridad que hacen cumplir una política, especialmente en un entorno tan evolutivo como es el de la seguridad de la información.

Con base en lo anterior, el concepto de control de seguridad es insuficiente, sin embargo, la literatura proporciona otro concepto más apropiado para los requerimientos de esta investigación, y es el de objetivo de control. Según *Public Company Account Oversight Board* (2017), aunque no es una definición, un objetivo de control proporciona una referencia específica respecto a la cual evaluar la eficacia de los controles. Leigh (2016) define un objetivo de control como una razón o un propósito para el cual se deben implementar uno o más controles.

Para efectos de este trabajo se construye una definición propia, más amplia que la encontrada en la literatura. Se considera que un de objetivo de control es una 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. Los detalles de implementación únicamente se incluyen cuando representan aspectos relevantes en los objetivos definidos por las políticas de seguridad de la información.

SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

Los servicios de seguridad de la información representan propiedades o requerimientos de la información que deben satisfacerse al momento de aplicar seguridad (Villalón, Solano, & Marín, 2014). A continuación, se presentan las definiciones de los servicios de seguridad de la información más relevantes para este trabajo:

- No repudio: es una propiedad de datos y procesos, la cual previene que una entidad pueda negar el haber realizado una acción particular que sí realizó (Buchmann, Evangelos, & Wiesmaier, 2013).
- Integridad: es la propiedad de la información que previene un cambio indebido o no autorizado de los datos (Bishop, 2002).
- Autenticación: es la verificación de la identidad de un sujeto (Instituto de Normas Técnicas de Costa Rica, 2007).
- Confidencialidad: es la propiedad que garantiza que la información no esté disponible ni se divulgue a personas o procesos no autorizados (Buchmann, Evangelos, & Wiesmaier, 2013).

- Disponibilidad: es el acceso oportuno y confiable a datos y servicios de información para los usuarios autorizados (Maconachy, Schou, Ragsdale, & Welch, 2001).

La seguridad de la información consiste en proteger los servicios de seguridad ante posibles ataques, a través de políticas y controles (Villalón, Solano, & Marín, 2014). En la práctica, para lograr lo anterior con mayor facilidad, existen modelos, que se describen en la siguiente subsección.

2.1.2. MODELOS DE ASEGURAMIENTO DE LA INFORMACIÓN

Seguidamente se presentan términos básicos relacionados con modelos y estándares de aseguramiento de la información, así como la descripción de los modelos y guías que sirven como base para el desarrollo del presente proyecto.

MODELOS Y ESTÁNDARES

En la industria existen diversos modelos y estándares para el aseguramiento de la información. Los modelos de aseguramiento de la información son herramientas para hacer cumplir políticas de seguridad de la información utilizando métodos formales o informales (Villalón, Solano, & Marín, 2014). Por otra parte, los estándares de seguridad son conjuntos de prácticas generalizadas para ayudar a reducir el número de ataques dirigidos hacia la información de un sistema (Villalón, Solano, & Marín, 2014).

En el trabajo de Villalón et al. (2014) se hace una comparación de estándares y modelos de seguridad en el contexto del aseguramiento de la información. Entre los elementos comparados se encuentra la serie de estándares ISO/IEC 27000, el estándar *Control Objectives for Information and Related Technology* (COBIT), líneas guía y estándares del *National Institute of Standards and Technology* (NIST), el modelo de McCumber, el modelo de Maconachy, el modelo *Reference Model for Information Assurance and Security* (RMIAS) y el modelo *Infosec-Tree*. Con base en las características exhibidas, el modelo de Maconachy, la guía para conducir evaluaciones de riesgo del NIST y el modelo *Infosec-Tree* son apropiados para el desarrollo de esta investigación.

MODELO DE MACONACHY

Según Maconachy et al. (2001), para garantizar el aseguramiento de la información se deben considerar cuatro dimensiones: estados de la información, servicios de seguridad de la información, controles de seguridad y tiempo, tal como se muestra en la FIGURA 1.

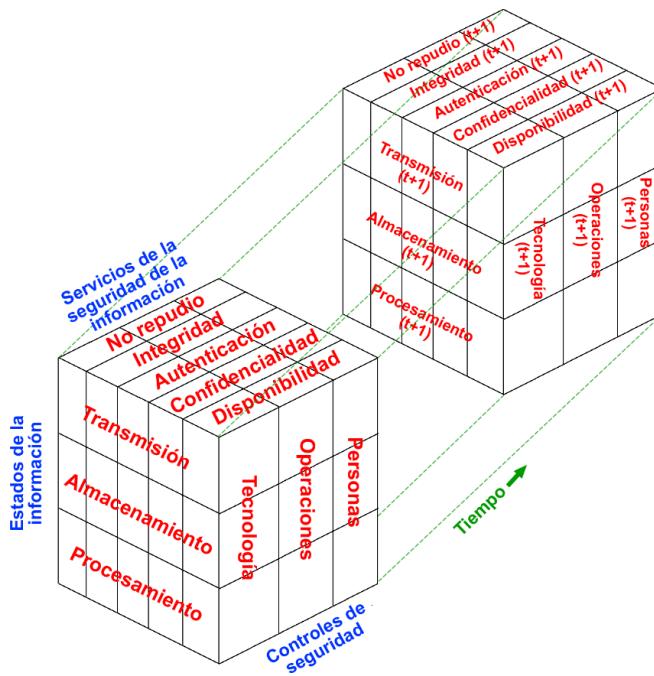


Figura 1. Modelo de aseguramiento de la información de Maconachy. Fuente: Elaboración propia:

A continuación, se describe cada una de las dimensiones de este modelo.

1) Estados de la información: dentro de un sistema, la información puede encontrarse en uno o más de tres estados posibles: almacenada, procesada o transmitida.

2) Servicios de seguridad de la información: uno de los principales objetivos del aseguramiento de la información es proveer servicios de seguridad, tales como no repudio, integridad, autenticación, confidencialidad y confidencialidad.

3) Controles de seguridad: cualquier plan de defensa de la seguridad de la información debe considerar controles de seguridad que mitiguen riesgos presentes dentro de las siguientes variables:

- Tecnología: incluye todo el *hardware, software y firmware* que compone un sistema o red.
- Operaciones: abarcan los procedimientos empleados por los usuarios de los sistemas y las configuraciones implementadas por los administradores, entre otros.
- Personas: son el centro de los sistemas seguros, y como tal, necesitan conciencia, entrenamiento y educación en materia de prácticas de seguridad.

4) Tiempo: es un agente de cambio que impacta a las demás dimensiones de un modelo de aseguramiento de la información. Cambios a través del tiempo en una dimensión, generalmente

requieren modificaciones en otras dimensiones para restaurar un sistema a un estado de operación seguro.

En este trabajo, se hace uso de todas esas dimensiones para cumplir con el objetivo de asegurar la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de *software* dentro del SNCD.

PUBLICACIÓN ESPECIAL DEL NIST 800-30 REVISIÓN 1, GUÍA PARA CONDUCIR EVALUACIONES DE RIESGO

Según el NIST (2012), las evaluaciones de riesgo son un componente básico en los procesos de gestión de riesgo a nivel organizacional, y son utilizadas para identificar, estimar y priorizar riesgos que pueden afectar a los individuos, así como a las operaciones y los recursos de la organización, como resultado del uso y operación de sistemas de información. La FIGURA 2 muestra el proceso de evaluación de riesgos propuesto por el NIST.

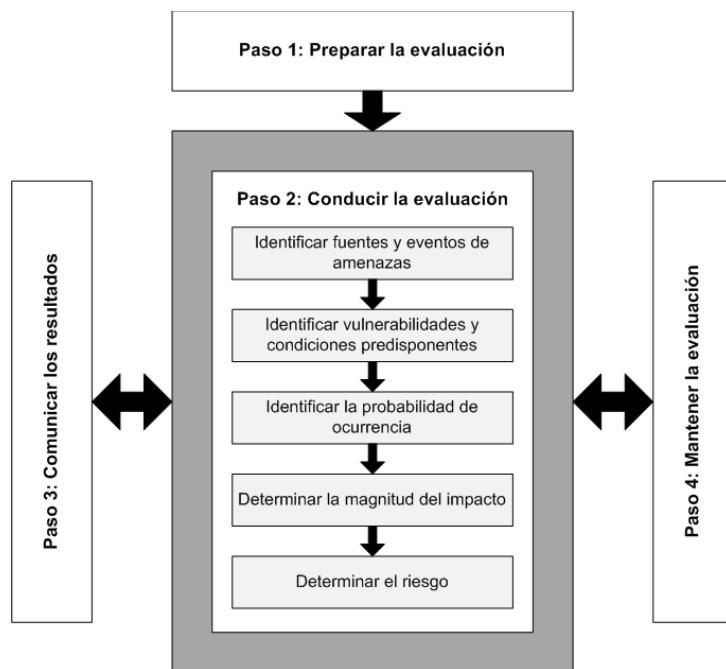


Figura 2. Proceso de evaluación de riesgos propuesto por el NIST. Fuente: NIST (National Institute of Standards and Technology, 2012).

A continuación, se describe cada uno de los pasos de este proceso de evaluación de riesgos.

1) Preparar la evaluación: tiene como objetivo definir el contexto del proceso de evaluación de riesgos, e incluye 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: tiene como objetivo 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. Incluye 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 predisponentes 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 adverso 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 los resultados: tiene como objetivo garantizar que las personas encargadas de la toma de decisiones en la organización tienen información apropiada acerca de los riesgos, de manera que puedan informar y guiar decisiones al respecto. Incluye las siguientes tareas:

- Comunicar los resultados de la evaluación de los riesgos.
- Compartir la información obtenida a partir de la evaluación, para soportar otras actividades relacionadas con la gestión de los riesgos.

4) Mantener la evaluación: tiene como objetivo mantener actualizado el conocimiento de los riesgos específicos en los cuales la organización puede incurrir. Incluye las siguientes tareas:

- Monitorear factores de riesgo identificados durante las evaluaciones de forma continua, y comprender los cambios subsecuentes de esos factores.
- Actualizar los componentes de las evaluaciones de riesgo, de manera que reflejen las actividades de monitoreo realizadas por la organización.

Con base en los pasos descritos, en la presente investigación se hace uso de este proceso de evaluación de riesgos como base para la definición de los requisitos de seguridad necesarios para desarrollar el proceso de aseguramiento de la información ya descrito.

MODELO INFOSEC-TREE

El *Infosec-Tree* es un modelo para el aseguramiento de la información que utiliza un enfoque jerárquico del todo y las partes. En este modelo, una aplicación de *software* o cualquier tipo de sistema tecnológico se descompone en los elementos que lo integran, utilizando un árbol. La raíz de ese árbol simboliza la totalidad del sistema. Los elementos en niveles más altos del árbol representan componentes más grandes del sistema, mientras que los elementos en niveles más bajos representan partes más pequeñas que componen los elementos más grandes que están sobre ellos en el árbol (Villalón, Solano, & Marín, 2014). Por ejemplo, suponga que existe una pequeña red de área local como la que se muestra en la FIGURA 3a, para la cual se requiere proteger la integridad de los documentos que se envían a imprimir.

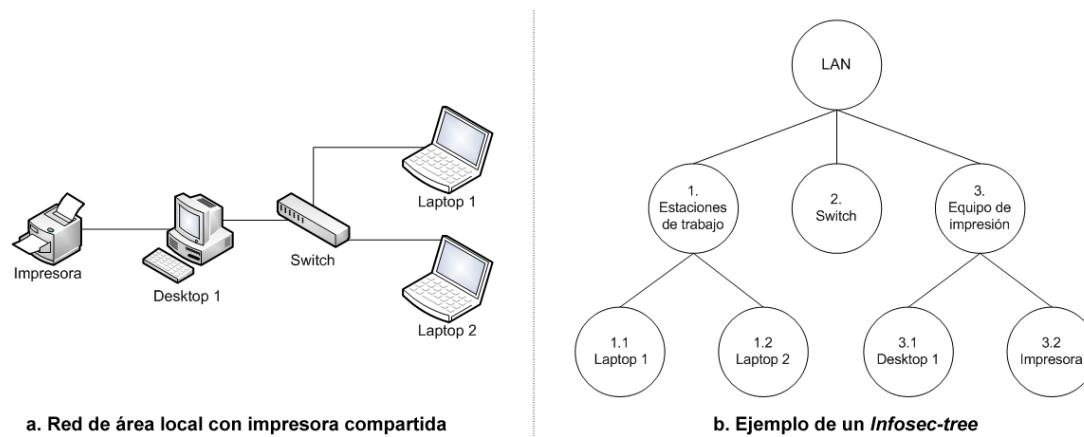


Figura 3. Infosec-tree para el aseguramiento de la información de una LAN con impresora compartida.
Fuente: Elaboración propia.

La red está compuesta por dos estaciones de trabajo que se comunican a través de un *switch* con una computadora de escritorio, dedicada a servir de acceso a una impresora que se encuentra compartida en la red. La FIGURA 3b muestra el *infosec-tree* que representa el sistema tecnológico que se

requiere asegurar utilizando un enfoque del todo y las partes. La raíz del árbol representa todo el sistema (la red de área local), cuya infraestructura está compuesta por las estaciones de trabajo, el *switch* y el equipo de impresión. El nodo “1. Estaciones de trabajo” está a su vez conformado por los nodos “1.1 Laptop 1” y “1.2 Laptop 2”, mientras que el nodo “3. Equipo de impresión” está integrado por los nodos “3.1 Desktop 1” y “3.2 Impresora”.

Los nodos en un *infosec-tree* pueden representar *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 en todos los niveles de la jerarquía (Villalón, Solano, & Marín, 2014).

El modelo *Infosec-Tree* utiliza triadas para representar requerimientos de seguridad. Cuando la triada especifica requerimientos de seguridad para la información contenida en un nodo, se denomina triada interna, mientras que, si los requerimientos de seguridad se definen para información transmitida entre dos nodos, se denomina triada de punto de conexión (*end-point triad*). Las triadas se definen mediante la siguiente estructura:

{Momento de seguridad, Estado de la información, Servicio de seguridad}

para representar la dimensión de tiempo del aseguramiento de la información (antes, durante o después de la ocurrencia del evento), el estado en que se encuentra la información, y el servicio de seguridad implementado, respectivamente (Villalón, Solano, & Marín, 2014). Considere el nodo que se muestra en la FIGURA 4, y suponga que se requiere proteger la integridad de la información mientras se procesa en él, así como la confidencialidad de los datos que entran y salen de él. La triada interna para ese nodo está representada por {protección, procesamiento, integridad}, mientras que la triada para el punto de conexión “a” es {protección, transmisión, confidencialidad}.

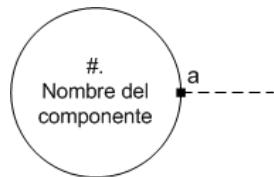


Figura 4. Nodo de un *infosec-tree*. Fuente: Villalón, Solano & Marín (Villalón, Solano, & Marín, 2014).

Otro componente del modelo *Infosec-Tree* son los diagramas de flujo de información, los cuales representan nodos que se comunican, conectados mediante triadas de punto de conexión (Villalón, Solano, & Marín, 2014). La FIGURA 5 muestra un ejemplo de diagrama de flujos de información, en el cual se retoma el escenario de la red de área local descrito con anterioridad. En él, los

componentes representados por los nodos “1.1 Laptop 1”, “1.2 Laptop 2” y “3.1 Desktop 1” se conectan físicamente mediante sus interfaces de red con un *switch* (nodo “2. Switch”). Asimismo, la computadora de escritorio (nodo “3.1 Desktop 1”) se conecta físicamente con la impresora (nodo “3.2 Impresora”) a través de un cable USB. Aunque en este caso específico los enlaces entre los componentes son físicos, en otros contextos las conexiones podrían ser lógicas, por ejemplo, la representación de una conexión entre el *firmware* de la impresora y el *driver* de la impresora instalado en la computadora de escritorio.

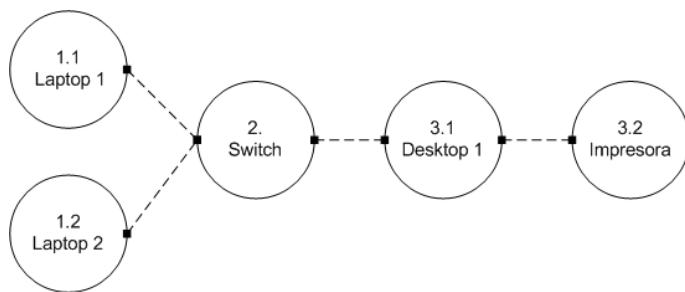


Figura 5. Diagrama de flujos de información, generado a partir de un *infosec-tree*. Fuente: Elaboración propia.

Por las características descritas, el modelo *Infosec-Tree* facilita el desarrollo de un proceso de aseguramiento de la información que es ordenado, y que puede cubrir todos los componentes relevantes en el contexto de las aplicaciones de *software* que implementan mecanismos de firma digital.

2.2. FIRMA DIGITAL

El aumento en el uso de documentos electrónicos ocasionó que personas y organizaciones tuvieran la necesidad de firmarlos con el fin de vincularlos con su autor, tal como la firma manuscrita ha sido aplicada a los documentos tradicionales (Aguilar et al., 2011). Como solución a esta necesidad, surgió el concepto de firma electrónica. Según Aguilar et al. (2011), si bien en la legislación costarricense no existe una definición para firma electrónica, a nivel internacional hay un consenso sobre su significado, y se dice que una firma electrónica es un conjunto de datos que se adjunta o se asocia a otro conjunto de datos, y es capaz de identificar al firmante.

Con base en lo indicado anteriormente, una firma electrónica puede ser la grabación de la voz de una persona, una imagen de sus huellas digitales, una imagen escaneada de su firma manuscrita, etcétera. Sin embargo, dado que ese tipo de archivos podría ser copiado, alterado o borrado con

relativa facilidad, no se puede considerar que una firma electrónica es un mecanismo equivalente a la firma manuscrita (Aguilar et al., 2011). Las firmas digitales, que basan su correcta implementación en la criptografía asimétrica y los certificados digitales, permiten resolver las deficiencias de las firmas electrónicas. De esta forma, es correcto afirmar que toda firma digital es una firma electrónica, pero no toda firma electrónica es una firma digital (Aguilar et al., 2011).

Una firma digital es un 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 (Gobierno de Costa Rica, 2005). A partir de esta definición, se entiende que las firmas digitales proveen los servicios de integridad, autenticación y no repudio.

En Costa Rica, la *Ley N° 8454: Ley de Certificados, Firmas Digitales y Documentos Electrónicos* define los requerimientos técnicos y legales que le otorgan a los mecanismos de firma digital el mismo peso probatorio que la firma manuscrita (Gobierno de Costa Rica, 2005).

Las siguientes secciones explican los aspectos técnicos más relevantes sobre los cuales se basa el funcionamiento de las firmas digitales.

2.3. CRIPTOGRAFÍA

De forma general, la criptografía es el arte y la ciencia de prevenir que algo sea visto o sabido (Bishop, 2002). Dentro del contexto del aseguramiento de la información, la criptografía es el estudio de técnicas matemáticas para proteger información, cálculos y sistemas digitales de ataques adversarios (Katz & Lindell, 2014).

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

El escenario más tradicional en el uso de la criptografía consiste en dos partes que requieren comunicarse a través de un canal inseguro, que podría ser intervenido por un adversario (Goldreich, 2004). Sean las partes Alice y Bob, y el adversario Eve, el objetivo es permitir que Alice envíe información a Bob a través de un canal inseguro, sin que Eve sea capaz de conocer esa información.

En ese escenario, es posible distinguir entre la información original que el emisor (Alice) quiere transmitir y mantener en secreto, que se conoce como texto plano, y el mensaje que viaja por el canal de comunicación inseguro, que se conoce como texto cifrado. El proceso de convertir el texto plano en texto cifrado se conoce como cifrar, mientras que el proceso inverso se denomina descifrar.

Dado que Alice está en capacidad de transformar el texto plano en texto cifrado, de forma tal que Bob puede obtener el texto plano a partir de ese texto cifrado sin que Eve pueda hacerlo, es claro que Bob posee algo que Eve no. Ese “algo” se conoce como llave (o clave) criptográfica, y se define como una pieza variable de datos que se proporciona como entrada a un algoritmo criptográfico para realizar una operación determinada (Microsoft, 2015).

Para cifrar un mensaje, se envían los datos del mensaje junto con una llave a un algoritmo criptográfico, teniendo como resultado datos cifrados. Cuando se requiere descifrar el mensaje, se envían los datos cifrados junto con la llave correspondiente a otro algoritmo criptográfico, obteniendo así los datos descifrados. Por lo tanto, una parte importante de la seguridad está determinada por el tamaño y la complejidad de las llaves criptográficas utilizadas (Aguilar et al., 2011).

El criterio básico para categorizar los tipos de esquema de cifrado está determinado por la relación que hay entre el par de llaves criptográficas utilizadas para cifrar y descifrar los datos (Goldreich, 2004). Se distinguen dos esquemas para realizar operaciones criptográficas: el simétrico y el asimétrico.

2.3.1. CIFRADO SIMÉTRICO

El esquema de cifrado simétrico emplea una sola llave, que sirve para cifrar y descifrar los datos (Menezes, van Oorschot, & Vanstone, 1997). Dicho esquema de cifrado se ilustra en la FIGURA 6.

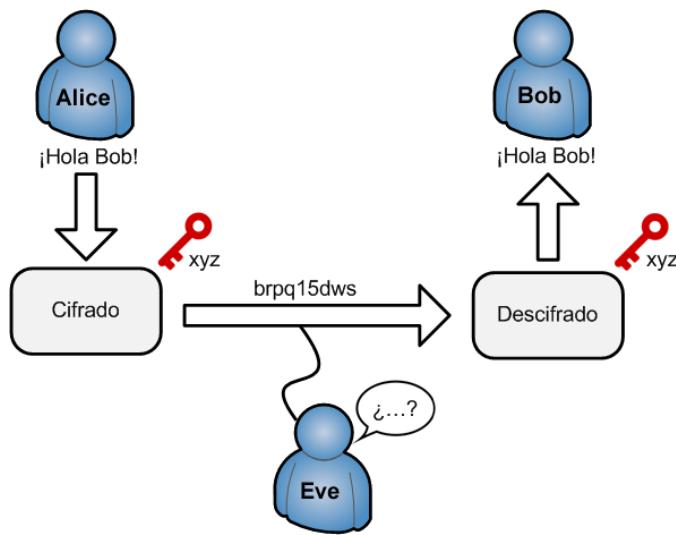


Figura 6. Esquema de cifrado simétrico. Fuente: Elaboración propia.

Inicialmente, las partes involucradas deben acordar y distribuir la llave que se utilizará. Por ejemplo, Alice genera aleatoriamente una llave y se la envía a Bob, utilizando un canal secundario que se asume seguro. Una vez que este proceso se llevó a cabo, Alice puede cifrar un mensaje usando la llave generada, enviarlo a Bob y él podrá descifrarlo usando la misma llave. Por su parte Eve, quien no tiene acceso a la llave, no puede descifrar la información transmitida.

El esquema de cifrado simétrico se caracteriza por utilizar llaves criptográficas relativamente pequeñas y tiende a ser comparativamente más rápido que el esquema asimétrico. Sin embargo, en sistemas en los que muchos usuarios deben establecer canales de información independientes y seguros, el esquema de cifrado simétrico tiene limitaciones prácticas debido a los requerimientos de distribución y gestión de las llaves criptográficas (OWASP, 2015).

Según el trabajo de Víquez & Montes (2013), algunos algoritmos criptográficos simétricos populares son: DES (*Data Encryption Standard*), 3DES (*Triple DES*), RC4, RC5, IDEA (*International Data Encryption Algorithm*), AES (*Advanced Encryption Standard*) y Blowfish.

2.3.2. CIFRADO ASIMÉTRICO

Este esquema, también conocido como criptografía de llave pública, utiliza dos llaves, de las cuales una es pública y puede ser entregada a cualquier entidad, y la otra es privada, por lo que el propietario debe mantenerla en secreto. Ambas llaves están matemáticamente relacionadas entre sí, sin embargo, para fines prácticos, no es viable calcular una llave pública dada su correspondiente llave privada, y viceversa (Bishop, 2002).

Cualquiera de las dos llaves puede usarse durante los procesos de cifrado y descifrado, de la siguiente forma: si la llave privada es usada para cifrar los datos, solo la correspondiente llave pública puede usarse para descifrar la información; por otra parte, si la llave pública se usa para cifrar los datos, debe usarse la llave privada para descifrarlos. La FIGURA 7 muestra un ejemplo de cifrado asimétrico, en el cual se utilizó la llave privada para cifrar los datos. En él, Alice tiene un par de llaves, “abc” que es su llave pública, y “xyz” que es su llave privada, y utiliza ésta última para cifrar un mensaje que es enviado a Bob. Para descifrar el mensaje, Bob utiliza la llave pública de Alice. En este ejemplo, Eve no ha podido acceder a la llave pública de Alice, por lo que no puede descifrar la información transmitida. Sin embargo, dado que una llave pública puede ser distribuida libremente, tan pronto como Eve la consiga, podrá descifrar cualquier dato cifrado con la llave privada de Alice.

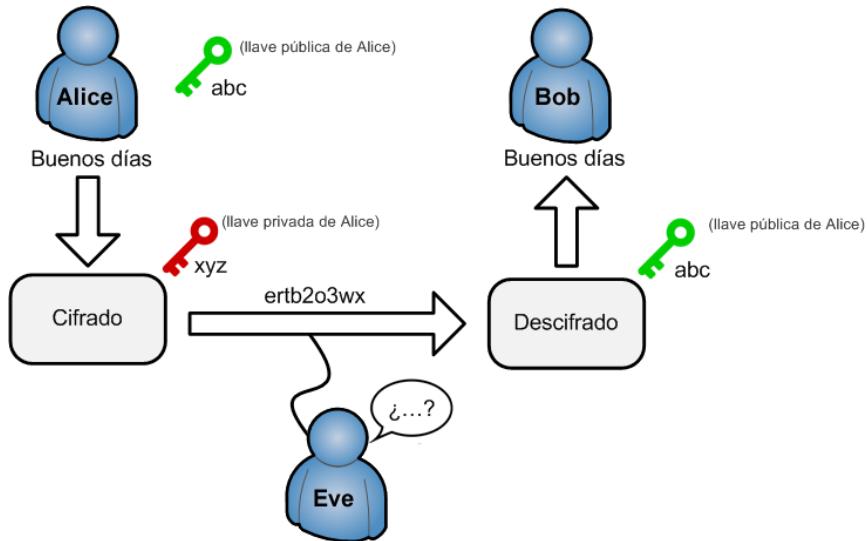


Figura 7. Esquema de cifrado asimétrico utilizando la llave privada para cifrar. Fuente: Elaboración propia.

El ejemplo de cifrado asimétrico explicado es el más relevante para esta investigación, ya que muestra el funcionamiento básico de una firma digital. En él se tiene un alto nivel de certeza de que el mensaje fue emitido por Alice, pues se presume que sólo ella tiene en su poder la llave privada que se utilizó para cifrar los datos recibidos por Bob. Sin embargo, el ejemplo no toma en cuenta factores que deben ser considerados en el mundo real, tales como la suplantación de la identidad del emisor, modificaciones no autorizadas al mensaje o la usurpación de la llave privada (Aguilar et al., 2011).

El esquema de cifrado asimétrico se caracteriza por no tener las limitaciones que el esquema simétrico en cuanto a la gestión de las llaves. La llave pública puede ser distribuida con libertad sin que ello implique que la correspondiente llave privada pueda ser comprometida. Además, la complejidad de gestionar las llaves en redes grandes es considerablemente menor, y el uso de las mismas llaves puede prolongarse incluso por años. Sin embargo, las llaves asimétricas son más grandes que las simétricas, y el poder computacional requerido en los procesos de cifrado y descifrado es mayor que en el esquema simétrico (Menezes, van Oorschot, & Vanstone, 1997).

Según el trabajo de Víquez & Montes (2013), algunos algoritmos criptográficos asimétricos populares son: Diffie-Hellman, RSA, el cifrado ElGamal y la criptografía de curvas elípticas.

2.4. DOCUMENTOS ELECTRÓNICOS

En el contexto de esta investigación, el papel de los documentos electrónicos tiene mucha relevancia debido a su estrecha relación con el uso de la firma digital. Se conoce como documento electrónico a cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático (Gobierno de Costa Rica, 2013). Dicho de otra manera, cualquier conjunto de datos creado, preservado, transmitido o visualizado a través de medios electrónicos, se considera un documento electrónico.

Por otra parte, un documento electrónico firmado digitalmente es aquel documento electrónico, cualquiera que sea su contenido, contexto y estructura, que tiene lógicamente asociada una firma digital (Gobierno de Costa Rica, 2013). En la práctica, no importa si el documento electrónico y la firma digital se encuentran representados por conjuntos de datos diferentes.

Existen distintos formatos que definen la estructura de un documento electrónico firmado digitalmente. Según Aguilar et al. (2011), algunos de estos formatos son: PKCS#7, *Cryptographic Message Syntax* (CMS), CMS *Advanced Electronic Signature* (CAdES), XMLDSig, XML *Advanced Electronic Signature* (XAdES), PDF 1.7 y PDF *Advanced Electronic Signature* (PAdES). Cuando un formato de firma digital permite la selección de atributos opcionales que se pueden incorporar en el contenido de la firma digital para soportar su interoperabilidad en distintos escenarios, se dice que dicho formato soporta la definición de perfiles de firma digital (Aguilar et al., 2011).

La *Política de formatos oficiales de los documentos electrónicos firmados digitalmente* (Gobierno de Costa Rica, 2013) especifica que los formatos y perfiles de firma digital que deben usarse en

Costa Rica son: CAdES-X-L (CAdES *Extended Long Term*), PAdES-LTV (PAdES *Long Term Validation*) y XAdES-X-L (XAdES *Extended Long Term*). Estos formatos se conocen como formatos avanzados, pues definen de manera estandarizada los atributos suficientes para garantizar la verificación de la validez del documento en el tiempo, están auspiciados por una entidad internacional reconocida y sus especificaciones técnicas son de acceso público (Gobierno de Costa Rica, 2013).

La Ley 8454 (Gobierno de Costa Rica, 2005), *Ley de Certificados, Firmas Digitales y Documentos Electrónicos*, define en sus artículos 9 y 10, los principios de valor equivalente, y presunción de autoría y responsabilidad, los cuales otorgan relevancia jurídica a los documentos electrónicos. El primero de los principios mencionados establece que las comunicaciones y documentos suscritos mediante firma digital tienen el mismo valor y eficacia probatoria de su equivalente firmado manuscrito. Por otra parte, el segundo principio indica que todo documento, mensaje electrónico o archivo digital asociado a una firma digital se presumirá, salvo prueba de lo contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.

2.5. FUNCIONES HASH

Las funciones *hash* son un componente fundamental de la criptografía. Una función *hash* es una función computacionalmente eficiente que asocia hileras de *bits* de longitud arbitraria con hileras de *bits* de tamaño fijo, conocidas como valores *hash* o resúmenes (Menezes, van Oorschot, & Vanstone, 1997). Las funciones *hash* criptográficas son funciones *hash* con las siguientes propiedades de seguridad adicionales:

- *La función es de una sola vía*: una función *hash* es de una sola vía si es computacionalmente inviable obtener la hilera de *bits* original a partir de su respectivo resumen; y
- *La función es resistente a colisiones*: una colisión ocurre cuando dos hileras de *bits* diferentes producen el mismo resumen. Una función *hash* es resistente a colisiones si es computacionalmente inviable encontrar dos hileras de *bits* que producen el mismo resumen cuando se les aplica la función (Bishop, 2002).

La calidad de una función *hash* está determinada por la facilidad de encontrar una colisión (Lowagie, 2012). Una vez que esto sucede, la función ya no se considera confiable para utilizarse

como método para diferenciar inequívocamente dos conjuntos de datos distintos (Aguilar et al., 2011), como es el caso de la función MD5 (Lowagie, 2012).

Algunos de los usos comunes de las funciones *hash* son:

- Firmas digitales: durante la creación de una firma digital, por lo general se calcula el resumen de un mensaje extenso, y solamente se firma ese resumen. Esto ahorra tiempo y espacio en comparación con firmar el mensaje directamente; y
- Chequeo de integridad de datos: suponga que el resumen de una entrada de datos se calcula en un punto del tiempo. Ese resumen se almacena, y su integridad es protegida de alguna forma. Posteriormente, se requiere comprobar si los datos han sido alterados o no. Para ello se calcula otro resumen de la entrada de datos que se tiene a mano (que se supone igual a la original), y se compara con el resumen calculado inicialmente. Si los resúmenes no son iguales, se concluye que los datos fueron alterados (Menezes, van Oorschot, & Vanstone, 1997).

2.6. PROCESOS DE CREACIÓN Y VERIFICACIÓN DE UNA FIRMA DIGITAL

Tal como se indicó previamente, la firma digital proporciona servicios de integridad, autenticación y no repudio del firmante. En esta sección se describe de forma simplificada cómo lo anterior se logra a partir de los procesos de creación y verificación de una firma digital.

Para crear una firma digital, el primer paso es calcular un resumen del documento electrónico que se requiere firmar, utilizando una función *hash* resistente a colisiones y de una sola vía. Posteriormente, utilizando la llave privada del firmante, se cifra el resumen obtenido. Ese resumen cifrado del documento electrónico, es la firma digital (Aguilar et al., 2011).

Para verificar la validez de una firma digital previamente creada, se toma esa firma y se descifra utilizando la llave pública del firmante, lo que produce un resumen, que se supone correspondiente 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 resúmenes son iguales, la firma digital se considera válida (Aguilar et al., 2011).

Con base en los procesos previamente descritos, se puede afirmar que una firma digital garantiza tres servicios de seguridad de la información, de la siguiente manera:

- Integridad: la comparación de los resúmenes durante la verificación de una firma digital proporciona la capacidad de detectar modificaciones en el documento electrónico, pues resúmenes distintos estarían asociados a documentos electrónicos diferentes, según las propiedades de las funciones *hash* criptográficas.
- Autenticación: considerando que es posible utilizar la llave pública del firmante para descifrar una firma digital, se puede conocer la identidad de la persona que firmó el documento electrónico.
- No repudio: dada la relación matemática existente entre la llave pública y su correspondiente llave privada, el firmante no puede negar que su llave privada se utilizó para firmar digitalmente el documento electrónico.

Los procesos de creación y verificación de firma digital utilizados en esta sección han sido convenientemente simplificados para explicar su funcionamiento, sin embargo, en aplicaciones del mundo real existen distintos aspectos que aumentan la complejidad de dichos procesos. Por ejemplo, los servicios de autenticación y no repudio señalados anteriormente, se cumplen solamente si existe una forma efectiva y confiable de asociar un par de llaves con una persona o entidad (Aguilar et al., 2011). En la siguiente sección se explica cómo las infraestructuras de llave pública son un mecanismo para lograr ese objetivo.

2.7. INFRAESTRUCTURA DE LLAVE PÚBLICA

Una infraestructura de llave pública (PKI por sus siglas en inglés), es una plataforma de *hardware*, *software*, personas, procesos y políticas que emplean tecnología de firma digital para proveer una asociación verificable entre una llave pública y un suscriptor específico que posee la llave privada correspondiente (Gobierno de Costa Rica, 2006). Las PKI están basadas en la criptografía de llave pública, sin embargo, este esquema de cifrado no posee por sí mismo los elementos suficientes para garantizar que un par de llaves criptográficas están asociadas a una persona, sea física o jurídica. Una PKI está constituida por un conjunto de componentes que permiten llenar ese vacío. En las siguientes subsecciones se explican dichos componentes.

2.7.1. CERTIFICADO DIGITAL

Un certificado digital es un documento electrónico, firmado por un tercero de confianza, que asocia datos de un individuo u organización con su identidad (Buchmann, Evangelos, & Wiesmaier, 2013). Los certificados digitales contienen una llave pública, y suficiente información para verificar que esa llave identifica de forma única a una entidad.

Existen distintos tipos de certificados, tales como certificados de persona física, certificados de agente electrónico o persona jurídica, y certificados de estampado de tiempo.

2.7.2. DISPOSITIVOS CRIPTOGRÁFICOS SEGUROS

Un dispositivo criptográfico seguro, también conocido como módulo seguro de creación de firmas, es un dispositivo que resguarda las llaves y el certificado de un suscriptor, utilizado para generar su firma digital, y que al menos garantiza:

- a. Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;
- b. Que existe una expectativa razonable de que los datos utilizados para la generación de la firma no pueden ser descubiertos por deducción, y la firma está protegida contra falsificación por medio de la tecnología disponible a la fecha, siendo posible detectar cualquier alteración posterior; y
- c. Que los datos utilizados en la generación de la firma pueden ser protegidos de modo fiable por el firmante legítimo, contra su utilización por cualesquiera terceros (Gobierno de Costa Rica, 2006).

Existen distintos tipos de dispositivos criptográficos. Entre ellos sobresalen:

- *Smart Cards o Tarjetas Inteligentes*: son tarjetas plásticas que cuentan con un microprocesador que es capaz de ejecutar operaciones criptográficas. Almacenan llaves privadas, que por lo general son utilizadas dentro de la tarjeta y nunca salen de ella. Para que una tarjeta inteligente funcione, se requiere de un lector, que típicamente se conecta a una computadora a través del puerto USB; y
- *Módulos de Seguridad de Hardware (HSM por sus siglas en inglés)*: son dispositivos de *hardware* que también son capaces de realizar operaciones criptográficas, y suelen usarse para generar números pseudoaleatorios, generar pares de llaves, y cifrar y descifrar datos. Dependiendo del HSM, éste puede conectarse a una computadora utilizando distintas interfaces, tales como PCI, USB o como dispositivo de red (Buchmann, Evangelos, & Wiesmaier, 2013).

2.7.3. USUARIOS FINALES

Son las entidades que se suscriben a la PKI para obtener certificados digitales que les permiten ser identificados dentro de la infraestructura y así ejecutar transacciones. Un usuario final puede ser una

persona física, un servidor, una aplicación, o cualquier otro medio que pueda interactuar con la PKI (Aguilar et al., 2011).

2.7.4. AUTORIDADES CERTIFICADORAS

Una Autoridad Certificadora (CA por sus siglas en inglés) es una entidad, nacional o extranjera, prestadora de los servicios de creación, emisión y operación de certificados digitales (Gobierno de Costa Rica, 2006). Dentro de una PKI, una CA es un tercero de confianza que permite resolver el problema de vincular la identidad de un suscriptor con su respectivo certificado. Lo anterior se logra por medio de un proceso de verificación de la identidad de los solicitantes, y la criptografía de llave pública, pues la CA es responsable de firmar digitalmente los certificados que emite.

2.7.5. AUTORIDADES DE REGISTRO

Una Autoridad de Registro (RA por sus siglas en inglés) es una entidad delegada por la CA para la verificación de la identidad de los solicitantes, y otras funciones dentro del proceso de expedición y manejo de certificados digitales. Representa el punto de contacto entre el usuario y la CA (Gobierno de Costa Rica, 2006). Una vez que el proceso de registro se ha completado exitosamente y el certificado ha sido emitido, se puede tener confianza en que la identidad del suscriptor y la respectiva llave pública están vinculadas de manera única.

2.7.6. REPOSITORIOS

Un repositorio es un sistema para el almacenamiento de información relevante para el funcionamiento de una PKI. En los repositorios se guardan los certificados de llave pública de la CA, la política de certificados y otra información requerida para verificar la validez de los certificados, que se explica más adelante (Kiran, Lareau, & Lloyd, 2002).

2.7.7. RUTAS DE CERTIFICACIÓN

Dentro de una PKI por lo general existe más de una CA. Cuando esto ocurre, las CA se organizan de forma jerárquica. La CA que se encuentra en el primer nivel de esa jerarquía, se conoce como CA Raíz. Las CA que se encuentran en el segundo nivel son autoridades certificadoras subordinadas a la CA Raíz. Estas a su vez pueden tener otras CA subordinadas en un tercer nivel, y así sucesivamente. Una CA en un nivel es responsable de firmar los certificados digitales emitidos para sus CA subordinadas en el nivel inferior.

A partir de lo anterior, surge el concepto de ruta o cadena de certificación, que es una secuencia ordenada de certificados de entidades que, junto con la llave pública de la entidad inicial en la ruta,

pueden ser procesadas para obtener la llave pública de la entidad final (raíz) en la ruta (Gobierno de Costa Rica, 2013).

Las rutas de certificación se utilizan para validar que un certificado digital fue emitido por una CA perteneciente a la jerarquía de autoridades certificadoras de una PKI. Por lo tanto, la llave pública de la CA debe estar disponible a todos los suscriptores de la infraestructura.

2.7.8. LISTAS DE REVOCACIÓN DE CERTIFICADOS (CRL)

Los certificados digitales tienen una fecha de expiración que delimita su periodo de validez. En condiciones ideales, un certificado digital es válido desde la fecha de su emisión hasta su fecha de expiración, a partir de la cual el certificado se considera inválido. Sin embargo, un certificado digital también puede revocarse debido a distintas razones. Por ejemplo, si un suscriptor sabe que su llave privada fue extraviada, debe solicitar que su certificado sea revocado.

Una Lista de Revocación de Certificados (CRL por sus siglas en inglés) es un listado de todos los certificados que han sido revocados y del momento en que se dio su revocación. La CA define un periodo de validez para la CRL, de tal forma que una vez que caduque, debe ser actualizada (Gobierno de Costa Rica, 2013). Por lo tanto, si bien las CRL son un mecanismo para verificar la vigencia de los certificados digitales, existe el riesgo de que certificados revocados se acepten como válidos si la revocación ocurrió después de la última actualización de la CRL (Aguilar et al., 2011).

2.7.9. PROTOCOLO EN LÍNEA DE ESTADO DE CERTIFICADO (OCSP)

El Protocolo en Línea de Estado de Certificado (OCSP por sus siglas en inglés) es un protocolo de implementación de servicios de respuesta en línea del estado de un certificado en el momento en que es solicitado. Este protocolo requiere de comunicación en línea con la autoridad certificadora (Gobierno de Costa Rica, 2013). De esta forma, OCSP no solo es otro mecanismo para verificar la vigencia de los certificados digitales, sino que permite mitigar los riesgos expuestos por las CRL, ya que el estado de los certificados se obtiene en tiempo real.

2.7.10. ESTAMPADO DE TIEMPO

En la sección 2.4 se mencionó que existen formatos de documentos electrónicos firmados digitalmente que garantizan la verificación de la validez del documento en el tiempo, los cuales se denominan formatos avanzados. Para lograrlo, entre otros atributos, se utilizan estampas de tiempo. Una estampa de tiempo es un *token* o cadena de caracteres, que permite relacionar un conjunto de datos con un tiempo concreto, estableciendo así la evidencia de que los datos existían antes de ese

tiempo (Gobierno de Costa Rica, 2013). El manejo de las estampas de tiempo está a cargo de las Autoridades de Estampado de Tiempo (TSA por sus siglas en inglés). Una TSA es un sistema de emisión y gestión de *tokens* de estampado de tiempo, basados en firma digital (Gobierno de Costa Rica, 2013).

El proceso de estampado de tiempo inicia con la aplicación de una función *hash* al dato que se quiere estampar, para luego enviarlo como entrada a la TSA. La TSA obtiene la hora oficial desde una fuente confiable de tiempo, y adjunta esa estampa de tiempo al dato provisto. Finalmente, el resumen calculado y la estampa de tiempo son firmados digitalmente utilizando la llave privada de la TSA, lo que produce un *token* de estampado de tiempo.

El estampado de tiempo es fundamental para permitir el uso de certificados expirados o revocados en la verificación de firmas digitales, siempre que las firmas hayan sido creadas antes de la invalidación de los certificados.

2.7.11. PKI DEL SNCD DE COSTA RICA

Dentro del SNCD de Costa Rica existe una PKI que entrega certificados digitales a los ciudadanos, con el fin de que puedan autenticarse en Internet y firmar documentos digitales con todo respaldo legal (MICITT, 2016). La FIGURA 8 muestra la jerarquía nacional de autoridades certificadoras para la emisión de certificados digitales, cuyos niveles se explican en los siguientes párrafos.

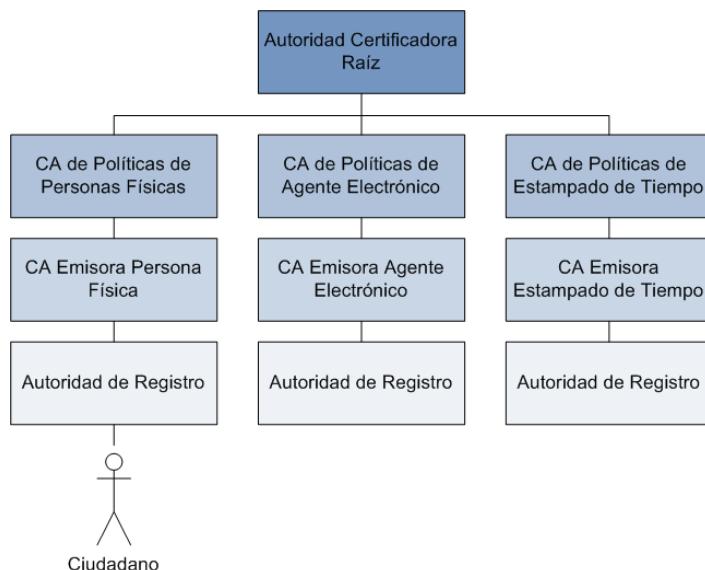


Figura 8. Jerarquía nacional de CAs para la emisión de certificados digitales. Fuente: MICITT (MICITT, 2016).

En el nivel superior de la jerarquía se encuentra la Autoridad Certificadora Raíz, que es custodiada y operada por el BCCR.

En el segundo nivel se encuentran las CA de políticas, subordinadas a la CA Raíz, y utilizadas para segmentar el riesgo según la política de emisión para un tipo de certificado (Gobierno de Costa Rica, 2013). Se distinguen tres tipos de certificados:

- *Certificados de persona física*: son certificados emitidos para que una persona mayor de edad pueda autenticarse en sistemas, o bien firmar digitalmente documentos electrónicos y transacciones, con relevancia jurídica;
- *Certificados de agente electrónico*: son certificados emitidos a sistemas informáticos u otros medios automáticos que realizan transacciones con relevancia jurídica de forma automática, sin intervención humana; y
- *Certificados de estampado de tiempo*: son certificados mediante los cuales una CA puede implementar un sistema de emisión y gestión de estampado de tiempo (MICITT, 2016).

En el tercer nivel se encuentran las CA emisoras, encargadas de emitir certificados digitales a los usuarios finales, y que han sido registradas en el MICITT, el cual reconoce su idoneidad para ejecutar las tareas de emisión y entrega de certificados digitales con un grado adecuado de confianza y seguridad para las partes que interactúan con esos certificados (MICITT, 2016). La primera CA emisora registrada dentro del SNCD es la Autoridad Certificadora del Sistema Nacional de Pagos Electrónicos (CA SINPE), implementada por el BCCR, y en funcionamiento desde el año 2009 (Aguilar et al., 2011).

Finalmente, se encuentran las RA, encargadas de distribuir los certificados digitales emitidos por las CA registradas (MICITT, 2016). En el caso de la CA SINPE, existen 16 entidades financieras y de gobierno autorizadas para entregar certificados oficiales, operando 42 oficinas distribuidas en todas las provincias de Costa Rica (BCCR, 2014).

2.8. TIPOS DE FIRMA DIGITAL

En la literatura internacional, principalmente en la europea, es posible distinguir diferentes tipos de firma digital, según su valor jurídico. En la directriz 1999/93/EC (The European Parliament, 1999), se definen tres tipos de firma digital, que se explican en las siguientes subsecciones.

2.8.1. FIRMA DIGITAL SIMPLE

La firma digital simple se define como datos en forma electrónica anexos a otros datos, o asociados de manera lógica con ellos, utilizados como medio de autenticación (The European Parliament, 1999). Este tipo de firma también se conoce como firma digital débil o firma digital liviana, y aunque permite vincular el documento electrónico firmado con la persona que tiene posesión de la llave privada requerida para crear la firma digital, no garantiza que esa persona sea el dueño de esa llave privada (Mazzeo, 2010).

2.8.2. FIRMA DIGITAL AVANZADA

La firma digital avanzada es aquella que cumple con los siguientes requisitos:

- Está vinculada al firmante de manera única;
- Permite la identificación del firmante;
- Ha sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; y
- Está vinculada a los datos relacionados, de modo que cualquier cambio ulterior de los mismos sea detectable (The European Parliament, 1999).

Una firma digital avanzada tiene un valor jurídico mayor que una firma digital simple, pues además de garantizar autenticación de origen, también garantiza la integridad de los datos (Mazzeo, 2010). Adicionalmente, es capaz de vincular el documento electrónico firmado no solo con el custodio de la llave privada requerida para crear la firma digital, sino también con su dueño (Aguilar et al., 2011).

2.8.3. FIRMA DIGITAL CALIFICADA

Este tipo de firma digital, también es conocido como firma digital avanzada basada en certificados calificados y creada con un dispositivo seguro de creación de firma, firma digital fuerte o firma digital segura. Todos los elementos requeridos para crear firmas digitales calificadas, tales como llaves criptográficas, *software*, dispositivos criptográficos seguros, etcétera, deben utilizar los últimos avances tecnológicos disponibles (Mazzeo, 2010). Las firmas digitales calificadas tienen las características de una firma digital avanzada, y adicionalmente:

- Se han creado utilizando un dispositivo criptográfico seguro que garantiza que la extracción y reproducción de la llave privada no es posible en un tiempo razonable.
- Se han creado utilizando certificados digitales calificados, los cuales deben contener:

- Una indicación de que el certificado se emitió como un certificado calificado;
- La identificación de la CA que emitió el certificado y del Estado en el que se encuentra establecida;
- El nombre y los apellidos del firmante, o un pseudónimo que conste como tal;
- Un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado;
- Los datos de verificación de firma que corresponden con los datos de creación de firma que están bajo control del firmante;
- Una indicación relativa al comienzo y fin del periodo de validez del certificado;
- El código de identificación del certificado;
- La firma digital avanzada de la CA que expide el certificado;
- Los límites de uso del certificado, si procede; y
- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede (The European Parliament, 1999).

Las firmas digitales calificadas tienen el valor jurídico más alto, pues garantizan autenticación, integridad, confidencialidad y no repudio (Mazzeo, 2010). En Costa Rica, las firmas digitales creadas bajo el amparo del SNCD cumplen con los requisitos establecidos anteriormente para las firmas digitales calificadas. Por lo tanto, en este documento, cuando se hace referencia a la creación o verificación de una firma digital, se hace alusión a este tipo de firma.

3. ESTADO DEL ARTE

Este capítulo describe el estado del arte a nivel internacional en cuanto a soluciones a nivel país para validar la seguridad de la información en aplicaciones de *software* que implementan firma digital. Se muestra una revisión de documentación internacional recopilada de diez países más la Unión Europea, ordenada según la relevancia de las soluciones que se analizaron.

3.1. FRANCIA

En Francia, la firma electrónica está regulada por el Código Civil. La sección 1316-4 de dicho código reconoce la firma electrónica como legal y aplicable, mientras que la Sección 1316-1 le otorga la misma equivalencia jurídica que la firma manuscrita (Gobierno de Francia, 2016).

En este país existe documentación para la certificación de aplicaciones que implementan firma digital, para procesos de creación y verificación de firma. Dichos documentos se describen a continuación:

- *Protection Profile Electronic Signature Creation Application*: este documento corresponde a un Perfil de Protección desarrollado según lo estipula *Common Criteria* (Agence Nationale de la Sécurité des Systèmes d'Information, 2008). En él se especifican los requisitos de seguridad para las aplicaciones de creación de firma electrónica. Este perfil de protección resguarda los siguientes activos de información:
 - El documento que será firmado.
 - Las representaciones derivadas del documento dentro de la aplicación.
 - El resumen del documento.
 - El documento firmado.
 - La política de firma utilizada.
 - El código ejecutable de la aplicación.
 - Datos que a lo interno de la aplicación tienen un formato distinto que el mostrado al usuario.
 - La asociación entre la aplicación y la aplicación externa usada para mostrar el documento al usuario.
- *Protection Profile Electronic Signature Verification Module*: este documento corresponde a otro Perfil de Protección desarrollado según lo estipula *Common Criteria* (Agence Nationale de la Sécurité des Systèmes d'Information, 2008). En él se especifican los requisitos de seguridad

para las aplicaciones de verificación de firma electrónica. Este perfil de protección resguarda los siguientes activos de información:

- El documento cuyas firmas serán verificadas.
- Las firmas contenidas en el documento.
- Atributos adicionales firmados en el documento.
- Datos de validación (datos que son útiles para verificar las firmas) incluidos en el documento.
- El resumen del documento firmado.
- El resultado de la verificación.
- El código ejecutable de la aplicación.
- Las políticas de firma aplicadas.
- Datos que a lo interno de la aplicación tienen un formato distinto que el mostrado al usuario.
- Asociación entre la aplicación y la aplicación externa usada para mostrar el documento al usuario.

3.2. ESPAÑA

En España, la ley de firma digital 59/2003 del 19 de diciembre del 2003 es la que regula la utilización de la firma digital y los certificados digitales en ese país. En ella se definen las obligaciones que debe cumplir cualquier proveedor de servicios de certificación, así como las infracciones y sanciones que se les impondrá cuando algún criterio sea incumplido (Gobierno de España, 2003).

Como complemento a la ley de firma digital, existe la “Política de Firma Electrónica y de Certificados de la Administración General del Estado” del 30 de mayo del año 2012, que tiene como principal objetivo establecer un conjunto de criterios comunes asumidos por la Administración General del Estado y sus organismos públicos, en relación con la autenticación y la firma electrónica (Administración General del Estado, 2012).

En España existe documentación para la certificación de aplicaciones que implementan firma digital, para procesos de creación y verificación de firma. Dichos documentos se describen a continuación:

- PPSCVA-T1, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante y nivel de evaluación de los requisitos de seguridad EAL1: este documento corresponde a un Perfil de Protección desarrollado según lo estipula Common Criteria (Instituto Nacional de Tecnologías de la Comunicación, 2009). En él se especifican los requisitos de seguridad para las aplicaciones de creación y verificación de firma electrónica, que se deben usar con el Documento Nacional de Identificación (DNI-e) como dispositivo seguro de creación de firma.

Este perfil de protección resguarda los siguientes activos de información:

- El documento del firmante, sus representaciones derivadas, y la integridad de todos los datos de usuario necesarios para las operaciones de creación o verificación de firma.
- La funcionalidad de la aplicación, de manera que se garantice que su comportamiento fiable no se puede modificar.
- Los datos de verificación de autenticación, que se transmiten al DNI-e para la realización de la operación de firma.

Asimismo, especifica los siguientes objetivos de seguridad de la aplicación:

- Garantizar la integridad de los datos que serán firmados, así como de todos los datos de usuario necesarios para la creación o verificación de las firmas electrónicas.
- Garantizar la confidencialidad de los datos de autenticación en el dispositivo criptográfico seguro, de manera que se garantice a su titular legítimo el control exclusivo de la funcionalidad de firma del DNI-e.
- Garantizar la integridad de la aplicación, de manera que su funcionalidad no se pueda comprometer.
- Definir un conjunto de formatos de documento electrónico que sean representables de manera no ambigua, y limitar la capacidad de firma a los documentos basados en estos formatos.
- Incluir un visor seguro de documentos, que detecte y rechace cualquier información oculta o de representación ambigua.
- Los algoritmos criptográficos que utilice la aplicación, así como el certificado seleccionado para crear o verificar una firma deberán ser tales que se verifiquen y produzcan firmas reconocidas con el DNI-e.
- La aplicación avisará al firmante sobre el hecho de que datos suyos de carácter personal se incluyen en la firma, tal como la realiza el DNI-e.

- PPSCVA-T1, EAL3. Perfil de Protección la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante y con nivel de evaluación de los requisitos de seguridad EAL3: este documento corresponde a otro Perfil de Protección, similar al PPSCVA-T1, EAL1 (Instituto Nacional de Tecnologías de la Comunicación, 2009). Este perfil protege los mismos activos de información que el descrito anteriormente y establece los mismos objetivos de seguridad de la aplicación, más uno:
 - La aplicación se diseñará y desarrollará implementando suficientes características de auto-protección, separación de dominios, y defensa frente a las amenazas definidas, de manera que proteja los activos definidos en combinación con los requisitos funcionales de seguridad aplicables.
- PPSCVA-T2, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL1: este documento corresponde a otro Perfil de Protección (Instituto Nacional de Tecnologías de la Comunicación, 2009). Protege los mismos activos de información y establece los mismos objetivos de seguridad que el perfil PPSCVA-T1, EAL1. Sin embargo, el tipo de aplicación evaluada se denomina Tipo 2, lo que significa que la aplicación no incluye todo el *hardware, firmware* y *software* necesario para realizar la funcionalidad, sino que utiliza una plataforma de propósito general que es confiable (por ejemplo, una computadora personal con un sistema operativo de propósito general), incluyendo la interfaz necesaria con el firmante.
- PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3: este documento define otro Perfil de Protección (Instituto Nacional de Tecnologías de la Comunicación, 2009). Protege los mismos activos de información y establece los mismos objetivos de seguridad que el perfil PPSCVA-T1, EAL3, y corresponde a aplicaciones Tipo 2, como se indica para el perfil PPSCVA-T2, EAL1.

3.3. BRASIL

En agosto del año 2001, se publicó en Brasil la “*Medida Provisória No 2.200-2, de 24 de Agosto de 2001*” (Presidência da República, 2001), por medio de la cual se establece la creación de la infraestructura de llave pública brasileña, conocida como ICP-Brasil, con la intención de garantizar la autenticidad, integridad y validez jurídica de los documentos en formato electrónico, aplicaciones

de soporte técnico y aplicaciones que utilizan certificados digitales, así como el aseguramiento de transacciones electrónicas.

En Brasil existe documentación para la homologación de aplicaciones que implementan firma digital, para procesos de creación y verificación de firma, y autenticación. Dichos documentos se describen a continuación:

- *Manual de Condutas Técnicas 4 - Volume I Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Assinatura Digital no Âmbito da ICP-Brasil*: este manual establece los requisitos técnicos necesarios para un proceso de homologación que permite garantizar la interoperabilidad y seguridad desde la perspectiva de la información de *software* que implementa firma digital (ICP-Brasil, 2007).

Durante el proceso de homologación, los requisitos técnicos que figuran en este manual deben ser cumplidos. Dichos requisitos son evaluados mediante la ejecución de pruebas, las cuales deben ir acompañadas con documentación que es requerida.

El ámbito de aplicación de las normas técnicas y la evaluación de *software* de firma digital se aplica a los siguientes componentes de *software* que realizan:

- La manipulación y comprobación del estado de revocación de los certificados digitales.
- Manipulación de contraseñas y datos sensibles.
- Generación y verificación de la firma digital de documentos electrónicos.
- Generación de mensajes de correo electrónico firmados digitalmente.
- Verificación de la autoría de los mensajes de correo electrónico.

El resultado del proceso de homologación de *software* de firma digital informa el cumplimiento de los requisitos técnicos establecidos en este manual.

- *Manual de Condutas Técnicas 4 - Volume II Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de Assinatura Digital no Âmbito da ICP-Brasil*: este documento describe los procedimientos de ensayo que deben ser aplicados en el proceso de homologación del *software* de firma digital dentro de la infraestructura de llave pública brasileña (ICP-Brasil, 2007).

Dichas pruebas se refieren al conjunto de métodos que se utilizan para evaluar si el *software* de firma digital está o no conforme con los requisitos técnicos establecidos por el *Manual de Condutas Técnicas 4 - Volume I*.

- *Manual de Condutas Técnicas 5 - Volume I Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Autenticação no Âmbito da ICP-Brasil*: de forma similar al manual para homologación de *software* de creación y verificación de firma digital, este manual establece los requisitos técnicos necesarios para un proceso de homologación que permite garantizar la interoperabilidad y seguridad desde la perspectiva de la información de *software* de autenticación (ICP-Brasil, 2007).

Durante el proceso de homologación, los requisitos técnicos que figuran en este manual deben ser cumplidos. Dichos requisitos son evaluados mediante la ejecución de pruebas, las cuales deben ir acompañadas con documentación que es requerida.

El ámbito de aplicación de las normas técnicas y la evaluación de *software* de firma digital se aplica a los siguientes componentes de *software* que realizan:

- La manipulación y comprobación del estado de revocación de los certificados digitales.
- Manipulación contraseñas y datos sensibles.
- Autenticación de cliente y servidor.
- Autenticación de usuario.

El resultado del proceso de homologación de *software* de autenticación informa el cumplimiento de los requisitos técnicos establecidos en este manual.

- *Manual de Condutas Técnicas 5 - Volume II Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de Autenticação no Âmbito da ICP-Brasil*: de forma similar al caso de creación y verificación de firma digital, este documento describe los procedimientos de ensayo que deben ser aplicados en el proceso de homologación del *software* de autenticación dentro de la infraestructura de llave pública brasileña (ICP-Brasil, 2007).

Dichas pruebas se refieren al conjunto de métodos que se utilizan para evaluar si el *software* de autenticación está o no conforme con los requisitos técnicos establecidos por el *Manual de Condutas Técnicas 5 - Volume I*.

3.4. ALEMANIA

La ley de firma digital en Alemania fue publicada el 16 de mayo del año 2001. Conocida como SigG, en ella se establecen los aspectos generales que regulan la firma digital en ese país. Esta ley define los requerimientos generales que deben cumplir las autoridades certificadoras que emiten certificados digitales. También establece la existencia de una Autoridad Competente, encargada de

acreditar a las autoridades certificadoras. El ente designado como Autoridad Competente es la *Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway* (Bundesnetzagentur en alemán) (Federal Gazette, 2001).

Como complemento a la ley, en noviembre del año 2001 se decretó un reglamento de firma digital, conocido como *SigV*. En él se brindan más detalles acerca de cómo debe implementarse lo estipulado por la ley de firma digital.

En Alemania, la Oficina Federal para la Seguridad de la Información (BSI en alemán), funge como la autoridad encargada de promover la seguridad en tecnologías de la información en ese país.

La BSI publica en su sitio *web* listas de productos que han sido certificados en diversas áreas, por ejemplo, firma digital (Federal Office for Information Security, 2016). Según la BSI (Federal Office for Information Security, 2012) confirmar que algún producto está conforme a la *SigG* requiere que éste sea evaluado de acuerdo con un procedimiento de certificación según los requerimientos de *Common Criteria*. Dicho procedimiento de certificación toma en cuenta las necesidades especiales de la *SigG* y el *SigV* respecto a la funcionalidad, el alcance y el nivel de la evaluación. La BSI recomienda el uso adecuado de perfiles de protección, sin embargo, durante la revisión de la documentación de este país no fue posible tener acceso a alguno de ellos.

3.5. UNIÓN EUROPEA

En diciembre del año 1999 la Unión Europea publicó la Directiva 1999/93/CE (The European Parliament, 1999), por medio de la cual se estableció el marco jurídico a nivel europeo para regular la firma electrónica, con el fin de facilitar su utilización y contribuir a su reconocimiento legal en todos los países miembros de la comunidad. Adicionalmente, la directiva se centró en la regulación de los proveedores de servicios de certificación mediante la definición de requisitos comunes que garantizan el reconocimiento transfronterizo de las firmas electrónicas y los certificados en la Unión Europea.

La Unión Europea no cuenta con una solución que permita certificar aplicaciones que utilizan firma digital a nivel comunitario. Sin embargo, el Comité Europeo de Estandarización (CEN por sus siglas en inglés) ha desarrollado una serie de *workshop agreements*, en apoyo a la Directiva 1999/93/CE, los cuales, a pesar de no haber sido acogidos como estándares europeos, están ampliamente relacionados con la firma electrónica, y han servido como base para el desarrollo de

soluciones de certificación en países como España y Francia. Dichos documentos se describen a continuación:

- *CWA 14170 Security requirements for signature creation applications*: especifica requisitos de seguridad y recomendaciones para el desarrollo de aplicaciones para la creación de firmas electrónicas. El documento provee un modelo funcional para aplicaciones que crean firmas electrónicas, especifica requisitos de seguridad para los componentes de ese modelo, excluyendo el dispositivo criptográfico seguro (European Committee for Standardization, 2004).
- *CWA 14171 General guidelines for electronic signature verification*: identifica los requisitos de seguridad para los distintos elementos de un sistema de verificación de firma electrónica. También identifica aquellos datos que necesitan ser capturados y archivados de manera que puedan ser utilizados más tarde para arbitraje, en caso de producirse una disputa entre un firmante y un verificador (European Committee for Standardization, 2004).

3.6. BÉLGICA

En Bélgica, las firmas electrónicas son reconocidas legalmente como resultado de la publicación de las actas del 20 de octubre del año 2000 y del 9 de julio de 2001, las cuales acatan los requerimientos estipulados por la Directiva 1999/93/CE de la Unión Europea (Vandendriessche, 2004).

A partir de los doce años, todo ciudadano belga es portador de un documento de identidad oficial, conocido como *eID*, que cuenta con un chip criptográfico donde se almacenan sus certificados digitales para autenticación y firma digital (Fedict, 2015). Debido a lo anterior, el Servicio Público Federal de Tecnología de Información y Comunicación (Fedict) se ha enfocado en velar por el crecimiento del número de aplicaciones que hacen uso del *eID*, así como en mejorar la calidad de las mismas. Se ha puesto a disposición de la comunidad informática el siguiente conjunto de piezas de *software*: *eID Software*, *eID Applet*, *eID Identity Provider*, *Digital Signature Service* y *Quick Key Toolset*, las cuales forman la base para aplicaciones que utilizan *eID*.

En este país no hay una solución para certificar aplicaciones que implementan firma digital, sino que se ha utilizado un enfoque de código abierto que permite a desarrolladores y otras partes interesadas ver el código fuente y hacer sugerencias para mejorarlo (Fedict, 2015). En adición a

ello, Fedict ha producido guías de desarrollo que contienen directrices para la creación de aplicaciones que utilizan *eID* por medio de ejemplos (Fedict, 2015).

3.7. RUSIA

En Rusia, la firma digital ha estado regulada desde el año 2002, cuando se promulgó la Ley 1-F3 (Gobierno de Rusia, 2002). Sin embargo, dicha ley presentaba deficiencias graves, entre las que se pueden citar:

- Falta de claridad acerca de las transacciones que podían hacer uso de la firma electrónica;
- Existía un proceso muy complejo para que el gobierno certificara la tecnología requerida para que una firma electrónica fuera reconocida como válida ante la ley;
- Hasta el año 2005, la ley no contemplaba un proceso para obtener una licencia que permitiera fungir como proveedor de servicios de certificación;
- Solamente las personas físicas podían tener certificados digitales;
- No se establecía con claridad las responsabilidades de una autoridad certificadora ante daños y perjuicios causados por el mal manejo de los certificados digitales; y
- No se menciona la obligación de las autoridades certificadoras de mantener en secreto las llaves privadas de sus usuarios (Naumov & Nikiforova, 2005).

Debido a lo anterior, el 6 de abril del año 2011 se hizo una enmienda a la Ley 1-F3, mediante la publicación de la Ley 63-FZ (Gobierno de Rusia, 2011). En ella se establecen, entre otros, aspectos como:

- La definición de dos tipos de firma electrónica: simples y reforzadas. Estas últimas a su vez pueden ser reconocidas o no reconocidas.
- Las condiciones en las que una firma electrónica es equivalente a la firma manuscrita.
- Las obligaciones de las partes involucradas en el intercambio de documentos electrónicos.
- Las responsabilidades de las autoridades certificadoras y los usuarios.
- Los requisitos para la emisión de certificados digitales.

La notificación FSS (notificación del Servicio Federal de Seguridad) es una notificación obligatoria para el registro de programas o dispositivos de *hardware* utilizados para el cifrado de datos. La notificación FSS es necesaria para distintos dispositivos (*hardware* y *software*) con funciones criptográficas, entre los que se incluye *software* de cifrado (Certificate.Net, 2015). En el desarrollo

de la presente revisión literaria, no se pudo identificar el conjunto de requisitos técnicos necesarios para obtener la certificación FSS, ni se pudo identificar alguna otra solución a nivel país para certificar aplicaciones que implementan firma digital.

3.8. DINAMARCA

En Dinamarca, la firma digital y la firma manuscrita tienen valor jurídico equivalente desde mayo del año 2000, cuando se publicó la “Ley de firma electrónica” (Ministry of Finance, 2000).

En este país no existe una solución para certificar aplicaciones que utilizan firma digital a nivel país, desde la perspectiva de la seguridad de la información. Sin embargo, se ha creado un proyecto de código abierto llamado *OpenSign* mediante el cual se implementa funcionalidad para la creación de firma digital y autenticación usando certificados x.509, pero deja fuera de su alcance la verificación de firmas digitales. *OpenSign* se encuentra actualmente en producción y es utilizado por al menos 10 organizaciones en territorio danés (OpenOCES, 2014).

3.9. CHILE

En abril del año 2002 se publicó en Chile la Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (Gobierno de Chile, 2002). Modificada posteriormente en el año 2007 (Gobierno de Chile, 2007), esta ley establece, en su artículo 7, que los actos, contratos y documentos de los órganos del Estado que sean suscritos de forma electrónica tendrán el mismo respaldo jurídico que sus equivalentes realizados en papel.

Adicionalmente, en su artículo 2, especifica el reconocimiento de dos tipos de firma:

- *Firma electrónica*: cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar al menos formalmente a su autor; y
- *Firma electrónica avanzada*: aquella firma certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría (Gobierno de Chile, 2002).

En Chile existen varias normas técnicas en materia de seguridad de la información, tales como:

- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información;
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model;
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2001);
- NCh.2820/1.Of2003 Tecnología de la información – Técnica de seguridad – Criterio de evaluación de la seguridad de TI – Parte 1: Introducción y modelo general; y
- NCh2829.Of.2003 Tecnología de la Información – Requisitos de Seguridad para Módulos Criptográficos (Entidad Acreditadora, 2016).

Sin embargo, no hay una solución a nivel país para la certificación de aplicaciones que implementan firma digital, desde la perspectiva de la seguridad de la información.

3.10. COLOMBIA

En Colombia, la firma digital está regulada por la Ley 52 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones (Congreso de Colombia, 1999). Dicha ley establece la equivalencia jurídica de la firma manuscrita y la firma digital si ésta última cumple con los siguientes requisitos:

- Es única a la persona que la usa.
- Es susceptible de ser verificada.
- Está bajo el control exclusivo de la persona que la usa.
- Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada.
- Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

En el año 2012 se publicó el DECRETO 2364 DE 2012 Por medio del cual se reglamenta el artículo 7º de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones (Gobierno de Colombia, 2012), por medio del cual se reglamenta el uso de firmas electrónicas.

En este país, tanto las firmas digitales como las firmas electrónicas son reconocidas, y aunque ambas pueden eventualmente producir los mismos efectos jurídicos, la diferencia es probatoria: mientras la firma digital incorpora automáticamente la autenticidad, integridad y no repudio, en la

firma electrónica es necesario probarlas, y se debe determinar que se trata de un mecanismo confiable y apropiable (Colombia Digital, 2015).

En el desarrollo de la presente revisión literaria, no se pudo identificar al menos una solución a nivel país para la certificación de aplicaciones que implementan firma digital, desde la perspectiva de la seguridad de la información.

3.11. MÉXICO

En México, hasta hace pocos años no había una ley que regulara el uso de la firma digital, sino que se contaba con una serie de normas y modificaciones al Código de Comercio para controlar su uso (Sistema Integral de Gestión Registral, 2008). Sin embargo, en el año 2012 entró en vigencia la Ley de Firma Electrónica Avanzada (Congreso General de los Estados Unidos Mexicanos, 2012). Dicha ley otorga a la firma electrónica avanzada el mismo valor jurídico que la firma manuscrita, y especifica los requisitos necesarios para que ello se cumpla.

En el año 2014 se publicó el Reglamento de la Ley de Firma Electrónica Avanzada (Gobierno de México, 2014), cuyo principal objetivo es establecer las normas reglamentarias para el uso de la Firma Electrónica Avanzada y los servicios relacionados con ésta.

En el desarrollo de la presente revisión literaria, no se pudo identificar al menos una solución a nivel país para la certificación de aplicaciones que implementan firma digital, desde la perspectiva de la seguridad de la información.

3.12. APPLICABILIDAD DE LAS SOLUCIONES IDENTIFICADAS

La revisión de la literatura desarrollada en esta sección ha permitido encontrar soluciones operativas a nivel internacional cuyos objetivos son similares a los planteados en la presente investigación. Se han identificado aspectos de seguridad relevantes que deben ser tomados en cuenta como parte de un proceso de aseguramiento de la información de aplicaciones de *software* que implementan mecanismos de firma digital, tales como:

- La gestión y el uso de los certificados digitales.
- La integridad de la información.
- La confidencialidad de las credenciales requeridas para acceder a los dispositivos criptográficos seguros.

Sin embargo, aplicar en nuestro país las soluciones identificadas internacionalmente no es viable de momento, pues en Costa Rica no existe una definición de los requisitos de seguridad para aplicaciones de *software* que implementan mecanismos de firma digital. Al no haber un punto de comparación, no es posible determinar si lo que otros países han implementado es aplicable en nuestro contexto. Por lo tanto, antes de tomar en consideración las soluciones provenientes de otros países, es necesario definir las pautas nacionales, a lo cual esta investigación contribuye.

4. METODOLOGÍA

En este capítulo se detallan las estrategias seleccionadas para cumplir con los objetivos definidos en esta investigación. Se inicia con la definición de los objetivos de seguridad generales que delimitan este trabajo. Después, se presentan las tareas realizadas para analizar los escenarios de firma digital sujetos al proceso de aseguramiento de la información. La metodología continúa con la descripción del proceso de identificación y valoración de riesgos. Posteriormente, se definen las actividades relacionadas con la definición de políticas de seguridad de la información y el establecimiento de controles de seguridad. Finalmente, se explican las acciones ejecutadas para desarrollar una guía que permite evaluar el aseguramiento de la información en aplicaciones que implementan firma digital. La FIGURA 9 muestra los pasos de la metodología seleccionada.



Figura 9. Diagrama resumen de los pasos de la metodología. Fuente: Elaboración propia.

4.1. DEFINICIÓN DE OBJETIVOS DE SEGURIDAD

Para definir una metodología que permita el desarrollo de un proceso de aseguramiento de la información, es importante establecer los objetivos de seguridad que se pretende conseguir, pues ellos son necesarios para delimitar el proceso.

Dado que la confianza es uno de los activos más importantes en el contexto del SNCD, el principal objetivo de seguridad de este proyecto es preservar el no repudio de la información dentro de dicho sistema, de manera que exista la certeza de que una entidad no puede negar que ejecutó una acción que sí realizó. En el contexto de las aplicaciones de *software* que implementan firma digital dentro del SNCD, esto significa garantizar, desde la perspectiva tecnológica, que nadie pueda argumentar que no firmó digitalmente un documento electrónico que sí firmó, o bien negar que se autenticó en un sistema por medio de su certificado digital, cuando en realidad sí lo hizo.

Para alcanzar lo anterior, esta investigación hace énfasis en la identificación de situaciones en las que el no repudio de la información se ve amenazado de forma directa, tal como se mostró en el ejemplo descrito en la sección 1.2, en el cual una entidad utiliza una herramienta que hace uso de funciones *hash* consideradas inseguras porque son susceptibles a colisiones.

Sin embargo, el no repudio también puede verse afectado de forma indirecta, a través de otros servicios de seguridad de la información. Por ejemplo, suponga que un usuario va a firmar digitalmente un documento. El documento se le muestra tal cual es, pero justo después de que el usuario da la instrucción de firmarlo, una aplicación maliciosa instalada en la máquina que calcula el resumen del documento altera la integridad de éste, cambiando su contenido. En un caso como el anterior, aun cuando la firma digital se haya creado con algoritmos considerados seguros, el usuario puede argumentar que le cambiaron el contenido del documento que creyó estar firmando. Esto constituye una afectación indirecta al servicio de no repudio, a través de un cambio en la integridad de los datos. En esta investigación, también se toman en cuenta este tipo de circunstancias, asociadas principalmente a los servicios de integridad, autenticación y confidencialidad.

Por otra parte, no se consideran escenarios relacionados con el servicio de disponibilidad, pues su relación con el no repudio de la información es mínima.

4.2. ANÁLISIS DE ESCENARIOS DE FIRMA DIGITAL

Esta sección describe la metodología utilizada para el análisis de los escenarios de firma digital sujetos al proceso de aseguramiento de la información. En este paso de la investigación, se llevaron a cabo dos actividades: la selección de los escenarios para ser analizados, y la definición de la funcionalidad mínima que cada escenario requiere para ser completado exitosamente. Las siguientes subsecciones describen cada una de las actividades ejecutadas.

4.2.1. SELECCIÓN DE ESCENARIOS

La selección de los escenarios no es arbitraria, sino que ha sido necesario consultar fuentes de información que permitan determinar los escenarios relevantes. Las fuentes seleccionadas se describen a continuación:

- *Directriz 067-MICITT-H-MEIC* (Gobierno de Costa Rica, 2014): directriz emitida por el Gobierno de Costa Rica, en la que se les ordena a las instituciones del sector público costarricense que lleven a cabo las medidas técnicas y financieras necesarias para masificar e implementar el uso de la firma digital.

- *Criterio experto de profesionales:* integrantes de la DCFD y del Área de Seguridad de la División de Servicios Tecnológicos del BCCR dieron su opinión acerca de los escenarios que consideraron relevantes en este contexto.

Una vez recopilada la información necesaria, el siguiente paso es la elaboración de una lista definitiva de los escenarios que deben ser analizados.

4.2.2. DEFINICIÓN DEL PRODUCTO MÍNIMO VIABLE PARA CADA ESCENARIO

En esta investigación, un producto mínimo viable (MVP por sus siglas en inglés) es un conjunto de requerimientos funcionales mínimos que deben implementarse para que cada escenario de firma digital seleccionado se complete exitosamente. La funcionalidad básica que cada escenario debe incorporar se determina aplicando un método analítico-sintético, en el cual, el objeto de estudio se descompone para estudiar cada una de sus partes, y luego, todas ellas se reintegran para comprender la esencia del mismo (Del Río Sánchez , 2014). Dentro del presente contexto, este método se aplica de la siguiente manera:

- Al conocer las generalidades de un escenario, es posible dividirlo en componentes más pequeños que ayudan a entender su funcionamiento.
- Por ejemplo, sabiendo de antemano que el escenario de creación de firma digital inicia con un documento electrónico que debe firmarse, y finaliza con un documento electrónico firmado digitalmente, dicho escenario se puede descomponer en partes más pequeñas, que representan el conjunto mínimo de pasos que permiten llevar el documento electrónico desde su estado inicial hasta su estado final.
- Finalmente, se procede a relacionar e integrar los pasos identificados, con el fin de comprender la funcionalidad básica resultante como un todo.

En este procedimiento es ideal que la descripción de los pasos sea lo más granular posible, pero que se mantengan en un nivel lo suficientemente alto como para especificar el “qué” debe hacerse, sin hacer referencia al “cómo”. Con ese enfoque se aplica el principio de neutralidad tecnológica, lo que es apropiado para aplicar un análisis que no depende de detalles de implementación.

4.3. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

Esta sección describe la metodología utilizada para la identificación y valoración de riesgos. En ella se aplica una combinación de estándares, mejores prácticas y técnicas utilizadas en la industria. En las siguientes subsecciones se describe cada uno de los pasos requeridos.

4.3.1. MODELADO DEL SISTEMA

Una forma conveniente y efectiva de iniciar un proceso de análisis de riesgos es realizar una caracterización del sistema que será analizado, haciendo un inventario de los componentes y las fronteras del mismo, así como de los datos sensibles que se desea proteger (Virginia Information Technologies Agency, 2006). En este trabajo, para modelar un sistema que implementa firma digital dentro del SNCD se utiliza un *infosec-tree*. Existen dos razones fundamentales para hacerlo:

- El patrón del todo y las partes permite el análisis sistémico de una aplicación de software, pues los nodos pueden representar módulos o componentes de la aplicación, en cualquier nivel. Esto facilita el análisis de la seguridad de diferentes aplicaciones de *software* utilizando una metodología consistente; y
- El objeto de evaluación puede componerse de *hardware*, *software* o una mezcla de ellos, y puede ser de cualquier tamaño. Esto habilita de una forma homogénea la definición de un proceso de aseguramiento que abarca una aplicación de *software* y su infraestructura tecnológica (Villalón-Fonseca, Mora-Castro, Bartels-González, Carballo-Chavarría, & Marín-Raventós, 2016).

El árbol resultante de este proceso se basa en el producto mínimo viable obtenido para cada escenario previamente analizado. Dicha estructura jerárquica representa un modelo de referencia, cuyos componentes son el factor común de cualquier aplicación de *software* de este tipo dentro del SNCD, tanto existente como futura.

A partir del *infosec-tree* creado, es posible identificar y caracterizar los componentes relevantes cuya información debe ser asegurada. Se utilizan los diagramas de flujos de información para analizar la forma en que ésta es transmitida a través de los componentes del sistema, de manera que se puedan conocer los recursos que son sujetos de riesgo, y que, por lo tanto, deben ser protegidos. Esta técnica permite tener un proceso de aseguramiento de la información sistemático, ya que es posible iterar de forma ordenada sobre todos los componentes del sistema, así como a través de los canales de comunicación existentes entre ellos.

El modelo original del *Infosec-Tree* está diseñado para definir controles de seguridad, sin embargo, la estructura puede extenderse de forma natural para soportar componentes adicionales de un proceso de aseguramiento de la información (Villalón-Fonseca, Mora-Castro, Bartels-González, Carballo-Chavarría, & Marín-Raventós, 2016). Dado que las tríadas del modelo *Infosec-Tree* representan lugares del sistema en los cuales la información se localiza, es posible utilizarlas para identificar puntos en los que ésta puede ser vulnerable. En este trabajo, las capacidades del modelo *Infosec-Tree* se extienden para soportar la identificación de vulnerabilidades y amenazas que permiten realizar un análisis de riesgos, y con base en ello, definir políticas de seguridad de la información y establecer de objetivos de control.

4.3.2. SELECCIÓN DE FUENTES DE VULNERABILIDAD

El siguiente paso en este análisis de riesgos es identificar vulnerabilidades en el sistema que se está analizando. Debido a que en este proyecto se está desarrollando un proceso de aseguramiento de la información a partir de una aplicación de referencia que excluye detalles de implementación, no es posible identificar vulnerabilidades específicas relacionadas con tecnologías particulares. Sin embargo, sí es factible seleccionar fuentes desde las cuales se pueden originar vulnerabilidades en cualquier sistema. La TABLA 2 agrupa por categorías las fuentes de vulnerabilidades seleccionadas para desarrollar el proceso de identificación y valoración de riesgos, obtenidas a partir de listas disponibles públicamente, tales como (Spacey, 2011), (OWASP, 2014) y (CVE Details, 2015).

Tabla 2. Fuentes de vulnerabilidades seleccionadas, agrupadas por categoría. Fuente: Elaboración propia.

Categoría	Fuentes de vulnerabilidades
Tecnología	<ul style="list-style-type: none"> • Navegadores de Internet • <i>Frameworks</i> de aplicación • Sistemas operativos • Protocolos
<i>Hardware</i>	<ul style="list-style-type: none"> • Fallos de diseño del <i>hardware</i> • <i>Hardware</i> desactualizado u obsoleto • <i>Hardware</i> incorrectamente configurado

Tabla 2. Fuentes de vulnerabilidades seleccionadas, agrupadas por categoría. Fuente: Elaboración propia. (Continuación)

Categoría	Fuentes de vulnerabilidades
Software	<ul style="list-style-type: none"> • Pruebas insuficientes o incompletas • Defectos en el <i>software</i> • Defectos en el diseño del <i>software</i> • Complejidad del <i>software</i> • <i>Software</i> corrupto (infectado con virus, <i>malware</i>, etcétera)
Red	<ul style="list-style-type: none"> • Comunicaciones de red desprotegidas • Puertos abiertos • Arquitectura de red insegura • Privilegios excesivos de usuarios o recursos • Comandos y/o <i>scripts</i> innecesarios
Gestión de TI	<ul style="list-style-type: none"> • Falta de parches de seguridad • Insuficiente gestión de incidentes • Errores de configuración

4.3.3. SELECCIÓN DE FUENTES DE AMENAZAS

El propósito de este paso es encontrar fuentes de amenazas que ponen en riesgo la información del sistema analizado. La guía del NIST (2012), acerca de cómo ejecutar evaluaciones de riesgo, provee una taxonomía en la que se clasifican las fuentes de amenazas en cuatro categorías: originadas por adversarios, accidentales, estructurales y ambientales. Para los intereses de este proyecto, se toman en consideración 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). La TABLA 3 muestra ejemplos de fuentes de amenazas originadas por adversarios.

Tabla 3. Ejemplos de fuentes de amenazas originadas por adversarios. Fuente: NIST (National Institute of Standards and Technology, 2012).

Sub categoría	Ejemplos de fuentes amenazas
Individuos	<ul style="list-style-type: none"> • Intrusos • Empleados / Colaboradores • Empleados de confianza • Empleados privilegiados
Grupos	<ul style="list-style-type: none"> • Ad hoc • Grupos de adversarios previamente reconocidos
Organizaciones	<ul style="list-style-type: none"> • Competidores • Proveedores • Socios • Clientes

4.3.4. IDENTIFICACIÓN DE RIESGOS

El cuarto paso en el proceso de análisis de riesgos consiste en la identificación de éstos. Para ello, se deben relacionar fuentes de amenazas y vulnerabilidades a través de eventos de amenazas. Un evento de amenaza es una acción que permite a una fuente de amenaza provocar un efecto adverso en algún recurso del sistema. Por ejemplo, llevar a cabo una modificación indebida en el tráfico de red es una acción que le permitiría a un adversario corromper sesiones de los usuarios.

Es importante aclarar que en esta etapa las fuentes de amenazas deben considerarse aceptables, es decir, que tienen el potencial de explotar al menos una fuente de vulnerabilidad identificada. En el ejemplo descrito en el párrafo anterior, la fuente de amenaza (un adversario) es aceptable, porque puede explotar (interceptar y corromper sesiones de los usuarios) una fuente de vulnerabilidad (comunicaciones de red desprotegidas).

Este paso debe aplicarse a cada uno de los escenarios analizados, tal como se explica en el ejemplo ilustrado por la FIGURA 10, en la que se muestra un sistema compuesto por los componentes *A*, *B*, *C*, *D*, *E* y *F*, representado por un diagrama de flujos de información (FIGURA 10a), en el cual las flechas indican la dirección en la que viaja la información de un componente a otro.

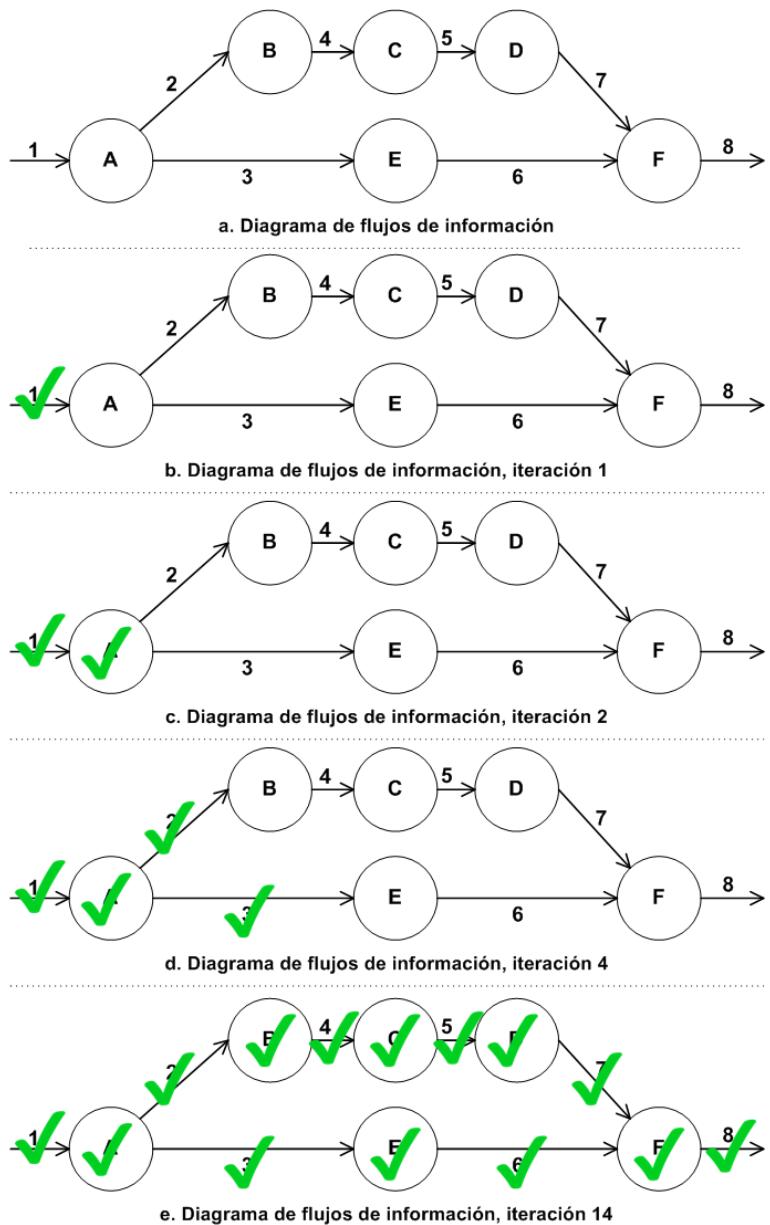


Figura 10. Ejemplo del proceso sistemático para la identificación de riesgos, usando el diagrama de flujos de información entre los componentes del sistema. Fuente: Elaboración propia.

En el flujo representado por (1), la información ingresa al sistema directamente hacia el componente A, que procesa o almacena esa información, y luego envía datos hacia los componentes B y E (mediante 2 y 3). A su vez, B procesa o almacena la información recibida y transmite otros datos hacia C (4). El proceso se repite para los demás componentes, hasta que F envía los datos fuera del sistema (8).

La identificación de riesgos se consigue iterando a través de los nodos y las conexiones del diagrama de flujos de información. La FIGURA 10b muestra la primera iteración sobre el diagrama. En ella se identifican y se documentan eventos de amenazas presentes en el flujo (1). Una vez que se han agotado las relaciones entre fuentes de amenaza y fuentes de vulnerabilidad en dicho flujo, se procede a marcarlo como procesado. En la siguiente iteración (FIGURA 10c), se aplica la misma idea para el componente representado por el nodo A. La FIGURA 10d muestra la iteración cuatro, en la cual los flujos (1, 2 y 3) y el nodo A ya han sido analizados. Finalmente, la FIGURA 10e muestra la iteración 14, en la cual todos los nodos y todos los flujos de información fueron procesados.

El ejemplo descrito anteriormente ilustra la capacidad sistémica y sistemática del proceso de aseguramiento de la información desarrollado en este proyecto. Es sistémico porque todos los componentes tecnológicos relevantes para el análisis de seguridad están representados por los nodos; y es sistemático porque se puede iterar de forma ordenada sobre todos los componentes del sistema y las conexiones entre ellos.

4.3.5. DETERMINACIÓN DE LA PROBABILIDAD DEL RIESGO

Una vez identificados los riesgos, lo siguiente por hacer es asignarles una valoración que permita determinar su grado de severidad. En la primera etapa, que se describe en este paso, se asigna una probabilidad de ocurrencia a los riesgos que fueron encontrados.

Según OWASP (2015), en el contexto de la valoración de riesgos, 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. 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. Por lo tanto, en este trabajo, cuando se hace referencia a la probabilidad de que un riesgo se materialice, se asume lo expuesto anteriormente, y no se utilizan definiciones más formales disponibles en fuentes como Ash (2008), que define probabilidad como el número de resultados favorables a un evento, dividido entre el número total de resultados, donde todos los resultados son igualmente posibles.

La probabilidad de ocurrencia de un riesgo se puede determinar a partir de múltiples factores, que pueden ser agrupados en dos conjuntos:

- Factores relacionados con la amenaza: tienen como objetivo estimar la probabilidad de que ocurra un ataque exitoso a partir de un grupo de posibles atacantes. Dado que puede haber

múltiples atacantes capaces de explotar una vulnerabilidad, lo usual es utilizar el peor de los escenarios; y

- Factores relacionados con la vulnerabilidad: tienen como objetivo estimar la probabilidad de que una vulnerabilidad sea encontrada y explotada (OWASP, 2015).

En este trabajo, se utiliza una metodología que toma como base la propuesta de OWASP (2015), con una serie de variantes que le permiten adaptarse a las necesidades del proyecto. Dicha metodología se describe en los siguientes párrafos.

Dado que en esta investigación se hace referencia a fuentes de amenazas y fuentes de vulnerabilidades, en lugar de amenazas y vulnerabilidades respectivamente, los factores para estimar la probabilidad de ocurrencia de los riesgos se asignan a fuentes de amenazas y fuentes de vulnerabilidades. Dentro de esta investigación, las fuentes de amenazas originadas por adversarios se caracterizan por nivel de habilidad, recompensa recibida y recursos tecnológicos requeridos por el atacante para realizar el ataque. Por otra parte, las vulnerabilidades se caracterizan por facilidad de descubrimiento y facilidad de explotación. Las tablas 4 y 5 describen con mayor detalle cada uno de esos factores.

Adicionalmente, los factores descritos en las tablas 4 y 5 están acompañados por una escala de valores que va de cero a nueve, la cual asigna un valor a cada factor de acuerdo con criterios cuantitativos previamente definidos. Por ejemplo, si un atacante requiere un nivel intermedio de habilidades técnicas para encontrar y explotar la vulnerabilidad, se le asigna un valor de cinco al factor nivel de habilidad. El propósito de hacerlo así es mantener un conjunto finito y predeterminado de criterios asignables, que permita minimizar las subjetividades en las que podría incurrir la persona encargada de hacer la estimación si esos criterios no estuvieran definidos.

Por último, a los factores de las tablas 4 y 5 se les asigna un identificador, que se utiliza posteriormente para representar el valor asignado a cada uno de ellos.

Tabla 4. Factores característicos de las fuentes de amenazas generadas por adversarios para determinar la probabilidad del riesgo. Fuente: Elaboración propia.

Id	Factor	Escala de valores
<i>H</i>	<p>Nivel de habilidad ¿Qué nivel técnico es requerido por la fuente de amenaza para encontrar la vulnerabilidad y explotarla?</p>	<ul style="list-style-type: none"> • 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 • Requiere un nivel omnisciente de habilidades técnicas = 0
<i>Ro</i>	<p>Recompensa ¿Cuál es la magnitud del incentivo que recibe la fuente de amenaza para encontrar la vulnerabilidad y explotarla?</p>	<ul style="list-style-type: none"> • 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
<i>Ru</i>	<p>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?</p>	<ul style="list-style-type: none"> • 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 5. Factores característicos de las fuentes de vulnerabilidades para determinar la probabilidad del riesgo. Fuente: Elaboración propia.

Id	Factor	Escala de valores
<i>D</i>	Facilidad de descubrimiento ¿Qué tan fácil es descubrir la vulnerabilidad para una fuente de amenaza?	<ul style="list-style-type: none"> • Inmediata = 9 • Fácil = 7 • Moderada = 5 • Difícil = 3 • Muy difícil = 1 • Imposible = 0
<i>E</i>	Facilidad de ser explotada ¿Qué tan fácil es explotar la vulnerabilidad para una fuente de amenaza?	<ul style="list-style-type: none"> • Inmediata = 9 • Fácil = 7 • Moderada = 5 • Difícil = 3 • Muy difícil = 1 • Imposible = 0

Una vez que se ha asignado un valor a cada factor, se debe determinar la probabilidad que se le asignará al riesgo. Como se indicó antes, lo que se busca es estimar la probabilidad en una escala cuantitativa, y esto se hace en dos etapas, que se describen seguidamente.

En la primera etapa, se debe obtener un promedio de los valores asignados a cada factor. La forma más simple de hacerlo consiste en sumar esos valores y luego dividir el resultado entre la cantidad de factores, tal como se muestra en la ECUACIÓN 1.

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

Ecuación 1. Promedio de los valores asignados a cada factor para estimar la probabilidad del riesgo.
Fuente: Elaboración propia.

Sin embargo, la anterior no es la única forma de utilizar los valores asignados a cada factor para estimar la probabilidad. Por ejemplo, suponga una hipótesis en la que se asume que tanto la facilidad de descubrimiento (*D*) como la facilidad de ser explotada (*E*) son proporcionales al nivel de habilidad (*H*) y a los recursos necesarios (*Ru*), de la siguiente manera:

$$\begin{array}{ll} D \propto H & E \propto H \\ D \propto Ru & E \propto Ru \end{array}$$

Suponga además que, en las relaciones de proporcionalidad descritas anteriormente, la constante de proporcional es igual a $\frac{1}{2}$, de manera que tanto D como E se pueden escribir en términos de H y Ru , como se indica a continuación:

$$D = \frac{1}{2} H + \frac{1}{2} Ru \quad E = \frac{1}{2} H + \frac{1}{2} Ru$$

Lo cual es equivalente a:

$$D = \frac{H + Ru}{2} \quad E = \frac{H + Ru}{2}$$

Con base en lo anterior, se tiene que:

$$D + E = H + Ru$$

El promedio de los factores para estimar la probabilidad del riesgo también podría calcularse sustituyendo D y E por H y Ru en la ECUACIÓN 1, lo que resulta en:

$$Promedio = \frac{H + Ro + Ru + H + Ru}{5}$$

Finalmente, la ECUACIÓN 2 muestra una forma alternativa de calcular el promedio de los valores asignados a cada factor para estimar la probabilidad del riesgo, considerando a las variables D y E como dependientes de H y Ru .

$$Promedio = \frac{Ro + 2H + 2Ru}{5}$$

Ecuación 2. Promedio de los valores asignados a cada factor para estimar la probabilidad del riesgo, utilizando variables dependientes. Fuente: Elaboración propia.

Con base en lo anterior, se muestra que este proceso de estimación de la probabilidad es flexible, y que funciona independientemente del método elegido para calcular el promedio de los valores asignados a los factores, sean los dos mencionados anteriormente o cualquier otro. Por ejemplo, en la ECUACIÓN 1 se asigna el mismo peso a todos los factores, lo que significa que cada factor tiene el mismo grado de influencia en la estimación de la probabilidad. Sin embargo, es posible definir

nuevas ecuaciones para estimar la probabilidad, asignando pesos diferentes a los factores si se llega a considerar que unos influyen más que otros en la estimación. Con base en la ECUACIÓN 2, se podrían generar razonamientos similares para considerar distintas otras dependientes, si las hay.

Por último, la segunda etapa para estimar la probabilidad del riesgo consiste en utilizar el promedio obtenido para seleccionar un valor dentro de una escala cuantitativa, que se muestra en la TABLA 6.

Tabla 6. Escala cuantitativa para el cálculo de la probabilidad del riesgo. Fuente: Elaboración propia.

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

Por ejemplo, si el promedio obtenido es 2.5, la probabilidad se considera baja, pues $1 < 2.5 < 3$, mientras que, si el promedio es 6.67, la probabilidad se considera alta, pues $5 < 6.67 < 7$.

4.3.6. DETERMINACIÓN DEL IMPACTO DEL RIESGO

En la segunda etapa de la valoración de los riesgos, que se describe en este paso, se asigna un nivel de impacto a los riesgos que fueron identificados.

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. Por lo tanto, en este contexto, el impacto es una estimación del nivel de los efectos adversos que se producirían en la aplicación y en el negocio tras un ataque exitoso. De manera similar a lo que sucede con la probabilidad, no es necesario ser excesivamente preciso en esa estimación, ya que en la práctica por lo general es suficiente identificar si el impacto es bajo, medio o alto.

El nivel de impacto de un riesgo se puede determinar a partir de múltiples factores, que pueden ser agrupados en dos conjuntos:

- Factores técnicos: tienen como objetivo estimar la magnitud del impacto sobre la aplicación si una vulnerabilidad es explotada, y están fuertemente relacionados con los servicios de seguridad de la información; y
- Factores del negocio: son factores comunes a diversas áreas de muchos negocios, sin embargo, su determinación requiere una comprensión profunda de lo que es importante para la organización que ejecuta el software (OWASP, 2015).

En este trabajo, se utiliza una metodología que toma como base la propuesta de OWASP (2015), con una serie de variantes que le permiten adaptarse a las necesidades del proyecto. Dicha metodología se describe en los siguientes párrafos.

Para cubrir la parte técnica de la estimación del impacto del riesgo, se utilizan las consecuencias de la interrupción de un servicio de seguridad de la información. En este trabajo, los servicios relevantes son: no repudio, integridad, autenticación y confidencialidad. Por otra parte, para abarcar la parte del negocio, se utiliza como factores la interrupción de la actividad del negocio, la pérdida económica y la pérdida de reputación.

En este punto, es fundamental hacer énfasis en cuál es la organización que ejecuta la actividad del negocio, y qué es importante para ella. Cuando en el presente análisis se hace referencia a factores del negocio, la organización en cuestión es el SNCD, y en este contexto, su principal objetivo es garantizar el no repudio de la información, para que los documentos electrónicos firmados digitalmente tengan el mismo valor legal que los documentos impresos. La TABLA 7 describe con mayor detalle todos los factores seleccionados.

Adicionalmente, los factores descritos en la TABLA 7 están acompañados por una escala de valores que va de cero a nueve, la cual asigna un valor a cada factor de acuerdo con criterios cuantitativos previamente definidos. Por ejemplo, si la materialización de un riesgo ocasiona una pérdida económica alta, se le asigna un valor de siete al factor pérdida económica. Al igual que con la probabilidad, el propósito de hacerlo así es mantener un conjunto finito y predeterminado de criterios asignables, que permita minimizar las subjetividades en las que podría incurrir la persona encargada de hacer la estimación si esos criterios no estuvieran definidos.

Por último, a los factores de la TABLA 7 se les asigna un identificador, que se utiliza posteriormente para representar el valor asignado a cada uno de ellos.

Tabla 7. Factores característicos para la determinación del impacto del riesgo. Fuente: Elaboración propia.

Id	Factor	Escala de valores
C	<p>Consecuencias de la interrupción de un servicio de seguridad de la información</p> <p>¿Cuál es el nivel de las consecuencias de la interrupción de un servicio de seguridad información como resultado del ataque?</p>	<ul style="list-style-type: none"> • 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	<p>Interrupción de la actividad del negocio</p> <p>¿Cuál es el grado de interrupción de la correcta prestación de servicios de firma digital por parte del SNCD como resultado del ataque?</p>	<ul style="list-style-type: none"> • 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
E	<p>Pérdida económica</p> <p>¿Cuál es el nivel de pérdida económica dentro del SNCD como resultado del ataque?</p>	<ul style="list-style-type: none"> • 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	<p>Pérdida de reputación</p> <p>¿Cuál es el nivel de afectación de la buena imagen del SNCD como resultado del ataque?</p>	<ul style="list-style-type: none"> • 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

Una vez que se ha asignado un valor a cada factor, se debe determinar el nivel de impacto que se le asignará al riesgo. Como se indicó antes, lo que se busca es estimar el impacto en una escala cuantitativa, y esto se hace en dos etapas, que se describen seguidamente.

En la primera etapa, se debe obtener un promedio de los valores asignados a cada factor. La forma más simple de hacerlo consiste en sumar esos valores y luego dividir el resultado entre la cantidad de factores, tal como se muestra en la ECUACIÓN 3.

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

Ecuación 3. Promedio de los valores asignados a cada factor para estimar el impacto del riesgo. Fuente:
Elaboración propia.

La anterior no es la única forma de utilizar los valores asignados a cada factor para estimar el impacto. Por ejemplo, suponga una hipótesis en la que la interrupción de la actividad del negocio (A) es proporcional a las consecuencias de la interrupción de un servicio de seguridad de la información (C), de la siguiente manera:

$$A \propto C$$

Suponga además que, en la relación de proporcionalidad descrita anteriormente, la constante de proporcional es igual a 1, de manera que A se puede escribir en términos de C , como se indica a continuación:

$$A = C$$

El promedio de los factores para estimar el impacto del riesgo también podría calcularse sustituyendo A por C en la ECUACIÓN 3, lo que resulta en:

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

Finalmente, la ECUACIÓN 4 muestra una forma alternativa de calcular el promedio de los valores asignados a cada factor para estimar el impacto del riesgo, considerando a la variable A como dependiente de C .

$$\text{Promedio} = \frac{2C + E + R}{4}$$

Ecuación 4. Promedio de los valores asignados a cada factor para estimar el impacto del riesgo, utilizando variables dependientes. Fuente: Elaboración propia.

Con base en lo anterior, se muestra que este proceso de estimación del impacto es flexible, y que funciona independientemente del método elegido para calcular el promedio de los valores asignados a los factores, sean los dos mencionados anteriormente o cualquier otro. Por ejemplo, en la ECUACIÓN 3 se asigna el mismo peso a todos los factores, lo que significa que cada factor tiene el mismo grado de influencia en la estimación del impacto. Sin embargo, es posible definir nuevas ecuaciones para la estimación del impacto, asignando pesos diferentes a los factores si se llega a considerar que unos influyen más que otros en la estimación. Con base en la ECUACIÓN 4, se podrían generar razonamientos para considerar otras variables dependientes, si las hay.

Por último, la segunda etapa para estimar el impacto del riesgo consiste en utilizar el promedio obtenido para seleccionar un valor dentro de una escala cuantitativa, que se muestra en la TABLA 8.

Tabla 8. Escala cuantitativa para el cálculo del impacto del riesgo. Fuente: Elaboración propia.

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

Por ejemplo, si el promedio obtenido es 4.5, el impacto se considera medio, pues $3 < 4.5 < 5$, mientras que, si el promedio es 8, el impacto se considera muy alto, pues $7 < 8 < 9$.

4.3.7. DETERMINACIÓN DEL NIVEL DE SEVERIDAD DEL RIESGO

Con base en la probabilidad y el impacto asignados, el último paso en la valoración de los riesgos consiste en asignarles un nivel de severidad. Para hacerlo, se utiliza una matriz como la que se muestra en la TABLA 9. El objetivo es encontrar la celda en la que se intersecan la probabilidad y el impacto obtenidos durante la estimación. Por ejemplo, si la probabilidad se estimó como media y el impacto se estimó como alto, al riesgo se le debe asignar un nivel de severidad alto.

Tabla 9. Niveles de severidad del riesgo. Fuente: Elaboración propia.

		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

El nivel de severidad asignado a los riesgos es muy importante. Una vez que todos los riesgos que se encontraron han sido valorados, se cuenta con una lista de prioridades para mitigarlos.

4.4. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Esta sección describe las acciones necesarias para la definición de políticas que mitigan los riesgos identificados. En este paso de la investigación, se llevan a cabo dos actividades: seleccionar los riesgos a ser mitigados, y definir las políticas de seguridad de la información. Las siguientes subsecciones describen brevemente cada una de las actividades.

4.4.1. SELECCIÓN DE LOS RIESGOS A SER MITIGADOS

La selección de los riesgos a ser mitigados se hace con base en el nivel de severidad asignado. Con el fin de obtener una relación costo-beneficio efectiva, se han de mitigar los riesgos identificados cuya severidad es media, alta o muy alta, y se ignoran aquellos riesgos cuya severidad es muy baja o baja.

4.4.2. REDACCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

En este trabajo, la redacción de las políticas de seguridad de la información se realiza a través de lenguaje natural, utilizando declaraciones que indican lo que un *software* o un usuario pueden o no hacer, y que describen los requisitos de seguridad necesarios para mitigar uno o varios riesgos.

La redacción de las políticas de seguridad de la información se realiza de forma iterativa, escribiendo políticas para cada riesgo seleccionado, hasta que todos los riesgos tienen al menos una política que lo considera.

4.5. ESTABLECIMIENTO DE OBJETIVOS DE CONTROL

Esta sección describe las actividades requeridas para el establecimiento de los objetivos de control que hacen cumplir las políticas definidas.

De forma similar a la definición de políticas, en este trabajo se utiliza lenguaje natural para establecer los objetivos de control. Se analizan los requisitos de seguridad definidos por las políticas, y se redactan especificaciones genéricas de los requerimientos mínimos que debe implementar un control de seguridad para ser considerado como efectivo a la hora de hacer cumplir la política correspondiente.

Este proceso se realiza de forma iterativa, escribiendo objetivos de control para cada política de seguridad definida, hasta que todas las políticas tienen al menos una definición de objetivo de control para garantizar su cumplimiento.

4.6. ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN

Esta sección describe las acciones que permiten crear una guía de implementación para asegurar la información de aplicaciones de *software* que utilizan certificados y firma digital dentro del SNCD.

El objetivo principal de la guía de implementación es proveer un instrumento que permita evaluar el cumplimiento de las políticas de seguridad de la información definidas en esta investigación, a través de los objetivos de control establecidos. Para cumplir con ello, se debe redactar un documento que al menos contenga las siguientes secciones:

- Ámbito de aplicabilidad: delimita los escenarios de uso en los cuales la guía de implementación puede ser aplicada.
- Modo de uso: indica la forma en que la guía de implementación debe ser utilizada para evaluar el cumplimiento de las políticas de seguridad de la información.
- Lista de políticas de seguridad de la información: conjunto de políticas de seguridad a ser evaluadas. Esta sección debe proveer un mecanismo para llevar el control del cumplimiento de las políticas.
- Lista de objetivos de control: conjunto de objetivos de control que sirven para evaluar el cumplimiento de las políticas de seguridad de la información. Esta sección sirve como referencia para determinar si las políticas se cumplen o no.

5. ANÁLISIS DE ESCENARIOS DE FIRMA DIGITAL

Este capítulo describe los resultados del análisis aplicado a los escenarios de firma digital. El capítulo inicia con un resumen de los escenarios de firma digital que fueron seleccionados, y finaliza con la descripción detallada de cada uno de ellos.

5.1. ESCENARIOS DE FIRMA DIGITAL SELECCIONADOS

Esta sección describe brevemente los escenarios sobre los cuales se aplicó el proceso de aseguramiento de la información. La escogencia se realizó con base en su relevancia en el contexto de aplicaciones de *software* dentro del SNCD.

Con base en lo estipulado en los artículos 3 y 4 de la directriz 067-MICITT-H-MEIC (Gobierno de Costa Rica, 2014), y el criterio experto de los integrantes de la DCFD y del Área de Seguridad de la División de Servicios Tecnológicos del BCCR, la lista definitiva de escenarios seleccionados es la siguiente:

- Creación de firma digital y sello electrónico: es la creación de un conjunto de datos electrónicos que se asocian a un documento electrónico, con el propósito de identificar inequívocamente al firmante, y garantizar la integridad del documento.
- Verificación de firma digital y sello electrónico: es la validación de la identidad del firmante, la integridad del documento firmado y la validez del certificado digital utilizado para crear la firma.
- Autenticación de usuarios mediante certificados digitales: es el proceso de demostrar la posesión de una llave privada, con el fin de validar la identidad del usuario.
- Conversión de una firma digital en formato simple a formato avanzado: es la adición de atributos a un documento firmado electrónicamente con un formato básico, con el propósito de garantizar la validación a largo plazo de las firmas digitales contenidas en él.

En las siguientes secciones se desarrolla cada uno de los escenarios seleccionados con el nivel de detalle requerido para su posterior análisis de seguridad. En relación con cada escenario, se describe el producto mínimo viable requerido para su ejecución exitosa desde la perspectiva funcional, se caracterizan sus componentes tecnológicos y se muestra cómo fluye la información a través de ellos.

5.2. CREACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

La presente sección describe el escenario de creación de firma digital y sello electrónico.

La creación de una firma digital y un sello electrónico difiere en dos aspectos fundamentales. Primero, la firma digital utiliza certificados de persona física, mientras que el sello electrónico utiliza certificados de persona jurídica. Segundo, el dispositivo criptográfico seguro que se utiliza para la creación de firma digital usualmente es una tarjeta inteligente con su respectivo lector, mientras que para el sello electrónico suele utilizarse un HSM (Módulo de Seguridad de *Hardware*). A pesar de ambas diferencias, éstas solo constituyen formas distintas de implementar un mismo proceso. Es por ello que en la presente investigación la creación de una firma digital y un sello electrónico se analizan dentro de un mismo escenario.

5.2.1. PRODUCTO MÍNIMO VIABLE PARA LA CREACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

El proceso de creación de firma digital comienza cuando un usuario selecciona un documento electrónico que será firmado, así como su certificado digital para identificarse. El certificado es validado utilizando un conjunto de criterios previamente definidos. Antes de crear la firma digital, una función *hash* es aplicada al contenido del documento, con el fin de generar un resumen. Posteriormente, el resumen es cifrado utilizando la llave privada del usuario, lo cual produce la firma digital. Finalmente, el documento original, la firma digital y el certificado digital del firmante son utilizados para generar el documento electrónico firmado. La FIGURA 11 muestra el proceso descrito anteriormente.

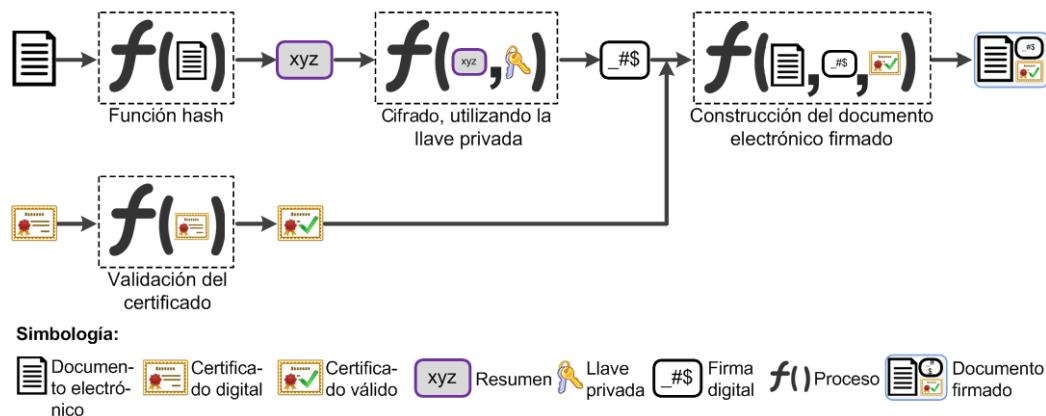


Figura 11. Proceso para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.

5.2.2. CARACTERIZACIÓN DE COMPONENTES PARA LA CREACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

En esta sección se hace una caracterización de los componentes requeridos para completar la creación de una firma digital.

La FIGURA 12 muestra los componentes de un módulo de creación de firma digital. Dicho módulo está formado por diez componentes, que se describen con mayor detalle en la TABLA 10.

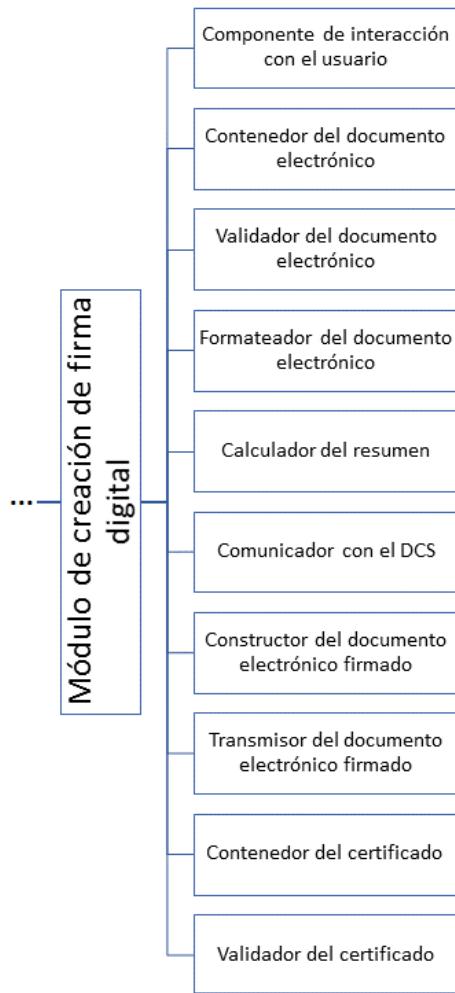


Figura 12. Componentes propuestos para un módulo de creación de firma digital y sello electrónico.
Fuente: Elaboración propia.

Tabla 10. Descripción de los componentes propuestos para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Componente de interacción con el usuario.	<ul style="list-style-type: none"> - Datos introducidos por el usuario. - Mensajes de estado provenientes de otros componentes. 	<ul style="list-style-type: none"> - Procesamiento de las interacciones del usuario con la aplicación para controlar el proceso de creación de firma digital y sello electrónico. - Procesamiento de mensajes de estado provenientes de otros componentes que deben ser mostrados al usuario. 	<ul style="list-style-type: none"> - Mensajes de estado (confirmaciones, errores, advertencias, etcétera).
Contenedor del documento electrónico.	<ul style="list-style-type: none"> - Documento electrónico. 	<ul style="list-style-type: none"> - Almacenamiento del documento electrónico, una vez que ha sido seleccionado, en una ubicación que depende del contexto de la aplicación. 	<ul style="list-style-type: none"> - Documento electrónico.
Validador del documento electrónico.	<ul style="list-style-type: none"> - Documento electrónico. 	<ul style="list-style-type: none"> - Aplicación de un conjunto de criterios para determinar la validez del documento electrónico. 	<ul style="list-style-type: none"> - Resultado de la validación.

Tabla 10. Descripción de los componentes propuestos para la creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Formateador del documento electrónico.	- Documento electrónico.	- Transformación del documento electrónico en una representación apropiada, según lo requiera el componente “Calculador del resumen”.	- Documento electrónico formateado.
Calculador del resumen.	- Documento electrónico formateado.	- Cálculo del resumen del documento electrónico utilizando una función <i>hash</i> .	- Resumen del documento electrónico.
Comunicador con el dispositivo criptográfico seguro.	- Resumen del documento electrónico.	- Invocación de las funciones criptográficas disponibles en el dispositivo criptográfico seguro.	- Resumen cifrado del documento electrónico.
Contenedor del certificado.	- Certificado digital.	- Almacenamiento del certificado digital, una vez que ha sido seleccionado, en una ubicación que depende del contexto de la aplicación.	- Certificado digital.
Validador del certificado.	- Certificado digital.	- Aplicación de un conjunto de criterios para determinar la validez del certificado digital.	- Resultado de la validación.

Tabla 10. Descripción de los componentes propuestos para la creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Constructor del documento electrónico firmado.	<ul style="list-style-type: none"> - Certificado digital. - Documento electrónico formateado. - Resumen cifrado del documento electrónico. 	<ul style="list-style-type: none"> - Generación de un documento electrónico firmado en formato simple. 	<ul style="list-style-type: none"> - Documento electrónico firmado.
Transmisor del documento electrónico firmado.	<ul style="list-style-type: none"> - Documento electrónico firmado. 	<ul style="list-style-type: none"> - Transmisión del documento electrónico hacia su ubicación final. 	<ul style="list-style-type: none"> - Documento electrónico firmado.

5.2.3. DIAGRAMA DE FLUJOS DE INFORMACIÓN PARA LA CREACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

Seguidamente se explica el diagrama de flujos de información generado a partir del producto mínimo viable propuesto para la creación de firma digital y sello electrónico, que describe cómo fluye la información entre los componentes requeridos para completar el escenario.

La FIGURA 13 muestra el diagrama de flujos de información propuesto. El flujo comienza cuando un documento electrónico es provisto (flujo 1 en la FIGURA 13) y es almacenado temporalmente en un *Contenedor del documento electrónico*. Posteriormente, el documento electrónico es validado (2 y 3) por un *Validador del documento electrónico*. El documento electrónico es luego enviado a un *Formateador del documento electrónico* (4), que lo prepara para ser enviado a un *Calculador del resumen* (5). Una vez que el resumen del documento electrónico ha sido calculado, un *Comunicador con el dispositivo criptográfico seguro* se encarga de que el *Dispositivo criptográfico seguro* cifre dicho resumen (7 y 8). Adicionalmente, el certificado digital del usuario es provisto (9) y almacenado temporalmente en un *Contenedor del certificado*, para luego ser validado (10 y 11) por un *Validador del certificado*. El certificado digital, el resumen cifrado del documento electrónico y el documento electrónico formateado son enviados (12, 13 y 14) a un *Constructor del documento electrónico firmado*, cuyo resultado es enviado (15) a un *Transmisor del documento electrónico firmado*, que se encarga de colocar el documento electrónico firmado en su ubicación final (16).

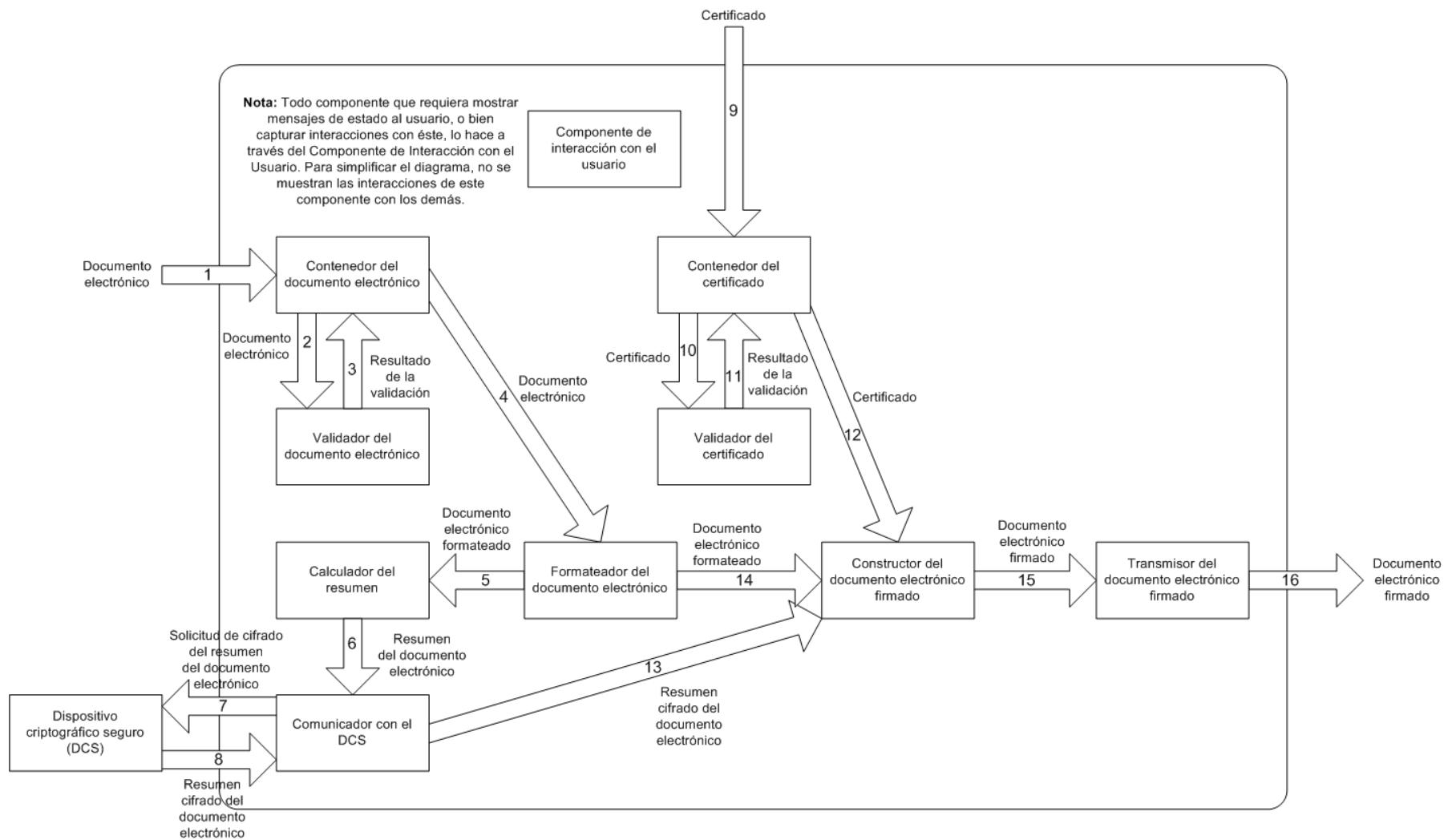


Figura 13. Diagrama de flujos de información de los componentes requeridos para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.

5.3. VERIFICACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

La presente sección describe el escenario de verificación de firma digital y sello electrónico.

La verificación de una firma digital y un sello electrónico difiere en un aspecto básico: la firma digital utiliza certificados de persona física, mientras que el sello electrónico utiliza certificados de persona jurídica. Sin embargo, dicha diferencia solo constituye una forma distinta de implementar un mismo proceso. Es por ello que en la presente investigación la verificación de una firma digital y un sello electrónico se analizan dentro de un mismo escenario.

5.3.1. PRODUCTO MÍNIMO VIABLE PARA LA VERIFICACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

El proceso de verificación de firma digital inicia cuando un usuario selecciona un documento electrónico firmado digitalmente, cuyas firmas necesita verificar. El documento es analizado, y para cada firma contenida en él se extraen tres piezas de información: el contenido del documento original (sin firmar), la firma digital y el certificado utilizado para crear la firma digital. Al contenido del documento original le es aplicada una función *hash*, para producir un resumen. La firma digital es descifrada utilizando la llave pública del usuario, lo que produce un segundo resumen. El certificado digital es validado, utilizando un conjunto de criterios previamente definidos. Por último, se realiza el proceso de validación de la firma, la cual se considera válida si ambos resúmenes calculados son iguales, y el certificado utilizado para crear la firma digital era válido al momento de crearla. La FIGURA 14 muestra el proceso descrito anteriormente.

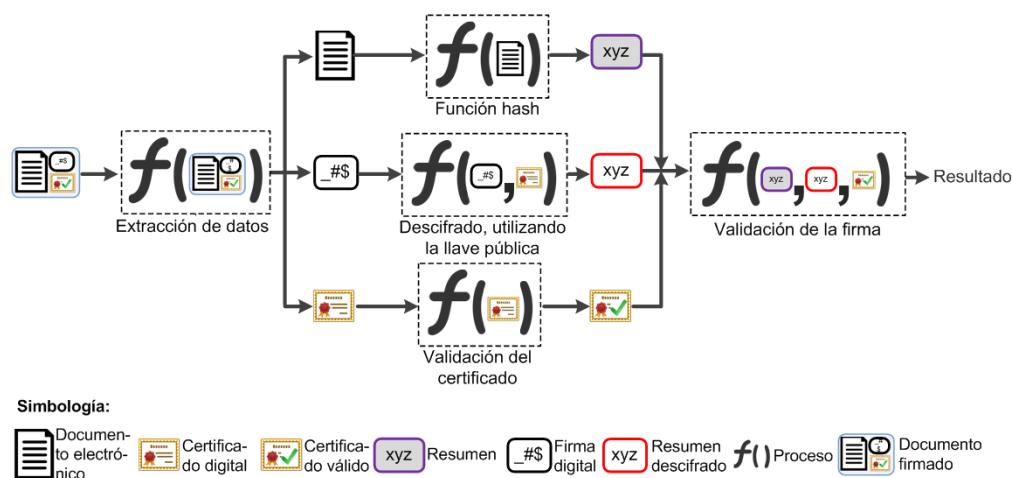


Figura 14. Proceso para la verificación de una firma digital. Fuente: Elaboración propia.

5.3.2. CARACTERIZACIÓN DE COMPONENTES PARA LA VERIFICACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

En esta sección se hace una caracterización de los componentes requeridos para completar la verificación de una firma digital.

La FIGURA 15 muestra los componentes de un módulo de verificación de firma digital. Dicho módulo está formado por diez componentes, que se describen con mayor detalle en la TABLA 11.

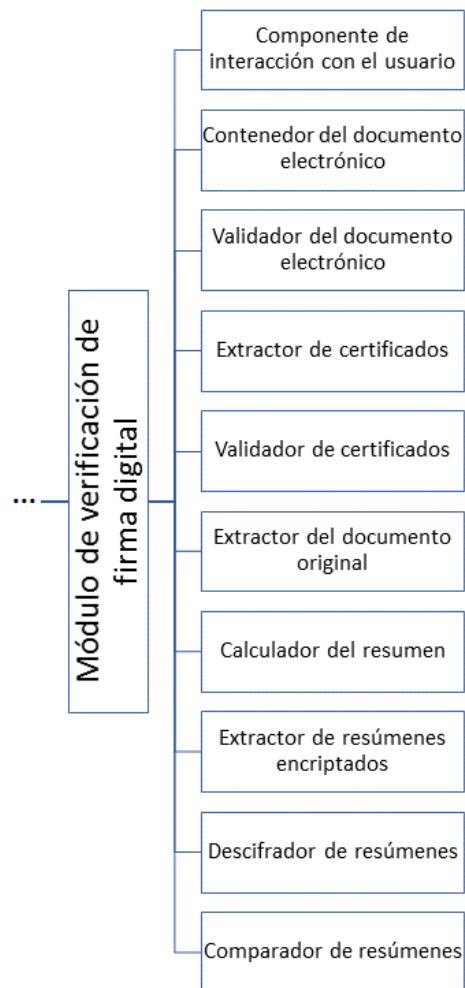


Figura 15. Componentes propuestos para un módulo de verificación de firma digital y sello electrónico.
Fuente: Elaboración propia.

Tabla 11. Descripción de los componentes propuestos para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia.

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Componente de interacción con el usuario.	<ul style="list-style-type: none"> - Datos introducidos por el usuario. - Mensajes de estado provenientes de otros componentes. 	<ul style="list-style-type: none"> - Procesamiento de las interacciones del usuario con la aplicación para controlar el proceso de creación de firma digital y sello electrónico. - Procesamiento de mensajes de estado provenientes de otros componentes que deben ser mostrados al usuario. 	<ul style="list-style-type: none"> - Mensajes de estado (confirmaciones, errores, advertencias, etcétera).
Contenedor del documento electrónico firmado en formato avanzado.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato avanzado. 	<ul style="list-style-type: none"> - Almacenamiento del documento electrónico firmado en formato avanzado, una vez que ha sido seleccionado, en una ubicación que depende del contexto de la aplicación. 	<ul style="list-style-type: none"> - Documento electrónico firmado en formato avanzado.
Validador del documento electrónico firmado en formato avanzado.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato avanzado. 	<ul style="list-style-type: none"> - Aplicación de un conjunto de criterios para determinar la validez del documento electrónico firmado en formato avanzado. 	<ul style="list-style-type: none"> - Resultado de la validación.
Extractor de certificados.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato avanzado. 	<ul style="list-style-type: none"> - Extracción de los certificados contenidos en las firmas digitales del documento. 	<ul style="list-style-type: none"> - Lista de certificados.

Tabla 11. Descripción de los componentes propuestos para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Validador de certificados.	- Lista de certificados digitales.	- Aplicación de un conjunto de criterios para determinar la validez de los certificados digitales.	- Resultado de la validación.
Extractor del documento original.	- Documento electrónico firmado en formato avanzado.	- Extractor del documento electrónico original, a partir del contenido del documento electrónico firmado en formato avanzado.	- Documento electrónico original.
Calculador del resumen.	- Documento electrónico original.	- Cálculo del resumen del documento electrónico original utilizando una función <i>hash</i> .	- Resumen del documento electrónico original.
Extractor de resúmenes cifrados.	- Documento electrónico firmado en formato avanzado.	- Extracción de los resúmenes cifrados contenidos en las firmas digitales del documento.	- Lista de resúmenes cifrados.
Descifrador de resúmenes.	- Lista de resúmenes cifrados. - Lista de certificados.	- Descifrado de los resúmenes cifrados, utilizando las llaves públicas contenidas en los certificados correspondientes.	- Lista de resúmenes descifrados.

Tabla 11. Descripción de los componentes propuestos para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Comparador de resúmenes.	<ul style="list-style-type: none"> - Resumen del documento electrónico original. - Lista de resúmenes descifrados. 	<ul style="list-style-type: none"> - Comparación del resumen del documento electrónico original con cada uno de los resúmenes descifrados. 	<ul style="list-style-type: none"> - Resultado de las comparaciones.

5.3.3. DIAGRAMA DE FLUJOS DE INFORMACIÓN PARA LA VERIFICACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

Seguidamente se explica el diagrama de flujos de información generado a partir del producto mínimo viable propuesto para la verificación de firma digital y sello electrónico, que describe cómo fluye la información entre los componentes requeridos para completar el escenario.

La FIGURA 16 muestra el diagrama de flujos de información. El flujo comienza cuando un documento electrónico firmado en formato avanzado es provisto (flujo 1 en la FIGURA 16) y es almacenado temporalmente en un *Contenedor del documento electrónico firmado en formato avanzado*. Posteriormente, el documento electrónico es validado (2 y 3) por un *Validador del documento electrónico en formato avanzado*. El documento electrónico firmado en formato avanzado es luego enviado a un *Extractor de certificados* (4), que obtiene del documento los certificados digitales de las firmas contenidas, y los envía (5 y 6) a validación en un *Validador de certificados*. El documento electrónico firmado en formato avanzado también es enviado (7) a un *Extractor de resúmenes cifrados*, que obtiene del documento los resúmenes cifrados de las firmas contenidas, y los envía a un *Descifrador de los resúmenes cifrados*, que junto a los certificados obtenidos previamente (9), genera los resúmenes descifrados. Adicionalmente, el documento electrónico firmado en formato avanzado es enviado (10) a un *Extractor del documento original*, que obtiene el documento electrónico original y lo envía (11) a un *Calculador del resumen del contenido del documento original*. Finalmente, el resumen del contenido del documento original y los resúmenes descifrados son enviados (12 y 13) a un *Comparador de resúmenes*, que se encarga de retornar (14) el resultado de la verificación de la firma digital.

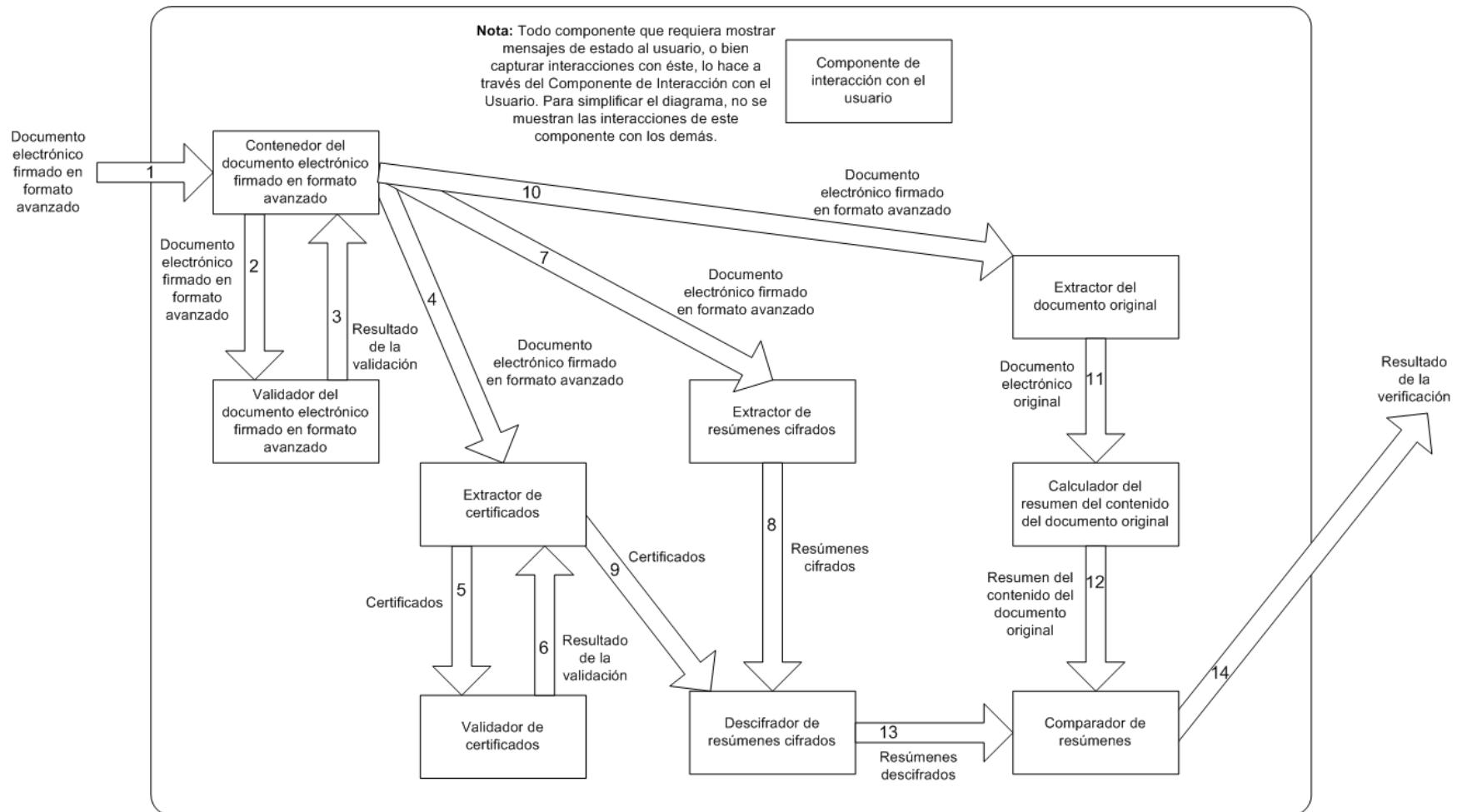


Figura 16. Diagrama de flujos de información de los componentes requeridos para la verificación de firma digital y sello electrónico. Fuente:
Elaboración propia.

5.4. CONVERSIÓN DE UNA FIRMA DIGITAL EN FORMATO SIMPLE A FORMATO AVANZADO

La presente sección describe el escenario de conversión de una firma digital en formato simple a formato avanzado.

5.4.1. PRODUCTO MÍNIMO VIABLE PARA LA CONVERSIÓN DE UNA FIRMA DIGITAL EN FORMATO SIMPLE A FORMATO AVANZADO

El proceso de conversión de una firma digital en formato simple a formato avanzado empieza cuando un usuario selecciona un documento electrónico firmado digitalmente con el propósito de actualizar las firmas digitales contenidas, con el fin de garantizar la validez de éstas a lo largo del tiempo. Los certificados digitales utilizados para crear cada firma son extraídos del documento, y para cada uno de ellos se obtiene información del estado del certificado al momento de realizar la conversión, así como estampas de tiempo de ese instante. Estos atributos son agregados al documento seleccionado por el usuario según lo requiere el formato avanzado correspondiente, produciendo un nuevo documento. La FIGURA 17 muestra el proceso descrito anteriormente.

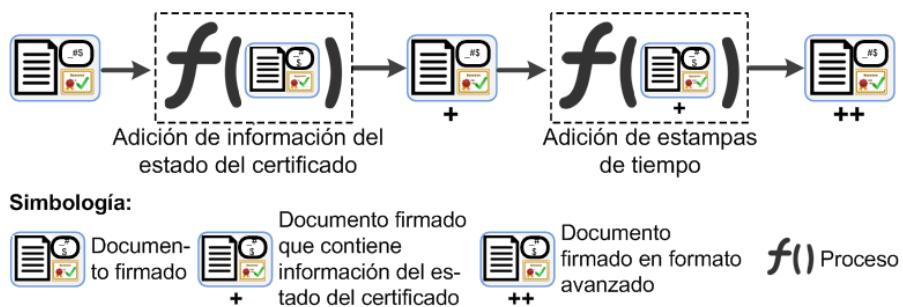


Figura 17. Proceso para la conversión de una firma digital en formato simple a formato avanzado.
Fuente: Elaboración propia.

5.4.2. CARACTERIZACIÓN DE COMPONENTES PARA LA CONVERSIÓN DE UNA FIRMA DIGITAL EN FORMATO SIMPLE A FORMATO AVANZADO

En esta sección se hace una caracterización de los componentes requeridos para completar la conversión de un documento electrónico firmado a formato avanzado.

La FIGURA 18 muestra los componentes de un módulo de conversión de una firma digital en formato simple a formato avanzado. Dicho módulo está formado por siete componentes, que se describen con mayor detalle en la TABLA 12.

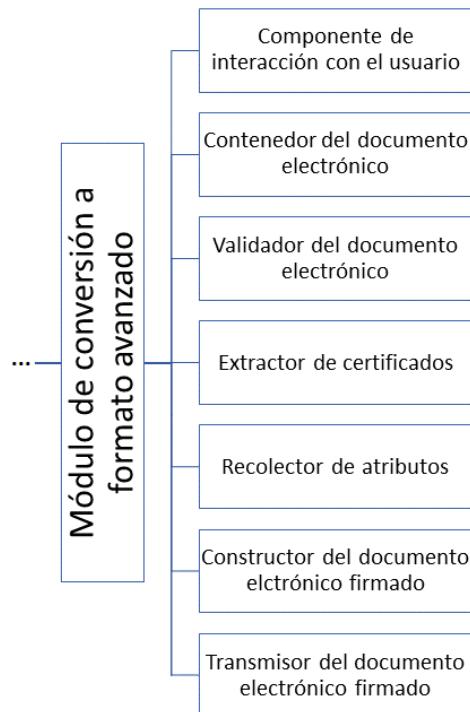


Figura 18. Componentes propuestos para un módulo de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

Tabla 12. Descripción de los componentes propuestos para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Componente de interacción con el usuario.	<ul style="list-style-type: none"> - Datos introducidos por el usuario. - Mensajes de estado provenientes de otros componentes. 	<ul style="list-style-type: none"> - Procesamiento de las interacciones del usuario con la aplicación para controlar el proceso de creación de firma digital y sello electrónico. - Procesamiento de mensajes de estado provenientes de otros componentes que deben ser mostrados al usuario. 	<ul style="list-style-type: none"> - Mensajes de estado (confirmaciones, errores, advertencias, etcétera).
Contenedor del documento electrónico firmado en formato simple.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato simple. 	<ul style="list-style-type: none"> - Almacenamiento del documento electrónico firmado en formato simple, una vez que ha sido seleccionado, en una ubicación que depende del contexto de la aplicación. 	<ul style="list-style-type: none"> - Documento electrónico firmado en formato simple.
Validador del documento electrónico.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato simple. 	<ul style="list-style-type: none"> - Aplicación de un conjunto de criterios para determinar la validez del documento electrónico firmado en formato simple. 	<ul style="list-style-type: none"> - Resultado de la validación.
Extractor de certificados.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato simple. 	<ul style="list-style-type: none"> - Extracción de los certificados contenidos en las firmas digitales del documento. 	<ul style="list-style-type: none"> - Lista de certificados digitales.

Tabla 12. Descripción de los componentes propuestos para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Recolector de los atributos requeridos por el formato avanzado.	- Lista de certificados digitales.	- Recolección, para cada certificado, de los atributos requeridos para convertir el documento electrónico en formato avanzado.	- Atributos requeridos por el formato avanzado (tokens de estampado de tiempo, rutas de certificación e información de revocación).
Constructor del documento electrónico firmado en formato avanzado.	<ul style="list-style-type: none"> - Documento electrónico firmado en formato simple. - Atributos requeridos por el formato avanzado. 	- Generación de un documento electrónico firmado en formato avanzado.	- Documento electrónico firmado en formato avanzado.
Transmisor del documento electrónico firmado en formato avanzado.	- Documento electrónico firmado en formato avanzado.	- Transmisión del documento electrónico firmado en formato avanzado hacia su ubicación final.	- Documento electrónico firmado en formato avanzado.

5.4.3. DIAGRAMA DE FLUJOS DE INFORMACIÓN PARA LA CONVERSIÓN DE UNA FIRMA DIGITAL EN FORMATO SIMPLE A FORMATO AVANZADO

Seguidamente se explica el diagrama de flujos de información generado a partir del producto mínimo viable propuesto para la conversión de una firma digital en formato simple a formato avanzado, que describe cómo fluye la información entre los componentes requeridos para completar el escenario.

La FIGURA 19 muestra el diagrama de flujos de información propuesto. El flujo comienza cuando un documento electrónico firmado en formato simple es provisto (flujo 1 en la FIGURA 19) y es almacenado temporalmente en un *Contenedor del documento electrónico firmado en formato simple*. Posteriormente, el documento electrónico es validado (2 y 3) por un *Validador del documento electrónico en formato simple*. El documento electrónico firmado en formato simple es luego enviado a un *Extractor de certificados* (4), que obtiene del documento los certificados digitales de las firmas contenidas, y los envía (5) a un *Recolector de atributos requeridos por el formato avanzado*. Los atributos son obtenidos a partir de distintas fuentes: un almacén de certificados (6 y 7), un servicio *web* de estampado de tiempo (8 y 9), un servicio *web* que provee CRLs (10 y 11) y/o un servicio *web* que provee OCSP (12 y 13). Posteriormente, tanto el documento electrónico firmado en formato simple como los atributos obtenidos son enviados (14 y 15) a un *Constructor del documento electrónico en formato avanzado*, cuyo resultado es enviado (16) a un *Transmisor del documento electrónico firmado*, que se encarga de colocar el documento electrónico firmado en su ubicación final (17).

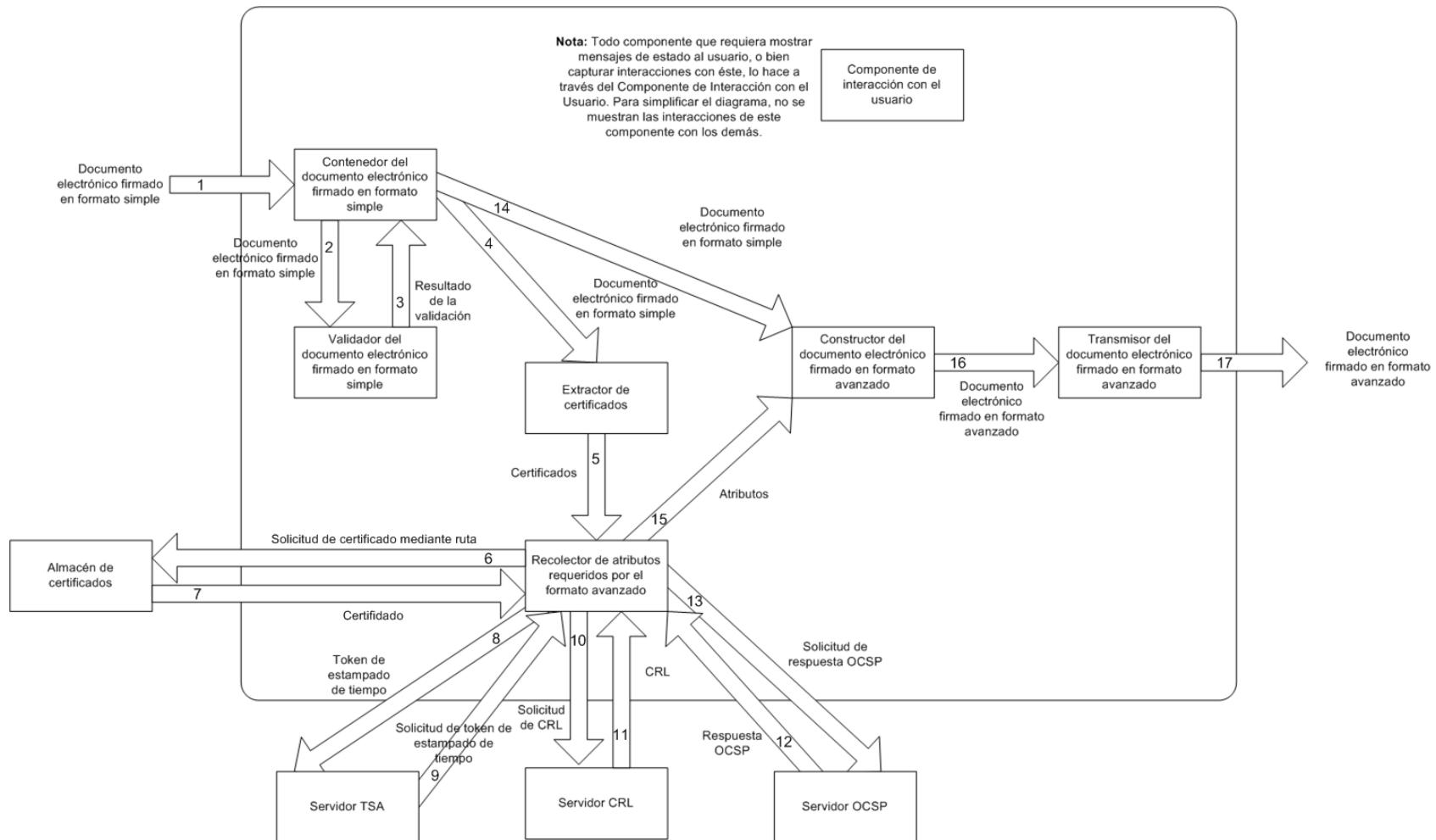


Figura 19. Diagrama de flujos de información de los componentes requeridos para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

5.5. AUTENTICACIÓN DE USUARIOS MEDIANTE CERTIFICADOS DIGITALES

La presente sección describe el escenario de autenticación de usuarios mediante certificados digitales.

5.5.1. PRODUCTO MÍNIMO VIABLE PARA LA AUTENTICACIÓN DE USUARIOS MEDIANTE CERTIFICADOS DIGITALES

El proceso de autenticación de usuarios mediante certificados digitales comienza cuando un usuario selecciona su certificado digital con el fin de comprobar su identidad. El sistema genera un conjunto de datos aleatorios, que son firmados digitalmente (como se describió en la subsección 5.2.1) utilizando la llave privada del usuario. La firma digital resultante es posteriormente verificada (como se describió en la subsección 5.3.1), utilizando la llave pública del usuario. Si la verificación de la firma es exitosa, el proceso de autenticación indica que el usuario es quien dice ser, pues pudo comprobar la posesión de su llave privada. La FIGURA 20 muestra el proceso descrito anteriormente

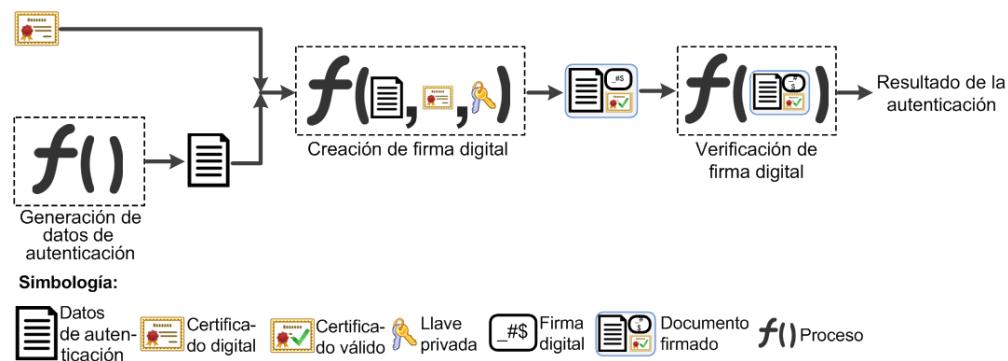


Figura 20. Proceso para la autenticación de usuarios por medio de certificados digitales. Fuente: Elaboración propia.

5.5.2. CARACTERIZACIÓN DE COMPONENTES PARA LA AUTENTICACIÓN DE USUARIOS MEDIANTE CERTIFICADOS DIGITALES

En esta sección se hace una caracterización de los componentes requeridos para completar la autenticación de usuarios mediante certificados digitales.

La FIGURA 21 muestra los componentes de un módulo de autenticación de usuarios mediante certificados digitales. Dicho módulo está formado por ocho componentes, que se describen con mayor detalle en la TABLA 13.

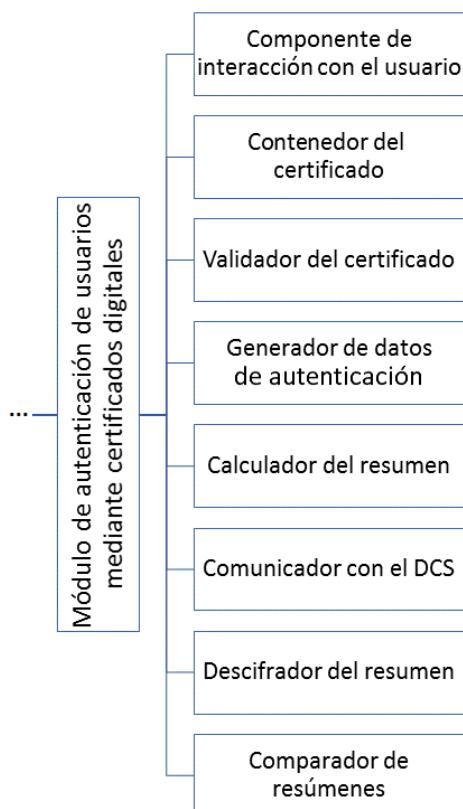


Figura 21. Componentes propuestos para un módulo de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

Tabla 13. Descripción de los componentes propuestos para la autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Componente de interacción con el usuario.	<ul style="list-style-type: none"> - Datos introducidos por el usuario. - Mensajes de estado provenientes de otros componentes. 	<ul style="list-style-type: none"> - Procesamiento de las interacciones del usuario con la aplicación para controlar el proceso de creación de firma digital y sello electrónico. - Procesamiento de mensajes de estado provenientes de otros componentes que deben ser mostrados al usuario. 	<ul style="list-style-type: none"> - Mensajes de estado (confirmaciones, errores, advertencias, etcétera).
Contenedor del certificado.	<ul style="list-style-type: none"> - Certificado digital. 	<ul style="list-style-type: none"> - Almacenamiento del certificado digital, una vez que ha sido seleccionado, en una ubicación que depende del contexto de la aplicación. 	<ul style="list-style-type: none"> - Certificado digital.
Validador del certificado.	<ul style="list-style-type: none"> - Certificado digital. 	<ul style="list-style-type: none"> - Aplicación de un conjunto de criterios para determinar la validez del certificado digital. 	<ul style="list-style-type: none"> - Resultado de la validación.
Generador de datos de autenticación.	<ul style="list-style-type: none"> - 	<ul style="list-style-type: none"> - Generación de datos de autenticación que serán firmados digitalmente para comprobar la posesión de la llave privada. 	<ul style="list-style-type: none"> - Datos de autenticación.

Tabla 13. Descripción de los componentes propuestos para la autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia. (Continuación)

Nombre del componente	Entradas de información	Estados de la información dentro del componente	Salidas de información
Calculador del resumen.	- Datos de autenticación.	- Cálculo del resumen de los datos de autenticación utilizando una función <i>hash</i> .	- Resumen de los datos de autenticación.
Comunicador con el dispositivo criptográfico seguro.	- Resumen de los datos de autenticación.	- Invocación de las funciones criptográficas disponibles en el dispositivo criptográfico seguro.	- Resumen de los datos de autenticación cifrados.
Descifrador del resumen de los datos de autenticación cifrados.	- Resumen cifrado de los datos de autenticación. - Certificado digital.	- Descifrado del resumen cifrado de los datos de autenticación utilizando la llave pública contenida en el certificado digital.	- Resumen descifrado de los datos de autenticación.
Comparador de resúmenes.	- Resumen de los datos de autenticación. - Resumen descifrado de los datos de autenticación.	- Comparación del resumen los datos de autenticación con el resumen descifrado de los datos de autenticación.	- Resultado de la comparación.

5.5.3. DIAGRAMA DE FLUJOS DE INFORMACIÓN PARA LA AUTENTICACIÓN DE USUARIOS MEDIANTE CERTIFICADOS DIGITALES

Seguidamente se explica el diagrama de flujos de información generado a partir del producto mínimo viable propuesto para la autenticación de usuarios mediante certificados digitales, que describe cómo fluye la información entre los componentes requeridos para completar el escenario.

La FIGURA 22 muestra el diagrama de flujos de información propuesto. El flujo comienza cuando un certificado digital es provisto (flujo 1 en la FIGURA 22) y es almacenado temporalmente en un *Contenedor del certificado*. Posteriormente, el certificado es validado (2 y 11) por un *Validador del certificado*, que accede a diversas fuentes, tales como un almacén de certificados (3 y 4), un servicio *web* de estampado de tiempo (5 y 6), un servicio *web* que provee CRLs (7 y 8) y/o un servicio *web* que provee OCSP (9 y 10), para realizar la validación correctamente. Mientras tanto, un *Generador de datos de autenticación* produce datos que se envían (12) a un *Calculador del resumen*. El resumen de los datos de autenticación es enviado (13) a un *Comunicador con el dispositivo criptográfico seguro* se encarga de que el *Dispositivo criptográfico seguro* cifre dicho resumen (14 y 15). El certificado y el resumen cifrado de los datos de autenticación son enviados (16 y 17) a un *Descifrador del resumen*, el cual genera un segundo resumen de los datos de autenticación. Dicho resumen y el que se tenía anteriormente, son enviados (18 y 19) a un *Comparador de resúmenes*, el cual se encarga de determinar si ambos resúmenes son iguales (20), lo que permite determinar si la autenticación fue exitosa o no.

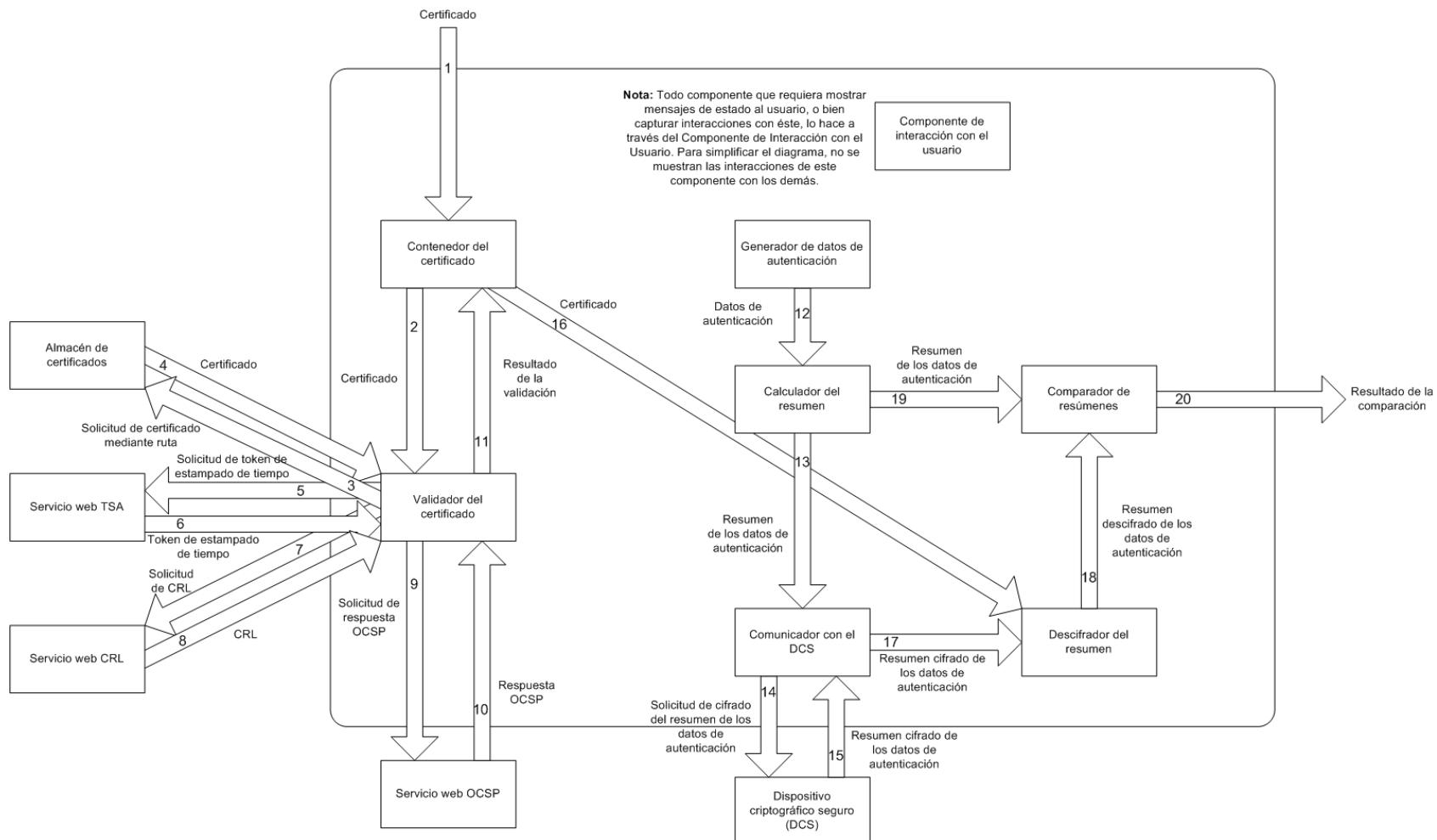


Figura 22. Diagrama de flujos de información de los componentes requeridos para la autenticación de usuarios mediante certificados digitales.

Fuente: Elaboración propia.

6. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

Este capítulo describe los resultados obtenidos al identificar y valorar los riesgos presentes en cada uno de los escenarios de firma digital analizados. El capítulo inicia con las consideraciones generales que delimitan el análisis de los riesgos. Posteriormente, continúa con la descripción de la estructura jerárquica utilizada para generar el modelo de referencia de los componentes de un sistema que implementa mecanismos de firma digital. Luego se presenta una descripción de la influencia que ejerce en el proceso de valoración de riesgos el ambiente de ejecución de los componentes tecnológicos en las aplicaciones. Finalmente, el capítulo concluye con un resumen del proceso de identificación y valoración de riesgos.

6.1. CONSIDERACIONES GENERALES

Esta sección describe las restricciones, limitaciones y verdades base relacionadas con el proceso de identificación y valoración de riesgos realizado.

6.1.1. RESTRICCIONES

Como se mencionó con anterioridad, el principal objetivo de seguridad de esta investigación es preservar el no repudio de la información dentro del SNCD. Sin embargo, existen escenarios en los que el no repudio de la información puede verse afectado indirectamente por circunstancias que están fuera del ámbito de la seguridad de la información. Por ejemplo, suponga que una persona es extorsionada para que firme digitalmente un documento electrónico que representa el traspaso de un bien. Aun cuando esa persona está utilizando su llave privada para crear la firma digital, podría eventualmente argumentar que lo hizo en contra de su voluntad.

En el presente análisis, quedan por fuera aquellos riesgos que no están relacionados directamente con la seguridad de la información, tales como actos de suplantación, amenazas, extorsión y coacción a personas, entre otros, pues forman parte de otros ámbitos que son ajenos al campo tecnológico, y, por lo tanto, no son competencia de este proyecto.

6.1.2. LIMITACIONES

En lo que respecta a la dimensión del tiempo, la identificación y valoración de los riesgos abarca los siguientes momentos de seguridad:

- Protección: se refiere al periodo de tiempo previo a la ocurrencia de un incidente que pone en riesgo la seguridad de la información. Para este momento de seguridad, el análisis de riesgos tiene como propósito la prevención de incidentes.
- Detección: se refiere al periodo de tiempo en el que ocurre un incidente que pone en riesgo la seguridad de la información. Para este momento de seguridad, el análisis de riesgos tiene como propósito identificar la ocurrencia de sucesos.

Finalmente, el análisis de riesgos no toma en consideración el momento de seguridad de respuesta, es decir, cuando se realizan las acciones correctivas pertinentes después de la ocurrencia de un incidente, pues el objetivo de esta investigación es prevenir y detectar la materialización de fallas en la seguridad de la información, mas no su corrección posterior.

6.1.3. VERDADES BASE

La confianza es un factor crucial para entender la seguridad de la información, por lo que cualquier política u objetivo de control se apoya sobre verdades base, que, si son incorrectas, destruyen la estructura que yace sobre ellas. En cualquier análisis de la seguridad de la información, es importante tener en cuenta lo anterior, pues si no están claras las verdades base sobre las que se apoya el análisis, se puede pasar de suposiciones aparentemente correctas a conclusiones erróneas (Bishop, 2002). Por ejemplo, suponga que un administrador recibe un parche de seguridad que debe ser instalado en un servidor, y lo instala. Se puede afirmar que la seguridad de la información del servidor mejoró al instalar el parche siempre y cuando las siguientes verdades base sean correctas:

- El administrador está asumiendo que el parche de seguridad no fue alterado en tránsito, y que ningún atacante malintencionado está tratando de hacerle instalar un parche que tiene contenido malicioso que podría producir agujeros de seguridad en el servidor;
- El administrador está asumiendo que el proveedor del parche de seguridad lo probó exhaustivamente. En muchas ocasiones, la presión que tienen los proveedores de *software* hace que se liberen parches rápidamente, y solamente los prueban respecto a ataques particulares. Bajo estas condiciones, un parche de seguridad podría no reparar el problema para el que fue desarrollado, o bien repararlo, pero agregar otros nuevos;
- El administrador está asumiendo que el ambiente de pruebas en el que el proveedor del parche de seguridad lo probó es igual al del servidor en el que el parche va a ser instalado. De no ser así, el parche podría no funcionar correctamente; y

- El administrador está asumiendo que el parche está correctamente instalado. Algunos parches de seguridad son fáciles de instalar, mientras que otros no. Un error durante la instalación podría ocasionar que el parche no corrija los problemas que debe corregir, o por el contrario, introduzca errores nuevos (Bishop, 2002).

En el ejemplo anterior, la invalidación de cualquiera de las verdades base hace que el parche de seguridad se convierta en un problema potencial de la seguridad de la información.

En esta investigación, algunas de las verdades base más relevantes que se asumen correctas, y sobre las que yace el proceso de aseguramiento de la información, son las siguientes:

- Los certificados digitales entregados por la PKI nacional identifican de forma única a los usuarios finales.
- Los dispositivos criptográficos seguros utilizados en cada escenario analizado han sido debidamente homologados dentro del SNCD, y, por lo tanto, no presentan riesgos en la seguridad de la información.
- Las actualizaciones del *software* complementario requerido para que las aplicaciones se ejecuten adecuadamente, tales como sistemas operativos, navegadores de Internet y *frameworks*, se asumen íntegras y correctas.
- Los componentes de *software* que no implementan funcionalidades relacionadas con los escenarios analizados en esta investigación, pero que forman parte de la aplicación, se asumen correctamente implementados, instalados y configurados.
- Los componentes de *hardware* requeridos para ejecutar las aplicaciones, tales como computadoras, *routers*, *firewalls*, entre otros, se asumen correctamente fabricados y conectados.

6.2. INFOSEC-TREE DE LOS ESCENARIOS ANALIZADOS

En la presente sección se describe el *infosec-tree* utilizado para generar el modelo de referencia de los componentes de un sistema que implementa mecanismos de firma digital. El *infosec-tree* se muestra en la FIGURA 23.

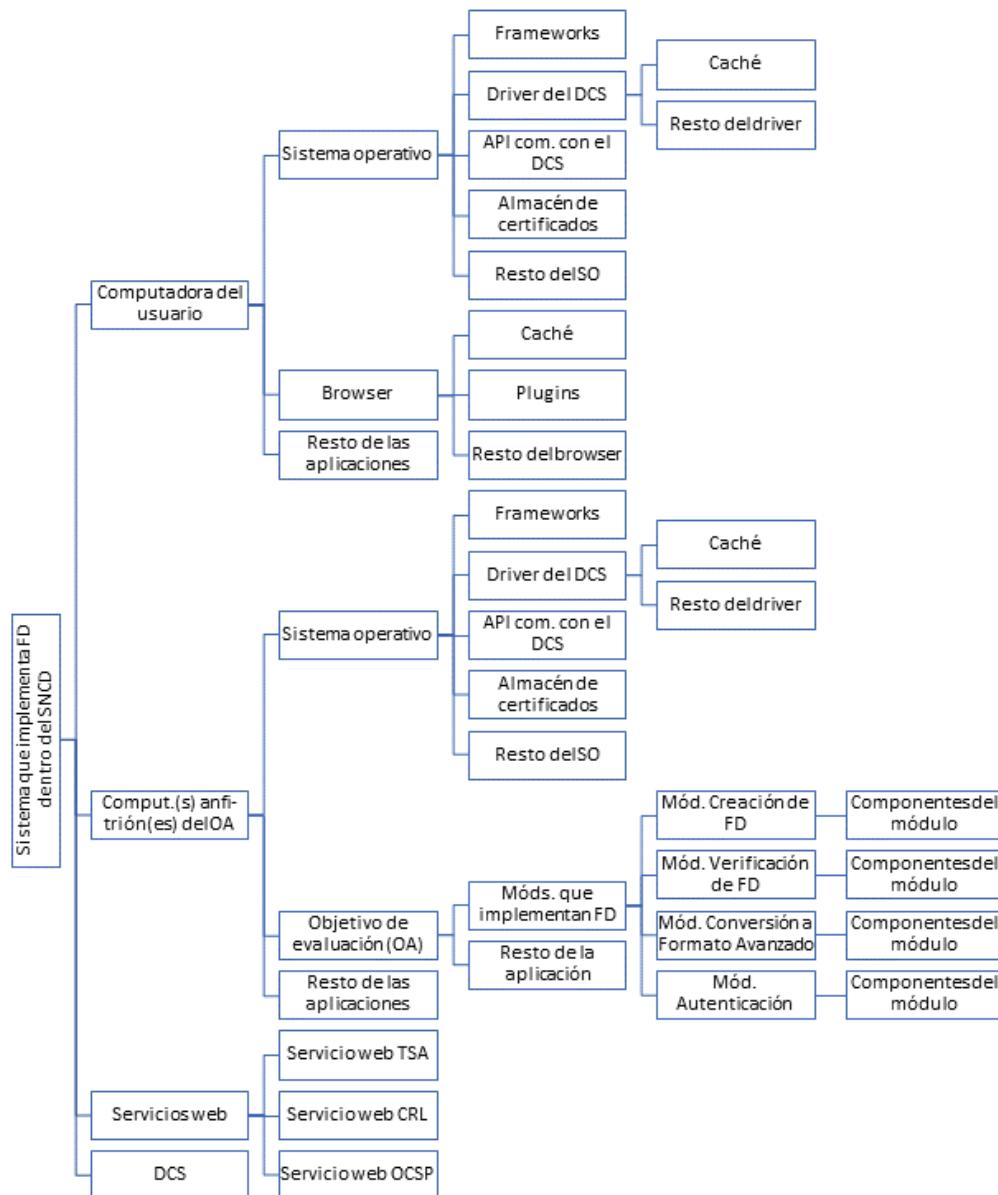


Figura 23. Infosec-tree propuesto para un sistema que implementa firma digital dentro del SNCD.
Fuente: Elaboración propia.

La raíz del árbol representa la totalidad del sistema que se quiere asegurar. Dicho sistema está compuesto por la computadora del usuario, la o las computadoras en las cuales se encuentra

instalado el objetivo de evaluación, un dispositivo criptográfico seguro y un conjunto de servicios *web* requeridos para la creación, verificación y conversión de las firmas digitales, así como para la autenticación de usuarios.

Por otra parte, la computadora del usuario está compuesta por el sistema operativo, el navegador de Internet (*browser*) y el resto de las aplicaciones instaladas en ella. Asimismo, la computadora donde se encuentra instalado el objetivo de evaluación está integrada por el sistema operativo, el objetivo de evaluación y el resto de las aplicaciones instaladas. En ambos casos, el sistema operativo se ha dividido a su vez en los *frameworks* que tiene instalados, el *driver* del DCS, el API de comunicación con el DCS, el almacén de certificados para acceder a la ruta de certificación y el resto del sistema operativo.

Finalmente, el objetivo de evaluación, que es una aplicación de *software*, está compuesto por los módulos que proveen la funcionalidad correspondiente a los escenarios descritos en la sección 5.1, y por otros elementos que quedan fuera del análisis de seguridad (Resto de la aplicación). Cada uno de los módulos mencionados anteriormente, está constituido por una serie de componentes más pequeños que implementan la funcionalidad de firma digital correspondiente. Estos componentes fueron descritos con mayor detalle en las secciones 5.2.2, 5.3.2, 5.4.2, y 5.5.2.

6.3. INFLUENCIA DEL AMBIENTE DE EJECUCIÓN DE LOS COMPONENTES TECNOLÓGICOS EN LA VALORACIÓN DE RIESGOS

En la presente sección se describe la influencia que ejerce en el proceso de valoración de riesgos el ambiente de ejecución de los componentes tecnológicos que integran las aplicaciones de *software* que implementan mecanismos de firma digital.

Existen distintos factores que afectan el diseño y la implementación de una aplicación de *software*, tales como la experiencia de los diseñadores y desarrolladores, el lenguaje de programación seleccionado, la plataforma sobre la cual se instalará el *software*, entre otros. Por lo tanto, es válido decir que existe una relación de tipo “uno a muchos” entre los requerimientos de una aplicación de *software* y las posibles formas de implementarla.

En el proceso de valoración de riesgos desarrollado en esta investigación hay una variable que se considera de suma importancia, debido a su influencia en el momento de decidir qué tan probable es que una vulnerabilidad sea explotada. Dicha variable es el ambiente de ejecución de los

componentes tecnológicos que intervienen en el evento. En este proceso de valoración de riesgos, el término ambiente de ejecución hace referencia a la computadora donde se ejecutan dos componentes que interactúan entre sí, de manera que, si un par de componentes está instalado en la misma máquina, se dice que los componentes están en un ambiente centralizado, mientras que, si los dos componentes están instalados en distintas máquinas, se dice que están en un ambiente distribuido. La FIGURA 24 presenta un ejemplo de componentes centralizados y distribuidos.

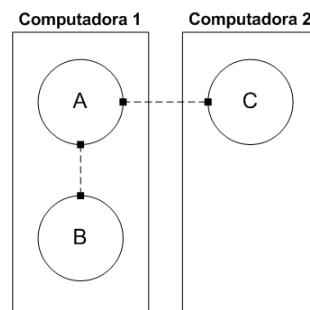


Figura 24. Ejemplo de componentes centralizados y distribuidos. Fuente: Elaboración propia.

En la FIGURA 24, tanto los pares de componentes *A* y *B* como *A* y *C* intercambian información. Sin embargo, en el diseño de la interacción de los componentes *A* y *B* se decidió que ambos componentes estuvieran centralizados en un solo ambiente, pues ambos se ejecutan en la computadora 1. Por otra parte, la interacción de los componentes *A* y *C* se diseñó de forma distribuida, pues el primero se ejecuta en la computadora 1, mientras que el segundo se ejecuta en la computadora 2.

Durante la valoración de un riesgo en información transmitida es fundamental conocer si los componentes que intercambian dicha información se ejecutan en la misma máquina o en máquinas distintas, pues tanto el ambiente centralizado como el distribuido están expuestos a diferentes riesgos de la seguridad de la información, debido a las amenazas y vulnerabilidades que pueden manifestarse en los componentes de cada ambiente. Por ejemplo, suponga que se debe hacer un análisis de riesgos de dos aplicaciones de *software* que implementan el proceso de creación de una firma digital, como las que se muestran en la FIGURA 25.

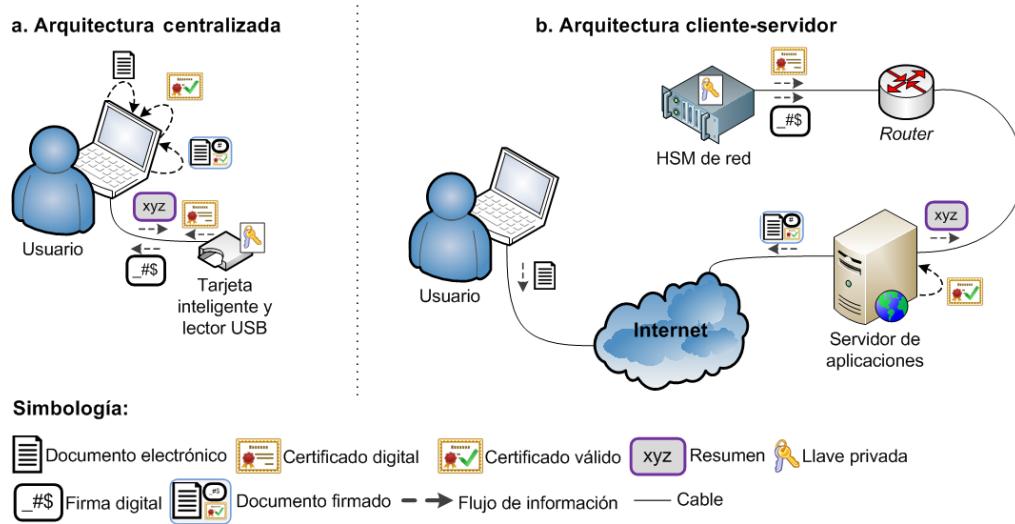


Figura 25. Implementación del proceso de creación de firma digital utilizando una arquitectura centralizada y una cliente-servidor. Fuente: Elaboración propia.

La arquitectura centralizada (FIGURA 25a) representa una aplicación instalada en la computadora del usuario, en la cual todos los componentes de *software* requeridos para crear una firma digital están ubicados en la misma máquina. En este ejemplo, el dispositivo criptográfico seguro que almacena la llave privada del usuario está conectado a la computadora por medio de un cable USB. Por otra parte, la arquitectura cliente-servidor (FIGURA 25b) representa una aplicación cuyos componentes de *software* se encuentran distribuidos en diferentes máquinas. Algunas operaciones ocurren en el lado del usuario, mientras que otras son ejecutadas en el servidor. En este caso, al dispositivo criptográfico seguro se accede de forma remota, utilizando comunicaciones de red. Ambas arquitecturas implementan la misma funcionalidad para la creación de firmas digitales, sin embargo, están expuestas a diferentes riesgos de la seguridad de la información, debido a que ambas utilizan diferentes canales de comunicación entre componentes. Por ejemplo, solicitar al dispositivo criptográfico seguro que firme un resumen requiere comunicaciones locales en la arquitectura centralizada porque los componentes se ejecutan en la misma máquina, pero es una operación remota en la arquitectura cliente-servidor, porque los componentes están distribuidos.

6.4. 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 3, presentadas en las

secciones 4.3.5 y 4.3.6, respectivamente. En general, se valoraron 228 riesgos, los cuales se visualizan a continuación desde diferentes perspectivas¹.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR ESCENARIO ANALIZADO

El GRÁFICO 1 muestra la cantidad de riesgos valorados, agrupados por escenario analizado. En él se observa que existen 7 riesgos que son comunes a todos los escenarios. Por ejemplo, el riesgo número 160 —el cual establece que la falta de actualizaciones en el sistema operativo puede permitir a un atacante malintencionado instalar *software* malicioso en la máquina donde se ejecuta algún componente de la aplicación— es común a todos los escenarios porque está relacionado con la infraestructura que da soporte a las aplicaciones de software, y no con funcionalidad específica de algún escenario.

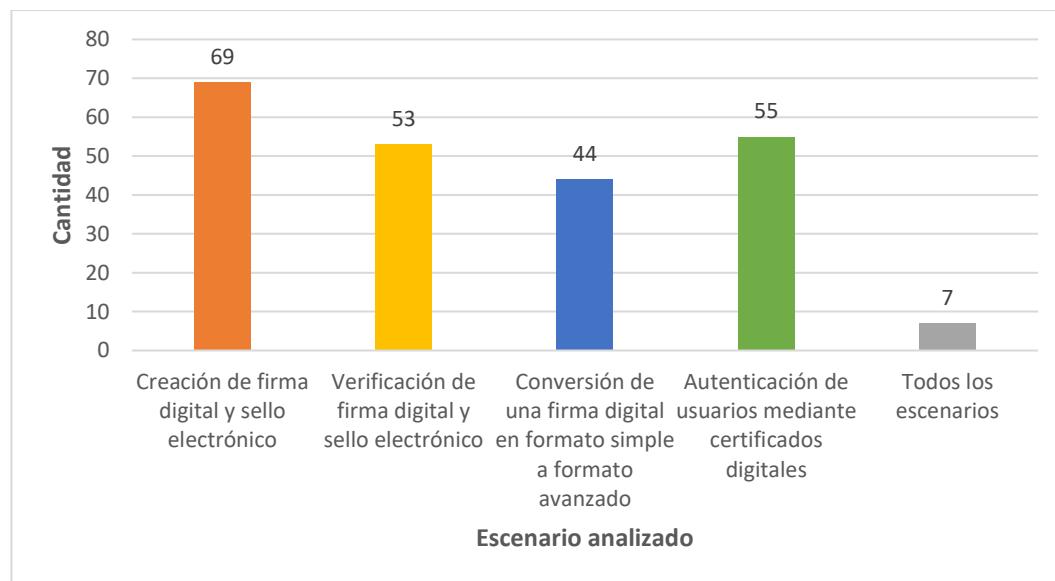


Gráfico 1. Cantidad de riesgos valorados, agrupados por escenario. Fuente: Elaboración propia.

Por otra parte, existen riesgos que se encuentran presentes en más de un escenario, pero no en todos. Por ejemplo, los riesgos número 13 y 120 —los cuales establecen que los defectos en el componente “Comunicador con el dispositivo criptográfico seguro” pueden hacer que la aplicación revele las credenciales de autenticación del “Dispositivo criptográfico seguro” a sus usuarios— están presentes en los escenarios de creación de firma digital y sello electrónico, y autenticación de

¹ El detalle completo de la identificación y valoración de los riesgos analizados en este capítulo se especifica en el Apéndice A: Riesgos Identificados, y en el Apéndice B: Detalle de la Valoración de los Riesgos Identificados.

usuarios mediante certificados digitales, respectivamente, porque en esos escenarios se requiere acceso a la llave privada del usuario.

Finalmente, existen riesgos que ocurren en escenarios específicos. Por ejemplo, el riesgo número 103 —el cual establece que los defectos en el componente “Constructor del documento electrónico firmado en formato avanzado” pueden permitir que la aplicación genere documentos electrónicos firmados cuyo formato avanzado no corresponde con alguno de los formatos oficiales soportados en Costa Rica— existe únicamente en el escenario de conversión de una firma digital en formato simple a formato avanzado.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR AMBIENTE DE EJECUCIÓN

El GRÁFICO 2 presenta la cantidad de riesgos valorados, agrupados por ambiente de ejecución. En él se observa que existen 56 riesgos cuya valoración es independiente del ambiente de ejecución de los componentes que intervienen en el riesgo. Ejemplo de lo anterior es el riesgo número 2 —el cual establece que los defectos en el componente “Contenedor del documento electrónico” pueden permitir a un atacante malintencionado modificar el contenido del documento electrónico mientras éste se encuentra almacenado dicho componente—, cuya valoración es la misma tanto en un ambiente centralizado y como en uno distribuido.

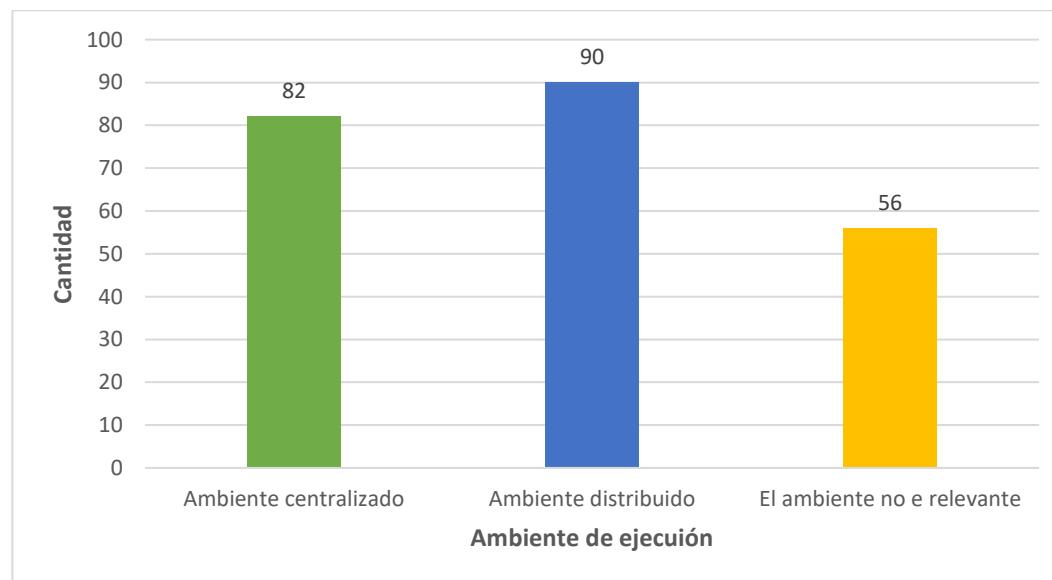


Gráfico 2. Cantidad de riesgos valorados, agrupados por ambiente de ejecución. Fuente: Elaboración propia.

Por otra parte, existen riesgos que ocurren tanto en un ambiente centralizado como en uno distribuido, sin embargo, requieren valoraciones diferentes. Por ejemplo, los riesgos 1 y 32 —los cuales establecen que la existencia de comunicaciones desprotegidas puede permitir a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico”— requieren valoraciones distintas porque los canales de comunicación utilizados por los componentes que intervienen en cada riesgo son distintos (en el riesgo número 1 la comunicación ocurre de forma local, mientras que en el riesgo número 32 la comunicación ocurre a través de una red).

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR NIVEL DE SEVERIDAD

El GRÁFICO 3 muestra la cantidad de riesgos valorados, agrupados por nivel de severidad. En total, 152 riesgos deben mitigarse, pues esa es la cantidad de riesgos con nivel de severidad medio, alto o muy alto. Por ejemplo, el riesgo número 8 —el cual establece que los defectos en el componente “Calculador del resumen” pueden permitir que la aplicación genere resúmenes a partir del uso de algoritmos *hash* inseguros— tiene un nivel de severidad muy alto, y por lo tanto debe ser mitigado.

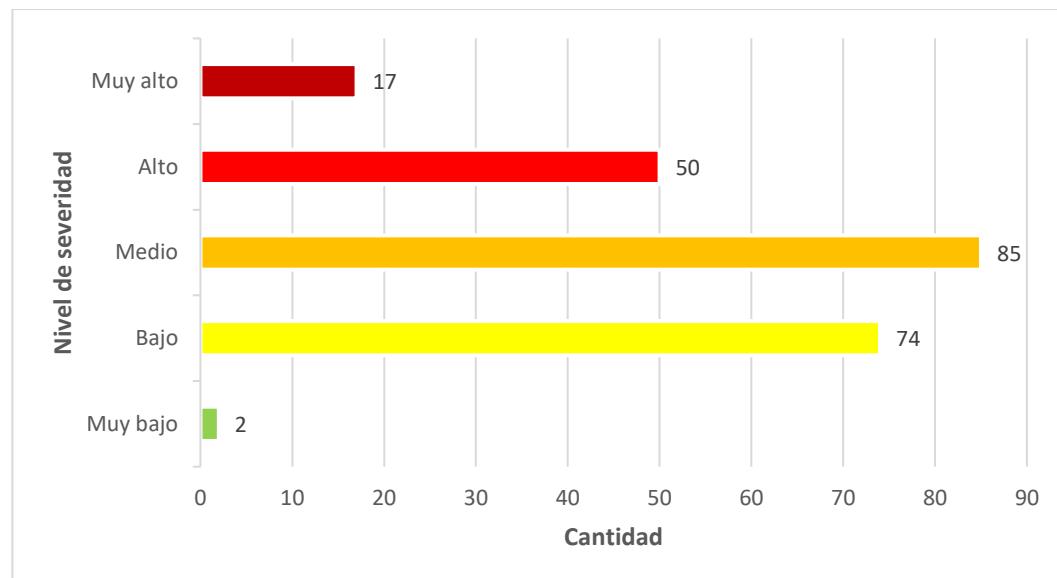


Gráfico 3. Cantidad de riesgos valorados, agrupados por nivel de severidad. Fuente: Elaboración propia.

Por otro lado, 76 riesgos podrían no mitigarse durante la definición de políticas de seguridad de la información, pues su severidad es baja o muy baja. Por ejemplo, el riesgo número 21 —el cual establece que la existencia de defectos en el componente “Contenedor del certificado” pueden

permitir a un atacante malintencionado modificar el certificado digital mientras éste se encuentra almacenado en dicho componente— tiene un nivel de severidad bajo, y por lo tanto podría no mitigarse.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR ESCENARIO ANALIZADO Y NIVEL DE SEVERIDAD

El GRÁFICO 4 presenta la cantidad de riesgos valorados, agrupados por escenario analizado y nivel de severidad. En él se puede observar que el escenario de creación de firma digital y sello electrónico es el que tiene más riesgos que deben ser mitigados, con un total de 44, mientras que el escenario de conversión de una firma digital en formato simple a formato avanzado es el que tiene menor cantidad, con un total de 30. Esta diferencia está dada por la cantidad de componentes que intervienen en cada escenario (10 en el primero y 7 en el segundo), pues mientras más grande es el número, mayor es la cantidad de riesgos que pueden estar presentes en las interacciones entre los componentes, y mayor es la cantidad de defectos que pueden estar presentes en el software.

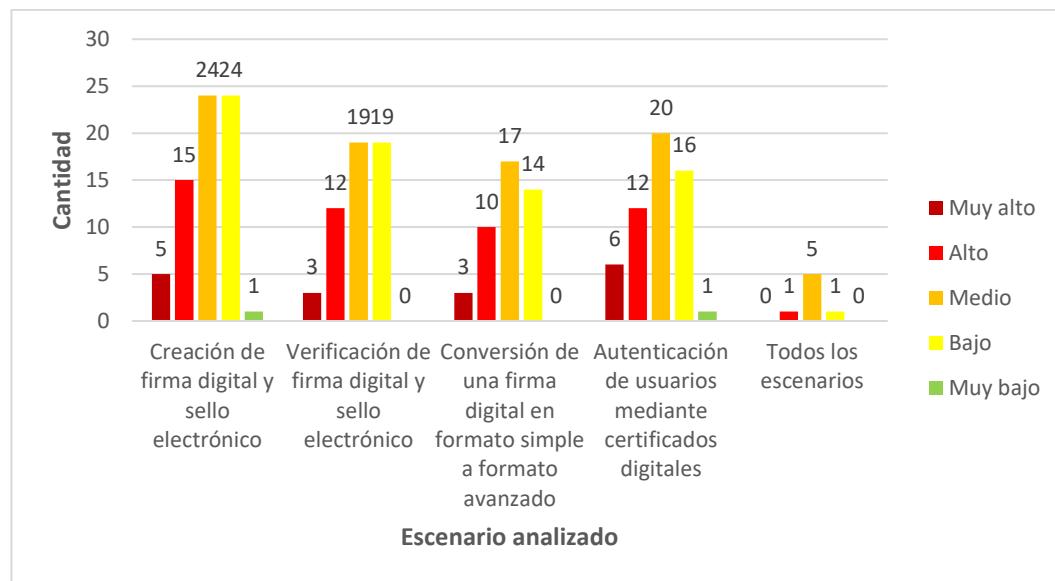


Gráfico 4. Cantidad de riesgos valorados, agrupados por escenario analizado y nivel de severidad.
Fuente: Elaboración propia.

Por otra parte, de los 7 riesgos valorados que están presentes en todos los escenarios, 6 deben ser mitigados.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR AMBIENTE DE EJECUCIÓN Y NIVEL DE SEVERIDAD

El GRÁFICO 5 muestra la cantidad de riesgos valorados, agrupados por ambiente de ejecución y nivel de severidad. En él se observa que el ambiente de ejecución distribuido es más riesgoso que el ambiente centralizado, pues el primero presenta 90 riesgos que deben ser mitigados, mientras que el segundo presenta solamente 13. Esta diferencia está dada por la mayor probabilidad que existe de explotar una vulnerabilidad cuando la comunicación entre dos componentes ocurre a través de una red.

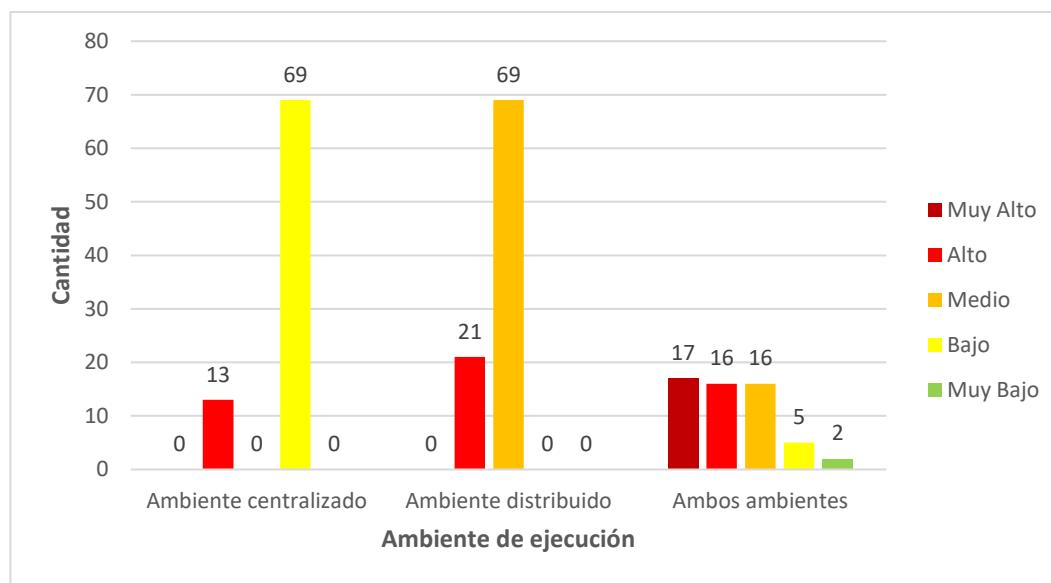


Gráfico 5. Cantidad de riesgos valorados, agrupados por ambiente de ejecución y nivel de severidad.
Fuente: Elaboración propia.

Por otra parte, de los riesgos que están presentes en ambos ambientes de ejecución, casi todos (49 de 56) deben ser mitigados.

7. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y ESTABLECIMIENTO DE OBJETIVOS DE CONTROL

Este capítulo describe las políticas de seguridad de la información definidas para mitigar los riesgos presentes en los escenarios de firma digital seleccionados, así como los objetivos de control que las hacen cumplir. El capítulo inicia con la definición de las políticas de seguridad en cada uno de los escenarios analizados, y concluye con el establecimiento de objetivos de control que especifican los requerimientos mínimos que deben satisfacerse para hacer cumplir dichas políticas.

7.1. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

En esta sección se presenta un resumen de la definición de políticas de seguridad de la información definidas. En general, se definieron 103 políticas, las cuales se visualizan a continuación desde diferentes perspectivas².

CANTIDAD DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEFINIDAS, AGRUPADAS POR SERVICIO DE SEGURIDAD DE LA INFORMACIÓN

El GRÁFICO 6 muestra la cantidad de políticas de seguridad de la información definidas, agrupadas por servicio de seguridad de la información. En total, se definieron 103 políticas, de las cuales, la mayoría (48) corresponden a integridad. Lo anterior se debe a que en los escenarios analizados es mayor la cantidad de flujos de información entre componentes que la cantidad de componentes, por lo que deben asegurarse los datos que se intercambian entre ellos. Aun cuando en ese intercambio la confidencialidad es otro servicio que podría proveerse, en muchos casos no es tan crítico como la integridad para el correcto funcionamiento de los escenarios analizados. Por ejemplo, considere el resumen de un documento electrónico, que se transmite desde un componente de una aplicación a otro. Si alguien lograra interceptar ese resumen para ver su contenido, el impacto en la seguridad de la información es menor al que se daría si ese resumen fuera modificado. Adicionalmente, es necesario preservar la integridad de los componentes como tales, lo que incrementa la cantidad de políticas para este servicio de seguridad de la información.

² El detalle completo de las políticas de seguridad de la información definidas se presenta en el Apéndice E: Políticas de Seguridad de la Información Definidas.

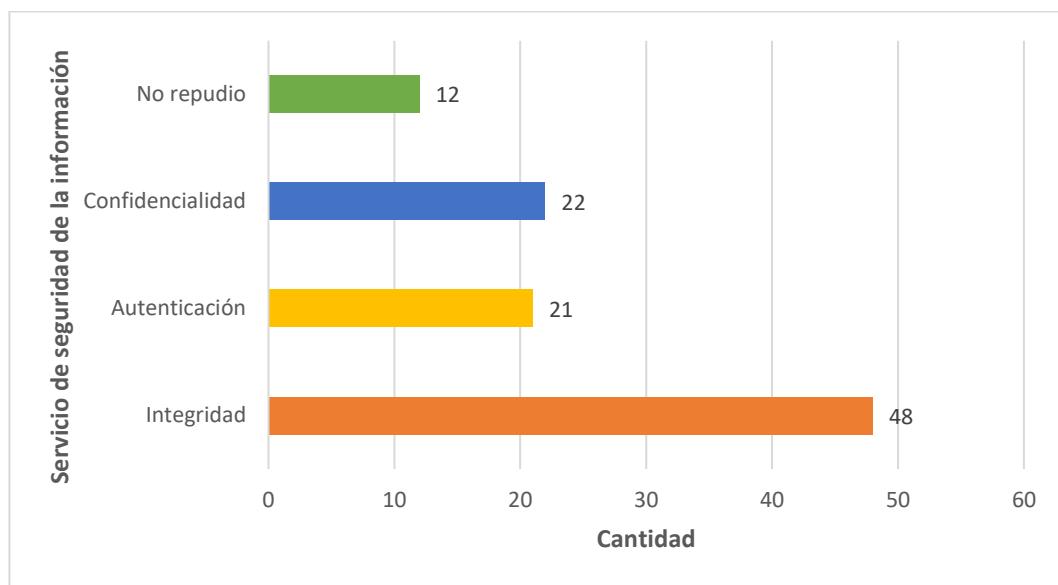


Gráfico 6. Cantidad de políticas de seguridad de la información definidas, agrupadas por servicio de seguridad de la información. Fuente: Elaboración propia.

Por otra parte, es destacable que, aunque este proyecto se enfoca en garantizar el no repudio de la información, este servicio es el que tiene la menor cantidad de políticas de seguridad definidas, con un total de 12. Ello se debe a que la PKI nacional mitiga de antemano muchos riesgos relacionados con el no repudio, por medio de la entrega de certificados digitales que identifican de forma única a los usuarios finales.

CANTIDAD DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEFINIDAS, AGRUPADAS POR ESCENARIO ANALIZADO Y SERVICIO DE SEGURIDAD DE LA INFORMACIÓN

El GRÁFICO 7 presenta la cantidad de políticas de seguridad de la información definidas, agrupadas por escenario analizado y servicio de seguridad de la información. El gráfico permite observar que, en los escenarios de verificación de firma digital y sello electrónico, y conversión de una firma digital en formato simple a formato avanzado, hay un predominio de políticas de integridad definidas en comparación con los otros servicios de seguridad de la información. Lo anterior se debe a que una amplia mayoría de los riesgos valorados que deben mitigarse están relacionados con cambios indebidos o no autorizados de datos que son fundamentales para el correcto funcionamiento de esos escenarios.

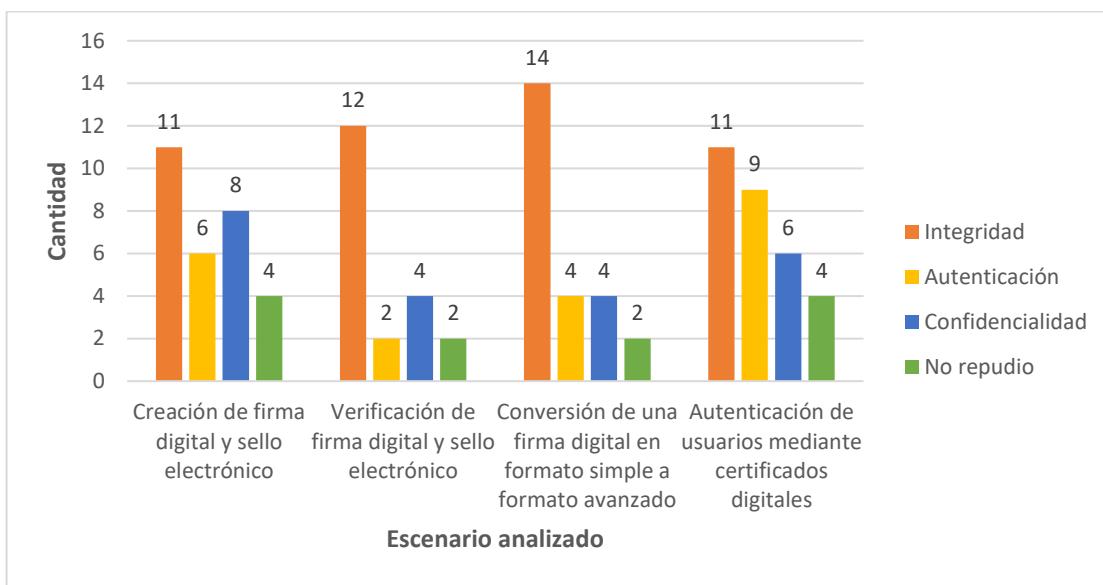


Gráfico 7. Cantidad de políticas de seguridad de la información definidas, agrupadas por escenario analizado y servicio de seguridad de la información. Fuente: Elaboración propia.

Por otra parte, en los escenarios de creación de firma digital y sello electrónico, y autenticación de usuarios mediante certificados digitales, aun cuando la mayor cantidad de políticas definidas también corresponden a integridad, hay un incremento en el número de políticas definidas para los otros servicios. Tome como ejemplo el escenario de autenticación de usuarios mediante certificados digitales. En él, la cantidad de políticas de autenticación se incrementa porque es necesario validar que el certificado digital utilizado es auténtico, y que también lo son las direcciones para acceder a los almacenes de certificados y a otros servicios requeridos (CRLs, OCSP y estampado de tiempo). A lo anterior debe sumarse que el acceso a la llave privada almacenada en el dispositivo criptográfico seguro debe estar dado solamente a usuarios autenticados. En cuanto a la confidencialidad, también aumenta el número de políticas, debido a que en este escenario es fundamental mantener en secreto las credenciales para autenticarse en el dispositivo criptográfico seguro. Por último, respecto al no repudio, en este escenario también aumenta ligeramente el número de políticas debido a que es crucial garantizar el uso de algoritmos *hash* seguros, y la vigencia del certificado digital utilizado, de las CRLs y de las solicitudes OCSP.

7.2. ESTABLECIMIENTO DE OBJETIVOS DE CONTROL

En esta sección se presenta un resumen de los objetivos de control establecidos para evaluar el cumplimiento de las políticas de seguridad de la información definidas. En general, se establecieron 26 objetivos de control, los cuales se visualizan a continuación desde diferentes perspectivas³.

CANTIDAD DE OBJETIVOS DE CONTROL ESTABLECIDOS, AGRUPADOS POR SERVICIO DE SEGURIDAD DE LA INFORMACIÓN

El GRÁFICO 8 muestra la cantidad de objetivos de control establecidos, agrupados por servicio de seguridad de la información. En él se observa que el servicio de integridad tiene la menor cantidad de objetivos de control establecidos, con un total de 5, lo cual es destacable, porque este servicio es el que tiene la mayor cantidad de políticas de seguridad definidas, con 48 en total. Lo anterior se debe a que los objetivos de control establecidos son capaces de especificar requerimientos mínimos que deben satisfacerse para hacer cumplir múltiples políticas. Por ejemplo, el objetivo de control número 3 —el cual establece que 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 validar el cumplimiento de 25 de las 48 políticas de integridad definidas.

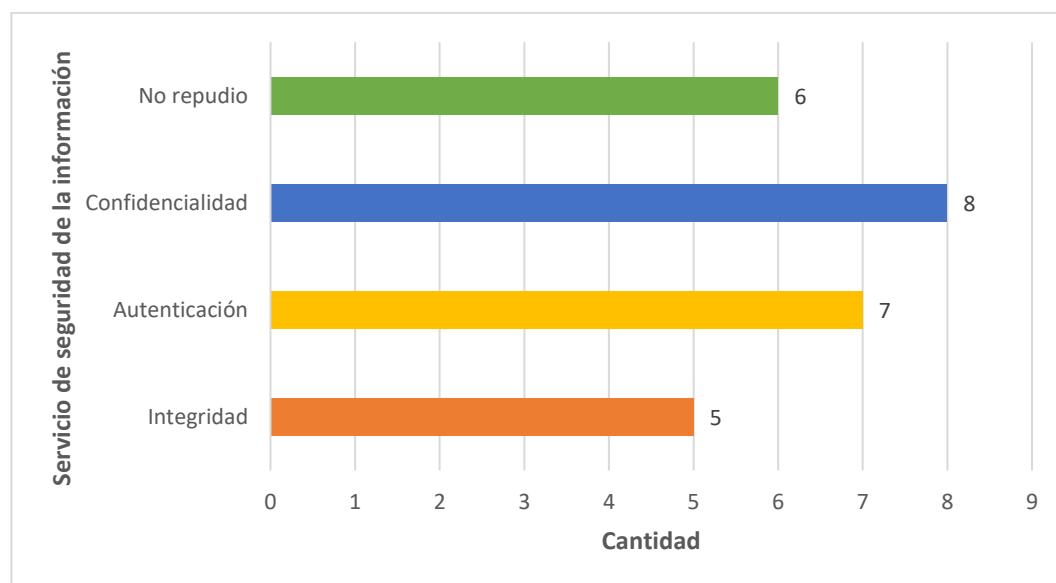


Gráfico 8. Cantidad de objetivos de control establecidos, agrupados por servicio de seguridad de la información. Fuente: Elaboración propia.

³ El detalle completo de los objetivos de control establecidos se presenta en el Apéndice F: Objetivos de Control Establecidos.

Por último, el servicio de confidencialidad es el que tiene la mayor cantidad de objetivos de control establecidos, con un total de 8. Lo anterior se debe a que existen políticas de seguridad definidas que requieren de más de un objetivo de control para evaluar su cumplimiento. Ejemplo de ello son las políticas 20 y 96, que requieren de la validación de los objetivos de control 15 y 20, o la política 18, que requiere de los objetivos de control 13 y 20.

8. GUÍA DE REQUERIMIENTOS TÉCNICOS PARA EL ASEGURAMIENTO DE LA INFORMACIÓN DE LOS COMPONENTES TECNOLÓGICOS QUE UTILIZAN CERTIFICADOS Y FIRMA DIGITAL EN APLICACIONES DE SOFTWARE DENTRO DEL SNCD

8.1. INTRODUCCIÓN

Dentro del Sistema Nacional de Certificación Digital (SNCD) se debe validar que las aplicaciones de *software* para implementar mecanismos de firma digital, que hacen uso de los certificados digitales emitidos dentro de dicho sistema, son seguras y confiables. La presente guía de implementación es un instrumento que permite evaluar el cumplimiento de un conjunto políticas de seguridad de la información 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.

8.2. DESCRIPCIÓN DE LA GUÍA DE IMPLEMENTACIÓN

En esta sección se describen los aspectos más relevantes en cuanto a la aplicabilidad y el modo de uso de esta guía de implementación.

8.2.1. ESCENARIOS DE USO

Los escenarios en los cuales esta guía de implementación puede ser utilizada, son aplicaciones de *software* que implementan al menos uno de los siguientes casos de uso de firma digital:

- Creación de firma digital y/o sello electrónico: es la creación de un conjunto de datos electrónicos que se asocian a un documento electrónico, con el propósito de identificar inequívocamente al firmante, y garantizar la integridad del documento.
- Verificación de firma digital y/o sello electrónico: es la validación de la identidad del firmante, la integridad del documento firmado y la validez del certificado digital utilizado para crear la firma.
- Autenticación de usuarios mediante certificados digitales: es el proceso de demostrar la posesión de una llave privada, con el fin de validar la identidad del usuario.

- Conversión de una firma digital en formato simple a formato avanzado: es la adición de atributos a un documento firmado electrónicamente con un formato básico, con el propósito de garantizar la validación a largo plazo de las firmas digitales contenidas en él.

8.2.2. SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

Esta guía de implementación define políticas de seguridad para los siguientes servicios de seguridad de la información:

- No repudio (NR): es una propiedad de datos y procesos, la cual previene que una entidad pueda negar el haber realizado una acción particular que sí realizó.
- Integridad (I): es la propiedad de la información que previene un cambio indebido o no autorizado de los datos.
- Autenticación (A): es la verificación de la identidad de un sujeto.
- Confidencialidad (C): es la propiedad que garantiza que la información no esté disponible ni se divulgue a personas o procesos no autorizados.

8.2.3. PASOS PARA APLICAR LA GUÍA DE IMPLEMENTACIÓN

Los pasos para aplicar esta guía de implementación se presentan en el diagrama de flujo de la FIGURA 26, y se describen a continuación:

1. Iterar sobre la lista de políticas de seguridad de la información a ser evaluadas, que se presenta en la sección 8.3, hasta que ya no queden políticas sin evaluar.
2. Para cada política, se debe determinar si ésta es aplicable en el contexto de la evaluación.
3. Si la política no es aplicable, debe marcarse como tal. Adicionalmente, se debe crear una observación en la lista de observaciones de la evaluación (sección 8.5), que indique las razones por las cuales la política no aplica. La observación debe referenciarse desde la política. Finalmente, se debe actualizar la entrada correspondiente a la política en la tabla resumen de la evaluación (sección 8.6), indicando que la política no es aplicable.
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 presentan en la sección 8.4.
5. Si al menos un control de seguridad implementado no satisface los requisitos establecidos por el objetivo de control correspondiente, se debe marcar en la política que su cumplimiento es negativo. Adicionalmente, se debe crear una observación en la lista de

observaciones de la evaluación, que indique las razones por las cuales la política no se cumple. La observación debe referenciarse desde la política. Finalmente, se debe actualizar la entrada correspondiente a la política en el cuadro resumen de la evaluación, indicando que la política no se cumple.

6. Si todos los controles de seguridad implementados satisfacen los requisitos de seguridad establecidos por los objetivos de control, se debe marcar en la política que su cumplimiento es positivo, y se debe actualizar la entrada correspondiente a la política en el cuadro resumen de la evaluación, indicando que la política sí se cumple.

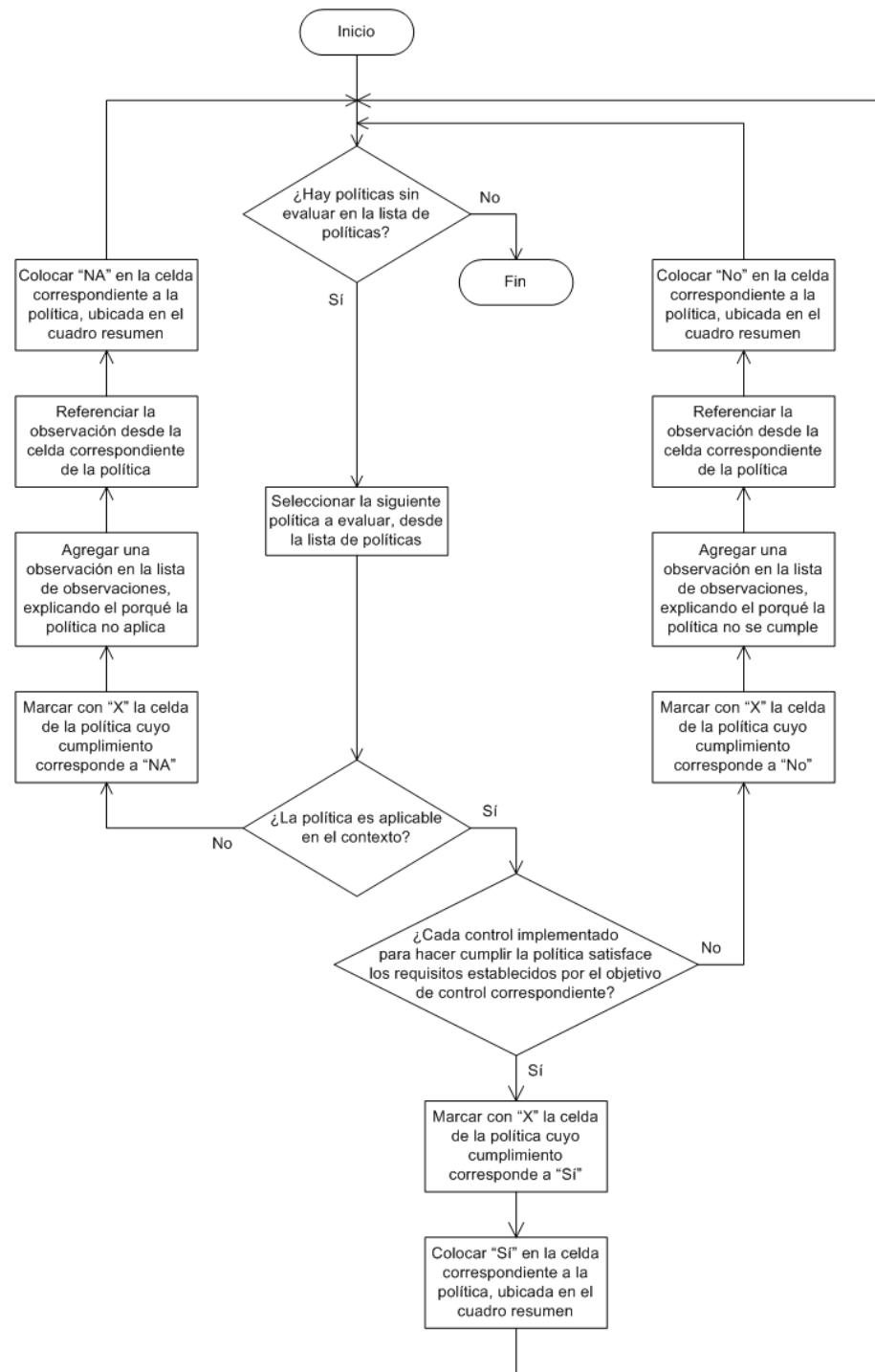


Figura 26. Diagrama de flujo para aplicar la guía de implementación. Fuente: Elaboración propia.

8.3. LISTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN A SER EVALUADAS

Las tablas 14, 15, 16 y 17 presentan las políticas de seguridad de la información a ser evaluadas⁴.

Tabla 14. Políticas de seguridad para la creación de firma digital y sello electrónico. Fuente: Elaboración propia.

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observaciones
				Sí	No	NA	
1	I	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.	1				
...	I				
12	A	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.	6				
...	A				
18	C	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.	13, 20				
...	C				
26	NR	El resumen del documento electrónico que se va a firmar debe calcularse utilizando algoritmos <i>hash</i> seguros.	21				
...	NR				

⁴ Con el fin de evitar la duplicación de información, solamente se incluyen algunas políticas de seguridad. En su formato completo, la guía de implementación debe incluir todas las políticas de seguridad de la información definidas en el Apéndice E: Políticas de Seguridad de la Información Definidas.

Tabla 15. Políticas de seguridad para la verificación de firma digital y sello electrónico. Fuente: Elaboración propia.

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observaciones
				Sí	No	NA	
30	I	Se debe validar que el formato del documento electrónico cuyas firmas se van a verificar, está soportado por el SNCD y por la aplicación, y que además es correcto.	1				
...	I				
42	A	Se debe validar que todos los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar, pertenecen a la jerarquía nacional de certificadores registrados.	8				
...	A				
44	C	Se debe proteger el documento electrónico cuyas firmas se van a verificar, así como sus representaciones derivadas (resúmenes cifrados extraídos, documento electrónico original, resumen del documento electrónico original, resúmenes descifrados), mientras se transmiten por red, de manera que no puedan ser revelados a usuarios no autorizados.	17				
...	C				
48	NR	Se debe validar que todos los certificados digitales, así como sus rutas de certificación, estaban vigentes cuando se incluyeron en el documento electrónico cuyas firmas se van a verificar.	22				
...	NR				

Tabla 16. Políticas de seguridad para la conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observaciones
				Sí	No	NA	
50	I	Se debe validar que el formato del documento electrónico cuyo formato se convertirá, está soportado por la aplicación, es correcto y puede convertirse a un formato avanzado válido.	1, 2				
...	I				
64	A	La dirección requerida para acceder al servicio que provee las CRL debe extraerse directamente del certificado, y de ninguna manera debe estar contenida en el código fuente, archivos de texto, base de datos o cualquier otro tipo de almacenamiento.	12				
...	A				
68	C	Se debe validar que el documento electrónico resultante, firmado en formato avanzado, no se entregue a usuarios no autorizados.	16				
...	C				
72	NR	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	25				
...	NR				

Tabla 17. Políticas de seguridad para la autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observaciones
				Sí	No	NA	
74	I	Se debe proteger la información de revocación del certificado digital que se utilizará durante el proceso de autenticación, obtenida mediante CRL, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	3				
...	I				
85	A	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.	6				
...	A				
94	C	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 alguien más.	13, 20				
...	C				
100	NR	El resumen de los datos de autenticación que se van a firmar debe calcularse utilizando algoritmos <i>hash</i> seguros.	21				
...	NR				

8.4. LISTA DE OBJETIVOS DE CONTROL PARA EVALUAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La TABLA 18 presenta los objetivos de control que permiten evaluar la efectividad de los controles de seguridad implementados para hacer cumplir las políticas de seguridad de la información definidas⁵.

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.

No.	Servicio de seguridad	Objetivo de Control	Políticas
1	I	<p>Se deben validar los datos que el usuario introduce en el sistema, verificando que cada entrada cumple al menos con los siguientes requisitos:</p> <p><i>Cuando la entrada es texto</i></p> <ul style="list-style-type: none"> • 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 mínimo y máximo 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. <p>...</p>	1, 2, 30, 31, 50

⁵ Con el fin de evitar la duplicación de información, solamente se incluyen algunos objetivos de control. En su formato completo, la guía de implementación debe incluir todos los objetivos de control establecidos en el Apéndice F: Objetivos de Control Establecidos.

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.
(Continuación)

No.	Servicio de seguridad	Objetivo de Control	Políticas
2	I	Se debe validar que los formatos de documento firmado en formato simple corresponden a alguno de los siguientes: PKCS#7, CMS, XMLDSig y PDF 1.7, y rechazar los demás.	3, 50
3	I	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.	4, 5, 6, 7, 32, 33, 34, 35, 36, 52, 53, 54, 55, 56, 57, 58, 59, 60, 74, 75, 76, 77, 78, 79, 80
...	I
6	A	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.	12, 85
...	A

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.
(Continuación)

No.	Servicio de seguridad	Objetivo de Control	Políticas
8	A	La pertenencia del certificado digital a la jerarquía nacional de certificadores registrados se debe implementar mediante una validación que sea funcionalmente equivalente al algoritmo descrito en la sección 6.1 del RFC 5280 (Cooper et al., 2008).	14, 42
...	A

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.
(Continuación)

No.	Servicio de seguridad	Objetivo de Control	Políticas
12	A	<p>Las direcciones para acceder a la CRL, el servicio OCSP, el certificado de la CA emisora (para validar la ruta de certificación) y el servicio de estampado de tiempo, se deben extraer de la siguiente manera:</p> <ul style="list-style-type: none"> • <u>CRL</u>: el valor está contenido en el certificado, y dado por el campo <i>Punto de distribución del CRL</i>, como lo indica la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013). • <u>OCSP</u>: el valor está contenido en el certificado, y dado por la primera posición del campo <i>Acceso a la información de la autoridad</i>, como lo indica la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013). • <u>Certificado de la CA emisora</u>: el valor está contenido en el certificado, y dado por la segunda posición del campo <i>Acceso a la información de la autoridad</i>, como lo indica la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013). • <u>Servicio de estampado de tiempo</u>: el valor está definido en la sección 6.1 del <i>Estándar electrónico – Servicios Firma Digital en Internet</i> (SINPE, 2016). 	64, 65, 66, 67, 90, 91, 92, 93

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.
(Continuación)

No.	Servicio de seguridad	Objetivo de Control	Políticas
13	C	<p>La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro debe cumplir al menos con los siguientes requisitos:</p> <ul style="list-style-type: none"> • 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. 	18, 94
...	C
16	C	Para que la entrega del documento electrónico firmado sea posible, se debe satisfacer al menos un control de autorización.	21, 68
17	C	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.	22, 44, 69, 97
...	C

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.
(Continuación)

No.	Servicio de seguridad	Objetivo de Control	Políticas
20	C	<p>Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, <i>malware</i> y cualquier otro tipo de <i>software</i> malicioso que facilite la divulgación no autorizada de datos, utilizando los siguientes criterios:</p> <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final</i></p> <p>Se debe validar la existencia de un procedimiento periódico, ejecutado como máximo cada 7 días naturales, 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:</p> <ul style="list-style-type: none"> • 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. • Lista de archivos analizados. • Resultado del análisis. <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final</i></p> <ul style="list-style-type: none"> • ... 	23, 45, 94

Tabla 18. Objetivos de control definidos para evaluar el cumplimiento de las políticas de seguridad de la información. Fuente: Elaboración propia.
(Continuación)

No.	Servicio de seguridad	Objetivo de Control	Políticas
21	NR	Se debe validar que los algoritmos de <i>hash</i> utilizados son seguros, y tienen una efectividad igual o superior a SHA-2, y rechazar los demás.	26, 49, 100
22	NR	<p>La validación de la vigencia del certificado debe cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> • 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. 	27, 48, 101
...	NR
25	NR	Para validar la vigencia de una CRL, debe verificarse que la fecha al momento de utilizar esa lista es anterior a la especificada en el campo llamado <i>Siguiente actualización</i> .	72, 102
...	NR

8.5. LISTA DE OBSERVACIONES DE LA EVALUACIÓN

La TABLA 19 provee un espacio para anotar cualquier observación relevante encontrada durante el proceso de evaluación. Cada observación debe tener un identificador numérico, y debe ser referenciada desde la política de seguridad correspondiente.

Tabla 19. Espacio para anotar observaciones encontradas durante el proceso de evaluación. Fuente: Elaboración propia.

8.6. TABLA RESUMEN DE LA EVALUACIÓN

La TABLA 20 permite mantener un resumen del estado de la evaluación durante la aplicación de la guía. Se debe colocar en cada casilla un valor (*Sí*, *No* o *NA*), según el grado de cumplimiento de la política correspondiente.

Tabla 20. Tabla desarrollada para mantener un resumen de la evaluación. Fuente: Elaboración propia.

Creación de firma digital y sello electrónico												
Servicios de seguridad	I	1	2	3	4	5	6	7	8	9	10	11
	A	12	13	14	15	16	17					
	C	18	19	20	21	22	23	24	25			
	NR	26	27	28	29							
	Verificación de firma digital y sello electrónico											
	I	30	31	32	33	34	35	36	37	38	39	40
	A	42	43									
	C	44	45	46	47							
	NR	48	49									
	Conversión de una firma digital en formato simple a formato avanzado											
	I	50	51	52	53	54	55	56	57	58	59	60
	A	64	65	66	67							
	C	68	69	70	71							
	NR	72	73									
	Autenticación de usuarios mediante certificados digitales											
	I	74	75	76	77	78	79	80	81	82	83	84
	A	85	86	87	88	89	90	91	92	93		
	C	94	95	96	97	98	99					
	NR	100	101	102	103							

9. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

En este capítulo se presentan las conclusiones de los principales hallazgos y logros al completar el presente trabajo. Adicionalmente, se propone una serie de recomendaciones que surgen a partir de los resultados, y se trazan las pautas a seguir como trabajo futuro.

9.1. CONCLUSIONES

La revisión de la literatura desarrollada en esta investigación permitió identificar que países como Francia, España y Brasil disponen de soluciones a nivel nacional para asegurar la información de aplicaciones de software que implementan mecanismos de firma digital. Esto significa que iniciativas similares a este trabajo, orientadas al aseguramiento de la información de este tipo de aplicaciones, han sido aceptadas y soportadas por países que desarrollaron importantes estrategias de gobierno electrónico.

Tomando como insumo los requerimientos gubernamentales planteados por la directriz 067-MICITT-H-MEIC (Gobierno de Costa Rica, 2014), más el criterio de expertos disponibles a nivel nacional en materia de firma digital, se recopiló la lista de escenarios de uso más relevante en el contexto de aplicaciones de *software* dentro del SNCD, dentro de los cuales se cuentan: la creación de firma digital y sello electrónico, la verificación de firma digital y sello electrónico, la conversión de una firma digital en formato simple a formato avanzado y la autenticación de usuarios mediante certificados digitales. La identificación de dichos escenarios es de suma importancia, pues permite generar conciencia acerca de las correctas consideraciones de seguridad que deben tomar en cuenta las instituciones que utilizan firma digital en la prestación de sus servicios.

En relación con el análisis de riesgos y la definición de políticas de seguridad de la información, en este proyecto se utilizó una metodología que es sistemática, pues permite ser aplicada a todos los componentes de un sistema en el nivel de detalle deseado, y, adicionalmente, es sistemática, debido a la forma ordenada en que se pueden analizar los requisitos de seguridad. En el contexto de las aplicaciones de *software* dentro del SNCD, estas características propician la definición de líneas guía de amplia cobertura, que permiten mejorar la calidad y la seguridad de los servicios provistos por las instituciones públicas y privadas, a las cuales el Gobierno de la República les ha ordenado poner a disposición de los ciudadanos, a través de medios electrónicos, los mismos servicios que tradicionalmente han recibido a través de medios de atención convencionales.

En esta investigación se utilizaron objetivos de control —estableciendo una definición propia del término— como líneas base genéricas que facilitan la evaluación de requisitos de seguridad de la información, y permiten determinar si una política de seguridad se cumple exitosamente o no. Lo anterior es relevante en el proceso de aseguramiento de la información desarrollado en este proyecto, porque facilita la aplicación de dicho proceso a grupos de aplicaciones de *software* con objetivos de seguridad similares, pero que han sido desarrollados con tecnologías heterogéneas.

A partir de los escenarios analizados, los riesgos identificados y valorados, las políticas definidas y los objetivos de control establecidos, se definió una guía de implementación que recopila los requisitos de seguridad que deben cumplir las aplicaciones de *software* que implementan firma digital dentro del SNCD. Esta guía puede usarse como una lista de requerimientos de seguridad de la información predefinidos, que deben ser tomados en cuenta por quienes estén a cargo de diseñar y desarrollar nuevas aplicaciones de este tipo. Adicionalmente, la guía puede servir como instrumento de evaluación para aquellas personas responsables de dar mantenimiento a aplicaciones existentes, con el fin de auditar el cumplimiento de dichos requerimientos.

9.2. RECOMENDACIONES

Dado que las tecnologías de la información y comunicación evolucionan continuamente, se recomienda revisar de forma periódica los requisitos de seguridad definidos en este proyecto. Lo anterior puede lograrse a través de nuevas iteraciones aplicadas a los diagramas de flujos de información generados, para así conservar el enfoque sistémico y sistemático. De esta manera, sería posible identificar y mitigar nuevos riesgos que pudieran aparecer como resultado de la constante evolución tecnológica.

También se recomienda someter la guía de implementación resultante a revisión de expertos. Esto permitiría obtener retroalimentación de personas con amplio conocimiento en materia de seguridad de la información y firma digital, con el fin de enriquecer la propuesta desarrollada en este trabajo.

Adicionalmente, se propone comparar la guía de implementación resultante con las soluciones encontradas en Brasil, España y Francia. Esto habilitaría el establecimiento de un conjunto de similitudes y diferencias que deben ser estudiadas, con el fin de tomar las acciones necesarias para ajustar los requisitos de seguridad propuestos en este proyecto, según corresponda.

9.3. TRABAJO FUTURO

Con base en la guía de implementación desarrollada, se debe crear una norma técnica a nivel nacional que permita a las instituciones que utilizan aplicaciones de *software* con firma digital, certificar que dicho software cumple con los requisitos de seguridad propuestos dentro del SNCD. Para alcanzar este objetivo, la guía de implementación desarrollada en esta investigación puede servir como el documento técnico que especifica los requisitos para la certificación.

Por último, aunque el proceso de aseguramiento de la información desarrollado en este proyecto es efectivo, realizarlo de forma manual es complejo. Por lo tanto, se sugiere desarrollar herramientas de *software* que faciliten la ejecución de procesos de aseguramiento de la información similares a este.

10. BIBLIOGRAFÍA

Administración General del Estado. (2012). *Política de Firma Electrónica y de Certificados de la Administración General del Estado.*

Adobe Systems Incorporated. (2008). *Document management — Portable document format — Part 1: PDF 1.7.* Obtenido de Adobe: http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf

Agence Nationale de la Sécurité des Systèmes d'Information. (2008). *Protection Profile Electronic Signature Creation Application.* Obtenido de https://www.commoncriteriaportal.org/files/ppfiles/DCSSI-profil_PP-2008-05en-1.pdf

Agence Nationale de la Sécurité des Systèmes d'Information. (2008). *Protection Profile Electronic Signature Verification Module.* Obtenido de <https://www.commoncriteriaportal.org/files/ppfiles/pp200806en.pdf>

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.

Ash, R. (2008). *Basic probability theory.* New York: Dover Publications, Inc.

Barquero, A. (Setiembre de 2014). *Comunicación personal.*

BCCR. (2014). *Oficinas de Registro.* Obtenido de http://www.bccr.fi.cr/firma_digital/firma_digital.html

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

Bishop, M. (2004). *Introduction to Computer Security.* Addison-Wesley Professional.

Buchmann, J., Evangelos, K., & Wiesmaier, A. (2013). *Introduction to Public Key Infrastructures.* Springer.

Certificate.Net. (2015). *FSS Notification.* Obtenido de <http://certificate.net/FSS-notification>

Colombia Digital. (2015). *La firma electrónica y la firma digital: mitos y realidades.* Obtenido de <http://www.colombiadigital.net/opinion/columnistas/certicamara/item/8078-la-firma-electronica-y-la-firma-digital-mitos-y-realidades.html>

Congreso de Colombia. (1999). *LEY 527 DE 1999 (agosto 18) por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* Obtenido de <http://www.alcaldiabogota.gov.co/sisjur/normas/Normal1.jsp?i=4276>

- Congreso General de los Estados Unidos Mexicanos. (2012). *Ley de firma electrónica avanzada*. Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf>
- CVE Details. (2015). *Vulnerabilities By Type*. Obtenido de CVE Details - The ultimate security vulnerability datasource: <http://www.cvedetails.com/vulnerabilities-by-types.php>
- Del Río Sánchez , J. (2014). *2.3 Tipos de métodos (inductivo, deductivo, analítico, sintético, comparativo, dialéctico, entre otros)*. Obtenido de Fundamentos de Investigación: <https://sites.google.com/site/tectijuanafi/unidad-ii/2-3-tipos-de-metodos-inductivo-deductivo-analitico-sintetico-comparativo-dialectico-entre-otros>
- Dierks, T., & Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. Obtenido de The Internet Engineering Task Force (IETF): <https://www.ietf.org/rfc/rfc5246.txt>
- Entidad Acreditadora. (2016). *Normas Técnicas*. Obtenido de <https://www.entidadacreditadora.gob.cl/normas-tecnicas/>
- European Committee for Standardization. (2004). *CWA 14170 Security requirements for signature creation applications*. Bruselas: CEN.
- European Committee for Standardization. (2004). *CWA 14171 General guidelines for electronic signature verification*. Bruselas: CEN.
- Federal Gazette. (2001). *Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations*. Obtenido de http://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/Areas/ElectronicSignature/LegalUnderpinnings/FrameworkforElectronicSignalId1850pdf.pdf?__blob=publicationFile
- Federal Office for Information Security. (2012). *Technical information on the IT security certification of products, protection profiles and sites*. Obtenido de https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7138_e_pdf.pdf?__blob=publicationFile&v=1
- Federal Office for Information Security. (2016). *Certified products - Digital Signature*. Obtenido de https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/Digitale_Signatur/Digitale_Signatur_node.htm#doc6618630bodyText3
- Fedict. (2015). *Developing eID applications*. Obtenido de http://eid.belgium.be/en/developing_eid_applications
- Fedict. (2015). *The Electronic Identity Card (eID) - Developers guide*. Obtenido de https://downloads.services.belgium.be/eid/UPD_Developers_Guide.pdf

Fedict. (2015). *The electronic identity documents.* Obtenido de http://eid.belgium.be/en/find_out_more_about_the_eid/the_electronic_identity_documents/he_eid

Gobierno de Chile. (2002). *SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACION DE DICHA FIRMA.* Obtenido de Biblioteca del Congreso Nacional de Chile: <http://www.leychile.cl/Navegar?idNorma=196640&idVersion=2007-11-12>

Gobierno de Chile. (2007). *MODIFICA EL CÓDIGO DE PROCEDIMIENTO CIVIL Y LA LEY N° 19.799 SOBRE DOCUMENTO ELECTRÓNICO, FIRMA ELECTRÓNICA Y LOS SERVICIOS DE CERTIFICACIÓN DE DICHAS FIRMAS.* Obtenido de Biblioteca del Congreso Nacional de Chile: <http://www.leychile.cl/Navegar?idNorma=266348&buscar=20217>

Gobierno de Colombia. (2012). *DECRETO 2364 DE 2012 (Noviembre 22) Por medio del cual se reglamenta el artículo 7º de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.* Obtenido de <http://www.alcaldiabogota.gov.co/sisjur/normas/Normal.jsp?i=50583#0>

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

Gobierno de Costa Rica. (2006). *Reglamento a la ley de certificados, firmas digitales y documentos electrónicos.* Costa Rica: Decreto Ejecutivo No 33018-MICIT.

Gobierno de Costa Rica. (20 de Mayo de 2013). Política de certificados para la jerarquía nacional de certificadores registrados. Dirección de Certificadores de Firma Digital.

Gobierno de Costa Rica. (20 de Mayo de 2013). Política de formatos oficiales de los documentos electrónicos firmados digitalmente. Dirección de Certificadores de Firma Digital.

Gobierno de Costa Rica. (25 de Abril de 2014). Masificación de la implementación y el uso de la firma digital en el sector público costarricense. *Diario Oficial La Gaceta*, págs. 49-51.

Gobierno de España. (2003). LEY 59/2003, de 19 de diciembre, de firma electrónica. *Boletín Oficial del Estado*, págs. 45329-45343.

Gobierno de Francia. (2016). *Code Civil.* Obtenido de https://www.legifrance.gouv.fr/affichCode.do;jsessionid=D38DDE67F1A153D577E3EA7BD40A30CE.tpdila17v_1?idSectionTA=LEGISCTA000006165596&cidTexte=LEGITEXT000006070721&dateTexte=20160221

Gobierno de México. (2014). *Reglamento de la Ley de Firma Electrónica Avanzada.* Obtenido de http://dof.gob.mx/nota_detalle.php?codigo=5337860&fecha=21/03/2014

- Gobierno de Rusia. (2002). *Federal Law of the Russian Federation on the electronic digital signature.* Obtenido de <http://calligraphy-expo.com/eng/AboutCalligraphy/Signatures/History.aspx?ItemID=1513>
- Gobierno de Rusia. (2011). *The federal law from 06.04.2011 N 63-FZ "On electronic signature".* Obtenido de http://www.consultant.ru/document/cons_doc_LAW_112701/
- Goldreich, O. (2004). *The Foundations of Cryptography - Volume 2.* Cambridge University Press.
- Housley, R. (2004). *Cryptographic Message Syntax (CMS).* Obtenido de The Internet Engineering Task Force (IETF): <https://www.ietf.org/rfc/rfc3852.txt>
- ICP-Brasil. (2007). *Manual de Condutas Técnicas 4 - Volume I Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Assinatura Digital no Âmbito da ICP-Brasil.* Obtenido de http://www.iti.gov.br/images/servicos/homologacao/MCT4_Vol.I.pdf
- ICP-Brasil. (2007). *Manual de Condutas Técnicas 4 - Volume II Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de Assinatura Digital no Âmbito da ICP-Brasil.* Obtenido de http://www.iti.gov.br/images/servicos/homologacao/MCT4_-_Vol.II.pdf
- ICP-Brasil. (2007). *Manual de Condutas Técnicas 5 - Volume I Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Autenticação no Âmbito da ICP-Brasil.* Obtenido de http://www.iti.gov.br/images/servicos/homologacao/MCT5_Vol_I.pdf
- ICP-Brasil. (2007). *Manual de Condutas Técnicas 5 - Volume II Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de Autenticação no Âmbito da ICP-Brasil.* Obtenido de http://www.iti.gov.br/images/servicos/homologacao/MCT5_-_Vol.II.pdf
- Instituto de Normas Técnicas de Costa Rica. (2007). *Norma INTE/ISO 21188:2007 - Infraestructura de llave pública para servicios financieros - Estructura de prácticas y políticas.* San José, Costa Rica.
- Instituto Nacional de Tecnologías de la Comunicación. (2009). *PPSCVA-T1, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante y nivel de evaluación de los requisitos de seguridad EAL1.* Obtenido de https://oc.ccn.cni.es/pdf/INTECO_PPSCVA_T1_EAL1_v2.0.pdf
- Instituto Nacional de Tecnologías de la Comunicación. (2009). *PPSCVA-T1, EAL3. Perfil de Protección la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante y con nivel de evaluación de los requisitos de seguridad EAL3.* Obtenido de https://oc.ccn.cni.es/pdf/INTECO_PPSCVA_T1_EAL3_v2.0.pdf

- Instituto Nacional de Tecnologías de la Comunicación. (2009). *PPSCVA-T2, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL1.* Obtenido de https://oc.ccn.cni.es/pdf/INTECO_PPSCVA_T2_EAL1_v2.0.pdf
- Instituto Nacional de Tecnologías de la Comunicación. (2009). *PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3.* Obtenido de https://oc.ccn.cni.es/pdf/INTECO_PPSCVA_T2_EAL3_v2.0.pdf
- Jøsang, A., & AlFayyadh, B. (2008). Robust WYSIWYS: a method for ensuring that what you see is what you sign. *6th Australasian Information Security Conference* (págs. 53-58). Wollongong: Australian Computer Society, Inc.
- Kaliski, B. (1998). *PKCS #7: Cryptographic Message Syntax Version 1.5.* Obtenido de The Internet Engineering Task Force (IETF): <https://www.ietf.org/rfc/rfc2315.txt>
- Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography.* CRC Press.
- Kiran, S., Lareau, P., & Lloyd, S. (2002). *PKI Basics - A Technical Perspective.* (P. Forum, Editor) Obtenido de OASIS PKI: PKI Basics - A Technical Perspective
- Leigh, N. (25 de Mayo de 2016). *What are Control Objectives?* Obtenido de Objective Controls The Risk Management App: http://www.objectivecontrols.com/blog_2016/2016-05-15_what_are_control_objectives.html
- Longley, D., & Shain, M. (1989). *Dictionary of standards concepts and terms.* Macmillan Publishers Ltd.
- Lowagie, B. (2012). Digital Signatures for PDF documents. iText Software.
- 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* (págs. 306-310). New York: IEEE.
- Mazzeo, M. (2010). *Digital Signatures and European Laws.* Obtenido de <http://www.symantec.com/connect/articles/digital-signatures-and-european-laws>
- Menezes, A., van Oorschot, P., & Vanstone, S. (1997). *Handbook of Applied Cryptography.* CRC Press.
- MICITT. (2016). *¿Qué beneficios ofrece?* Obtenido de Mi Firma Digital: <http://www.mifirmadigital.go.cr/>
- MICITT. (2016). *¿Qué es la firma digital?* Obtenido de Mi Firma Digital: <http://www.mifirmadigital.go.cr/>

- MICITT. (2016). *Jerarquía Nacional*. Obtenido de Sistema Nacional de Certificación Digital: <http://www.firmadigital.go.cr/jerarquia.html>
- MICITT. (2017). *Entidades que utilizan Firma Digital*. Obtenido de Mi Firma Digital: <http://www.mifirmadigital.go.cr/fdigital/pdf/fd-instituciones.pdf>
- Microsoft. (2002). *Microsoft Computer Dictionary*. Microsoft Press.
- Microsoft. (2015). *Cryptographic Keys*. Obtenido de [https://msdn.microsoft.com/en-us/library/windows/desktop/aa380241\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa380241(v=vs.85).aspx)
- Ministry of Finance. (2000). *Law on electronic signatures*. Obtenido de <https://www.retsinformation.dk/forms/r0710.aspx?id=6193>
- National Institute of Standards and Technology. (2012). *SP 800-30. Guide for Conducting Risk Assessments*. Gaithersburg, MD: NIST.
- Naumov, V., & Nikiforova, T. (2005). *Electronic Signatures in Russia Law*. Obtenido de Russian Law: <http://www.russianlaw.net/files/law/english/ae08.doc>
- OpenOCES. (2014). *OpenSign*. Obtenido de <http://www.openoces.org/opensign/index.html>
- OWASP. (16 de Junio de 2014). *OWASP Periodic Table of Vulnerabilities*. Obtenido de OWASP: https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities
- OWASP. (12 de Setiembre de 2015). *Guide to Cryptography*. Obtenido de https://www.owasp.org/index.php/Guide_to_Cryptography
- OWASP. (3 de Setiembre de 2015). *OWASP Risk Rating Methodology*. Obtenido de OWASP: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- Presidência da República. (2001). *Medida Provisória No 2.200-2, de 24 de AGOSTO de 2001*. Obtenido de http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm
- Public Company Account Oversight Board. (2017). *APPENDIX A - Definitions*. Obtenido de Auditing Standard No. 5 An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements: https://pcaobus.org//Standards/Auditing/Pages/Auditing_Standard_5_Appendix_A.aspx
- Shirey, R. (1994). *Security Architecture for Internet Protocols: A Guide for Protocol Designs and Standards*. Internet Engineering Task Force.
- SINPE. (2016). *Firma Digital*. Obtenido de Banco Central de Costa Rica: http://www.bccr.fi.cr/firma_digital/EEFIRMAINTERNET.pdf
- Sistema Integral de Gestión Registral. (2008). *Marco legal*. Obtenido de <http://www.firmadigital.gob.mx/marcolegal.html>

- Spacey, J. (21 de Febrero de 2011). *The Big List of Information Security Vulnerabilities*. Obtenido de Simplicable: <http://simplicable.com/new/the-big-list-of-information-security-vulnerabilities>
- The European Parliament. (13 de Diciembre de 1999). *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. Obtenido de <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31999L0093&from=EN>
- The PHP Group. (2017). *Prepared statements and stored procedures*. Obtenido de PHP.net: <http://php.net/manual/en/pdo.prepared-statements.php>
- Vandendriessche, J. (2004). *Introduction to the Belgian laws on e-signatures*. Obtenido de <http://sas-space.sas.ac.uk/5461/1/1732-2329-1-SM.pdf>
- 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.
- Villalón-Fonseca, R., Mora-Castro, A., Bartels-González, R., Carballo-Chavarría, M., & Marín-Raventós, G. (2016). Promoting Quality E-government Solutions by Applying a Comprehensive Information Assurance Model: Use Cases for Digital Signature. San José, Costa Rica.
- Víquez, P., & Montes, M. (2013). *Modelo de implementación de mecanismos de firma digital*. Costa Rica: Universidad Nacional.
- Virginia Information Technologies Agency. (2006). *ITRM Guideline SEC506-01. Appendix D – Risk Management Guideline Assessment Instructions*. Chester, VA: VITA.
- W3C. (2008). *XML Signature Syntax and Processing (Second Edition)*. Obtenido de W3C: <https://www.w3.org/TR/xmldsig-core/>

11. APÉNDICES

11.1. APÉNDICE A: RIESGOS IDENTIFICADOS

El presente apéndice muestra todos los riesgos identificados después de aplicar la metodología seleccionada. La TABLA 21 lista los riesgos identificados en el escenario de creación de firma digital y sello electrónico. En la TABLA 22 se describen los riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Por otra parte, en la TABLA 23 se muestran los riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. En la TABLA 24 se presentan los riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Por último, la TABLA 25 indica los riesgos que son comunes a todos los escenarios.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
1	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico”.
2	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Contenedor del documento electrónico” permiten a un atacante malintencionado modificar el contenido del documento electrónico mientras éste se encuentra almacenado dicho componente.
3	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde el componente “Contenedor del documento electrónico” hacia el componente “Validador del documento electrónico”.
4	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del documento electrónico” permiten que la aplicación acepte del usuario documentos electrónicos cuyos formatos no son soportados o son incorrectos.
5	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Validador del documento electrónico” permiten que la aplicación acepte de un atacante malintencionado documentos electrónicos que contienen código oculto o malicioso.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
6	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del documento electrónico, mientras se transmite desde el componente “Validador del documento electrónico” hacia el componente “Contenedor del documento electrónico”.
7	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde el componente “Contenedor del documento electrónico” hacia el componente “Formateador del documento electrónico”.
8	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Calculador del resumen” permiten que la aplicación genere resúmenes a partir del uso de algoritmos <i>hash</i> inseguros.
9	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde el componente “Formateador del documento electrónico” hacia el componente “Calculador del resumen”.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
10	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico formateado, mientras se transmite desde el componente “Formateador del documento electrónico” hacia el componente “Constructor del documento electrónico firmado”.
11	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen del documento electrónico, mientras se transmite desde el componente “Calculador del resumen” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.
12	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación acceda a las operaciones criptográficas del “Dispositivo criptográfico seguro” sin utilizar un mecanismo de autenticación.
13	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación revele las credenciales de autenticación del “Dispositivo criptográfico seguro” a sus usuarios.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
14	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación revele las credenciales de autenticación del “Dispositivo criptográfico seguro” a un atacante malintencionado que ejecuta un ataque de fuerza bruta.
15	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen del documento electrónico, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el “Dispositivo criptográfico seguro”.
16	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación almacene en caché las credenciales del “Dispositivo criptográfico seguro” para uso posterior.
17	Centralizado y Distribuido	Defectos en el <i>hardware</i>	Usuario	Defectos en el componente “Dispositivo criptográfico seguro” permiten que la aplicación genere datos cifrados mediante el uso de algoritmos de cifrado inseguros.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
18	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado del documento electrónico, mientras se transmite desde el componente “Dispositivo criptográfico seguro” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.
19	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado del documento electrónico, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Constructor del documento electrónico firmado”.
20	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital que será utilizado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del certificado”.
21	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Contenedor del certificado” permiten a un atacante malintencionado modificar el certificado digital mientras éste se encuentra almacenado en dicho componente.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
22	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Validador del certificado”.
23	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación acepte del usuario certificados digitales inválidos.
24	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente de “Interacción con el usuario” permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.
25	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación.
26	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del certificado, mientras se transmite desde el componente “Validador del certificado” hacia el componente “Contenedor del certificado”.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
27	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital que será utilizado, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Constructor del documento electrónico firmado”.
28	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Constructor del documento electrónico firmado” permiten que la aplicación generare documentos electrónicos en formato simple que no pueden ser convertidos a formato avanzado posteriormente.
29	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado, mientras se transmite desde el componente “Constructor del documento electrónico firmado” hacia el componente “Transmisor del documento electrónico firmado”.
30	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Transmisor del documento electrónico firmado” permiten que la aplicación revele el documento electrónico firmado a usuarios no autorizados.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
31	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado, mientras se transmite desde el componente “Transmisor del documento electrónico firmado” hacia su ubicación final.
32	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico”.
33	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde el componente “Contenedor del documento electrónico” hacia el componente “Validador del documento electrónico”.
34	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del documento electrónico, mientras se transmite desde el componente “Validador del documento electrónico” hacia el componente “Contenedor del documento electrónico”.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
35	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde el componente “Contenedor del documento electrónico” hacia el componente “Formateador del documento electrónico”.
36	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será firmado, mientras se transmite desde el componente “Formateador del documento electrónico” hacia el componente “Calculador del resumen”.
37	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico formateado, mientras se transmite desde el componente “Formateador del documento electrónico” hacia el componente “Constructor del documento electrónico firmado”.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
38	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen del documento electrónico, mientras se transmite desde el componente “Calculador del resumen” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.
39	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen del documento electrónico, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Dispositivo criptográfico seguro”.
40	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado del documento electrónico, mientras se transmite desde el componente “Dispositivo criptográfico seguro” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
41	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado del documento electrónico, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Constructor del documento electrónico firmado”.
42	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital que será utilizado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del certificado”.
43	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Validador del certificado”.
44	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del certificado, mientras se transmite desde el componente “Validador del certificado” hacia el componente “Contenedor del certificado”.

Tabla 21. Riesgos identificados en el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
45	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital que será utilizado, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Constructor del documento electrónico firmado”.
46	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado, mientras se transmite desde el componente “Constructor del documento electrónico firmado” hacia el componente “Transmisor del documento electrónico firmado”.
47	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado, mientras se transmite desde el componente “Transmisor del documento electrónico firmado” hacia su ubicación final.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
48	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico firmado en formato avanzado”.
49	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Contenedor del documento electrónico firmado en formato avanzado” permiten a un atacante malintencionado modificar el contenido del documento electrónico mientras éste se encuentra almacenado en dicho componente.
50	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde el componente “Contenedor del documento electrónico en formato avanzado” hacia el componente “Validador del documento electrónico firmado en formato avanzado”.
51	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del documento electrónico firmado en formato avanzado” permiten que la aplicación acepte del usuario documentos electrónicos cuyos formatos no son soportados o son incorrectos.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
52	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Validador del documento electrónico firmado en formato avanzado” permiten que la aplicación acepte de un atacante malintencionado documentos electrónicos que contienen código oculto o malicioso.
53	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del documento electrónico que contiene las firmas, mientras se transmite desde el componente “Validador del documento electrónico firmado en formato avanzado” hacia el componente “Contenedor del documento electrónico firmado en formato avanzado”.
54	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será verificado, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Extractor de certificados”.
55	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los certificados extraídos, mientras se transmite desde el componente “Extractor de certificados” hacia el componente “Validador de certificados”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
56	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador de certificados” permiten que la aplicación valide incorrectamente que todos los certificados y sus rutas de certificación estaban vigentes cuando se incluyeron en el documento.
57	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador de certificados” permiten que la aplicación valide incorrectamente la pertenencia a la jerarquía del SNCD de todos los certificados contenidos en el documento.
58	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación.
59	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación de los certificados, mientras se transmiten desde el componente “Validador del certificado” hacia el componente “Extractor de certificados”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
60	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los certificados extraídos, mientras se transmiten desde el componente “Extractor de certificados” hacia el componente “Descifrador de resúmenes cifrados”.
61	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Extractor de resúmenes cifrados”.
62	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los resúmenes cifrados extraídos, mientras se transmiten desde el componente “Extractor de resúmenes cifrados” hacia el componente “Descifrador de resúmenes cifrados”.
63	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Extractor del documento original”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
64	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico original, mientras se transmite desde el componente “Extractor del documento original” hacia el componente “Calculador del resumen del contenido del documento original”.
65	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Calculador del resumen del contenido del documento original” permiten que la aplicación genere resúmenes a partir del uso de algoritmos <i>hash</i> inseguros.
66	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen del contenido del documento original, mientras se transmite desde el componente “Calculador del resumen del contenido del documento original” hacia el componente “Comparador de resúmenes”.
67	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los resúmenes descifrados, mientras se transmiten desde el componente “Descifrador de resúmenes cifrados” hacia el componente “Comparador de resúmenes”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
68	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la verificación de las firmas mientras se transmiten desde el componente “Comparador de resúmenes” hacia el componente de “Interacción con el usuario”.
69	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico firmado en formato avanzado”.
70	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Validador del documento electrónico firmado en formato avanzado”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
71	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del documento electrónico firmado en formato avanzado, mientras se transmite desde el componente “Validador del documento electrónico firmado en formato avanzado” hacia el componente “Contenedor del documento electrónico firmado en formato avanzado”.
72	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será verificado, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Extractor de certificados”.
73	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los certificados extraídos, mientras se transmiten desde el componente “Extractor de certificados” hacia el componente “Validador de certificados”.
74	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación de los certificados, mientras se transmite desde el componente “Validador de certificados” hacia el componente “Extractor de certificados”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
75	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los certificados extraídos, mientras se transmite desde el componente “Extractor de certificados” hacia el componente “Descifrador de resúmenes cifrados”.
76	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Extractor de resúmenes cifrados”.
77	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los resúmenes cifrados extraídos, mientras se transmiten desde el componente “Extractor de resúmenes cifrados” hacia el componente “Descifrador de resúmenes cifrados”.
78	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que contiene las firmas, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato avanzado” hacia el componente “Extractor del documento original”.

Tabla 22. Riesgos identificados en el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
79	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico original, mientras se transmite desde el componente “Extractor del documento electrónico original” hacia el componente “Calculador del resumen del contenido del documento original”.
80	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen del contenido del documento original, mientras se transmite desde el componente “Calculador del resumen del contenido del documento original” hacia el componente “Comparador de resúmenes”.
81	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los resúmenes descifrados, mientras se transmiten desde el componente “Descifrador de resúmenes cifrados” hacia el componente “Comparador de resúmenes”.
82	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la verificación de las firmas digitales, mientras se transmite el componente “Comparador de resúmenes” hacia el componente de “Interacción con el usuario”.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
83	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será convertido a formato avanzado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico firmado en formato simple”.
84	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Contenedor del documento electrónico firmado en formato simple” permiten a un atacante malintencionado modificar el contenido del documento electrónico mientras éste se encuentra almacenado en dicho componente.
85	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será convertido a formato avanzado, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato simple” hacia el componente “Validador del documento electrónico firmado en formato simple”.
86	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del documento electrónico firmado en formato simple” permiten que la aplicación acepte del usuario documentos electrónicos cuyos formatos no son soportados, son incorrectos o no pueden convertirse a formato avanzado.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
87	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Validador del documento electrónico firmado en formato simple” permiten que la aplicación acepte de un atacante malintencionado documentos electrónicos que contienen código oculto o malicioso.
88	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del documento electrónico firmado en formato simple, mientras se transmite desde el componente “Validador del documento electrónico firmado en formato simple” hacia el componente “Contenedor del documento electrónico firmado en formato simple”.
89	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será convertido a formato avanzado, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato simple” hacia el componente “Extractor de certificados”.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
90	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los certificados extraídos, mientras se transmiten desde el componente “Extractor de certificados” hacia el componente “Recolector de atributos requeridos por el formato avanzado”.
91	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado” permiten que la aplicación valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante CRLs.
92	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado” permiten que la aplicación valide incorrectamente la vigencia de la CRL.
93	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado” permiten que la aplicación valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante OCSP.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
94	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado” permiten que la aplicación reutilice posteriormente información de revocación obtenida mediante OCSP.
95	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado” permiten que la aplicación valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener las rutas de certificación del (los) firmante(s).
96	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado” permiten que la aplicación valide incorrectamente la dirección para obtener los <i>tokens</i> de estampado de tiempo.
97	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar la información de revocación obtenida mediante CRLs, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Recolector de atributos requeridos por el formato avanzado”.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
98	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar la información de revocación obtenida mediante OCSP, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Recolector de atributos requeridos por el formato avanzado”.
99	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado obtenido, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Recolector de atributos requeridos por el formato avanzado”.
100	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los <i>tokens</i> de estampado de tiempo, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Recolector de atributos requeridos por el formato avanzado”.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
101	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los atributos obtenidos, mientras se transmiten desde el componente “Recolector de atributos requeridos por el formato avanzado” hacia el componente “Constructor del documento electrónico firmado en formato avanzado”.
102	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado en formato simple, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato simple” hacia el componente “Constructor del documento electrónico firmado en formato avanzado”.
103	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Constructor del documento electrónico firmado en formato avanzado” permiten la aplicación generar documentos electrónicos firmados cuyo formato avanzado no corresponde con alguno de los formatos oficiales soportados en Costa Rica.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
104	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado en formato avanzado, mientras se transmite desde el componente “Constructor del documento electrónico firmado en formato avanzado” hacia el componente “Transmisor del documento electrónico firmado en formato avanzado”.
105	Centralizado y Distribuido	Defectos en el <i>software</i>	Desarrollador	Defectos en el componente “Transmisor del documento electrónico firmado” permiten que la aplicación revele el documento electrónico firmado a usuarios no autorizados.
106	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado en formato avanzado, mientras se transmite desde el componente “Transmisor del documento electrónico firmado en formato avanzado” hacia su ubicación final.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
107	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será convertido a formato avanzado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del documento electrónico firmado en formato simple”.
108	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será convertido a formato avanzado, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato simple” hacia el componente “Validador del documento electrónico firmado en formato simple”.
109	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del documento electrónico firmado en formato simple, mientras se transmite desde el componente “Validador del documento electrónico firmado en formato simple” hacia el componente “Contenedor del documento electrónico firmado en formato simple”.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
110	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico que será convertido a formato avanzado, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato simple” hacia el componente “Extractor de certificados”.
111	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los certificados extraídos, mientras se transmiten desde el componente “Extractor de certificados” hacia el componente “Recolector de atributos requeridos por el formato avanzado”.
112	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los atributos obtenidos, mientras se transmiten desde el componente “Recolector de atributos requeridos por el formato avanzado” hacia el componente “Constructor del documento electrónico firmado en formato avanzado”.

Tabla 23. Riesgos identificados en el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
113	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado en formato simple, mientras se transmite desde el componente “Contenedor del documento electrónico firmado en formato simple” hacia el componente “Constructor del documento electrónico firmado en formato avanzado”.
114	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado en formato avanzado, mientras se transmite desde el componente “Constructor del documento electrónico firmado en formato avanzado” hacia el componente “Transmisor del documento electrónico firmado en formato avanzado”.
115	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el documento electrónico firmado en formato avanzado, mientras se transmite desde el componente “Transmisor del documento electrónico firmado en formato avanzado” hacia su ubicación final.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
116	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de autenticación generados, mientras se transmiten desde el componente “Generador de datos de autenticación” hacia el componente “Calculador del resumen”.
117	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Calculador del resumen” permiten la aplicación genere resúmenes a partir del uso de algoritmos <i>hash</i> inseguros.
118	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen de los datos de autenticación generados, mientras se transmite desde el componente “Calculador del resumen” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.
119	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación acceda a las operaciones criptográficas del “Dispositivo criptográfico seguro” sin utilizar un mecanismo de autenticación.
120	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación revele las credenciales de autenticación del “Dispositivo criptográfico seguro” a sus usuarios.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
121	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación revele las credenciales de autenticación del “Dispositivo criptográfico seguro” a un atacante malintencionado que ejecuta un ataque de fuerza bruta.
122	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen de los datos de autenticación generados, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Dispositivo criptográfico seguro”.
123	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro” permiten que la aplicación almacene en caché las credenciales del “Dispositivo criptográfico seguro” para uso posterior.
124	Centralizado y Distribuido	Defectos en el <i>hardware</i>	Usuario	Defectos en el componente “Dispositivo criptográfico seguro” permiten que la aplicación genere datos cifrados mediante el uso de algoritmos de cifrado inseguros.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
125	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado de los datos de autenticación generados, mientras se transmite desde el componente “Dispositivo criptográfico seguro” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.
126	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado de los datos de autenticación, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Descifrador del resumen”.
127	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital que será utilizado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del certificado”.
128	Centralizado y Distribuido	Defectos en el <i>software</i>	Atacante malintencionado	Defectos en el componente “Contenedor del certificado” permiten a un atacante malintencionado modificar el certificado digital mientras éste se encuentra almacenado en dicho componente.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
129	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar certificado digital, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Validador del certificado”.
130	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación acepte del usuario certificados digitales inválidos.
131	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente de “Interacción con el usuario” permiten que la aplicación acepte del usuario certificados digitales que no están almacenados en un dispositivo criptográfico seguro.
132	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación.
133	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del certificado, mientras se transmite desde el componente “Validador del certificado” hacia el componente “Contenedor del certificado”.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
134	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante CRLs.
135	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación valide incorrectamente la vigencia de la CRL.
136	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado o” permiten que la aplicación valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante OCSP.
137	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación reutilice posteriormente la información de revocación obtenida mediante OCSP.
138	Centralizado y Distribuido	Defectos en el <i>software</i>	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la cadena de certificación correspondiente al certificado.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.
(Continuación)

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
139	Centralizado y Distribuido	Defectos en el software	Usuario	Defectos en el componente “Validador del certificado” permiten que la aplicación valide incorrectamente la dirección para obtener los <i>tokens</i> de estampado de tiempo.
140	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar la información de revocación obtenida mediante CRLs, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Validador del certificado”.
141	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar la información de revocación obtenida mediante OCSP, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Validador del certificado”.
142	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado obtenido, mientras se transmite desde el servidor proveedor del servicio hacia el componente “Validador del certificado”.
143	Centralizado y Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar los <i>tokens</i> de estampado de tiempo, mientras se transmiten desde el servidor proveedor del servicio hacia el componente “Validador del certificado”.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
144	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Descifrador del resumen”.
145	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen descifrado de los datos de autenticación generados, mientras se transmite desde el componente “Descifrador del resumen” hacia el componente “Comparador de resúmenes”.
146	Centralizado	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la comparación de los resúmenes, mientras se transmite desde el componente “Comparador de resúmenes” hacia el componente de “Interacción con el usuario”.
147	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar los datos de autenticación generados, mientras se transmiten desde el componente “Generador de datos de autenticación” hacia el componente “Calculador del resumen”.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
148	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen de los datos de autenticación generados, mientras se transmite desde el componente “Calculador del resumen” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.
149	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen de los datos de autenticación generados, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Dispositivo criptográfico seguro”.
150	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado de los datos de autenticación generados, mientras se transmite desde el componente “Dispositivo criptográfico seguro” hacia el componente “Comunicador con el dispositivo criptográfico seguro”.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
151	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen cifrado de los datos de autenticación, mientras se transmite desde el componente “Comunicador con el dispositivo criptográfico seguro” hacia el componente “Descifrador del resumen”.
152	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital que será utilizado, mientras se transmite desde su ubicación original hacia el componente “Contenedor del certificado”.
153	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital, mientras se transmite desde el componente “Contenedor del certificado” hacia el componente “Validador del certificado”.
154	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la validación del certificado, mientras se transmite desde el componente “Validador del certificado” hacia el componente “Contenedor del certificado”.

Tabla 24. Riesgos identificados en el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Ambiente de ejecución	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
155	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el certificado digital, mientras se transmite desde el componente “Contenedor del resumen” hacia el componente “Descifrador del resumen”.
156	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar o revelar el resumen descifrado de los datos de autenticación generados, mientras se transmite desde el componente “Descifrador del resumen” hacia el componente “Comparador de resúmenes”.
157	Distribuido	Comunicaciones desprotegidas	Atacante malintencionado	Comunicaciones desprotegidas permiten a un atacante malintencionado modificar el resultado de la comparación de los resúmenes, mientras se transmite desde el componente “Comparador de resúmenes” hacia el componente de “Interacción con el usuario”.

Tabla 25. Riesgos identificados en todos los escenarios. Fuente: Elaboración propia.

ID	Fuente de vulnerabilidad	Fuente de amenaza	Descripción del riesgo
158	Errores de configuración	Atacante malintencionado	Errores de configuración en la(s) máquina(s) donde la aplicación está instalada permiten a un atacante malintencionado modificar algún componente de la aplicación por otro que ha sido creado con fines maliciosos.
159	Errores de configuración	Atacante malintencionado	Errores de configuración en la(s) máquina(s) donde la aplicación está instalada permiten a un atacante malintencionado acceder a recursos a los que no está autorizado.
160	<i>Software</i> desactualizado	Atacante malintencionado	La falta de actualizaciones en el sistema operativo permite a un atacante malintencionado instalar <i>software</i> malicioso en la máquina donde se ejecuta algún componente de la aplicación.
161	<i>Software</i> desactualizado	Atacante malintencionado	La falta de actualizaciones en el navegador de internet permite a un atacante malintencionado instalar <i>software</i> malicioso en la máquina donde se ejecuta algún componente de la aplicación.
162	<i>Software</i> desactualizado	Atacante malintencionado	La falta de actualizaciones en <i>frameworks</i> utilizados por la aplicación permite a un atacante malintencionado instalar <i>software</i> malicioso en la máquina donde se ejecuta algún componente de la aplicación.
163	Errores de configuración	Atacante malintencionado	Errores de configuración de la(s) máquina(s) donde la aplicación está instalada permite la divulgación de <i>stack traces</i> u otro tipo de información a través del “Componente de interacción con el usuario”, lo que permite que algún atacante malintencionado obtenga datos suficientes para realizar un ataque exitoso.

11.2. APÉNDICE B: DETALLE DE LA VALORACIÓN DE LOS RIESGOS IDENTIFICADOS

En este apéndice se presenta el detalle de la valoración de los riesgos identificados.

Los riesgos se agruparon en categorías, como se muestra en la TABLA 26. A cada categoría se le asignó un identificador, se determinó la fuente de amenaza y la fuente de vulnerabilidad correspondiente, y se estableció una descripción genérica de los riesgos específicos asociados. Dichos riesgos se denominan instancias, y corresponden a riesgos concretos presentes en los escenarios analizados. Las instancias se encuentran detalladas en el Apéndice A: Riesgos Identificados.

La notación de llaves dentro de la descripción de cada categoría, sirve para representar un elemento parametrizado de riesgo, que puede variar de una instancia a otra. Por ejemplo, en una instancia el parámetro *{una pieza de información}* puede ser un documento electrónico, mientras que en otra puede ser un resumen del documento electrónico, sin embargo, en ambos casos la pieza información está propensa a un riesgo similar.

Adicionalmente, para cada categoría se especifica el ambiente de ejecución sobre la cual se realizó la valoración. En la TABLA 26 se utiliza el término “Distribuido” para representar aquellos riesgos que pueden ocurrir cuando los dos componentes que intervienen se encuentran localizados en distintas máquinas. De manera similar, se utiliza el término “Centralizado” cuando los componentes que intervienen se encuentran ubicados en la misma computadora.

Finalmente, cada instancia de riesgo especifica el nivel de severidad asignado, que se obtiene a partir de la probabilidad y el impacto estimado.

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia.

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
1	Centralizado	Atacante malintencionado	Comunicaciones desprotegidas		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} modificar {una pieza de información}, mientras se transmite desde {el punto A} hacia {el punto B}.												
				1	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, su ubicación original, el componente “Contenedor del documento electrónico”.	3	1	9	1	3	1	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				3	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Validador del documento electrónico”.	3	1	9	1	3	1	8	9	9	7	7	Alto
				6	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del documento electrónico, el componente “Validador del documento electrónico”, el componente “Contenedor del documento electrónico”.	2.6	1	7	1	3	1	7	7	7	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				7	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Formateador del documento electrónico”.	3	1	9	1	3	1	8	9	9	7	7	Alto
				9	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Formateador del documento electrónico”, el componente “Calculador del resumen”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				10	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico formateado, el componente “Formateador del documento electrónico”, el componente “Constructor del documento electrónico firmado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				11	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				15	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el “Dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				18	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				19	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Constructor del documento electrónico firmado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				20	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital que será utilizado, su ubicación original, el componente “Contenedor del certificado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				22	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital, el componente “Contenedor del certificado”, el componente “Validador del certificado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				26	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del certificado, el “Validador del certificado”, el componente “Contenedor del certificado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				27	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital que será utilizado, el componente “Contenedor del certificado”, el componente “Constructor del documento electrónico firmado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				29	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Constructor del documento electrónico firmado”, el componente “Transmisor del documento electrónico firmado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				31	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Transmisor del documento electrónico firmado”, su ubicación final.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				48	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato avanzado”.	3	1	9	1	3	1	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				50	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico en formato avanzado”, el componente “Validador del documento electrónico firmado en formato avanzado”.	2.6	1	7	1	3	1	7	7	7	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				53	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del documento electrónico que contiene las firmas, el componente "Validador del documento electrónico firmado en formato avanzado", el componente "Contenedor del documento electrónico firmado en formato avanzado".	3	1	9	1	3	1	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				54	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será verificado, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de certificados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				55	Comunicaciones desprotegidas, un atacante malintencionado, los certificados extraídos, el componente “Extractor de certificados”, el componente “Validador de certificados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				59	Comunicaciones desprotegidas, atacante malintencionado, el resultado de la validación de los certificados, el componente “Validador del certificado”, el componente “Extractor de certificados”.	3	1	9	1	3	1	8	9	9	7	7	Alto
				60	Comunicaciones desprotegidas, un atacante malintencionado, los certificados extraídos, el componente “Extractor de certificados”, el componente “Descifrador de resúmenes cifrados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				61	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de resúmenes cifrados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				62	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes cifrados extraídos, el componente “Extractor de resúmenes cifrados”, el componente “Descifrador de resúmenes cifrados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				63	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor del documento original”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				64	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico original, el componente “Extractor del documento original”, el componente “Calculador del resumen del contenido del documento original”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				66	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del contenido del documento original, el componente “Calculador del resumen del contenido del documento original”, el componente “Comparador de resúmenes”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				67	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes descifrados, el componente “Descifrador de resúmenes cifrados”, el componente “Comparador de resúmenes”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				68	Comunicaciones desprotegidas, atacante malintencionado, el resultado de la verificación de las firmas, el componente “Comparador de resúmenes”, el componente de “Interacción con el usuario”.	3	1	9	1	3	1	8	9	9	7	7	Alto
				83	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato simple”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				85	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Validador del documento electrónico firmado en formato simple”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				88	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del documento electrónico firmado en formato simple, el componente “Validador del documento electrónico firmado en formato simple”, el componente “Contenedor del documento electrónico firmado en formato simple”.	2.6	1	7	1	3	1	7	7	7	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				89	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Extractor de certificados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				90	Comunicaciones desprotegidas, un atacante malintencionado, los certificados extraídos, el componente “Extractor de certificados”, el componente “Recolector de atributos requeridos por el formato avanzado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				101	Comunicaciones desprotegidas, un atacante malintencionado, los atributos obtenidos, el componente “Recolector de atributos requeridos por el formato avanzado”, el componente “Constructor del documento electrónico firmado en formato avanzado”.	3	1	9	1	3	1	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				102	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato simple, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Constructor del documento electrónico firmado en formato avanzado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				104	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Constructor del documento electrónico firmado en formato avanzado”, el componente “Transmisor del documento electrónico firmado en formato avanzado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				106	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Transmisor del documento electrónico firmado en formato avanzado”, su ubicación final.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				116	Comunicaciones desprotegidas, un atacante malintencionado, los datos de autenticación generados, el componente “Generador de datos de autenticación”, el componente “Calculador del resumen”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				118	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				122	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				125	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación generados, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				126	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Descifrador del resumen”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				127	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital que será utilizado, su ubicación original, el componente “Contenedor del certificado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				129	Comunicaciones desprotegidas, un atacante malintencionado, certificado digital, el componente “Contenedor del certificado”, el componente “Validador del certificado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				133	Comunicaciones desprotegidas, atacante malintencionado, el resultado de la validación del certificado, el componente “Validador del certificado, el componente “Contenedor del certificado”.	3	1	9	1	3	1	8	9	9	7	7	Alto
				144	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital, el componente “Contenedor del certificado”, el componente “Descifrador del resumen”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				145	Comunicaciones desprotegidas, un atacante malintencionado, el resumen descifrado de los datos de autenticación generado se, el componente “Descifrador del resumen”, el componente “Comparador de resúmenes”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				146	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la comparación de los resúmenes, el componente “Comparador de resúmenes”, el componente de “Interacción con el usuario”.	3	1	9	1	3	1	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
2	Centralizado	Atacante malintencionado	Comunicaciones desprotegidas		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} revelar {una pieza de información}, mientras se transmite desde {el punto A} hacia {el punto B}.												
				1	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, su ubicación original, el componente “Contenedor del documento electrónico”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				3	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Validador del documento electrónico”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo
				7	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Formateador del documento electrónico”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				9	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Formateador del documento electrónico”, el componente “Calculador del resumen”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo
				10	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico formateado, el componente “Formateador del documento electrónico”, el componente “Constructor del documento electrónico firmado”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				11	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				15	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el “Dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				18	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				19	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Constructor del documento electrónico firmado”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				29	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Constructor del documento electrónico firmado”, el componente “Transmisor del documento electrónico firmado”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				31	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Transmisor del documento electrónico firmado”, su ubicación final.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo
				48	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato avanzado”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				50	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico en formato avanzado”, el componente “Validador del documento electrónico firmado en formato avanzado”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				54	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será verificado, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de certificados”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo
				61	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de resúmenes cifrados”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				62	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes cifrados extraídos, el componente “Extractor de resúmenes cifrados”, el componente “Descifrador de resúmenes cifrados”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				63	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor del documento original”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				64	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico original, el componente “Extractor del documento original”, el componente “Calculador del resumen del contenido del documento original”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo
				66	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del contenido del documento original, el componente “Calculador del resumen del contenido del documento original”, el componente “Comparador de resúmenes”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				67	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes descifrados, el componente “Descifrador de resúmenes cifrados”, el componente “Comparador de resúmenes”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				83	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato simple”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				85	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Validador del documento electrónico firmado en formato simple”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				89	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Extractor de certificados”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				102	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato simple, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Constructor del documento electrónico firmado en formato avanzado”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				104	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Constructor del documento electrónico firmado en formato avanzado”, el componente “Transmisor del documento electrónico firmado en formato avanzado”.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				106	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Transmisor del documento electrónico firmado en formato avanzado”, su ubicación final.	2.2	1	5	1	3	1	3.5	5	3	3	3	Bajo
				116	Comunicaciones desprotegidas, un atacante malintencionado, los datos de autenticación generados, el componente “Generador de datos de autenticación”, el componente “Calculador del resumen”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				118	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				122	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				125	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación generados, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				126	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación generados, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Descifrador del resumen”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				145	Comunicaciones desprotegidas, un atacante malintencionado, el resumen descifrado de los datos de autenticación generados, el componente “Descifrador del resumen”, el componente “Comparador de resúmenes”.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
3	Distribuido	Atacante malintencionado	Comunicaciones desprotegidas		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} modificar {una pieza de información}, mientras se transmite desde {el punto A} hacia {el punto B}.												
				32	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, su ubicación original, el componente “Contenedor del documento electrónico”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				33	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Validador del documento electrónico”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				34	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del documento electrónico, el componente “Validador del documento electrónico”, el componente “Contenedor del documento electrónico”.	3.8	3	7	3	3	3	7	7	7	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				35	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Formateador del documento electrónico”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				36	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Formateador del documento electrónico”, el componente “Calculador del resumen”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				37	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico formateado, el componente “Formateador del documento electrónico”, el componente “Constructor del documento electrónico firmado”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				38	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				39	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				40	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				41	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Constructor del documento electrónico firmado”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				42	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital que será utilizado, su ubicación original, el componente “Contenedor del certificado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				43	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital, el componente “Contenedor del certificado”, el componente “Validador del certificado”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				44	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del certificado, el componente “Validador del certificado”, el componente “Contenedor del certificado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				45	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital que será utilizado, el componente “Contenedor del certificado”, el componente “Constructor del documento electrónico firmado”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				46	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Constructor del documento electrónico firmado”, el componente “Transmisor del documento electrónico firmado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				47	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Transmisor del documento electrónico firmado”, su ubicación final.	3	3	3	3	3	3	3	3	3	3	3	Medio
				69	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				70	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Validador del documento electrónico firmado en formato avanzado”.	3.8	3	7	3	3	3	7	7	7	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				71	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del documento electrónico firmado en formato avanzado, el componente “Validador del documento electrónico firmado en formato avanzado”, el componente “Contenedor del documento electrónico firmado en formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				72	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será verificado, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de certificados”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				73	Comunicaciones desprotegidas, un atacante malintencionado, los certificados extraídos, el componente “Extractor de certificados”, el componente “Validador de certificados”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				74	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación de los certificados, el componente “Validador de certificados”, el componente “Extractor de certificados”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				75	Comunicaciones desprotegidas, un atacante malintencionado, los certificados extraídos, el componente “Extractor de certificados”, el componente “Descifrador de resúmenes cifrados”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				76	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de resúmenes cifrados”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				77	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes cifrados extraídos, el componente “Extractor de resúmenes cifrados”, el componente “Descifrador de resúmenes cifrados”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				78	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor del documento original”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				79	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico original, el componente “Extractor del documento electrónico original”, el componente “Calculador del resumen del contenido del documento original”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				80	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del contenido del documento original, el componente “Calculador del resumen del contenido del documento original”, el componente “Comparador de resúmenes”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				81	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes descifrados, el componente “Descifrador de resúmenes cifrados”, el componente “Comparador de resúmenes”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				82	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la verificación de las firmas digitales, el componente “Comparador de resúmenes”, el componente de “Interacción con el usuario”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				97	Comunicaciones desprotegidas, un atacante malintencionado, la información de revocación obtenida mediante CRLs, el servidor proveedor del servicio, el componente “Recolector de atributos requeridos por el formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				98	Comunicaciones desprotegidas, un atacante malintencionado, la información de revocación obtenida mediante OCSP, el servidor proveedor del servicio, el componente “Recolector de atributos requeridos por el formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				99	Comunicaciones desprotegidas, un atacante malintencionado, el certificado obtenido, el servidor proveedor del servicio, el componente “Recolector de atributos requeridos por el formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				100	Comunicaciones desprotegidas, un atacante malintencionado, los <i>tokens</i> de estampado de tiempo, el servidor proveedor del servicio, el componente “Recolector de atributos requeridos por el formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				107	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato simple”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				108	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Validador del documento electrónico firmado en formato simple”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				109	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del documento electrónico firmado en formato simple, el componente “Validador del documento electrónico firmado en formato simple”, el componente “Contendor del documento electrónico firmado en formato simple”.	3.8	3	7	3	3	3	7	7	7	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				110	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Extractor de certificados”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				111	Comunicaciones desprotegidas, un atacante malintencionado, los certificados extraídos, el componente “Extractor de certificados”, el componente “Recolector de atributos requeridos por el formato avanzado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				112	Comunicaciones desprotegidas, un atacante malintencionado, los atributos obtenidos, el componente “Recolector de atributos requeridos por el formato avanzado”, el componente “Constructor del documento electrónico firmado en formato avanzado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				113	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato simple, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Constructor del documento electrónico firmado en formato avanzado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				114	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Constructor del documento electrónico firmado en formato avanzado”, el componente “Transmisor del documento electrónico firmado en formato avanzado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				115	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Transmisor del documento electrónico firmado en formato avanzado”, su ubicación final.	3	3	3	3	3	3	3	3	3	3	3	Medio
				140	Comunicaciones desprotegidas, un atacante malintencionado, la información de revocación obtenida mediante CRLs, el servidor proveedor del servicio, el componente “Validador del certificado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				141	Comunicaciones desprotegidas, un atacante malintencionado, la información de revocación obtenida mediante OCSP, el servidor proveedor del servicio, el componente “Validador del certificado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				142	Comunicaciones desprotegidas, un atacante malintencionado, el certificado obtenido, el servidor proveedor del servicio, el componente “Validador del certificado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				143	Comunicaciones desprotegidas, un atacante malintencionado, los <i>tokens</i> de estampado de tiempo, el servidor proveedor del servicio, el componente “Validador del certificado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				147	Comunicaciones desprotegidas, un atacante malintencionado, los datos de autenticación generados, el componente “Generador de datos de autenticación”, el componente “Calculador del resumen”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				148	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				149	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				150	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación generados, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				151	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los de autenticación, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Descifrador del resumen”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				152	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital que será utilizado, su ubicación original, el componente “Contenedor del certificado”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				153	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital, el componente “Contenedor del certificado”, el componente “Validador del certificado”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				154	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la validación del certificado, el componente “Validador del certificado”, el componente “Contenedor del certificado”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto
				155	Comunicaciones desprotegidas, un atacante malintencionado, el certificado digital, el componente “Contenedor del resumen”, el componente “Descifrador del resumen”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				156	Comunicaciones desprotegidas, un atacante malintencionado, el resumen descifrado de los datos de autenticación generados, el componente “Descifrador del resumen”, el componente “Comparador de resúmenes”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				157	Comunicaciones desprotegidas, un atacante malintencionado, el resultado de la comparación de los resúmenes, el componente “Comparador de resúmenes”, el componente de “Interacción con el usuario”.	4.2	3	9	3	3	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
4	Distribuido	Atacante malintencionado	Comunicaciones desprotegidas		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} revelar {una pieza de información}, mientras se transmite desde {el punto A} hacia {el punto B}.												
				32	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, su ubicación original, el componente “Contenedor del documento electrónico”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				33	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Validador del documento electrónico”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio
				35	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Contenedor del documento electrónico”, el componente “Formateador del documento electrónico”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				36	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será firmado, el componente “Formateador del documento electrónico”, el componente “Calculador del resumen”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio
				37	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico formateado, el componente “Formateador del documento electrónico”, el componente “Constructor del documento electrónico firmado”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				38	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				39	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				40	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				41	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado del documento electrónico, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Constructor del documento electrónico firmado”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				46	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Constructor del documento electrónico firmado”, el componente “Transmisor del documento electrónico firmado”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				47	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado, el componente “Transmisor del documento electrónico firmado”, su ubicación final.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio
				69	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato avanzado”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				70	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Validador del documento electrónico firmado en formato avanzado”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				72	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será verificado, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de certificados”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio
				76	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor de resúmenes cifrados”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				77	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes cifrados extraídos, el componente “Extractor de resúmenes cifrados”, el componente “Descifrador de resúmenes cifrados”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				78	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que contiene las firmas, el componente “Contenedor del documento electrónico firmado en formato avanzado”, el componente “Extractor del documento original”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				79	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico original, el componente “Extractor del documento electrónico original”, el componente “Calculador del resumen del contenido del documento original”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				80	Comunicaciones desprotegidas, un atacante malintencionado, el resumen del contenido del documento original, el componente “Calculador del resumen del contenido del documento original”, el componente “Comparador de resúmenes”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				81	Comunicaciones desprotegidas, un atacante malintencionado, los resúmenes descifrados, el componente “Descifrador de resúmenes cifrados”, el componente “Comparador de resúmenes”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				107	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, su ubicación original, el componente “Contenedor del documento electrónico firmado en formato simple”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				108	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Validador del documento electrónico firmado en formato simple”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				110	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico que será convertido a formato avanzado, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Extractor de certificados”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				113	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato simple, el componente “Contenedor del documento electrónico firmado en formato simple”, el componente “Constructor del documento electrónico firmado en formato avanzado”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				114	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Constructor del documento electrónico firmado en formato avanzado”, el componente “Transmisor del documento electrónico firmado en formato avanzado”.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				115	Comunicaciones desprotegidas, un atacante malintencionado, el documento electrónico firmado en formato avanzado, el componente “Transmisor del documento electrónico firmado en formato avanzado”, su ubicación final.	3.4	3	5	3	3	3	3.5	5	3	3	3	Medio
				147	Comunicaciones desprotegidas, un atacante malintencionado, los datos de autenticación generados, el componente “Generador de datos de autenticación”, el componente “Calculador del resumen”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				148	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Calculador del resumen”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				149	Comunicaciones desprotegidas, un atacante malintencionado, el resumen de los datos de autenticación generados, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				150	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación generados, el componente “Dispositivo criptográfico seguro”, el componente “Comunicador con el dispositivo criptográfico seguro”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				151	Comunicaciones desprotegidas, un atacante malintencionado, el resumen cifrado de los datos de autenticación generados, el componente “Comunicador con el dispositivo criptográfico seguro”, el componente “Descifrador del resumen”.	3	3	3	3	3	3	3	3	3	3	3	Medio
				156	Comunicaciones desprotegidas, un atacante malintencionado, el resumen descifrado de los datos de autenticación, el componente “Descifrador del resumen”, el componente “Comparador de resúmenes”.	3	3	3	3	3	3	3	3	3	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
5	Centralizado y Distribuido	Atacante malintencionado	Defectos en el software		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} modificar {una pieza de información} mientras ésta se encuentra almacenada en {un componente}.												
				2	Defectos en el componente “Contenedor del documento electrónico”, un atacante malintencionado, el contenido del documento electrónico, dicho componente.	3	1	9	1	3	1	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				21	Defectos en el componente “Contenedor del certificado”, un atacante malintencionado, el certificado digital, dicho componente.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				49	Defectos en el componente “Contenedor del documento electrónico firmado en formato avanzado”, un atacante malintencionado, el contenido del documento electrónico, dicho componente.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
				84	Defectos en el componente “Contenedor del documento electrónico firmado en formato simple”, un atacante malintencionado, el contenido del documento electrónico, dicho componente.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				128	Defectos en el componente “Contenedor del certificado”, un atacante malintencionado, el certificado digital, dicho componente.	1.8	1	3	1	3	1	3	3	3	3	3	Bajo
6	Centralizado y Distribuido	Usuario	Defectos en el software		{Una fuente de vulnerabilidad} permite que la aplicación revele {una pieza de información} a {una fuente de amenaza}.												
				13	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, las credenciales de autenticación del “Dispositivo criptográfico seguro”, sus usuarios.	7.4	9	9	7	5	7	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				30	Defectos en el componente “Transmisor del documento electrónico firmado”, el documento electrónico firmado, usuarios no autorizados.	6.2	9	3	7	5	7	3	3	3	3	3	Alto
				105	Defectos en el componente “Transmisor del documento electrónico firmado”, el documento electrónico firmado, usuarios no autorizados.	6.2	9	3	7	5	7	3	3	3	3	3	Alto
				120	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, las credenciales de autenticación del “Dispositivo criptográfico seguro”, sus usuarios.	7.4	9	9	7	5	7	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
7	Centralizado y Distribuido	Atacante malintencionado	Defectos en el software		{Una fuente de vulnerabilidad} permite que la aplicación revele {una pieza de información} a {una fuente de amenaza} que ejecuta un ataque de fuerza bruta.												
				14	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, las credenciales de autenticación del “Dispositivo criptográfico seguro”, un atacante malintencionado.	4.2	3	9	1	5	3	8	9	9	7	7	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				121	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, las credenciales de autenticación del “Dispositivo criptográfico seguro”, un atacante malintencionado.	4.2	3	9	1	5	3	8	9	9	7	7	Alto
8	Centralizado y Distribuido	Usuario	Defectos en el software		{Una fuente de vulnerabilidad} permite que la aplicación {ejecute acciones que son repudiables}.												
				8	Defectos en el componente “Calculador del resumen”, genere resúmenes a partir del uso de algoritmos hash inseguros.	7.4	9	9	9	1	9	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				12	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, acceda a las operaciones criptográficas del “Dispositivo criptográfico seguro” sin utilizar un mecanismo de autenticación.	8.6	9	9	9	7	9	8	9	9	7	7	Muy alto
				16	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, almacene en caché las credenciales del “Dispositivo criptográfico seguro” para uso posterior.	6.6	5	9	5	5	9	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				56	Defectos en el componente “Validador de certificados”, valide incorrectamente que todos los certificados y sus rutas de certificación estaban vigentes cuando se incluyeron en el documento.	8.2	9	9	7	7	9	8	9	9	7	7	Muy alto
				57	Defectos en el componente “Validador de certificados”, valide incorrectamente la pertenencia a la jerarquía del SNCD de todos los certificados contenidos en el documento.	8.2	9	9	7	7	9	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				65	Defectos en el componente “Calculador del resumen del contenido del documento original”, genere resúmenes a partir del uso de algoritmos <i>hash</i> inseguros.	7.4	9	9	9	1	9	8	9	9	7	7	Muy alto
				92	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado”, valide incorrectamente la vigencia de la CRL.	8.2	9	9	7	7	9	8	9	9	7	7	Muy alto
				94	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado”, reutilice posteriormente información de revocación obtenida mediante OCSP.	7.8	9	9	9	3	9	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				117	Defectos en el componente “Calculador del resumen”, genere resúmenes a partir del uso de algoritmos hash inseguros.	7.4	9	9	9	1	9	8	9	9	7	7	Muy alto
				119	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, acceda a las operaciones criptográficas del “Dispositivo criptográfico seguro” sin utilizar un mecanismo de autenticación.	8.6	9	9	9	7	9	8	9	9	7	7	Muy alto
				123	Defectos en el componente “Comunicador con el dispositivo criptográfico seguro”, almacene en caché las credenciales del “Dispositivo criptográfico seguro” para uso posterior.	6.6	5	9	5	5	9	8	9	9	7	7	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				4	Defectos en el componente “Validador del documento electrónico”, el usuario, documentos electrónicos cuyos formatos no son soportados o son incorrectos.	7	7	3	9	7	9	3	3	3	3	3	Alto
				5	Defectos en el componente “Validador del documento electrónico”, un atacante malintencionado, documentos electrónicos que contienen código oculto o malicioso.	3	1	7	3	3	1	7	7	7	7	7	Alto
				23	Defectos en el componente “Validador del certificado”, el usuario, certificados digitales inválidos.	5.8	7	3	5	7	7	3	3	3	3	3	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				24	Defectos en el componente de “Interacción con el usuario”, el usuario, certificados digitales que no están almacenados en un dispositivo criptográfico seguro.	6.2	7	3	7	7	7	3	3	3	3	3	Alto
				51	Defectos en el componente “Validador del documento electrónico firmado en formato avanzado”, el usuario, documentos electrónicos cuyos formatos no son soportados o son incorrectos.	7	7	3	9	7	9	3	3	3	3	3	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				52	Defectos en el componente “Validador del documento electrónico firmado en formato avanzado”, un atacante malintencionado, documentos electrónicos que contienen código oculto o malicioso.	3	1	7	3	3	1	7	7	7	7	7	Alto
				86	Defectos en el componente “Validador del documento electrónico firmado en formato simple”, el usuario, documentos electrónicos cuyos formatos no son soportados, son incorrectos o no pueden convertirse a formato avanzado.	7	7	3	9	7	9	3	3	3	3	3	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				87	Defectos en el componente “Validador del documento electrónico firmado en formato simple”, un atacante malintencionado, documentos electrónicos que contienen código oculto o malicioso.	3	1	7	3	3	1	7	7	7	7	7	Alto
				130	Defectos en el componente “Validador del certificado”, el usuario, certificados digitales inválidos.	5.8	7	3	5	7	7	3	3	3	3	3	Alto
				131	Defectos en el componente de “Interacción con el usuario”, el usuario, certificados digitales que no están almacenados en un dispositivo criptográfico seguro.	5.4	7	3	7	3	7	3	3	3	3	3	Alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
10	Centralizado y Distribuido	Usuario	Defectos en el software		{Una fuente de vulnerabilidad} permite que la aplicación {ejecute acciones que comprometen la integridad de la información}.												
				28	Defectos en el componente “Constructor del documento electrónico firmado”, generare documentos electrónicos en formato simple que no pueden ser convertidos a formato avanzado posteriormente.	7.8	9	9	9	5	7	6	7	7	5	5	Muy alto

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				25	Defectos en el componente “Validador del certificado”, ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación.	5.8	9	3	7	5	5	2	5	1	1	1	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				58	Defectos en el componente “Validador del certificado”, ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación.	5.8	9	3	7	5	5	2	5	1	1	1	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				91	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado”, valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante CRLs.	5.8	9	3	7	3	7	2.5	5	3	1	1	Medio
				93	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado”, valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante OCSP.	5.8	9	3	7	3	7	2.5	5	3	1	1	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				95	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado”, valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener las rutas de certificación del (los) firmante(s).	5.8	9	3	7	3	7	2.5	5	3	1	1	Medio
				96	Defectos en el componente “Recolector de atributos requeridos por el formato avanzado”, valide incorrectamente la dirección para obtener los tokens de estampado de tiempo.	5.8	9	3	7	3	7	2.5	5	3	1	1	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				132	Defectos en el componente “Validador del certificado”, ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación.	5.8	9	3	7	5	5	2	5	1	1	1	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				134	Defectos en el componente “Validador del certificado”, valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante CRLs.	5.8	9	3	7	3	7	2.5	5	3	1	1	Medio
				136	Defectos en el componente “Validador del certificado o”, valide incorrectamente el uso de direcciones contenidas en el código fuente para obtener la información de revocación de los certificados mediante OCSP.	5.8	9	3	7	3	7	2.5	5	3	1	1	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				17	Defectos en el componente “Dispositivo criptográfico seguro”, datos cifrados mediante el uso de algoritmos de cifrado inseguros.	0	0	0	0	0	0	0	0	0	0	Muy bajo	
				124	Defectos en el componente “Dispositivo criptográfico seguro”, datos cifrados mediante el uso de algoritmos de cifrado inseguros.	0	0	0	0	0	0	0	0	0	0	Muy bajo	
13	Centralizado y Distribuido	Atacante malintencionado	Errores de configuración		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} revelar recursos a los que no está autorizado.												
				159	Errores de configuración en la(s) máquina(s) donde la aplicación está instalada, un atacante malintencionado.	2.6	1	7	1	3	1	4.5	7	5	3	3	Bajo

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				158	Errores de configuración en la(s) máquina(s) donde la aplicación está instalada, un atacante malintencionado, algún componente de la aplicación.	2.6	1	9	1	1	1	8	9	9	7	7	Alto
16	Centralizado y Distribuido	Atacante malintencionado	Software desactualizado		{Una fuente de vulnerabilidad} permite a {una fuente de amenaza} instalar software malicioso en la máquina donde se ejecuta algún componente de la aplicación.												
				160	La falta de actualizaciones en el sistema operativo, un atacante malintencionado.	2.2	1	7	1	1	1	5	7	7	3	3	Medio
				161	La falta de actualizaciones en el navegador de internet, un atacante malintencionado.	2.2	1	7	1	1	1	5	7	7	3	3	Medio

Tabla 26. Valoración de los riesgos identificados. Fuente: Elaboración propia. (Continuación)

ID	Ambiente de ejecución	Fuente de amenaza	Fuente de vulnerabilidad	Instancias	Descripción del riesgo	Probabilidad	H	Ro	Ru	D	E	Impacto	C	A	E	R	Nivel de severidad
				162	La falta de actualizaciones en <i>frameworks</i> utilizados por la aplicación, un atacante malintencionado.	2.2	1	7	1	1	1	5	7	7	3	3	Medio
17	Centralizado y Distribuido	Atacante malintencionado	Errores de configuración		{Una fuente de vulnerabilidad} permite la divulgación de {alguna pieza de información} a través del “Componente de interacción con el usuario”, lo que permite que {una fuente de amenaza} obtenga datos suficientes para realizar un ataque exitoso.												
				163	Errores de configuración de la(s) máquina(s) donde la aplicación está instalada, <i>stack traces</i> u otro tipo de información, un atacante malintencionado.	4.6	3	5	7	5	3	3	3	3	3	3	Medio

11.3. APÉNDICE C: RESUMEN DE LA VALORACIÓN DE RIESGOS UTILIZANDO UN PROCEDIMIENTO ALTERNATIVO

En las secciones 4.3.5 y 4.3.6 de este documento se presentaron los métodos para la determinación de la probabilidad y el impacto que permiten asignar el nivel de severidad del riesgo. Los resultados descritos en la sección 6.4 se obtuvieron a partir del cálculo de promedios de las ecuaciones 1 y 3. En este apéndice, se presenta un resumen de la valoración de los riesgos identificados utilizando como procedimiento alternativo el cálculo de promedios con variables dependientes de las ecuaciones 2 y 4.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR NIVEL DE SEVERIDAD

El GRÁFICO 9 muestra la cantidad de riesgos valorados, agrupados por nivel de severidad, utilizando el proceso de valoración alternativo.

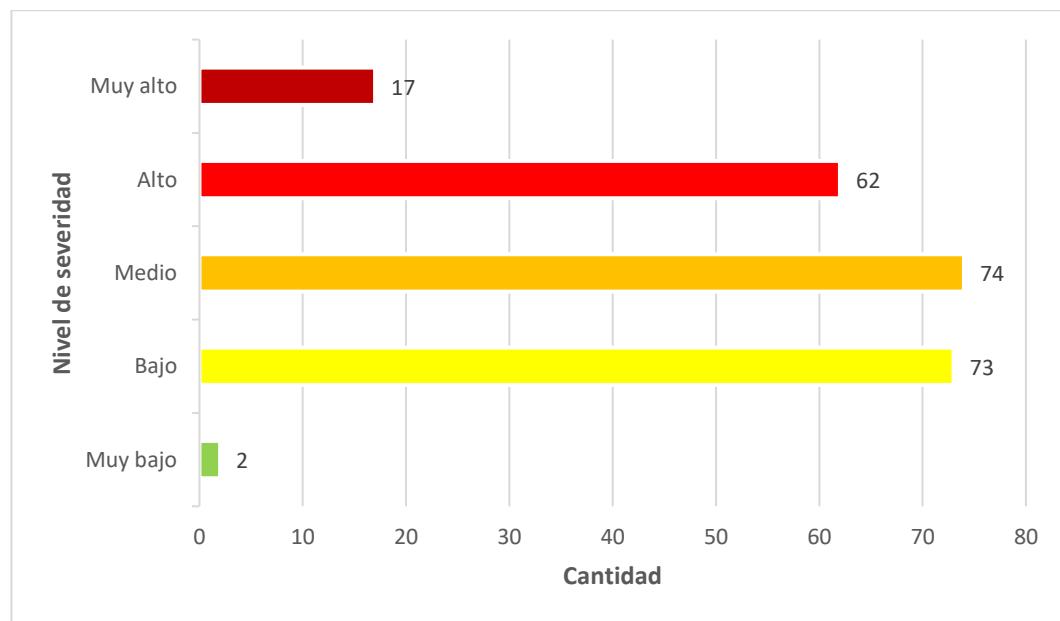


Gráfico 9. Cantidad de riesgos valorados, agrupados por nivel de severidad, utilizando el procedimiento de valoración alternativo. Fuente: Elaboración propia.

En total, 153 riesgos tienen que ser mitigados, pues esa es la cantidad de riesgos cuyo nivel de severidad es medio, alto o muy alto. Al comparar estos resultados con la valoración obtenida en la sección 6.4, en la que 152 riesgos fueron mitigados, se determina que el procedimiento alternativo requiere atender un riesgo más que el procedimiento original. Sin embargo, la variación va más allá de un riesgo adicional por mitigar, pues, aunque la cantidad de riesgos con nivel de severidad muy

alto se mantuvo en 17 utilizando ambos procedimientos, el número de riesgos con niveles de severidad alta y media cambió considerablemente. Con el procedimiento alternativo, los riesgos con nivel de severidad alto se incrementaron de 50 a 62, mientras que los riesgos con nivel de severidad medio disminuyeron de 85 a 74. Un ejemplo de riesgo cuya valoración cambió al utilizar el procedimiento alternativo es el riesgo número 25 —el cual establece que la presencia de defectos en el componente “Validador del certificado” permiten que la aplicación ignore el campo “Uso de la llave” de los certificados digitales, de forma tal que certificados de autenticación se pueden usar para crear firmas digitales, y certificados para la creación de firma digital se pueden usar para autenticación—, que pasó de tener un nivel de severidad medio con el procedimiento de valoración original, a tener un nivel de severidad alto al utilizar el procedimiento alternativo.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR ESCENARIO ANALIZADO Y NIVEL DE SEVERIDAD

El GRÁFICO 10 presenta la cantidad de riesgos valorados, agrupados por escenario analizado y nivel de severidad, utilizando el procedimiento de valoración alternativo. En comparación con los resultados obtenidos en la sección 6.4, no hubo una variación en la cantidad de riesgos que deben ser mitigados en los escenarios analizados.

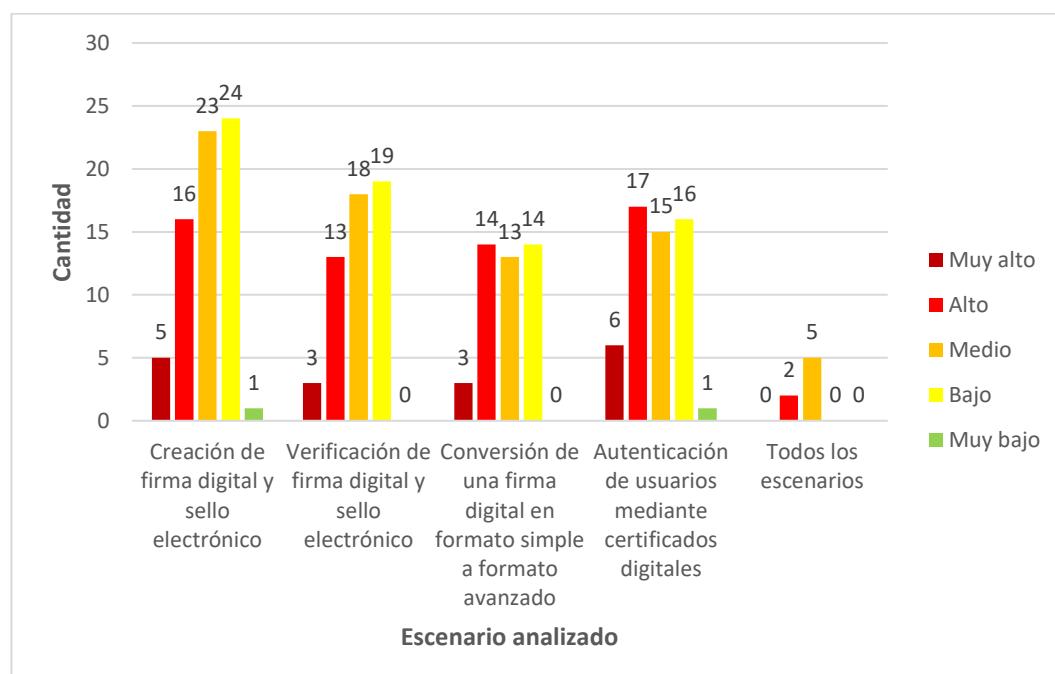


Gráfico 10. Cantidad de riesgos valorados, agrupados por escenario analizado y nivel de severidad, utilizando el procedimiento de valoración alternativo. Fuente: Elaboración propia.

Sin embargo, sí hubo algunos movimientos en la cantidad de riesgos presentes en los niveles de severidad de algunos escenarios, tales como creación de firma digital y sello electrónico, verificación de firma digital y sello electrónico, y autenticación de usuarios mediante certificados digitales, en los cuales la cantidad de riesgos con severidad media disminuyó, mientras que la cantidad de riesgos con severidad alta aumentó. Por ejemplo, en el escenario de autenticación de usuarios mediante certificados digitales, el número de riesgos con severidad media pasó de ser 20 con el procedimiento de valoración original, a 15 con el procedimiento de valoración alternativo, mientras que la cantidad de riesgos con severidad alta cambió de 12 a 17.

CANTIDAD DE RIESGOS VALORADOS, AGRUPADOS POR AMBIENTE DE EJECUCIÓN Y NIVEL DE SEVERIDAD

Finalmente, el GRÁFICO 11 muestra la cantidad de riesgos valorados, agrupados por ambiente de ejecución y nivel de severidad, utilizando el procedimiento de valoración alternativo. Según dicho gráfico, el procedimiento de valoración alternativo y el utilizado en la sección 6.4 produjeron la misma valoración para los riesgos identificados en los ambientes de ejecución centralizado y distribuido. En los riesgos que se identificaron dentro de ambos ambientes, la cantidad de riesgos con severidad muy alta se mantiene en 17 al usar cualquiera de los dos procedimientos, sin embargo, los de severidad media se redujeron de 16 en el procedimiento original, a 5 en el procedimiento alternativo, mientras que los de severidad alta se incrementaron de 16 a 28.

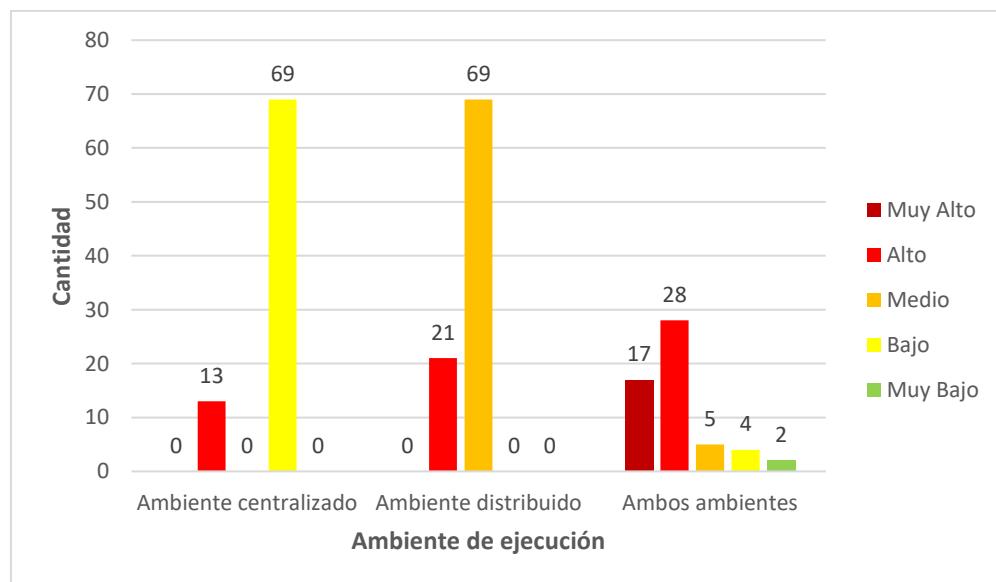


Gráfico 11. Cantidad de riesgos valorados, agrupados por ambiente de ejecución y nivel de severidad, utilizando el procedimiento de valoración alternativo. Fuente: Elaboración propia.

11.4. APÉNDICE D: TERMINOLOGÍA RELEVANTE EN LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL

A continuación, se presenta la terminología relevante en la definición de políticas de seguridad de la información y el establecimiento de objetivos de control. Cuando en el Apéndice E: Políticas de Seguridad de la Información Definidas y en el Apéndice F: 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” (*Cryptographic Message Syntax* en inglés), 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).

Macro: es un conjunto de instrucciones grabadas (pulsaciones de teclas y acciones del *mouse*), utilizadas para automatizar tareas repetitivas (Microsoft, 2002). Las macros son comunes en hojas de cálculo y aplicaciones de procesamiento de texto.

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).

PDF 1.7: es la abreviatura de “Formato de Documentos Portables versión 1.7” (*Portable Document Format* 1.7 en inglés), un formato de documento electrónico para el cual se define una especificación de firma digital que consiste en agregar una estructura de datos llamada diccionario de firma al documento. El diccionario contiene la firma digital e información adicional de la misma (Adobe Systems Incorporated, 2008).

PKCS#7: es la abreviatura de “Estándar de Criptografía de Llave Pública 7” (*Public Key Cryptography 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 (The PHP Group, 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).

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. (Jøsang & AlFayyadh, 2008).

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).

11.5. APÉNDICE E: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEFINIDAS

Seguidamente se presenta la definición de las políticas de seguridad de la información para mitigar los riesgos cuyo nivel de severidad se valoró como medio, alto o crítico, y que fueron identificados en cada uno de los escenarios analizados.

El detalle completo de la identificación y valoración de los riesgos referenciados por las políticas de seguridad de la información definidas en esta sección se especifica en el Apéndice A: Riesgos Identificados, y en el Apéndice B: Detalle de la Valoración de los Riesgos Identificados.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CREACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

A continuación, se presentan las políticas de seguridad de la información establecidas para el escenario de creación de firma digital y sello electrónico. Las tablas 27, 28, 29 y 30 describen las políticas de integridad, autenticación, confidencialidad y no repudio, respectivamente.

Tabla 27. Políticas de integridad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
1	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 4
2	Se debe validar que el documento electrónico que se va a firmar no contiene código oculto o malicioso.	Mitiga riesgo 5
3	Se debe validar que los documentos electrónicos resultantes, firmados en formato simple, puedan convertirse posteriormente a formatos avanzados válidos.	Mitiga riesgo 28
4	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: 32, 33, 35, 36, 37, 38, 39, 40, 41, 46, 47
5	Se debe proteger el resultado de la validación del documento electrónico que se va a firmar, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 34
6	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: 42, 43, 45
7	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 riesgo 44
8	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 riesgos: 1, 3 y 7

Tabla 27. Políticas de integridad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
9	Se debe proteger el resultado de la validación del documento electrónico que se va a firmar mientras transita por la memoria local, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 6
10	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 riesgo 2
11	El <i>software</i> complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, <i>frameworks</i> , <i>plug-ins</i> y <i>drivers</i> , debe tener instaladas las actualizaciones de seguridad más recientes.	Mitiga riesgos: 160, 161 y 162

Tabla 28. Políticas de autenticación para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
12	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 riesgo 12
13	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de firma es válido.	Mitiga riesgo 23
14	Se debe validar que el certificado digital que se utilizará en el proceso de firma pertenece a la jerarquía nacional de certificadores registrados.	Mitiga riesgo 23
15	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 riesgo 23

Tabla 28. Políticas de autenticación para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
16	Se debe validar que el certificado digital que se utilizará en el proceso de firma se encuentra almacenado en un dispositivo criptográfico seguro.	Mitiga riesgo 24
17	Se debe validar el uso correcto del certificado que se utilizará en el proceso de firma.	Mitiga riesgo 25

Tabla 29. Políticas de confidencialidad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
18	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 riesgo 13
19	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 14
20	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no sean almacenadas en caché para su uso posterior, exceptuando aquellos casos excepcionales en los que dicho almacenamiento sea un requisito funcional explícito de la aplicación, por ejemplo, en la firma por lotes.	Mitiga riesgo 16
21	Se debe validar que el documento electrónico firmado resultante no se entregue a usuarios no autorizados.	Mitiga riesgo 30
22	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 red, de manera que no puedan ser revelados a usuarios no autorizados.	Mitiga riesgos: 32, 33, 35, 36, 37, 38, 39, 40, 41, 46, 47

Tabla 29. Políticas de confidencialidad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
23	Se debe proteger el documento electrónico que se va a firmar, mientras transita por la memoria local, de manera que no pueda ser revelado a usuarios no autorizados.	Mitiga riesgos: 1, 3 y 7
24	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 159
25	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	Mitiga riesgo 163

Tabla 30. Políticas de no repudio para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
26	El resumen del documento electrónico que se va a firmar debe calcularse utilizando algoritmos <i>hash</i> seguros.	Mitiga riesgo 8
27	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 23
28	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)

Tabla 30. Políticas de no repudio para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
29	Antes de iniciar con el proceso de firma digital, se debe capturar al menos una acción explícita que demuestre afirmativamente la manifestación de la voluntad del usuario para crear la firma digital.	Ley de certificados, firmas digitales y documentos electrónicos N° 8454 (artículo 10)

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA VERIFICACIÓN DE FIRMA DIGITAL Y SELLO ELECTRÓNICO

A continuación, se presentan las políticas de seguridad de la información establecidas para el escenario de verificación de firma digital y sello electrónico. Las tablas 31, 32, 33 y 34 describen las políticas de integridad, autenticación, confidencialidad y no repudio, respectivamente.

Tabla 31. Políticas de Integridad para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
30	Se debe validar que el formato del documento electrónico cuyas firmas se van a verificar, está soportado por el SNCD y por la aplicación, y que además es correcto.	Mitiga riesgo 51
31	Se debe validar que el documento electrónico cuyas firmas se van a verificar, no contiene código oculto (por ejemplo, macros) o malicioso.	Mitiga riesgo 52

Tabla 31. Políticas de Integridad para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
32	Se debe proteger el documento electrónico cuyas firmas se van a verificar, así como sus representaciones derivadas (resúmenes cifrados extraídos, documento electrónico original, resumen del documento electrónico original, resúmenes descifrados), mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos: 69, 70, 72, 76, 77, 78, 79, 80, 81
33	Se debe proteger el resultado de la validación del documento electrónico cuyas firmas se van a verificar, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 71
34	Se debe proteger los certificados digitales extraídos del documento electrónico cuyas firmas se van a verificar, mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos: 73, 75
35	Se debe proteger el resultado de las validaciones de los certificados extraídos del documento electrónico cuyas firmas se van a verificar, mientras se transmiten por una red, de manera que no puedan ser modificadas por usuarios no autorizados.	Mitiga riesgo 74
36	Se debe proteger el resultado de las verificaciones de las firmas digitales, mientras se transmiten por una red, de manera que no puedan ser modificadas por usuarios no autorizados.	Mitiga riesgo 82
37	Se debe proteger el documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos: 48 y 50
38	Se debe proteger el resultado de la validación del documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 53
39	Se debe proteger el resultado de las validaciones de los certificados extraídos del documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no puedan ser modificadas por usuarios no autorizados.	Mitiga riesgo 59

Tabla 31. Políticas de Integridad para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
40	Se debe proteger el resultado de las verificaciones de las firmas digitales, mientras transita por la memoria local, de manera que no puedan ser modificadas por usuarios no autorizados.	Mitiga riesgo 68
41	El <i>software</i> complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, <i>frameworks</i> , <i>plug-ins</i> y <i>drivers</i> , debe tener instaladas las actualizaciones de seguridad más recientes.	Mitiga riesgos: 160, 161 y 162

Tabla 32. Políticas de autenticación para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
42	Se debe validar que todos los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar, pertenecen a la jerarquía nacional de certificadores registrados.	Mitiga riesgo 57
43	Se debe validar el uso correcto de los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar.	Mitiga riesgo 58

Tabla 33. Políticas de confidencialidad para el escenario de creación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
44	Se debe proteger el documento electrónico cuyas firmas se van a verificar, así como sus representaciones derivadas (resúmenes cifrados extraídos, documento electrónico original, resumen del documento electrónico original, resúmenes descifrados), mientras se transmiten por red, de manera que no puedan ser revelados a usuarios no autorizados.	Mitiga riesgos: 69, 70, 72, 76, 77, 78, 79, 80, 81
45	Se debe proteger el documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser revelado a usuarios no autorizados.	Mitiga riesgos: 48 y 50
46	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 159
47	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	Mitiga riesgo 163

Tabla 34. Políticas de no repudio para el escenario de verificación de firma digital y sello electrónico. Fuente: Elaboración propia.

ID	Política	Base lógica
48	Se debe validar que todos los certificados digitales, así como sus rutas de certificación, estaban vigentes cuando se incluyeron en el documento electrónico cuyas firmas se van a verificar.	Mitiga riesgo 56
49	El resumen del documento electrónico cuyas firmas se van a verificar debe calcularse utilizando algoritmos <i>hash</i> seguros.	Mitiga riesgo 65

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CONVERSIÓN DE UNA FIRMA DIGITAL EN FORMATO SIMPLE A FORMATO AVANZADO

A continuación, se presentan las políticas de seguridad de la información establecidas para el escenario de conversión de una firma digital en formato simple a formato avanzado. Las tablas 35, 36, 37 y 38 describen las políticas de integridad, autenticación, confidencialidad y no repudio, respectivamente.

Tabla 35. Políticas de integridad para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

ID	Política	Base lógica
50	Se debe validar que el formato del documento electrónico cuyo formato se convertirá, está soportado por la aplicación, es correcto y puede convertirse a un formato avanzado válido.	Mitiga riesgo 86
51	Se debe validar que el documento electrónico cuyo formato se convertirá, no contiene código oculto (por ejemplo, macros) o malicioso.	Mitiga riesgo 87
52	Se debe proteger la información de revocación de los certificados digitales contenidos en el documento electrónico cuyo formato se convertirá, obtenida mediante CRL, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 97
53	Se debe proteger la información de revocación de los certificados digitales contenidos en el documento electrónico cuyo formato se convertirá, obtenida mediante OCSP, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 98
54	Se debe proteger los certificados obtenidos desde almacenes de certificados, mientras se transmiten por una red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 99
55	Se debe proteger los <i>tokens</i> de estampado de tiempo, mientras se transmiten por red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 100

Tabla 35. Políticas de integridad para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (Continuación)

ID	Política	Base lógica
56	Se debe validar que el formato de los documentos electrónicos resultantes, firmados en formato avanzado, corresponde con alguno de los formatos oficiales soportados en Costa Rica.	Mitiga riesgo 103
57	Se debe proteger el documento electrónico cuyo formato se convertirá, así como sus representaciones derivadas (documento electrónico firmado en formato avanzado), mientras se transmite por una red, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos: 107, 108, 110, 113, 114, 115
58	Se debe proteger el resultado de la validación del documento electrónico cuyo formato se convertirá, mientras se transmite por una red, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgo 109
59	Se debe proteger los certificados digitales extraídos del documento electrónico cuyo formato se convertirá, mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 111
60	Se debe proteger los atributos obtenidos para la creación del documento electrónico en formato avanzado, mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 112
61	Se debe proteger el resultado de la validación del documento electrónico cuyo formato se convertirá, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgo 88
62	Se debe proteger los atributos obtenidos para la creación del documento electrónico en formato avanzado, mientras transitán por la memoria local, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 101
63	El <i>software</i> complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, <i>frameworks</i> , <i>plug-ins</i> y <i>drivers</i> , debe tener instaladas las actualizaciones de seguridad más recientes.	Mitiga riesgos: 160, 161 y 162

Tabla 36. Políticas de autenticación para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

ID	Política	Base lógica
64	La dirección requerida para acceder al servicio que provee las CRL debe extraerse directamente del certificado, y de ninguna manera debe estar contenida en el código fuente, archivos de texto, base de datos o cualquier otro tipo de almacenamiento.	Mitiga riesgo 91
65	La dirección requerida para acceder al servicio que provee OCSP debe extraerse directamente del certificado, y de ninguna manera debe estar contenida en el código fuente, archivos de texto, base de datos o cualquier otro tipo de almacenamiento.	Mitiga riesgo 93
66	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 riesgo 95
67	La dirección requerida para obtener los <i>tokens</i> de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.	Mitiga riesgo 96

Tabla 37. Políticas de confidencialidad para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

ID	Política	Base lógica
68	Se debe validar que el documento electrónico resultante, firmado en formato avanzado, no se entregue a usuarios no autorizados.	Mitiga riesgo 105

Tabla 37. Políticas de confidencialidad para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia. (*Continuación*)

ID	Política	Base lógica
69	Se debe proteger el documento electrónico cuyo formato se convertirá, así como sus representaciones derivadas (documento electrónico firmado en formato avanzado), mientras se transmite por una red, de manera que no pueda ser revelado a usuarios no autorizados.	Mitiga riesgos: 107, 108, 110, 113, 114 y 115
70	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 159
71	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	Mitiga riesgo 163

Tabla 38. Políticas de no repudio para el escenario de conversión de una firma digital en formato simple a formato avanzado. Fuente: Elaboración propia.

ID	Política	Base lógica
72	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	Mitiga riesgo 92
73	Se debe validar que las respuestas OCSP no sean reutilizables.	Mitiga riesgo 94

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA AUTENTICACIÓN DE USUARIOS MEDIANTE CERTIFICADOS DIGITALES

A continuación, se presentan las políticas de seguridad de la información establecidas para el escenario de conversión de una firma digital en formato simple a formato avanzado. Las tablas 39, 40, 41 y 42 describen las políticas de integridad, autenticación, confidencialidad y no repudio, respectivamente.

Tabla 39. Políticas de integridad para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

ID	Política	Base lógica
74	Se debe proteger la información de revocación del certificado digital que se utilizará durante el proceso de autenticación, obtenida mediante CRL, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 140
75	Se debe proteger la información de revocación del certificado digital que se utilizará durante el proceso de autenticación, obtenida mediante OCSP, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 141
76	Se debe proteger los certificados obtenidos desde almacenes de certificados, mientras se transmiten por una red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 142
77	Se debe proteger los <i>tokens</i> de estampado de tiempo, mientras se transmiten por una red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgo 143
78	Se debe proteger los datos de autenticación generados, así como sus representaciones derivadas (resumen de los datos de autenticación generados y resumen cifrado de los datos de autenticación generados), mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	Mitiga riesgos: 147, 148, 149, 150, 151, 156
79	Se debe proteger el certificado digital que se utilizará en el proceso de autenticación, mientras se transmite por una red, de manera que no pueda ser modificado por usuarios no autorizados.	Mitiga riesgos: 152, 153, 155

Tabla 39. Políticas de integridad para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

(Continuación)

ID	Política	Base lógica
80	Se debe proteger el resultado de la validación del certificado digital que se utilizará en el proceso de autenticación, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 154
81	Se debe proteger el resultado de la comparación de los resúmenes calculados en el proceso de autenticación, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 157
82	Se debe proteger el resultado de la validación del certificado digital que se utilizará en el proceso de autenticación, mientras transita por la memoria local, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 133
83	Se debe proteger el resultado de la comparación de los resúmenes calculados en el proceso de autenticación, mientras transita por la memoria local, de manera que no pueda ser modificada por usuarios no autorizados.	Mitiga riesgo 146
84	El <i>software</i> complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, <i>frameworks</i> , <i>plug-ins</i> y <i>drivers</i> , debe tener instaladas las actualizaciones de seguridad más recientes.	Mitiga riesgos: 160, 161 y 162

Tabla 40. Políticas de autenticación para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

ID	Política	Base lógica
85	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 riesgo 119

Tabla 40. Políticas de autenticación para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.*(Continuación)*

ID	Política	Base lógica
86	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de autenticación es válido.	Mitiga riesgo 130
87	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación pertenece a la jerarquía nacional de certificadores registrados.	Mitiga riesgo 130
88	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación se encuentra almacenado en un dispositivo criptográfico seguro.	Mitiga riesgo 131
89	Se debe validar el uso correcto del certificado que se utilizará en el proceso de autenticación.	Mitiga riesgo 132
90	La dirección requerida para acceder al servicio que provee las CRL debe extraerse directamente del certificado, y de ninguna manera debe estar contenida en el código fuente, archivos de texto, base de datos o cualquier otro tipo de almacenamiento.	Mitiga riesgo 134
91	La dirección requerida para acceder al servicio que provee OCSP debe extraerse directamente del certificado, y de ninguna manera debe estar contenida en el código fuente, archivos de texto, base de datos o cualquier otro tipo de almacenamiento.	Mitiga riesgo 136
92	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 riesgo 138
93	La dirección requerida para obtener los <i>tokens</i> de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.	Mitiga riesgo 139

Tabla 41. Políticas de confidencialidad para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

ID	Política	Base lógica
94	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 alguien más.	Mitiga riesgo 120
95	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 121
96	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no sean almacenadas en caché para su uso posterior.	Mitiga riesgo 123
97	Se debe proteger los datos de autenticación generados para el proceso de autenticación, así como sus representaciones derivadas (resumen de los datos de autenticación y resumen cifrado de los datos de autenticación), mientras se transmiten por una red, de manera que no sean revelados a usuarios no autorizados.	Mitiga riesgos: 147, 148, 149, 150, 151, 156
98	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 159
99	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	Mitiga riesgo 163

Tabla 42. Políticas de no repudio para el escenario de autenticación de usuarios mediante certificados digitales. Fuente: Elaboración propia.

ID	Política	Base lógica
100	El resumen de los datos de autenticación que se van a firmar debe calcularse utilizando algoritmos <i>hash</i> seguros.	Mitiga riesgo 117
101	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación se encuentra vigente.	Mitiga riesgo 130
102	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	Mitiga riesgo 135
103	Se debe verificar que las respuestas OCSP no sean reutilizables.	Mitiga riesgo 137

11.6. APÉNDICE F: OBJETIVOS DE CONTROL ESTABLECIDOS

A continuación, se presentan los objetivos de control establecidos para hacer cumplir las políticas de seguridad de la información definidas. Las tablas 43, 44, 45 y 46 describen los objetivos de control para las políticas de integridad, autenticación, confidencialidad y no repudio, respectivamente.

Tabla 43. Objetivos de control para hacer cumplir las políticas de integridad definidas. Fuente:
Elaboración propia.

ID	Objetivo de control	Base lógica
1	<p>Se deben validar los datos que el usuario introduce en el sistema, verificando que cada entrada cumple al menos con los siguientes requisitos:</p> <p><i>Cuando la entrada es texto</i></p> <ul style="list-style-type: none"> • 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 mínimo y máximo 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 (<i>prepared statements</i>), 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. <p><i>Cuando la entrada es un archivo</i></p> <ul style="list-style-type: none"> • 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, <i>malware</i>, 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, <i>.htaccess</i> en Apache, o <i>Web.conf</i> en IIS, entre otros. 	Permite evaluar políticas: 1, 2, 30, 31, 50, 51

Tabla 43. Objetivos de control para hacer cumplir las políticas de integridad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
2	Se debe validar que los formatos de documento firmado en formato simple corresponden a alguno de los siguientes: PKCS#7, CMS, XMLDSig y PDF 1.7, y rechazar los demás.	Permite evaluar políticas: 3, 50
3	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: 4, 5, 6, 7, 32, 33, 34, 35, 36, 52, 53, 54, 55, 56, 57, 58, 59, 60, 74, 75, 76, 77, 78, 79, 80

Tabla 43. Objetivos de control para hacer cumplir las políticas de integridad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
4	<p>Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, <i>malware</i> y cualquier otro tipo de <i>software</i> malicioso que facilite la modificación no autorizada de datos, utilizando los siguientes criterios:</p> <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final</i></p> <p>Se debe validar la existencia de un procedimiento periódico, ejecutado como máximo cada 7 días naturales, 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:</p> <ul style="list-style-type: none"> • 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. • Lista de archivos analizados. • Resultado del análisis. <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final</i></p> <p>Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique:</p> <ul style="list-style-type: none"> • Recomendaciones para mantener la máquina libre de infecciones. • La importancia que tiene el mantener una máquina libre de infecciones, en lo que respecta al no repudio de la información. 	Permite evaluar políticas: 8, 9, 10, 37, 38, 39, 40, 61, 62, 81, 82, 83

Tabla 43. Objetivos de control para hacer cumplir las políticas de integridad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
5	<p>Se debe validar que el <i>software</i> complementario, requerido para ejecutar la aplicación, se encuentra actualizado en la máquina donde se ejecuta, utilizando los siguientes criterios:</p> <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final</i></p> <p>Se debe validar la existencia un procedimiento periódico, ejecutado como máximo cada 7 días naturales, para comprobar que al menos el sistema operativo, los navegadores de Internet, los <i>frameworks</i>, los <i>plugins</i> y los <i>drivers</i> necesarios, están actualizados. Se debe registrar una bitácora cada vez que el procedimiento se ejecuta, en la que se almacene al menos la siguiente información:</p> <ul style="list-style-type: none"> • Nombre del responsable de ejecutar el procedimiento. • Fecha y hora en la que se ejecuta el procedimiento. • Identificador de la máquina. • Nombre del software comprobado. • Versión original del software. • Versión actualizada del software (si aplica). <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final</i></p> <p>Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique:</p> <ul style="list-style-type: none"> • Recomendaciones para mantener el <i>software</i> complementario actualizado en la máquina. • La importancia que tiene el mantener dicho <i>software</i> actualizado, en lo que respecta al no repudio de la información. 	Permite evaluar políticas: 11, 41, 63, 84

Tabla 44. Objetivos de control para hacer cumplir las políticas de autenticación definidas. Fuente:
Elaboración propia.

ID	Objetivo de control	Base lógica
6	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: 12, 85
7	Se debe validar que el perfil del certificado digital cumple con los requisitos establecidos en la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013).	Permite evaluar políticas: 13, 86
8	La pertenencia del certificado digital a la jerarquía nacional de certificadores registrados se debe implementar mediante una validación que sea funcionalmente equivalente al algoritmo descrito en la sección 6.1 del RFC 5280 (Cooper et al., 2008).	Permite evaluar políticas: 14, 42, 87
9	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 política 15
10	Se debe garantizar que los certificados digitales utilizados se cargan desde los dispositivos criptográficos seguros conectados.	Permite evaluar políticas: 16, 88
11	Se debe validar que el uso del certificado digital cumple con los requisitos establecidos en la sección 1.4.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013).	Permite evaluar políticas: 17, 43, 89

Tabla 44. Objetivos de control para hacer cumplir las políticas de autenticación definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
12	<p>Las direcciones para acceder a la CRL, el servicio OCSP, el certificado de la CA emisora (para validar la ruta de certificación) y el servicio de estampado de tiempo, se deben extraer de la siguiente manera:</p> <ul style="list-style-type: none"> • <u>CRL</u>: el valor está contenido en el certificado, y dado por el campo <i>Punto de distribución del CRL</i>, como lo indica la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013). • <u>OCSP</u>: el valor está contenido en el certificado, y dado por la primera posición del campo <i>Acceso a la información de la autoridad</i>, como lo indica la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013). • <u>Certificado de la CA emisora</u>: el valor está contenido en el certificado, y dado por la segunda posición del campo <i>Acceso a la información de la autoridad</i>, como lo indica la sección 7.1 de la <i>Política de certificados para la jerarquía nacional de certificadores registrados</i> (Gobierno de Costa Rica, 2013). • <u>Servicio de estampado de tiempo</u>: el valor está definido en la sección 6.1 del <i>Estándar electrónico – Servicios Firma Digital en Internet</i> (SINPE, 2016). 	Permite evaluar políticas: 64, 65, 66, 67, 90, 91, 92, 93

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente: Elaboración propia.

ID	Objetivo de control	Base lógica
13	<p>La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro debe cumplir al menos con los siguientes requisitos:</p> <ul style="list-style-type: none"> • 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: 18, 94
14	<p>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:</p> <ul style="list-style-type: none"> • 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 políticas: 19, 95

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
15	<p>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:</p> <p><i>Cuando el almacenamiento en caché está prohibido</i></p> <ul style="list-style-type: none"> • 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. <p><i>Cuando el almacenamiento en caché es requerido</i></p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ▪ Se debe mostrar al usuario una llamada a la acción que describa clara y concisamente la operación que está por ejecutar. ▪ 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: <ul style="list-style-type: none"> ▪ Datos que permitan identificar a la entidad actualmente autenticada. ▪ La fecha y la hora del suceso. ▪ El propósito de uso que justifique el almacenamiento en caché de las credenciales. 	Permite evaluar políticas: 20, 96

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
	<ul style="list-style-type: none"> ● Las bitácoras generadas deben almacenarse como se indica a continuación: <ul style="list-style-type: none"> ▪ Si todos los componentes de la aplicación se encuentran centralizados, y, por lo tanto, se ejecutan en una sola máquina, las bitácoras deben almacenarse en ella. ▪ Si los componentes de la aplicación se encuentran distribuidos, y, por lo tanto, se ejecutan en varias máquinas, las bitácoras deben almacenarse al menos en una de ellas. ● Se debe validar la existencia de un procedimiento periódico, ejecutado como máximo cada 7 días naturales, para auditar las bitácoras generadas. Dicho procedimiento debe cumplir al menos con los siguientes requerimientos: <ul style="list-style-type: none"> ▪ Debe designarse una persona responsable de tomar decisiones según los resultados de las auditorías. ▪ Debe designarse un responsable de ejecutar las auditorías. ▪ Durante la ejecución del procedimiento, se debe revisar las bitácoras generadas desde la última vez que el procedimiento se ejecutó. ▪ Se debe comprobar que la entidad identificada en cada bitácora está autorizada a ejecutar operaciones que acceden a su llave privada a través de credenciales almacenadas en caché. ▪ Se debe comprobar que el propósito de uso para el almacenamiento en caché de las credenciales es válido, según el grado de tolerancia al riesgo. ▪ Se debe entregar el resultado de cada auditoría a la persona responsable de tomar decisiones. 	

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
16	Para que la entrega del documento electrónico firmado sea posible, se debe satisfacer al menos un control de autorización.	Permite evaluar políticas: 21, 68
17	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: 22, 44, 69, 97
18	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 políticas: 24, 46, 70, 98

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
19	<p>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:</p> <ul style="list-style-type: none"> • 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 <i>stack traces</i>. • 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: 25, 47, 71, 99

Tabla 45. Objetivos de control para hacer cumplir las políticas de confidencialidad definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
20	<p>Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, <i>malware</i> y cualquier otro tipo de <i>software</i> malicioso que facilite la divulgación no autorizada de datos, utilizando los siguientes criterios:</p> <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final</i></p> <p>Se debe validar la existencia de un procedimiento periódico, ejecutado como máximo cada 7 días naturales, 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:</p> <ul style="list-style-type: none"> • 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. • Lista de archivos analizados. • Resultado del análisis. <p><i>Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final</i></p> <p>Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique:</p> <ul style="list-style-type: none"> • Recomendaciones para mantener la máquina libre de infecciones. • La importancia que tiene el mantener una máquina libre de infecciones, en lo que respecta al no repudio de la información. 	Permite evaluar políticas: 18, 20, 23, 45, 94, 96

Tabla 46. Objetivos de control para hacer cumplir las políticas de no repudio definidas. Fuente:
Elaboración propia.

ID	Objetivo de control	Base lógica
21	Se debe validar que los algoritmos de <i>hash</i> utilizados son seguros, y tienen una efectividad igual o superior a SHA-2, y rechazar los demás.	Permite evaluar políticas: 26, 49, 100
22	<p>La validación de la vigencia del certificado debe cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> • 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 políticas: 27, 48, 101
23	La visualización del documento electrónico debe utilizar un método que cumpla con el principio WYSIWYS.	Permite evaluar política 28
24	<p>La captura de la manifestación de la voluntad del usuario debe cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> • Se debe mostrar al usuario una llamada a la acción que describa clara y concisamente la operación que está por ejecutar. • Antes de que la operación mencionada anteriormente se ejecute, el usuario debe satisfacer al menos un método de tipo desafío-respuesta. 	Permite evaluar política 29
25	Para validar la vigencia de una CRL, debe verificarse que la fecha al momento de utilizar esa lista es anterior a la especificada en el campo llamado <i>Siguiente actualización</i> .	Permite evaluar políticas: 72, 102

Tabla 46. Objetivos de control para hacer cumplir las políticas de no repudio definidas. Fuente:
Elaboración propia. (Continuación)

ID	Objetivo de control	Base lógica
26	Las solicitudes OCSP deben implementarse de manera tal que siempre accedan al proveedor del servicio, es decir, nunca deben ser almacenadas en caché para su uso posterior.	Permite evaluar políticas: 73, 103

