UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

DESARROLLO DE UNA APLICACIÓN DE REFERENCIA PARA EVALUAR LA GUÍA DE IMPLEMENTACIÓN DE APLICACIONES DE SOFTWARE QUE UTILIZAN CERTIFICADOS Y FIRMA DIGITAL 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 al grado y título de Maestría Profesional en Computación e Informática

VIVIANA MARÍA DURÁN VEGA

Ciudad Universitaria Rodrigo Facio, Costa Rica
2019

Dedicado a,

Dios por ser quien siempre me da las fuerzas para lograr mis metas.

A mi esposo por ser quien me inspira y me apoya en todo momento.

A mi padres y hermanos por su amor y apoyo en cada paso que realizo.

Agradecimientos

Quiero expresar mi más sincero agradecimiento al Dr. Ricardo Villalón Fonseca, quien siempre fue constante en su apoyo para la realización del proyecto, además de su gran disponibilidad, empatía y conocimientos a lo largo de todo este proceso.

También quiero agradecer a la Dra. Gabriela Marín Raventós, directora del programa de posgrado por su comprensión y apoyo durante los últimos meses de finalización del proyecto.

A mis padres, con mucho amor les doy gracias porque la mejor herencia que me dejaron es la posibilidad de ser una mujer profesional.

Finalmente, agradezco a los profesores del sistema de Estudios de Posgrado de la Universidad de Costa Rica, que durante los últimos años con sus enseñanzas han ayudado en mi formación académica que me ha permitido ser mejor 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 al grado y título de Maestría Profesional en Computación e informática.

Dra. Gabriela Barrantes Sliesarieva

Representante del Decano Sistema de Estudios de Posgrado

Dr. Ricardo Villalón Fonseca

Profesor Guía

Dra. Gabriela Marín Raventós

Directora del Programa de Posgrado en Computación e Informática

Viviana María Durán Vega

Estudiante

Tabla de contenidos

Resumen

En Costa Rica, la implementación de firma digital ha incrementado durante los últimos años. A partir de la aprobación del proyecto de ley en el año 2005, titulado "Ley de Certificados, Firmas Digitales y Documentos Electrónicos", y la publicación de la directriz "Masificación de la implementación y el uso de la firma digital en el sector público costarricense" donde el gobierno promueve el uso de firma digital y solicita a las instituciones costarricenses que empiecen a facilitar a los usuarios servicios de forma electrónica utilizando firma digital. Sin embargo, hasta el día de hoy no existe una regulación o recurso técnico disponible a nivel nacional que provea algún tipo de orientación para el aseguramiento de este tipo de aplicaciones en Costa Rica.

El objetivo principal de este proyecto de investigación es desarrollar una aplicación de referencia con el fin de asegurarla utilizando una *Guía de implementación,* para crear una referencia práctica para futuras implementaciones de firma y certificados digitales dentro del Sistema Nacional de Certificación Digital (SNCD). Dicha guía fue desarrollada por el estudiante Alejandro Mora en su TFIA titulado "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".

Inicialmente, se desarrolla una aplicación de referencia de firma digital y se asegura utilizando la *Guía de implementación*. Seguidamente, se realiza un análisis para identificar si dicha guía es factible y eficiente para el aseguramiento aplicaciones de firma digital dentro del SNCD, ya que es un recurso que se desea proveer en el futuro al público costarricense.

Una vez realizada la evaluación de la guía, se concluye que es factible de utilizar y fácil de comprender para el aseguramiento de aplicaciones de firma digital. Se identificó que la guía es de gran utilidad ya que, durante el aseguramiento de la aplicación de referencia, se encontraron aspectos de seguridad que no se habían tomado en cuenta durante el desarrollo. Adicionalmente, se encontró que algunas políticas de seguridad planteadas en la guía no se pudieron cumplir por la forma en que actualmente la PKI de Costa Rica provee sus servicios de "Listas de Revocaciones". Finalmente, respecto a la eficiencia de la guía, se detectaron algunos puntos a considerar relacionados a la longitud y formulación de la misma que se deben tomar en cuenta para futuras mejoras.

Summary

In Costa Rica, the implementation of the digital signature has increased during the last years. After the approval of *"Ley de Certificados, Firmas Digitales y Documentos Electrónicos"* and the publication of *"Masificación de la implementación y el uso de la firma digital en el sector público costarricense"* in 2005, where the government promotes the use of digital signature and request to the Costa Rican institutions start providing users with services electronically using a digital signature. However, until today there is no regulation or technical resource available that provides any kind of guidance for the assurance of this type of applications in Costa Rica.

The main objective of this research project is to develop a reference application in order to secure it using the *Implementation Guide*, to create a practical reference for future digital signature implementations within the National Digital Certification System (SNCD). This guide was developed by the student Alejandro Mora in his TFIA entitled *"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"*.

Firstly, a digital signature reference application is developed and secured using the *Implementation Guide*. Next, an analysis is carried out to identify if this guide is feasible and efficient for the assurance of digital signature applications within the SNCD, since it is a resource that it is desired to provide in the future to the Costa Rican public.

Once the evaluation of the guide has been completed, it is concluded that it is feasible to use and easy to understand for secure digital signature applications. Besides, it was identified that the guide is very useful because during the process of secure the reference application, some security vulnerabilities that had not been considered during the development were found. Additionally, it was found that some security policies of the guide could not be met because of the way in which the PKI of Costa Rica currently provides its "Revocation Lists" services. Finally, regarding the efficiency of the guide, some points to consider related to the length and formulation thereof were detected that should be considered for future improvements.

Índice de tablas

Índice de figuras

Índice de Abreviaturas

API	Aplication Programming Interface
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BCCR	Banco Central de Costa Rica
CA	Certificate Authority
CITIC	Centro de Investigaciones en Tecnologías de la Información y la Comunicación
CRL	Certificate Revocation List
DCFD	Dirección de Certificadores de Firma Digital
DSS	Digital Signature Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunication Standardization Sector
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MICITT	Ministro de Ciencia, Tecnología y Telecomunicaciones
MVC	Modelo Vista Controlador
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OID-IRI	OID-Identifier Internationalized Resource Identifier
OS	Operating System
OWASP	Open Web Application Security Project
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RA	Registration Authority

REST	Representational State Transfer
SHA	Secure Hash Algorithm
SNCD	Sistema Nacional de Certificación Digital
SQL	Structured Query Language
TFIA	Trabajo Final de Investigación Aplicada
TSA	Time Stamp Authority
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	Xtensible Markup Language
XSS	Cross Site Scripting
XXE	XML External Entity

1. Introducción

Durante los últimos años el uso de firma digital ha incrementado en Costa Rica para reemplazar los trámites personales por los trámites electrónicos [1]. De esta manera, se simplifican las gestiones en instituciones públicas y privadas. La firma digital ofrece grandes ventajas para los usuarios de las diferentes entidades ya que les da flexibilidad en el uso de los sistemas, por ejemplo: en horarios para realizar trámites, ahorro de tiempo, fácil acceso, trasparencia del proceso, entre otros. Adicionalmente, las entidades que prestan los servicios también obtienen ventajas al tener menos usuarios que atender físicamente, por ejemplo: ahorro de papel y otros recursos que utilizan normalmente cuando se hacen los trámites forma personal.

Mediante la directriz 067-MICITT-H-MEIC [2] publicada en el año 2005 y titulada "Masificación de la implementación y el uso de la firma digital en el sector público costarricense", el gobierno de Costa Rica promueve el uso de firma digital y define un periodo de tres años para que las instituciones del gobierno empiecen a facilitar a los usuarios servicios de forma electrónica utilizando firma digital. Como consecuencia, durante los últimos años muchas instituciones públicas empiezan a implementar firma digital como parte de sus procesos y servicios [1]. Por lo tanto, se ha dado un gran auge en la implementación de este tipo de sistemas electrónicos. Sin embargo, hasta el día de hoy no existe una regulación o recurso técnico de parte del gobierno de Costa Rica que oriente a estas instituciones en el desarrollo y aseguramiento de sus aplicaciones de firma digital.

Por consiguiente, el presente TFIA tiene como fin realizar un aporte a los proyectos de la Universidad de Costa Rica que están involucrados en el tema de firma digital en el país. Actualmente, el Centro de Investigaciones en Tecnologías de la Información y la Comunicación (CITIC) ha desarrollado un proyecto titulado *"Desarrollo de esquemas para certificar autoridades y aplicaciones de software en el Sistema Nacional de Certificación Digital (SNCD)"*, el cual tiene dentro de sus objetivos principales:

- Evaluar la aplicabilidad, dentro del SNCD (Sistema Nacional de Certificación Digital), 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.

Por consiguiente, el enfoque principal de esta investigación es el desarrollo de una aplicación de referencia de firma digital, la cual se evaluará con la *Guía de implementación* [3] creada en el TFIA titulado "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" [4], con el fin de generar una aplicación de referencia para futuras implementaciones de firma digital dentro del SNCD. La guía mencionada está compuesta por un conjunto de políticas y controles de seguridad que se aplican específicamente a los componentes de firma digital para atender los problemas de seguridad en el tema de no repudio de dichos componentes. Por ende, una de las contribuciones generadas por la presente investigación es evaluar la factibilidad y eficiencia del proceso de desarrollo de una aplicación de firma digital con respecto a los mecanismos de aseguramiento de la información planteados en la guía.

Para realizar la aplicación prototipo, primero se realiza la búsqueda de un tema con el fin de generar una aplicación base en la cual se pueda implementar la funcionalidad de los diferentes componentes de firma digital que serán asegurados con la *Guía de implementación*. Por lo tanto, una vez realizada la búsqueda y luego de un análisis, se selecciona el tema de "Autoridad de Registro de OID" para la aplicación base. Se escoge este tema ya que en él es posible implementar la funcionalidad de los diferentes componentes de firma digital y, adicionalmente, se identificó que actualmente el gobierno de Costa Rica utiliza los Identificador de Objetos (OID por sus siglas en inglés). Sin embargo, solamente es una estructura administrada a lo interno, esto lo podemos observar en el uso de los OID para identificar documentos oficiales, pero, actualmente no existe una autoridad oficial registradora de OID disponible a nivel nacional. Un ejemplo de documento oficial es la

"Política de Certificados para la Jerarquía Nacional de Certificadores Registrados" [7], podemos ver en la **Tabla 1** cómo el documento hace una descripción del OID que lo identifica.

Tabla 1. *Política de Certificados para la Jerarquía Nacional de Certificadores Registrados*

Sección	Descripción
2	joint-iso-itu-t
16	Country
188	Costa Rica
1	Organización
1	Dirección de Certificadores de Firma Digital
1	Políticas
1	Política de Certificados para la jerarquía nacional de certificadores registrados

Por consiguiente, para efectos de este proyecto se selecciona este dominio para la aplicación base ya que además de permitir implementar la funcionalidad de firma digital necesaria para esta investigación, se generará un aporte al SNCD. En los siguientes capítulos de este documento se explican más detalles acerca la aplicación "Autoridad de Registro de OID", por ejemplo: cómo se selecciona el dominio de la aplicación, la definición de conceptos de OID para comprender mejor su funcionalidad, así como el análisis y desarrollo de la misma.

También, en las siguientes secciones de este primer capítulo se explica con más detalle el contexto de esta investigación.

1.1. Antecedentes

En Costa Rica el concepto de certificación digital nace con un proyecto de Ley presentado por el Poder Ejecutivo a la Asamblea Legislativa el 29 de febrero del 2002, el cual pretendía legislar lo relacionado a firma digital en nuestro país [5]. Después de años de deliberaciones sobre el tema, y varias modificaciones, el 22 de agosto del año 2005 el proyecto se aprueba como la Ley número 8454, titulada "Ley de Certificados, Firmas Digitales y Documentos Electrónicos" [5].

Por medio de esta ley, se define el marco jurídico para la utilización transparente, confiable y segura de los documentos electrónicos y la firma digital en las entidades públicas y privadas de Costa Rica [6].

En esta ley el estado le otorga la tarea de "Autoridad Certificadora raíz" del Sistema Nacional de Certificación Nacional (SNCD) a la Dirección de Certificadores de Firma Digital (DCFD) la cual fue creada dentro del MICITT (Ministerio de Ciencia, Tecnología y Telecomunicaciones). Sin embargo, como la DCFD no cuenta con la infraestructura adecuada para operar como "Autoridad Certificadora raíz" se realiza un convenio entre el MICITT y el Banco Central de Costa Rica (BCCR), para que este último se encargue de administrar la raíz del Sistema de Firma en Costa Rica [5].

Con la Ley 8454 decretada en el 2015, y la infraestructura brindada por el BCCR, se facilitó que las entidades nacionales empezaran a implementar y hacer uso de firma y certificados digitales en sus sistemas. Según un informe del MICITT a noviembre del 2017, 58 entidades públicas y privadas ya utilizan firma digital en diferentes proyectos, para un total de 112 aplicaciones [1].

Sin embargo, actualmente ninguna institución del gobierno de Costa Rica provee algún tipo de directriz, documentación, modelo, o guía de implementación que oriente a las diferentes instituciones públicas o privadas que desarrollan servicios de firma digital para realizar implementaciones de firma y certificados digitales de forma segura.

1.2. Descripción del problema

Con la ley 8454 se logra un gran avance en términos de firma electrónica y certificados digitales en el país. No obstante, esta ley solamente define un marco legal, hasta el momento no existe un recurso oficial del Estado que defina procesos o regulaciones técnicas de cómo implementar sistemas de firma de forma segura. La implementación y aseguramiento de una aplicación es algo que puede variar entre diferentes entidades, desde el tipo de tecnología que utilicen, hasta la forma en que se implemente, lo que resulta en una gran variedad de implementaciones que pueden dar paso a vulnerabilidades en la seguridad de la información

de dichos sistemas, para el Sistema Nacional de Certificación Digital (SNCD) y a los usuarios que lo utilizan.

Dado este escenario, surge la necesidad de generar un modelo de implementación de firma digital y certificados digitales que contenga orientación técnica relacionada a la implementación segura de este tipo de sistemas. Por consiguiente, el estudiante Alejandro Mora, de la Maestría en Computación de la Universidad de Costa Rica, genera un modelo teórico en su trabajo "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" [4]; de ahora en adelante, se referirá a esta investigación como *Modelo de implementación*. Como resultado de dicha investigación, se obtuvo una "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 Sistema Nacional de Certificación Digital" [3] que de ahora en adelante se le referirá como *Guía de implementación"*.

Con la guía [3] ya se cuenta con un estudio teórico de pautas a tomar en cuenta para lograr una implementación segura de sistemas de firma digital. Sin embargo, con el fin de continuar aportando en la mejora de los recursos y guías de seguridad que se ofrecen en el país, en la presente investigación se realiza una evaluación de la factibilidad y eficiencia del proceso de desarrollo de una aplicación de firma digital con respecto a los mecanismos de aseguramiento de la información planteados en la *Guía de implementación*, ya que esta guía se quiere proveer en un futuro a las entidades costarricenses como guía a seguir al momento de que realicen sus propias implementaciones de firma digital, o en el caso de que evalúen las ya existentes.

1.3. Justificación del proyecto

Como se mencionó anteriormente, debido al auge que se ha dado en el país los últimos años en el uso de firma y certificados digitales tanto en el sector público como privado [1], y a la creación de leyes y directivas, cada vez hay más entidades que implementan firma digital en

sus sistemas y servicios que ofrecen. En consecuencia, es vital para el gobierno de Costa Rica fomentar el uso de firma, y proveer algún tipo de guía técnica para implementaciones seguras de firma y certificados digitales, con el objetivo de proteger la integridad del SNCD, a las instituciones que lo están implementando, y, por ende, a los ciudadanos que harán uso de las mismas.

A causa del aumento dado de implementaciones de firma digital sin la existencia de alguna regulación o guía, se genera la incertidumbre de si todas estas entidades estarán aplicando en sus sistemas informáticos todos los lineamentos de seguridad necesarios para garantizar un software seguro. Cada entidad tiene su propia implementación de sus sistemas de firma digital, todas varían, ya sea en la selección de la plataforma, configuraciones, lenguajes, librerías, entre otros; lo que abre paso a la posibilidad de que puedan presentar diferentes vulnerabilidades. Por lo tanto, la intención de modelo generado [4] es proveer una guía con las normativas fundamentales que se deben de tener en cuenta al desarrollar sistemas de firma digital.

El objetivo de la *Guía de implementación* es realizar un proceso de análisis al software que envuelva funcionalidad de firma digital, para asegurarse que dicho software cubra todos los aspectos de seguridad de la información que son considerados como fundamentales para así garantizar sistemas seguros en el ámbito de firma digital. En consecuencia, en esta investigación se desarrolla una aplicación que contiene la funcionalidad de firma digital para aplicar la guía en un escenario real y práctico, y de esta manera, comprobar si durante el desarrollo de dicho software es factible utilizar la *Guía de implementación* para su aseguramiento, así como conocer el nivel de dificultad y tiempo que llevó aplicarla.

1.4. Objetivos

El objetivo general de esta investigación es desarrollar un software prototipo guiado por el *Modelo de implementación*, como referencia para futuras implementaciones de firma y certificados digitales dentro del Sistema Nacional de Certificación Digital.

1.4.1. Objetivos específicos

1. Elegir un dominio de aplicación que permita evaluar los escenarios identificados en el *Modelo de implementación.*
2. Desarrollar un software prototipo siguiendo la guía teórica de implementación brindada en el *Modelo de implementación.*
3. Evaluar la factibilidad y eficiencia del proceso de desarrollo de la aplicación prototipo con respecto a los mecanismos de aseguramiento de la información planteados en la *Guía de implementación*.

1.5. Relevancia e impacto

Con la realización de este proyecto se pretende promover y apoyar al sistema costarricense en la digitalización de los procesos en el ámbito de firma digital tanto en el sector público como privado. Al lograr esto, se verán beneficiadas tanto las instituciones que lo implementen como los ciudadanos que lo utilicen. Para el caso de las instituciones, tendrá un impacto positivo al lograr automatizar y agilizar las gestiones que actualmente se realizan de forma física, con esto podrán evitar mucho trabajo manual, reducir la atención de los clientes en ventanillas, ahorro de papel y otros recursos. A los ciudadanos también les generará un impacto favorable, al ejercer su derecho de igualdad en el acceso por medios electrónicos a todos los servicios que se ofrecen por medios físicos; facilitará abrir negocios propios, también podrán generar consultas, transacciones, solicitudes por medio electrónicos de manera más rápida y efectiva, reduciendo además el costo social, por ejemplo: en filas, presas, contaminación, entre otros. Al reducir el uso de papel y otros recursos también se generará un impacto positivo en el medio ambiente también.

Otro impacto significativo inherente a esta investigación es que el gobierno podrá ofrecer una herramienta para apoyar la implementación de firma y certificados digitales. Es una forma de ayudar a las instituciones a generar sistemas más seguros, lo cual ayudará por consecuencia a todo el sistema costarricense en general para el beneficio y confianza de todos sus usuarios.

1.6. Alcance

La presente investigación se enfoca en el desarrollo de una aplicación prototipo, la cual es asegurada utilizando de la *Guía de implementación*, con el fin de evaluar esta última. Es decir, se desarrolla una aplicación prototipo que implementa certificados y firma digital en los escenarios identificados en el *Modelo de implementación*, los cuales son:

- Creación de firma digital y sello electrónico
- Verificación de firma digital y sello electrónico
- Autenticación de usuarios mediante certificados digitales
- Conversión de una firma digital en formato simple a formato avanzado

La aplicación prototipo de firma digital se desarrolla con el propósito de generar un ambiente real y práctico para así probar y evaluar la *Guía de implementación*, en los escenarios de casos de uso mencionados. Para lograr esto se realiza la búsqueda de un dominio de aplicación concerniente al tema de firma digital dentro de la cual se pueda llevar a cabo la implementación y pruebas necesarias del prototipo con la guía. Como se mencionó anteriormente se ha seleccionado el dominio de aplicación de "Autoridad de Registro de OID", porque es un elemento importante dentro de la SNCD que aún no es administrado formalmente por alguna autoridad en el país, por lo tanto, por el momento los OID no pueden ser utilizados ni accedidos a nivel nacional.

1.7. Organización del documento

Este documento tiene la siguiente organización. En el Capítulo 2 se desarrolla el marco teórico de esta investigación, donde se mencionan conceptos de seguridad de la información, firma digital y certificados digitales, infraestructura de llave pública. Seguidamente, se explican los conceptos del objeto OID, árbol internacional identificador de objetos, gestión del árbol y funcionamiento de una autoridad de registro de OID. En el Capítulo 3 se describe la metodología utilizada en esta investigación para cumplir con los objetivos planteados. En el Capítulo 4 expone la selección de un dominio de aplicación, es decir cómo se selecciona el ámbito sobre el cual se desarrolla esta investigación. En el Capítulo 5 se describe el

desarrollo de la estructura de la aplicación prototipo. En el Capítulo 6 muestra el proceso de evaluación realizado y los resultados del mismo. Finalmente, en el Capítulo 7 se presentan las principales conclusiones resultantes de la investigación realizada, así como el impacto de los resultados obtenidos y el trabajo futuro.

2. Marco teórico

En este capítulo se desarrolla un resumen de los principales conceptos de seguridad de la información y fundamentos de OID necesarios para comprender mejor la investigación realizada en torno al desarrollo de la aplicación de OID que utiliza firma digital. Primero se definen conceptos relacionados al de tema de seguridad de la información, seguidamente firma digital y certificados digitales. Posteriormente se explican los principales elementos de infraestructura pública (PKI). Y finalmente se explica el concepto y funcionamiento de los OID.

2.1. Seguridad de la información

A continuación, se explicarán algunos conceptos básicos importantes para comprender el tema de seguridad de la información.

Una **amenaza** es una potencial violación de seguridad. La violación no necesita ocurrir para que la amenaza exista. El hecho de que la violación pueda ocurrir significa que el sistema debe prepararse para las acciones que pueden causarla [7]. Es decir, se deben de tomar medidas de seguridad para protegerse de las posibles violaciones. Quienes realizan las violaciones reciben el nombre de "atacantes". Las amenazas se dividen en cuatro clases [8]:

- **Divulgación (*Disclosure*):** es el acceso no autorizado a la información.
- **Engaño (*Deception*):** o 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 del sistema.

Una **vulnerabilidad** o falla de seguridad, es la falla específica de los controles de un sistema. Utilizar una falla para violar las políticas de seguridad del sistema se llama "explotar la vulnerabilidad". Es cuando alguien irrumpe en un sistema informático y esa persona toma

ventaja de los fallos en sus procedimientos, tecnologías o administración, permitiéndose acceso o acciones no autorizadas [7].

Los **objetivos de seguridad** más relevantes para esta investigación se describen a continuación [9]:

- **Confidencialidad:** es la propiedad donde los datos no están disponibles a personas o procesos sin autorización.
- **Integridad:** se refiera a la propiedad donde los datos no han sido alterados o modificados sin consentimiento.
- **Autenticación:** es el método mediante el cual un ente verificador identifica la identidad de un usuario. Tanto el usuario como el verificador pueden ser personas, componentes de sistemas, procesos, etc.
- **No repudio:** es la propiedad de los datos, o procesos que impide que una entidad niegue haber realizado una acción.

Un **riesgo** es la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y, por lo tanto, cause daño a la organización. Se mide en términos de una combinación de la probabilidad de ocurrencia de un evento y su consecuencia. El propósito de la identificación de un riesgo es determinar qué puede ocurrir para causar una pérdida potencial y obtener conocimiento de cómo, dónde y por qué puede ocurrir la pérdida. Para identificar riesgos se deben realizar pasos descritos a continuación [10]:

- Identificación de activos.
- Identificación de amenazas
- Identificación de controles de seguridad existentes
- Identificación de vulnerabilidades

Las políticas y mecanismos de seguridad, son dos conceptos que van de la mano y son sumamente importantes en el ámbito de seguridad de la información, por lo tanto, es importante conocer su significado y distinguirlos uno del otro. Una **política de seguridad** es una declaración de lo que se permite y lo que no. Un **mecanismo de seguridad**, es un método, herramienta o procedimiento para hacer cumplir una política de seguridad [7].

Una política y mecanismo útil debe equilibrar los beneficios de la protección con el costo de diseño, implementación y uso del mecanismo. Este balance puede determinarse analizando los riesgos de una amenaza de seguridad y la probabilidad de que ocurra. Sin embargo, este análisis es hasta cierto punto, subjetivo, porque en muy pocas situaciones los riesgos pueden cuantificarse rigurosamente [7].

2.2. Infraestructura de llave pública

La Infraestructura de llave pública (PKI por sus siglas en inglés) tiene como principal tarea asegurarse de la correcta generación de las llaves públicas y privadas para los usuarios que las solicitan. Además, es importante que proporcione pruebas de autenticidad para las llaves públicas. La herramienta que utiliza para realizar dichas pruebas son los certificados digitales. Otra de las tareas importantes de PKI es poner las llaves públicas a disposición de los usuarios. Otra de sus tareas es lidiar con el problema de que las llaves públicas puedan a llegar a ser inseguras [9].

Para lograr todo esto PKI está conformado por múltiples componentes, es una estructura 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 [6]. Para comprender mejor la constitución dicha estructura a continuación se presentan sus principales componentes.

2.2.1. Certificado digital

Como ya se mencionó, una de las principales tareas de PKI es proveer pruebas de autenticidad para llaves públicas, y los certificados digitales son las herramientas principales para llevar a cabo esta función. Los certificados digitales son estructuras de datos que relacionan llaves públicas a entidades y están firmadas por un tercero de confianza [9]. Por lo tanto, es una estructura de datos creada y firmada digitalmente por un certificador, cuyo propósito primordial es posibilitar a sus suscriptores la creación de firmas digitales, así como

la identificación personal en transacciones electrónicas. En Costa Rica la DCFD es la encargada de autorizar a los certificadores registrados la generación de certificados.

2.2.2. Autoridad certificadora

Una Autoridad Certificadora (CA), es una autoridad encargada de emitir certificados digitales [7]. La CA genera un certificado de acuerdo con el standard que utilice y lo firma con su llave privada. Si una solicitud no contiene la llave pública, entonces la CA genera un par de llaves, una pública y una privada para el solicitante. La CA incluye la llave pública en el certificado y le entrega al solicitante la llave privada, usualmente la llave privada se almacena en un dispositivo electrónico, que es una tarjeta llamada tarjeta inteligente (*smart card)*. El uso de la tarjeta inteligente es protegido por un PIN que solo lo debe conocer el propietario. Otra función de una CA es proveer una lista de revocación de certificados (CRL) es decir una lista de certificados que ya no son válidos o han sido revocados por lo tanto no se pueden confiar en ellos [9].

2.2.3. Listas de Revocación de Certificados (CRL)

Una Lista de Revocación de Certificados (CRL por sus siglas en inglés), es una lista con marca de tiempo que identifica los certificados revocados y es firmada por una CA, además esta disponible gratuitamente en un repositorio público. Por ejemplo, si un sistema utiliza un certificado para verificar la firma de un usuario, ese sistema no solo debe comprobar la firma y validez del certificado, si no que también adquiere un CRL reciente para validar que dicho certificado no esté en el CRL. Un certificado puede estar revocado porque ya se ha vencido, o porque por ejemplo un usuario perdió su llave privada por lo tanto solicita que su certificado sea revocado. Un CRL reciente es la CRL emitida más recientemente. Se emite una CRL nueva de forma periódica (Por ejemplo, por hora, por día o por semana). Por lo tanto, existe un espacio de tiempo en el que un certificado revocado sea aceptado como válido si la revocación se procesó después de la última emisión del CRL [11].

2.2.4. Protocolo en Línea del Estado de un Certificado (OCSP)

El Protocolo en Línea del Estado de un Certificado (OCSP por sus siglas en ingles), es un protocolo utilizado para determinar el estado (de revocación) actual de un certificado digital sin utilizar una CRL. Permite proveer información más actualizada de lo que es posible con una CRL [12]. Además, un CRL puede llegar a ser muy grande, su descarga y procesamiento puede consumir mucho tiempo, y su almacenamiento consumir mucho espacio. A diferencia de los CRL, el protocolo OCSP permite consultar la validez de un certificado en forma individual, por lo que no requiere mucho consumo al descargarlo o almacenarlo [9]. Con este protocolo se elimina el riesgo que existe con el espacio de tiempo entre la actualización periódica de la CRL.

2.2.5. Estampa de Tiempo

Un servicio de estampa de tiempo concede afirmaciones de prueba de que un dato o documento existió en un tiempo particular por medio de la generación de un *token* o cadena de caracteres [13]. Dicho servicio es brindado por una Autoridad de Sellado de Tiempo (TSA por sus siglas en inglés), la cual certifica que un documento existió en un momento determinado al firmar un documento con la fecha y hora actuales.

2.2.6. Autoridad de registro

La Autoridad de Registro (RA por sus sigas en inglés) forma parte muy importante del proceso de PKI, ya que se encarga de recopilar y validar datos necesarios para generar un certificado. Es el punto de contacto entre el usuario y la autoridad certificadora. La RA y la CA generalmente son entidades separadas, ya que la RA tiene gran contacto con el usuario, al contrario de la autoridad emisora de certificados, la cual solamente interactúa con procesos del sistema y debe ser protegida de interferencia por usuarios no autorizados [9]. En Costa Rica las Autoridades de Registro se regulan por el documento emitido por la DCFD titulado *"Directrices para las Autoridades de Registro. Características de cumplimiento de*

Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica".

2.2.7. Repositorio

Un repositorio es un sistema para el almacenamiento de certificados digitales de la llave pública de la CA, CRLs, y este los hace disponibles para el uso de otras entidades ya sean usuarios u otras CA.

2.2.8. Tarjetas inteligentes y lectores

Las tarjetas inteligentes son tarjetas de plástico que contiene un microprocesador capaz de realizar operaciones criptográficas. Esta contiene las llaves privadas, proporcionándoles almacenamiento seguro y al mismo tiempo son portátiles del tamaño de una tarjeta de crédito. Para poder acceder a la llave privada dentro de una tarjeta inteligente es necesario que el usuario proporcione un PIN de acceso. Normalmente es una secuencia de dígitos del 0 al 9, este PIN se debe conocer solo por el dueño de la tarjeta para garantizar su seguridad.
Para leer una tarjeta inteligente se requiere de un lector de tarjetas inteligentes que esté conectado a una computadora. El lector es el que opera la comunicación entre la computadora y la tarjeta inteligente [9].

2.2.9. Usuarios

Los usuarios son la entidad final en el árbol de PKI, no pueden generar más certificados debajo de ellos, solamente utilizarlos en procesos criptográficos, como firmar un documento, autenticarse ante un sistema, cifrado de contenido, entre otros.

2.3. Firma digital

La definición de firma digital se explica a partir del ejemplo de "Bobo y Alice". En un esquema de firma digital, el firmante Bob utiliza su llave privada secreta para calcular la

firma digital de un documento. Los posibles verificadores pueden utilizar la llave pública de Bob que corresponde a su llave privada para verificar la firma de Bob en dicho documento. Es importante destacar que las llaves privadas en un esquema de firma no pueden ser calculadas a partir de sus llaves públicas correspondientes. Las firmas digitales se pueden utilizar para probar la integridad y autenticidad de los datos. Además, proporcionan autenticación de entidad y no repudio. Por lo tanto, son herramientas extremadamente importantes [9].

Según la ley de la unión europea, la firma electrónica simple significa: datos en formato electrónico que se adjuntan o están asociados lógicamente con otros datos electrónicos y que sirven como método de autenticación". Y la firma electrónica avanzada significa: una firma electrónica que cumple con los siguientes requisitos [14]:
[a] está vinculado únicamente al firmante;
[b] es capaz de identificar al signatario;
[c] se crea utilizando medios que el firmante puede mantener bajo su control exclusivo; y
[d] está vinculado a los datos con los que se relaciona que cualquier cambio posterior de los datos es detectable

Por lo tanto, la firma simple se utiliza para la autenticación, es decir para asegurarse de que la persona que envió el texto es el titular de la firma electrónica. Por otra parte, la firma avanzada, además de ser utilizada para la autenticación, también garantiza la integridad del documento firmado. Es decir, da seguridad de que el documento recibido es el mismo que se envió, que no ha sido modificado [15].

2.4. Identificador de objetos (OID)

Los Identificadores de objeto (OID por sus siglas en inglés) son un mecanismo utilizado para identificar cualquier objeto de interés de forma inequívoca y universal. Se organizan como una estructura jerárquica en forma de árbol, denominada “Árbol internacional identificador de objetos”. Fue desarrollado por la ITU-T (*International Telecomunication Union*, por sus siglas en inglés) y la ISO/IEC (*International Organization for Standardization/International*

Electrotechnical Commission, por sus siglas en inglés) las cuales son la raíz del árbol y ellas derivan el resto de nodos del árbol.

La diferencia entre los OID y otros sistemas de identificación como los códigos de barra, números de teléfono, entre otros; es que los OID no tienen un contexto, es decir pueden identificar cualquier cosa, algunos ejemplos de uso son:

- Una Recomendación de la ITU-T.
- Un estándar Internacional de la ISO.
- País, entidad, compañía, institución o proyecto.
- Un algoritmo de encriptación (ejemplo SHA-1).
- E-salud, datos médicos electrónicos.
- Un documento oficial del gobierno de Costa Rica ver **Figura 1**.

Los OID pueden ser definidos en tres notaciones, la cuales son:

1. ASN.1 (*Abstract Syntax Notation One*)

Cada arco OID está asociado con un número obligatorio (utilizado para transferencias de datos) y un identificador opcional, recomendado (para legibilidad). Esto se llama **NameAndNumberForm** [17]. Un "identificador" comienza con una letra minúscula y es seguido por letras, dígitos y guiones.

Ejemplo de notación ASN.1 de un OID: {joint-iso-itu-t(2) example(999)}

2. Puntos (Dots)

La IETF (Internet Engineering Task Force, por sus siglas en inglés) pensó que la notación ASN.1 era inconveniente, y decidió que en lugar de usar corchetes y espacios usar una notación libre de espacios [18]. Por lo tanto, esta notación consiste en los valores del entero primario separado por puntos desde la raíz del árbol.

Ejemplo de notación de puntos de un OID: “2.999”

3. OID IRI (Object Identifier Internationalized Resource Identifier)

Anteriormente, solo existían notaciones ASN.1 y de puntos, las cuales, solo permitían caracteres ASCII. Sin embargo, la OID IRI surge para proveer una notación más legible al humano y que no está limitada al alfabeto latín. Consiste en una cadena de caracteres separadas por barras inclinadas desde la raíz del árbol de OID.

Ejemplo de notación OID IRI de un OID: "/Joint-ISO-ITU-T/Example"

2.5. Árbol internacional identificador de objetos

El árbol internacional identificador de objetos tiene (únicamente) tres arcos raíz. En la **Tabla 2** vemos la asignación de valores enteros primarios, etiquetas Unicode, identificadores secundarios y la sobre los arcos subordinados para cada arco raíz [16]:

Tabla 2. *Árbol internacional identificador de objetos*

Valor entero primario	Etiqueta Unicode de valor entero resultante	Etiqueta Unicode (de valor no entero)	Identificador(es) secundario(s)	Autoridad sobre los arcos subordinados
0	“0”	“ITU-T”	itu-t	Administrado por el ITU-T
1	“1”	“ISO”	Iso	Administrado por la ISO
2	“2”	“Joint-ISO-ITU-T”	Joint-iso-itu-t	Administrado conjuntamente por la ISO y el ITU-T

Para ejemplificar el uso del árbol y nomenclaturas utilizadas para los OID, utilicemos un ejemplo real que ya está definido en la recomendación de la ITU-T.

Debajo del nodo con valor entero primario 1 con la etiqueta Unicode *"ITU-T"* se han definido cuatro arcos, según detalle en la **Tabla 2** [13].

Tabla 3. *Nodo de la ISO*

Valor entero primario	Etiqueta Unicode de valor entero resultante	Etiqueta Unicode (de valor no entero)	Identificador(es) secundario(s)	Autoridad sobre los arcos subordinados
0	"0"	"Standard"	standard	
1	"1"	"Registration-Authority"	registration-authority	
2	"2"	"Member-body"	member-body	
3	"3"	"Identified-organization"	Identified-organization	

Debajo del nodo con valor entero primario "2" (ver **Tabla 3**) con la etiqueta Unicode *"Member-Body"* tiene asignados valores enteros primarios que son indicativos de país numéricos que identifica los Órganos Miembros de la ISO en cada país, como podemos ver en la **Figura 1**.

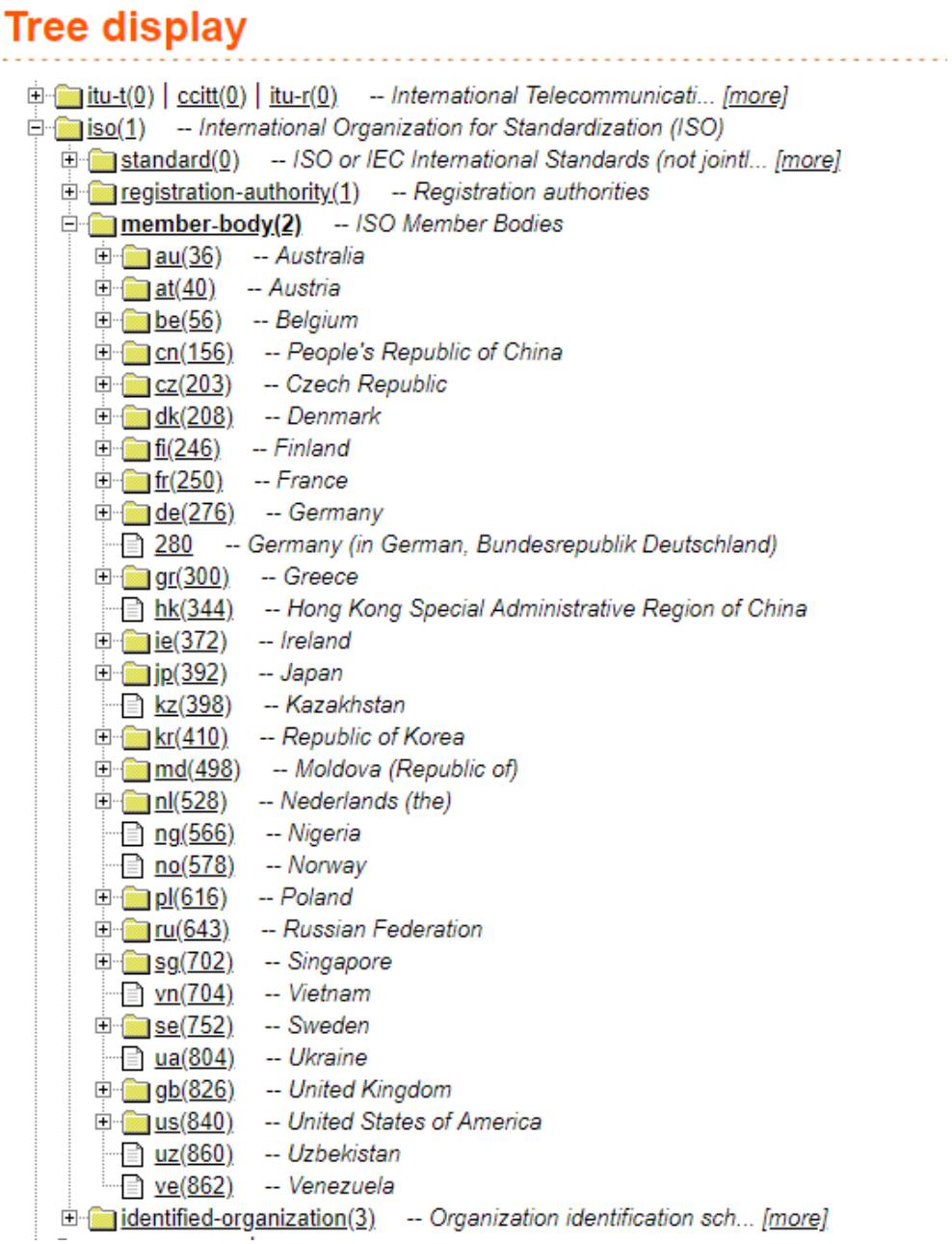

Figura 1. *Nodo para los organismos miembros de la ISO [19]*

Como ejemplo, el OID para el país Estados Unidos miembro de la ISO se muestra en la **Tabla 4**.

Tabla 4. *Estados Unidos, miembro de la ISO*

Notación	OID
ASN.1	{iso(1) member-body(2) us(840)}
Puntos	1.2.840
OID-IRI	/ISO/Member-Body/US

2.6. Gestión del árbol OID

La gestión de todo el árbol de OID se lleva a cabo mediante un proceso de delegación de autoridad. En este proceso, la RA de OID responsable de un OID determinado puede delegar la responsabilidad de registro para cada OID posterior a una autoridad de registro subordinada. Esta delegación de responsabilidad de registro se puede aplicar en varias ocasiones [16].

Para el caso de Costa Rica, como se mencionó anteriormente aún no existe una Autoridad Registradora de OID. Por lo tanto, uno de los propósitos de este proyecto es generar un software base para la Autoridad Registradora de OID en el país, con el objetivo de funcionar como la RA de OID principal y de esta manera, podrá registrar y administrar OID, así como también delegar a otras Autoridades subordinadas la administración de sus OID posteriores.

2.7. Funcionamiento de una Autoridad de Registro de OID

Una Autoridad de Registro es una entidad, como una organización o una instalación automatizada que realiza el registro de uno o más tipos de objetos [16].

La autoridad de registro (RA) responsable de un OID determinado debe asignar un nombre al OID subsiguiente que administrará una sub-autoridad determinada. El nombre asignado será globalmente no ambiguo y se concatenará como un prefijo para todos los nombres

asignados por esa sub-autoridad. La aplicación repetida de este proceso a través de una jerarquía de agentes de registro garantiza la generación de nombres inequívocos [16].

Una "Autoridad de Registro de OID" puede tener dos funcionamientos:

- **Función administrativa:** Puede ocuparse exclusivamente a la asignación unívoca de nombres.
- **Función técnica:** Puede ocuparse además de registrar definiciones de objetos y verificar que tales definiciones estén en consonancia con la recomendación de la ITU-T y/o Norma Internacional.

Sin embargo, los criterios para registrar definiciones de objetos pueden variar de una autoridad de registro a otra. En la recomendación ITU-T X.660 se menciona que es responsabilidad de cada autoridad de registro establecer esos criterios y que además una autoridad de registro podría definir criterios para las autoridades subordinadas a ella.

En síntesis, se han definido los principales conceptos considerados como fundamentales para la comprensión de los siguientes capítulos de desarrollo de la presente investigación. Se definieron conceptos de seguridad de la información, firma digital, certificados digitales y PKI. Además, se explicaron los fundamentos de OID para tener un mejor panorama de lo que son, su uso y como se gestionan. Seguidamente, se describe la metodología utilizada para el cumplimiento de cada uno de los objetivos planteados en esta investigación.

3. Metodología

En este capítulo se explican las estrategias utilizadas con el fin de cumplir los objetivos planteados en esta investigación. Empezando por seleccionar un dominio de aplicación sobre el cual se desarrollará el prototipo planteado. Seguidamente, el desarrollo de la aplicación prototipo. Finalmente, la evaluación de factibilidad y eficiencia del proceso de desarrollo haciendo uso de la *Guía de implementación*.

En la **Figura 2** se muestran los pasos generales a seguir como metodología de esta investigación.

***Figura 2**. Diagrama de pasos generales de la metodología*

3.1. Selección del dominio

Para cumplir con el primer objetivo específico que se define como: "Elegir un dominio de aplicación que permita evaluar los escenarios identificados en el *Modelo de implementación",* se realizan las tareas que podemos ver en la **Figura 3**.

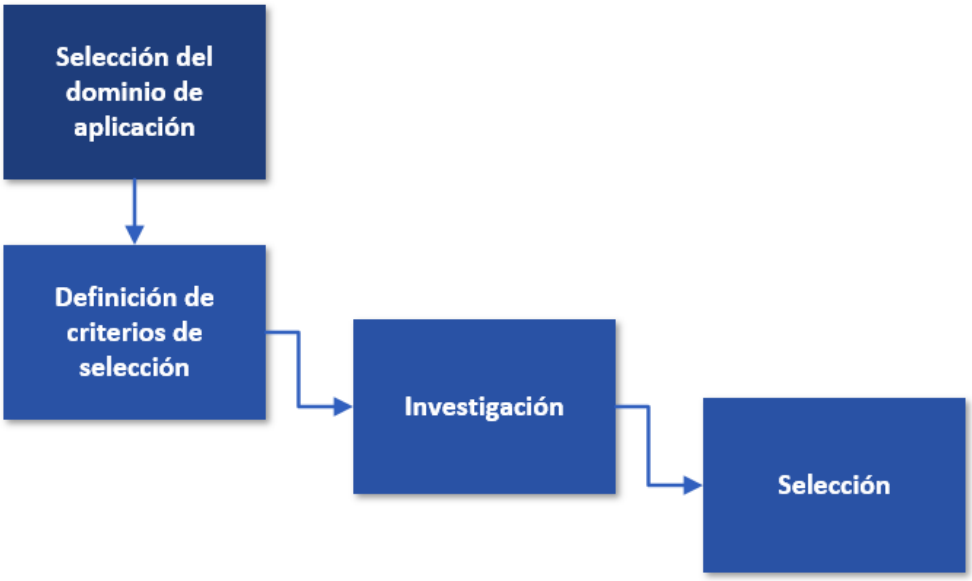

Figura 3. *Metodología para la selección del dominio de aplicación*

Primero, se definen los criterios de selección con el fin de delimitar las opciones según el interés de esta investigación y del SNCD. De esta manera, podemos observar en la **Tabla 5** los criterios definidos para la búsqueda de dicho dominio.

Tabla 5. *Criterios de selección para el dominio de aplicación*

Criterios de selección	
Alcance	La aplicación debe cumplir con los cuatro escenarios de firma digital identificados en la *Guía de implementación*.
Aporte	La aplicación debe realizar algún aporte al SNCD.
Tamaño	La aplicación no debe ser muy extensa ya que no es el punto principal de la presente investigación.

Segundo, se realiza una investigación en el tema, buscando dentro de la documentación del MICITT y además considerando el conocimiento de personas expertas e involucradas en el tema de firma digital en Costa Rica. Por lo tanto, se toma como referencia el conocimiento

de colaboradores de la DCFD, el BCCR, y las investigaciones realizadas en la Universidad de Costa Rica relacionadas al tema, las fuentes utilizadas son las siguientes:

- Documentación oficial publicada por el MICITT, por ejemplo, el documento titulado "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados".
- El proyecto de investigación 834-B5-181 del Centro de Investigaciones en Tecnologías de la Información y la Comunicación (CITIC), titulado "Desarrollo de esquemas para certificar autoridades y aplicaciones de software en el Sistema Nacional de Certificación Digital (SNCD)".
- TFIA del Estudiante Rodrigo A, Bartels, titulado "Análisis de estándares internacionales para la certificación de autoridades certificadoras y su aplicabilidad en el Sistema Nacional De Certificación Digital de Costa Rica".

Finalmente, como tercer paso, se realiza un análisis del cumplimiento de los criterios de selección definidos, y de la investigación del tema realizada. Y se concluye que existe evidencia del uso de los OID por el gobierno de Costa Rica. Sin embargo, no se encontró una fuente o referencia de la existencia de una autoridad registradora de OID en el país oficial, el cual es un ente necesario para organizar y representar de forma universal e inequívoca todos los elementos dentro del SNCD.

Por lo tanto, se procede con la selección del domino de aplicación "Autoridad de Registro de OID" ya que cumple con los criterios de selección establecidos. Adicionalmente, como valor agregado es una aplicación novedosa, ya que no existe a nivel nacional. En el Capítulo 4 se explican más detalles de la selección realizada.

3.2. Desarrollo de la aplicación prototipo

Una vez seleccionado el dominio de aplicación en el paso anterior, se continúa con el segundo objetivo específico, el cual se define como "Desarrollar un software prototipo siguiendo la guía teórica de implementación brindada en el *Modelo de implementación*". Por lo tanto, se da a la tarea de desarrollar dicho prototipo, en esta sección se explica la metodología utilizada para su desarrollo, y en el Capítulo 5 de este documento se pueden encontrar más detalles.

La aplicación prototipo desarrollada está compuesta por una serie de componentes que en conjunto proveen la funcionalidad necesaria para cumplir con los objetivos de esta investigación. Los componentes a modo general son los siguientes:

- Aplicación base. “Autoridad de Registro de OID”
    - Aplicación web
    - Aplicación lector de tarjetas inteligentes
    - Módulo de conexión a servicios REST
- Aplicación criptográfica
    - Librería de criptografía
    - Módulo de servicios web tipo REST

Por lo consiguiente, para cumplir con el segundo objetivo, podemos observar los pasos a seguir en la **Figura 4** y se explican con más detalle a continuación:

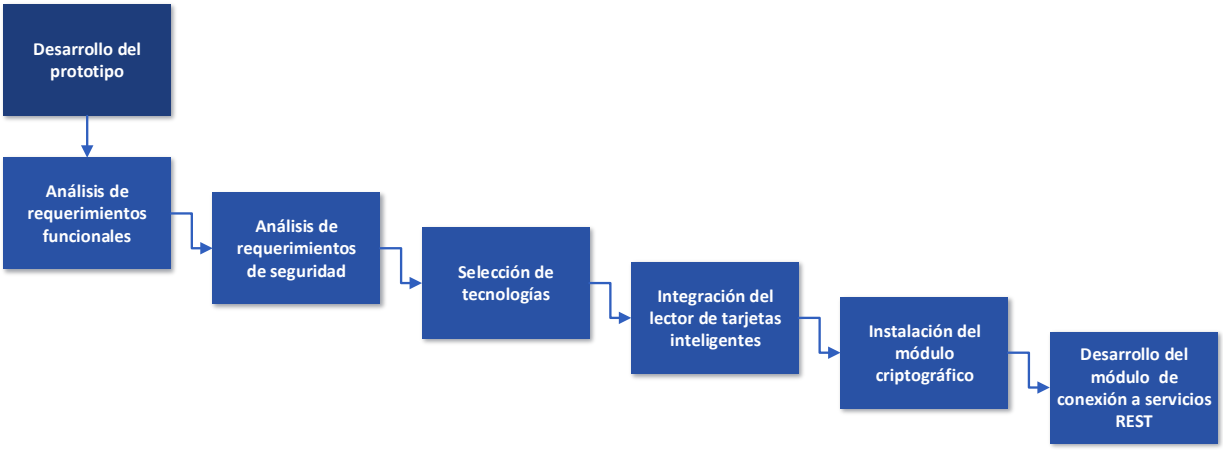

Figura 4. *Metodología para el desarrollo de la aplicación prototipo*

Análisis de requerimientos funcionales. Se realiza un análisis de requerimientos funcionales para la aplicación “Autoridad de registro de OID”. Primero, se identifica el contexto del sistema. Seguido, se definen los términos fundamentales para comprender mejor el sistema que se esta analizando. A continuación, se identifican los afectados del sistema. Finalmente, se realiza una lista de los requerimientos funcionales que se pueden ver con más detalle en la primera sección del **Apéndice 1**.

Análisis de requerimientos de seguridad. A pesar de que la aplicación "Autoridad de registro de OID" no es punto de análisis principal de esta investigación, también debe ser asegurada. Por lo tanto, como es una aplicación web, se utiliza el estándar conocido como OWASP Top 10 [20], que es un estándar refinado, probado y muy utilizado por la comunidad desarrolladora para aplicaciones web. Por lo tanto, se genera la lista de requerimientos de seguridad que se pueden ver con más detalle en la segunda sección del **Apéndice 1**.

Selección de tecnologías. Se realiza una investigación con los interesados (*stakeholders*) de la aplicación "Autoridad de registro de OID" y por conveniencia se selecciona la plataforma *.NET*. El motivo es que todas las aplicaciones de firma digital dentro de la DCFD que es representada por el BCCR están desarrolladas en *.NET*. Por lo tanto, optar por esta plataforma facilitará la integración, mantenimiento y desarrollo futuro de la aplicación.

Integración del lector de tarjetas inteligentes. Se implementa dentro de la aplicación de OID una solución para la lectura de tarjetas inteligentes con el fin de obtener la información del certificado del usuario para realizar las operaciones de firma de las solicitudes de OID en la aplicación prototipo.

Instalación del módulo criptográfico. Se selecciona la aplicación de java de la Unión Europea DSS (*Digital Signature Serv*ice, por sus siglas en inglés). Los motivos de esta selección es que es un software de código abierto que es desarrollado, probado, proveído y utilizado por la Unión europea por lo que contiene la mayoría de funcionalidad criptográfica necesaria para poder ejecutar los cuatro escenarios de firma digital mencionados anteriormente. Además, es compatible ya que maneja los formatos de documentos oficiales y algoritmos criptográficos que estipulan las políticas de Costa Rica. Por lo tanto, se compila la librería y por medio de un servidor web se hacen disponibles los servicios web de tipo REST que este contiene, para que la aplicación de registradora de OID pueda acceder a ellos.

Desarrollo del módulo de conexión a servicios REST. Es el módulo desarrollado dentro de la aplicación "Autoridad de Registro de OID" que se conecta con los servicios web de DSS, con el fin de acceder a los servicios REST que contienen la funcionalidad criptográfica.

3.3. Evaluación

Finalmente, con la aplicación prototipo desarrollada, se procede a cumplir con el último objetivo específico el cual es "Evaluar la factibilidad y eficiencia del proceso de desarrollo de la aplicación prototipo con respecto a los mecanismos de aseguramiento de la información planteados en la *Guía de implementación*". Por consiguiente, se procede a aplicar la *Guía de implementación* a los componentes de software desarrollados que envuelven la funcionalidad de firma digital, para evaluar su aseguramiento.

Se itera sobre la lista de las 103 políticas de la guía en los cuatro escenarios de uso, de forma que se verifica si la aplicación desarrollada el cumple con los objetivos de control para cada política. Finalmente, se hace un análisis de la utilización de dicha guía en el proceso de aseguramiento de una aplicación de firma digital, para determinar la factibilidad y eficiencia de la misma en un caso de uso práctico real. Dicha evaluación se explica con más detalle en el Capítulo 6 de este documento.

4. Selección de un dominio de aplicación

Como ya se ha explicado a lo largo de este documento, el contexto principal sobre el cual se desarrolla la presente investigación es firma y certificados digitales en el SNCD. Por consiguiente, se establece como objetivo general: desarrollar un software prototipo guiado por el *Modelo de implementación*, como referencia para futuras implementaciones de firma y certificados digitales dentro del Sistema Nacional de Certificación Digital. Por tanto, para cumplir el primer objetivo específico el cual se define como "Elegir un dominio de aplicación que permita evaluar los escenarios identificados en el *Modelo de implementación.* Surge la primera tarea a realizar, que es buscar un dominio de aplicación sobre el cual se pueda desarrollar el módulo de firma digital y que además asegurar que dicha aplicación haga uso de los cuatro escenarios identificados en la *Guía de implementación*, las cuales son:

- Creación de firma digital y sello electrónico
- Verificación de firma digital y sello electrónico
- Autenticación de usuarios mediante certificados digitales
- Conversión de una firma digital en formato simple a formato avanzado

Como consecuencia, se tomaron en cuenta los criterios de selección en la **Tabla 5**, se realizaron investigaciones en el área y además se utilizó el conocimiento de personas expertas en el tema, dentro de las cuales están: colaboradores de la DCFD, del BCCR e investigaciones realizadas en la Universidad de Costa Rica relacionados al tema. Durante la búsqueda y estudio de temas relacionados a firma digital, se observó que los documentos oficiales del gobierno están identificados de forma única con un identificador numérico, por ejemplo, el documento titulado *"Política de Certificados para la Jerarquía Nacional de Certificadores Registrados"* [7], tiene asociado un número identificador denominado OID, el cual corresponde a *2.16.188.1.1.1.1*. Además, dentro del documento hay una tabla que explica el significado de cada número en la secuencia, lo podemos ver en la **Figura 1**.

Observamos una jerarquía numérica donde el primer número en la secuencia es el **2**, el cual corresponde a una raíz en el árbol internacional identificador de objetos "joint-itu-t" que corresponde la ISO y a la ITU-T. Seguidamente, el segundo número identificado es el **16**,

correspondiente al objeto “Country”. Y como tercer nodo en la serie aparece el número **188** que corresponde al país Costa Rica.

Por tanto, se demuestra que Costa Rica ya tiene un número OID asignado para su identificación universal e inequívoca. Justo después del número **188** que identifica a Costa Rica encontramos una serie de números que son **1** “Organización”, **1** “Dirección de Certificados de Firma Digital”, **1** “Políticas” y como último nodo, el nombre del documento en observación con el número **1** denominado “Política de Certificados para la jerarquía nacional de certificadores registrados”.

Como se muestra, actualmente el gobierno de Costa Rica utiliza los Identificador de Objetos (OID por sus siglas en inglés), sin embargo, es una estructura administrada a lo interno, ya que podemos observar que sí hace uso de los OID para identificar sus documentos oficiales, pero, actualmente no existe una autoridad oficial registradora de OID disponible a nivel nacional.

En resumen, el dominio para una aplicación de “Autoridad de Registro de OID” cumple con los criterios de selección de la aplicación dominio definidos en esta investigación:

- En la aplicación “Autoridad de Registro de OID” podemos implementar la funcionalidad de los cuatro escenarios identificados. Por ejemplo: podemos utilizar el escenario “Autenticación” para que los usuarios inicien sesión. “Firma básica”, “Firma avanzada” y “Verificación”, para realizar las gestiones de un OID, donde el usuario obtenga un documento firmado para hacer una constancia formal de su solicitud.
- Realiza un aporte al SNCD, específicamente al sector de tecnologías del MICITT, ya que es un elemento que actualmente, de algún modo se utiliza, pero no tiene una forma oficial de gestionarlo y hacerlo disponible para el uso público.
- Es un sistema simple de gestión de identificadores. Más adelante se define el alcance de esta aplicación.
- Adicionalmente, como valor agregado es una aplicación novedosa, ya que actualmente no existe una autoridad registradora de OID en el país.

Finalmente, los puntos anteriores son los que motivan a tomar el dominio “Autoridad de Registro de OID” para Costa Rica como aplicación base sobre la cual trabajar la aplicación prototipo propuesta en esta investigación.

5. Desarrollo de la aplicación prototipo

Como ya se mencionó al inicio de este documento, uno de los objetivos de la presente investigación es desarrollar un software prototipo siguiendo la guía teórica de implementación brindada en el *Modelo de implementación.* Además, como se explicó en la sección anterior después de una investigación se selecciona el dominio de aplicación "Autoridad de Registro de OID".

En consecuencia, se genera dicho prototipo, el cual está compuesto por un conjunto de componentes de software e infraestructura para su correcto funcionamiento. El objetivo principal de todos estos componentes en conjunto es proveer una aplicación que permita realizar las funciones de firma en los cuatro escenarios: firma simple, firma avanzada, verificación y autenticación, para el caso de uso de una "Autoridad de Registro de OID".

Para el desarrollo de la aplicación generada se realizaron las siguientes tareas que serán mencionadas a continuación:

- Se realiza un análisis y recolección de requerimientos de funcionalidad y de seguridad para la aplicación "Autoridad de Registro de OID".
- Se desarrolla una aplicación de "Autoridad de Registro de OID", en .NET.
- Se integra un software para lectura de tarjetas inteligentes a la aplicación de "Autoridad de Registro de OID", para que pueda leer las llaves y certificados del usuario con el fin de que la aplicación pueda realizar todas sus funcionalidades.
- Se compila y configura el módulo de DSS, el cual contiene las operaciones criptográficas para firma. Seguidamente, se instala y configura un servidor apache para levantar la aplicación.
- Se desarrolla un módulo de software de conexión a los servicios REST en *.NET* con el fin de enlazar la aplicación "Autoridad de Registro de OID" con el módulo de DSS que contiene las funciones para realizar las operaciones criptográficas.
- Finalmente se realizan pruebas manuales para verificar el funcionamiento todos los componentes en conjunto.

En las siguientes secciones se explicará con más detalle cada una de las actividades mencionadas para el desarrollo de la aplicación prototipo. Empezando por el análisis de requerimientos, desarrollo de la aplicación web, la integración del lector de tarjetas inteligentes, configuración del módulo de DSS, generación del módulo de conexión a servicios REST.

5.1. Análisis de requerimientos

En esta sección se hace mención al análisis realizado de los requerimientos de funcionalidad y seguridad para la aplicación web de OID desarrollada, la cual es uno de los componentes del prototipo final desarrollado. Primero, se analiza el contexto del sistema y se explican algunas definiciones necesarias para comprender el uso de esta aplicación, seguidamente se hace un análisis de los posibles afectados de la aplicación "Autoridad de Registro de OID". Finalmente, se listan de forma resumida los requerimientos de funcionalidad y de seguridad obtenidos para dicha aplicación. Adicionalmente, en el Apéndice 1 se podrá ver mejor el detalle de cada requerimiento.

5.1.1. Contexto del sistema

El ámbito de uso de la "Autoridad de Registro de OID" es únicamente dentro de Costa Rica. Dicha autoridad solamente podrá delegar OID debajo de su dominio según la jerarquía del árbol.

Además, se identifican dos grupos de usuarios que pueden hacer uso de los servicios de la Autoridad de Registros de OID. El primer grupo son personas físicas y el segundo grupo son personas jurídicas. Por lo tanto, cualquier persona, empresa, institución dentro del dominio de Costa Rica, puede hacer uso de los OID para identificar los objetos que desee y necesite. Por ejemplo, una empresa puede hacer uso de los OID para representar sus proyectos o activos de forma inequívoca e internacionalmente. Otro ejemplo es para el gobierno de Costa Rica que por medio de esta aplicación podrá asignar a un documento oficial un identificador, como lo hace actualmente, pero de una forma digital, más formal y organizada utilizando la

jerarquía de árbol dentro del sistema nacional, de esta forma dichos documentos pueden ser identificados inequívocamente, de forma pública e incluso referenciados desde fuera del país.

La "Autoridad de Registro de OID" puede generar un OID a cualquier entidad y como consecuencia delegarle la responsabilidad de generar cualquier otro OID debajo de él según la jerarquía del árbol [16].

5.1.2. Definición de términos

A continuación, se describen algunos términos importantes para la comprensión del sistema desarrollado.

- **Autoridad de Registro de OID:** Es el ente encargado de administrar oficialmente los OID debajo de su nodo. Para este contexto el nodo principal del cual derivaran el resto de nodos es Costa Rica.
- **OID:** es un número identificador de algún objeto (empresa, persona, documento), debajo de nodo de Costa Rica según el árbol internacional identificador de objetos.
- **Usuario persona física:** es un individuo físico que tiene una identificación de identidad válida y vigente.
- **Usuario persona jurídica:** es ente que existe no como individuo si no como institución y que tiene derechos y obligaciones.
- **Documento firmado digitalmente:** es un documento electrónico que contiene una firma o sello digital.

5.1.3. Descripción de los afectados del sistema

Los usuarios que serán afectados directamente por este sistema son:

- **Usuarios finales:** Son las entidades o personas que hacen uso de los OID. Realizan solicitudes de OID para asignarlos a el objeto que deseen y administrar cualquier OID debajo de él.

- **Administrador de la Autoridad Registradora de OID:** Es la persona detrás del sistema administrador de OID encargada de aprobar o rechazar las solicitudes de OID hechas por los usuarios finales.

5.1.4. Lista de requerimientos funcionales

A continuación, se muestra una lista de los requerimientos funcionales identificados como principales para tomados en cuenta al desarrollar la funcionalidad básica de la aplicación "Autoridad de Registro de OID". Se explica de manera general cada requerimiento, para ver más detalles de cada uno por favor referirse al Apéndice 1 de este documento.

- **RFOID01 – Crear OID:** Un usuario debe poder solicitar la inclusión de un nuevo OID hijo o hermano a partir de uno ya existente.
- **RFOID02 – Modificar OID:** Un usuario debe poder solicitar la actualización de un OID existente.
- **RFOID03 – Notificación de solicitud:** A partir de la creación o modificación de un OID el sistema deberá crear una notificación al administrador de la autoridad de registros de OID para que sea informado de dicha solicitud.
- **RFOID04 – Aprobación de solicitud:** El usuario administrador del sistema, una vez conforme con la solicitud de creación/modificación de OID podrá aprobar la solicitud realizada.
- **RFOID05 – Rechazo de solicitud:** El usuario administrador del sistema si está inconforme o ve algún problema con la información solicitada, puede rechazar la solicitud.
- **RFOID06 – Autenticación:** Los usuarios se deben autenticar en el sistema para poder ingresar en el mismo.
- **RFOID07 – Generación de un documento comprobante firmado:** El sistema debe generar un documento oficial firmado digitalmente con la información del nuevo OID.

5.1.5. Lista de requerimientos de seguridad

Para definir los requerimientos de seguridad en la aplicación prototipo, se utiliza como referencia el OWASP TOP 10 más reciente publicado el 2017 para aplicaciones web, ya que es un estándar de seguridad para aplicaciones web muy utilizado que abarca las principales vulnerabilidades que una aplicación web puede tener. Por lo tanto, se ha seleccionado este estándar como guía para asegurar la aplicación web "Autoridad de Registro de OID". A continuación, se listan los riesgos identificados por el OWASP Top 10 [20] y se explica de manera general cada uno, para ver más detalles de como se mitiga cada uno por favor referirse al Apéndice 1 de este documento.

- **A1:2017 Inyección:** Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
- **A2:2017 Pérdida de Autenticación:** Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, *token* de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
- **A3:2017 Exposición de datos sensibles:** Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.
- **A4:2017 Entidades Externas XML (XXE):** Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

- **A5:2017 Pérdida de Control de Acceso:** Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.
- **A6:2017 Configuración de Seguridad Incorrecta:** La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, *frameworks*, dependencias y componentes desactualizados, etc.
- **A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS):** Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (*defacement*) los sitios web, o redireccionar al usuario hacia un sitio malicioso.
- **A8:2017 Deserialización Insegura:** Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.
- **A9:2017 Componentes con vulnerabilidades conocidas:** Los componentes como bibliotecas, *frameworks* y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.
- **A10:2017 Registro y Monitoreo Insuficientes:** El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el

ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos.

5.2. Desarrollo de la aplicación en .NET

Se desarrolló una aplicación web en .NET para la administración de los OID. Con el objetivo de que los usuarios puedan hacer solicitudes de OID, y que se tenga un registro del árbol OID dentro del ámbito de Costa Rica. La aplicación se divide en módulos separados con el fin de generar un sitio fácil de adaptar. Es decir, si en un futuro se necesita un cambio, por ejemplo, en del motor de base de datos, entonces fácilmente se puede sustituir sin tener que hacer mucho trabajo en las otras capas de la aplicación. También se podría cambiar el módulo de interfaz gráfica sin necesidad de modificar el resto de la aplicación, y así con las demás capas.

Los módulos que se generan son:

- **Módulo Web:** Es la interfaz gráfica de la aplicación web, en ella se hacen validaciones (*client-side*) de entrada de datos por el usuario.
- **Módulo lógico:** es donde se encuentran todas las operaciones lógicas, de la aplicación. Aquí también podemos encontrar validaciones de datos (*server-side*). Esta capa es la que conecta la interfaz grafica y el módulo de acceso de datos.
- **Módulo de acceso de datos:** Es el módulo que une la capa lógica con la base de datos.
- **Módulo de modelo de datos:** Se crea un modelo de datos en SQL Server.

5.2.1. Modelo de datos

De acuerdo con los datos obtenidos del análisis de requerimientos se identificaron entidades las cuales son los actores principales del modelo de datos diseñado.

- **OID:** Es la entidad principal, que representa el objeto OID.

- **OIDSubmitter:** El Submitter es el usuario que generó la solicitud relacionada a un nuevo OID o la modificación de un OID.
- **OIDFirstCurrentRA**: Es la Autoridad de Registro actual que está a cargo de los OID hijos asignados a ella. Y la Autoridad de Registro Primera es la responsable de administrar el OID. Si se el usuario que solicita el nuevo OID conoce el RA actual o la RA Primera, y llena esta sección entonces el contacto respectivo identificado será notificado automáticamente por correo electrónico cada vez que alguien cree un OID secundario, o envíe modificaciones al OID actual o a cualquier OID secundario. Esta información se guarda para propósitos históricos.
- **Country:** Es el país al cual está relacionado el OID. En este caso todos los que se generen nuevos debajo del nodo de Costa Rica, que es el ámbito de interés.

5.3. Integración de lector de tarjetas inteligentes

Para poder ejecutar las funciones criptográficas de la librería DSS, primero se necesita acceder al certificado del cliente para obtener la información necesaria para realizar dichas operaciones. Por lo tanto, se integra un software para leer las tarjetas inteligentes, con el fin de leer el certificado dentro de la tarjeta y poder autenticar el cliente en la aplicación web y firmar documentos.

La aplicación lectora de tarjetas seleccionada se llama Nexu [21]. La cual es una aplicación *open source* y la ventaja es que es independiente a la plataforma que utilice el usuario, ya que utiliza JavaScript para conectarse al servicio que instala en la computadora local. Por lo tanto, esta funcionalidad se implementa mediante la agregación del script de la aplicación lectora de tarjetas dentro de módulo web de la aplicación prototipo “Autoridad de Registro de OID”, de esta forma se podrá hacer lectura de la información del certificado del usuario con el fin de ejecutar las operaciones de firma necesarias en la aplicación prototipo.

5.4. Instalación del módulo de DSS

Una vez generada la aplicación web gestora de OID e integrada la funcionalidad del lector de tarjetas inteligentes, el siguiente paso es realizar las operaciones criptográficas para autenticar al usuario o generar las firmas desde la aplicación web. Por lo tanto, se utiliza la librería de la unión europea DSS (Digital Signature Service, por sus siglas en inglés) [22]. Esta librería es de código abierto, y contiene la funcionalidad para crear y validar firma digital, adicionalmente utiliza el estándar de la UIT-T X.509 para los certificados digitales, al igual que lo requiere Costa Rica como se estipula en la "Política de certificados para la jerarquía nacional de certificadores registrados" [23]. Para hacer disponible esta librería a la aplicación web de OID, se descarga el código fuente del repositorio proveído por la Unión Europea y se procede con su instalación y configuración en una máquina local. Se compila el código fuente y se levanta un servidor apache, para que por medio de un URL se pueda proveer acceso a los servicios web de tipo REST que ofrece DSS, por medio de los cuales se accederá a la funcionalidad criptográfica de firma digital.

5.5. Generación del módulo de conexión a los servicios REST de DSS

Posteriormente, para poder acceder a los servicios web de DSS desde la aplicación web de OID, se crea dentro de la aplicación web de OID un módulo de conexión a servicios REST, el cual tiene la función de acceder a cada uno de los servicios REST de DSS para para poder realizar las operaciones criptográficas de firma necesarias para cumplir con los requerimientos de la aplicación prototipo.

Finalmente, como resultado del desarrollo de los componentes descritos anteriormente podemos observar la arquitectura lógica del prototipo en la **Figura 5**. Además, en la **Figura 6** se muestra la arquitectura del sistema desarrollado a un nivel físico, donde podemos distinguir desde el punto donde el usuario interactúa con la computadora y a partir de ahí, la interacción del resto de componentes como el lector de tarjetas inteligentes y los servidores que almacenan cada uno de los componentes de software desarrollados en la aplicación prototipo.

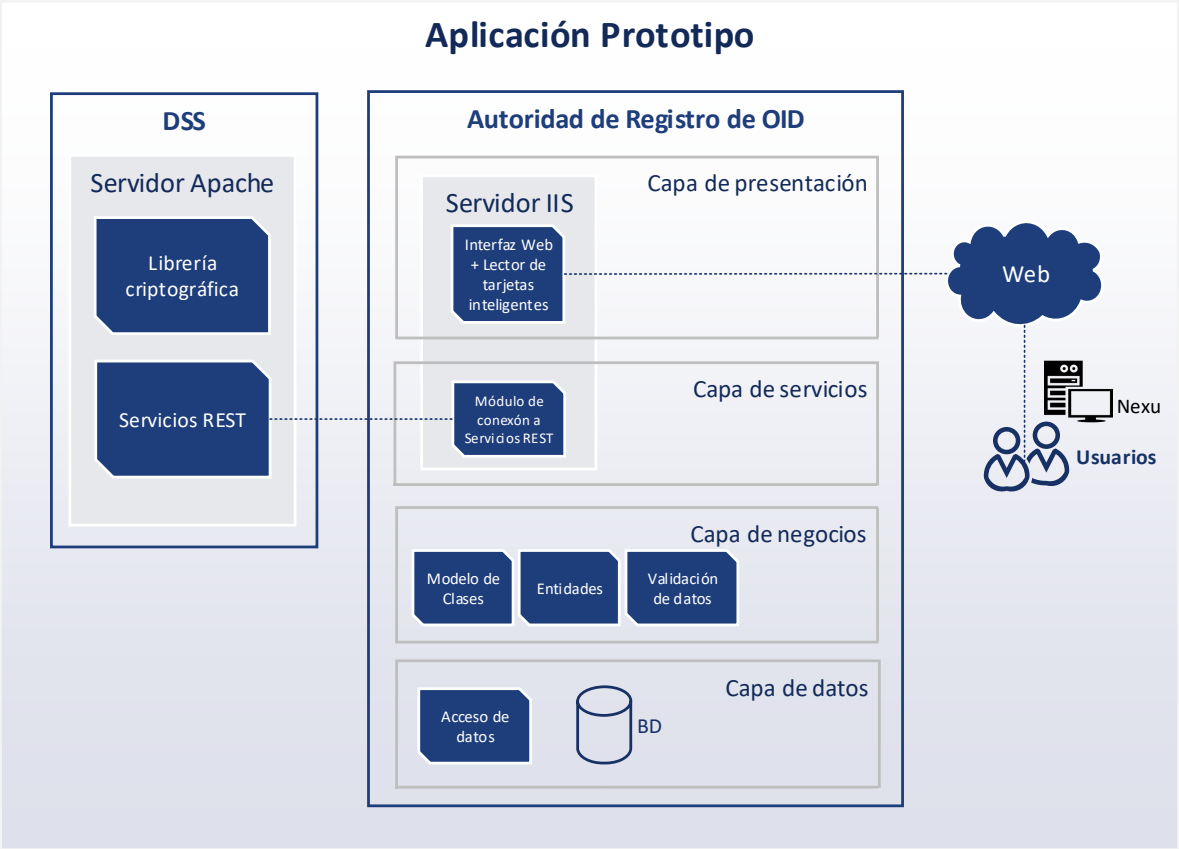

Figura 5. *Arquitectura lógica de la Aplicación Prototipo*

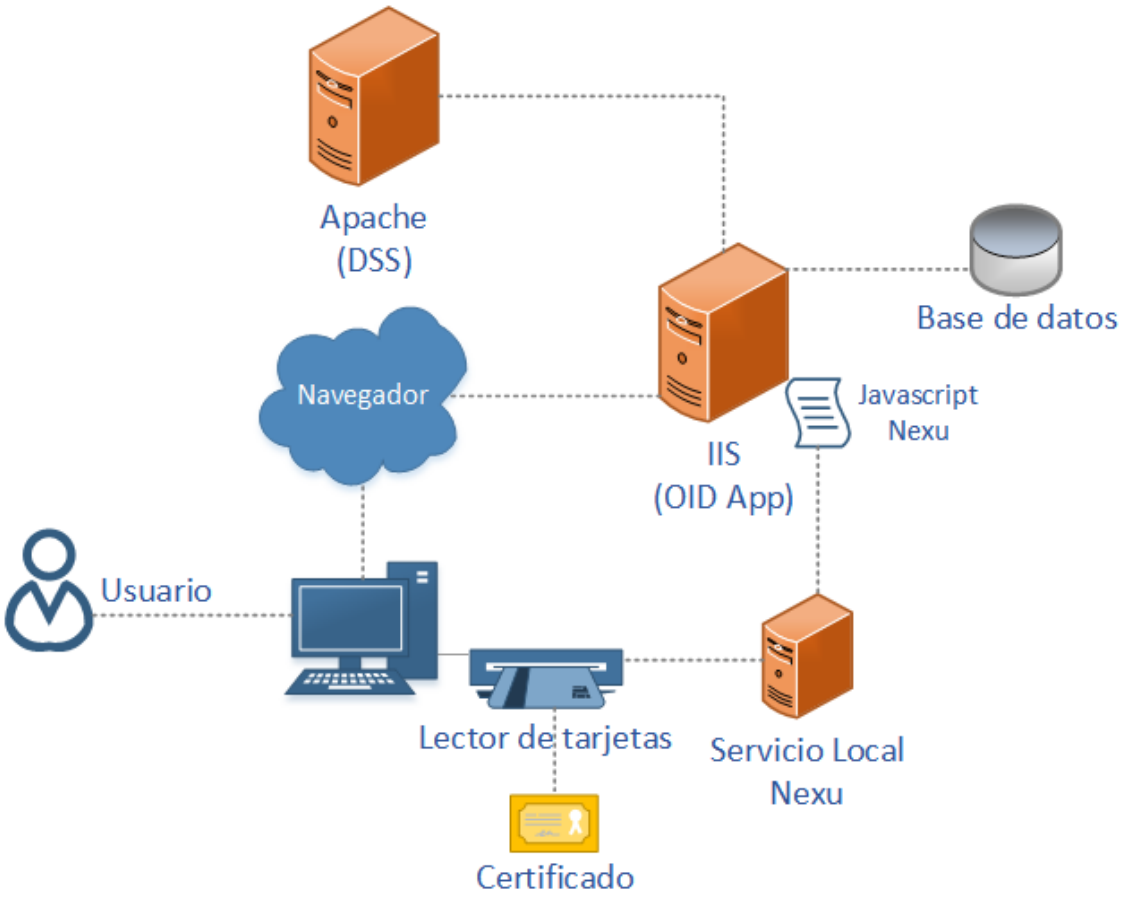

Figura 6. *Arquitectura física de la Aplicación Prototipo*

6. Evaluación de la aplicación prototipo con la Guía de implementación

En este capítulo se explica con más detalle cómo se cumple el tercer objetivo específico planteado en esta investigación, el cual se define como: "Evaluar la factibilidad y eficiencia del proceso de desarrollo de la aplicación prototipo con respecto a los mecanismos de aseguramiento de la información planteados en la *Guía de implementación*". Primero, se explica el contenido de la guía. Segundo, se realiza el proceso de aplicación de la guía al segmento de software de firma digital de la aplicación desarrollada. Seguidamente, la evaluación de la factibilidad y eficiencia al utilizarla. Finalmente, se hacen algunas observaciones que se encontraron durante el proceso.

6.1. Contenido de la *Guía de implementación*

La *Guía de implementación* contiene 103 políticas de seguridad que deben ser aplicadas al segmento de la aplicación que envuelve la funcionalidad de firma digital con el fin de asegurarla en los cuatro escenarios que se presentan. Además, todas las políticas explican los objetivos de control que se deben implementar con el fin de cumplir cada una. Las primeras 29 políticas están relacionas al escenario "Creación de firma digital y sello electrónico", según detalle en la **Tabla 27** en la sección **9.2.1** del Apéndice 2. Luego, desde la política 30 a la 49 corresponden al escenario "Verificación de firma digital y sello electrónico", según detalle en la **Tabla 28** en la sección **9.2.2** del Apéndice 2. Seguidamente, desde la política 50 a la 73 corresponden al escenario "Conversión de una firma digital en formato simple a formato avanzado", según detalle en la **Tabla 29** en la sección **9.2.3** del Apéndice 2. Finalmente, desde la política 74 a la 103 corresponden a "Autenticación de usuarios mediante certificados digitales", según detalle en la **Tabla 30** en la sección **9.2.4** del Apéndice 2. Uno de los principales objetivos de este proyecto de investigación es valuar toda la guía, por lo tanto, como se explicó en los capítulos anteriores, en la aplicación prototipo se desarrollaron las funcionalidades para cumplir con los cuatro escenarios mencionados, de esta manera poder evaluar todas las 103 políticas que expone la guía.

6.2. Proceso de aplicación de la *Guía de implementación*

En esta sección se muestra cómo se aplicó la *Guía de implementación* al software prototipo desarrollado. Para aplicar la guía, se hace uso de la metodología de aplicación que provee la misma guía, la cual ofrece un diagrama de flujo con los pasos a seguir. A continuación, se describen los pasos del diagrama que se siguieron al aplicar la guía de implementación [3]:

- Iterar sobre la lista de políticas de seguridad de la información a ser evaluadas, que se presenta en el Apéndice 9.2, hasta que ya no queden políticas sin evaluar.
- Para cada política, se debe determinar si ésta es aplicable en el contexto de la evaluación.
- 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 9.2.6), 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 el cuadro resumen de la evaluación, indicando que la política no es aplicable.
- 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 9.2.5.
- 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.
- 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.

6.3. Evaluación de la guía

El primer paso realizado para poder evaluar la guía, fue desarrollar la aplicación prototipo, donde el desarrollador toma en cuenta solo los aspectos de seguridad conocidos por experiencia adquirida hasta el momento. Cabe destacar que es la primera vez para el autor de este proyecto de investigación que desarrolla una aplicación de firma digital. Al final del desarrollo se procede a aplicar la guía sólo a los componentes de la aplicación prototipo que involucran la funcionalidad de firma digital. Como se explica en la sección anterior se realizaron los pasos propuestos dentro la misma guía, de esta manera, se iteraron una a una cada política hasta llegar a la última. Los detalles del resultado de la evaluación, del cumplimiento de las políticas y las observaciones realizadas se encuentran en el Apéndice 2. En muchas ocasiones mientras se iteraba sobre la lista de políticas, se encontraron objetivos de control que no se estaban considerando dentro de la aplicación prototipo. Por lo tanto, inmediatamente se procede con la implementación de dichos objetivos dentro de la aplicación para cumplir la política.

6.3.1. Factibilidad

A continuación, en la **Tabla 6** se muestra un resumen de los aspectos de factibilidad valorados durante la aplicación de la guía.

Tabla 6*. Aspectos de factibilidad valorados*

Aspecto de factibilidad valorado	Descripción
Aplicación simple	La guía provee una metodología de aplicación clara y sencilla.
Fácil comprensión	La guía explica de forma clara las políticas y hace referencia a los objetivos de control que se deben implementar para cumplir con cada política.

Útil para asegurar aplicaciones de firma digital	La guía funciona para asegurar el software de firma digital ya que contempla muchos riesgos de seguridad que no siempre son de detectados por los desarrolladores.

Así mismo, con la aplicación de la *Guía de implementación* al prototipo desarrollado, se lograron detectar objetivos de control que faltaban, por lo que sin ninguna duda el uso de la guía agrega una mejora a la seguridad de la información del producto final. Los objetivos de control que faltaban, y posteriormente se implementaron, son los siguientes:

- Política de seguridad 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.
- Política de seguridad 28: 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.
- Política de seguridad 29: 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.

6.3.2. Eficiencia

Respecto a la eficiencia del uso de la guía, se detectó que a lo largo de la lista hay 28 políticas con la misma redacción, y si las compactamos se podrían reducir a solamente 12 políticas (ver Apéndice 3). Esto sucede porque como se mencionó al principio de este capítulo, la guía se divide en cuatro secciones que corresponden a los cuatro escenarios identificados, por ende, muchas políticas están presentes en más de un escenario por lo que parece que están repetidas. Incluso, hay unas políticas que aparecen dentro del mismo escenario con la única diferencia de la clasificación del servicio de seguridad. Por esta razón, para efectos prácticos y de usabilidad de la guía esto aumenta la complejidad y tamaño de la misma ya que genera una lista mucho más larga de políticas, que hasta cierto punto causa confusión a la persona

que la está utilizando. Por lo tanto, no es tan eficiente en este sentido, porque al haber más políticas en la lista se necesita más tiempo para aplicarla en su totalidad, además de que es más difícil de manipular.

Algunos ejemplos de las políticas con la misma redacción que se mencionan son, la política que se enuncia como: "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.", la cual aparece dos veces para el escenario "Creación de firma digital y sello electrónico", primero está en la política número 4 para el servicio de seguridad de "Integridad" y luego está en la política número 22 para el servicio de seguridad de "Confidencialidad", según detalle en la **Tabla 27**. Los controles de seguridad para estas dos políticas son los mismos y al implementarlos hacen cumplir la política en ambos servicios de seguridad. Por lo tanto, no es necesario enunciar la política dos veces para cada servicio de seguridad, de hecho, se podría enunciar una sola vez con la aclaración de que aplica para el servicio de seguridad de "Integridad" y "Confidencialidad".

Otro ejemplo es la política que se enuncia como: "El software complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks, plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes", la cual se encuentra en cuatro ocasiones, en la política número 11, 41, 63 y 84, una para cada escenario, según detalle en las tablas del Apéndice 2. Sin embargo, si nos fijamos en los objetivos de control siempre se hace referencia al mismo, por lo tanto, repetir la política para cada escenario solo aumenta el tamaño de la guía dificultando su comprensión y manipulación. La lista completa de políticas encontradas con la misma redacción en la *Guía de implementación* se puede observar en el Apéndice 3.

Como resultado del análisis realizado a la guía, se detecta en la lista de 103 políticas que además de que algunas tienen redacciones iguales o similares, también se encuentran políticas que tienen distinta redacción, pero tienen contextos relacionados y hacen referencia

a los mismos objetivos de control. Por consiguiente, en este proyecto se realiza una organización de dichas políticas y se crea una lista reducida, tomando las políticas que pueden ser formuladas de manera que abarque varias políticas y ser planteadas como una, con el fin de reducir el tamaño de la guía. En la **Tabla 7** podemos ver un resumen de los métodos de organización aplicados a las 103 políticas de la *Guía de implementación* para reducir el total de la lista de políticas. Los métodos de organización utilizados son los siguientes:

1. Textos idénticos: Se identifican las políticas que en su redacción son idénticas.
2. Textos similares: Se identifican las políticas que en su redacción son muy similares, solamente cambian pocas palabras, pero en esencia se refieren al mismo tema y además tienen los mismos objetivos de control.
3. Textos idénticos + textos similares + contexto relacionado: Consiste en la suma de los dos métodos anteriores, y adicionalmente toma en cuenta el contexto de las políticas, es decir, que tienen redacciones muy distintas, pero se refieren al mismo tema y tienen los mismos objetivos de control.

Además, en el Apéndice 4 se despliega con más detalle cómo se organizaron las 103 políticas y cómo al compactarlas utilizando los tres métodos mencionados anteriormente se resumen finalmente en una lista de 30 políticas.

Tabla 7*. Métodos de Organización de las políticas*

Método de organización	**Total final de Políticas re-organizadas**
Textos idénticos	85
Textos similares	63
Textos idénticos + textos similares + contexto relacionado	30

Así mismo, se encontraron objetivos de control con redacciones iguales, con la única diferencia de su clasificación según el servicio de seguridad. También, se encontraron objetivos de control con la redacción muy similar, pero con una palabra de diferencia. Los objetivos mencionados se muestran en la **Tabla 8.**

Tabla 8. *Análisis de Objetivos de Control*

Objetivo de Control	Diferencias
#3 (Integridad) 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. #17 (Confidencialidad) 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.	• Servicio de Seguridad
#4 (Integridad) Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, Malware… #20 (-) Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, Malware…	• Servicio de Seguridad • Una palabra: divulgación/modificación

Para el caso del objetivo de control con la misma redacción, se encontró el objetivo de control número 3 y 17. No es necesario enunciar el objetivo de control dos veces para cada servicio de seguridad, en su lugar, se podría enunciar una sola vez con la aclaración de que aplica para ambos servicios de seguridad.

Para el objetivo de control número 4 y 20 sólo tiene una palabra de diferencia. Además, el objetivo de control número 4 corresponde al servicio de seguridad de Integridad y el número 20 no tiene definido un servicio de seguridad (esto es un error en la guía). Por lo tanto, para este caso se puede enunciar una única vez de forma que apliquen para ambos objetivos de seguridad.

Posteriormente, a la lista de Objetivos de control se le aplicaron los mismos tres métodos de organización utilizados con la lista de políticas. Sin embargo, para este caso no se obtuvo una reducción tan significativa como con las políticas. Por ejemplo, utilizando el tercer método que es: textos idénticos + textos similares + contexto relacionado, se obtuvo que de los 26

Objetivos de control en la guía se logra reducir a solamente 23. Por lo tanto, no agrega tanto valor realizar una organización a la lista de objetivos de control.

Por otra parte, durante el proceso de aplicación de la guía al software prototipo, se logra identificar que existen dos clasificaciones de políticas, unas que están relacionadas a la codificación de la aplicación y otras a la configuración de la infraestructura para la implementación de la aplicación. Estas dos clasificaciones de políticas que se detectaron están mezcladas por toda la guía, lo que produce que el proceso sea un poco más complejo de seguir, ya que para el contexto de este proyecto sólo se necesitan cumplir las políticas relacionadas al desarrollo y sin embargo se deben revisar y evaluar todas las demás relacionadas a infraestructura.

Finalmente, en la **Tabla 9** se muestra un resumen de los aspectos de eficiencia valorados durante la aplicación de la guía.

Tabla 9. *Aspectos de eficiencia valorados*

Aspecto valorado	Problema	Recomendación
Redacciones idénticas, similares y con contexto relacionado. *(En Políticas y Objetivos de Control)*	• Reduce la eficiencia de la aplicación de la guía al ser tan larga. • Genera confusión.	Re-organizar la guía para reducir su tamaño y mejorar su tiempo de aplicación.
Se identifican dos tipos de políticas. *(De desarrollo y de implementación)*	• Ambos tipos se encuentran mezclados a lo largo de toda la guía. • No es eficiente desde el punto de vista de la etapa en que se encuentre proyecto.	Dividir la guía en dos clasificaciones para facilitar su aplicación según la etapa del proyecto: • Políticas Desarrollo • Políticas de implementación

6.4. Observaciones finales de la evaluación de la *Guía de implementación*

A continuación, se hace una lista con los puntos más relevantes encontrados durante el proceso de evaluación de la *Guía de implementación*:

- En definitiva, la guía funciona para asegurar el software de firma digital ya que contempla muchos riesgos de seguridad que no siempre son detectados por los desarrolladores, lo que permite realizar un aseguramiento más completo de las aplicaciones.
- La guía provee una metodología de aplicación clara y sencilla, lo que hace fácil comprender su uso.
- La guía explica de forma clara las políticas y hace referencia a los objetivos de control que se deben implementar para cumplir con cada política, por lo que hace que sea fácil seguirla.
- Durante el proceso de evaluación se detectó la repetición de políticas para diferentes escenarios y diferentes servicios de seguridad (Integridad, Confidencialidad, Autenticación, No Repudio). Como consecuencia, esto reduce la eficiencia de la aplicación de la guía por ser tan larga.
- Se encontraron objetivos de control duplicados, con la única diferencia de su clasificación según el servicio de seguridad. Por ejemplo: objetivo de control número 3 y 18 (ver **Tabla 27**), para el servicio de seguridad "Integridad" y "Confidencialidad" respectivamente. Lo que hace que la lista se más larga y genera confusión.
- Durante el proceso de evaluación se identifican dos tipos de políticas, las que están relacionadas a la codificación de la aplicación, y las que son de configuración de la infraestructura. Por lo que sería útil dividir la guía en esas dos clasificaciones, de esta forma facilitará el proceso de aseguramiento según la etapa del proyecto, lo que agilizará la aplicación de la guía al software de firma digital.
- Se encontró que las políticas número 52, 53, 55, 74, 75, 77 (ver **Tabla 28** y **Tabla 30**), tienen como objetivo de control 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". Estas políticas no se lograron cumplir en la

aplicación prototipo desarrollada, ya que los protocolos indicados en el objetivo de control no están disponibles en los servicios de CRL y OCSP que pertenecen al BCCR.

- Se encontró un error en la guía. La política número 56 (ver **Tabla 29**) que se enuncia como: “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.”, hace referencia al objetivo de control número 3, el cual no tiene relación a esta política.
- Se encontró un error en la guía. El objetivo de control número 20 hace referencia la política número 18, la cual no tiene relación al objetivo de control, según detalle en la **Tabla 31**.

7. Conclusiones

En este capítulo se presentan las conclusiones obtenidas durante la realización de esta investigación, se describen algunas recomendaciones respecto a la *Guía de implementación* y finalmente se hace una lista de elementos que se pueden realizar como trabajo futuro.

Como parte del primer objetivo planteado en este proyecto se realiza una investigación en la búsqueda de un dominio de aplicación y se identifica que dentro del SNCD no existe ninguna autoridad que administre los OID en Costa Rica. Como se mencionó en capítulos anteriores, los Identificadores de Objeto, son un mecanismo utilizado para identificar cualquier objeto de forma inequívoca y universal, y para el caso del gobierno de Costa Rica, utiliza los OID para identificar documentos oficiales, certificados digitales, entre otros; pero es una administración a lo interno por lo que ninguna otra entidad o persona puede hacer uso formal de los OID en el país. Por lo tanto, al seleccionar este dominio se realiza un aporte en el tema de la creación de una "Autoridad de Registro de OID" para Costa Rica, ya que se realiza un análisis de requerimientos para una aplicación administradora de OID y adicionalmente se desarrolló la aplicación es su forma básica.

Por otra parte, con la aplicación base de OID desarrollada, se procede con el desarrollo del módulo de firma digital que se utiliza dentro de ella. Se realizan funcionalidades para los cuatro escenarios identificados en la *Guía de implementación*, los cuales son: "Creación de firma digital y/o sello electrónico", "Verificación de firma digital y/o sello electrónico", "Autenticación de usuarios mediante certificados digitales" y "Conversión de una firma digital en formato simple a formato avanzado" con el fin de evaluar la *Guía de implementación* en su totalidad. Durante el desarrollo de los componentes del módulo de firma digital se encontró con una gran complejidad en el ámbito, desde el tema de leer las tarjetas inteligentes hasta generar la firma. La firma y certificados digitales no son un tema trivial y requieren de mucha lógica de encripción, manejo de formatos y de muchos procesos para poderla implementar de una forma correcta y segura. Por lo que para efectos del alcance de esta investigación no se desarrolló toda la funcionalidad de criptografía de firma y certificados digitales, en su lugar se selecciona un software de código abierto que pertenece

a la Unión Europea, el cual utiliza los estándares de la UIT-T X.509 para los certificados digitales, al igual que lo requiere Costa Rica como se estipula en la “Política de certificados para la jerarquía nacional de certificadores registrados” [23].

Con la aplicación base y el módulo de firma digital contemplados, como último objetivo se realiza la evaluación de la utilización de la *Guía de implementación* para el aseguramiento de una aplicación de firma digital para un caso práctico real. A partir de la evaluación realizada a la guía, se encontró que es una herramienta útil y realmente necesaria para el SNCD. La guía cubre muchos aspectos de seguridad que deben ser implementados en un contexto de firma digital y que por falta de conocimiento u orientación de los desarrolladores podrían pasar por alto, generando vulnerabilidades de seguridad en sus aplicaciones. Durante la aplicación de la guía al prototipo desarrollado, se encontraron varios objetivos de seguridad que no estaban siendo considerados. Por lo tanto, queda en evidencia que es importante proveer una guía al público en Costa Rica, para que evalúen sus aplicaciones desarrolladas o en proceso de desarrollo y puedan garantizar que las mismas cuentan con los aspectos de seguridad necesarios para brindar aplicaciones confiables y seguras a sus usuarios.

Por otra parte, se observó que la guía es una herramienta fácil de comprender y utilizar, ya que metodología de cómo se debe aplicar correctamente es simple de seguir. Además, se explica de forma clara y concisa las políticas y objetivos de control que se deben aplicar. Por lo tanto, el nivel de complejidad de su comprensión es bajo.

Otro hallazgo en la evaluación de la guía con respecto a su eficiencia, es la forma en que está formulada hace que sea muy extensa. En consecuencia, hace que requiera mucho más tiempo para su aplicación y que el proceso no sea tan ágil. Como se mencionó anteriormente hay muchas políticas que se repiten para diferentes escenarios y clasificaciones de servicios de seguridad (Integridad, Confidencialidad, Autenticación” y No repudio), que podrían ser resumidas, para reducir el tamaño de la guía y de esta forma se más clara y fácil de manipular. Se recomienda reformular la guía, revisar la lista de políticas y de objetivos de control para redactarlos de un modo que no se repitan para cada escenario o servicio de seguridad. Con el

objetivo de obtener una lista más corta, clara y concisa, para mejorar el tiempo de su aplicación.

Como se mencionó en el capítulo anterior, durante la evaluación se identificaron dos tipos de políticas, unas relacionadas al desarrollo del software y otras a la configuración de la infraestructura al momento de su implementación. Como consecuencia, se recomienda que la guía se organice en dos partes. La primera en políticas de software y la segunda en políticas de implementación, con el objetivo de facilitar la aplicación de la guía según la etapa del proyecto, ya sea desarrollo o implementación.

Otro aspecto importante es que se encontró que existen políticas que solicitan implementar ciertos mecanismos de control que no se lograron cumplir, ya que están fuera del alcance del desarrollo de esta investigación. Por ejemplo, los servicios de CRL, OCSP y TSA proveídos por el SNCD solo se encontraron en protocolo HTTP, sin embargo, las políticas que no se lograron cumplir solicitan que estas conexiones se realicen por un protocolo seguro como HTTPS.

Finalmente, la guía utilizada para validar la aplicación prototipo es la primera versión del TFIA de Alejandro Mora, la cual, actualmente esta siendo modificada para corregir algunos detalles. Por lo tanto, se recomienda tomar en cuenta las observaciones referentes a la guía en esta investigación para las modificaciones que se están haciendo con el objetivo de generar la versión final de la guía.

7.1. Trabajo futuro

Como se explicó anteriormente, la aplicación base desarrollada “Autoridad de Registro de OID”, fue asegurada utilizando OWASP Top 10 [20]. Sin embargo, hay algunos mecanismos de seguridad que no fueron implementados porque la aplicación administradora de OID no es parte de los objetivos principales del este proyecto de investigación y requieren más tiempo de desarrollo. Los riesgos a los que se hace referencia son “A5:2017 Pérdida de Control de Acceso”, “A6:2017 Configuración de Seguridad Incorrecta”, “A10:2017 Registro

y Monitoreo Insuficientes", ver más detalles de los riesgos en la segunda sección del Apéndice 2.

Así mismo, el aporte realizado en este proyecto es iniciar con las investigaciones y análisis del tema de los OID. Por lo tanto, no se desarrollada toda la funcionalidad para una "Autoridad de Registro de OID", si no más bien se desarrolla una funcionalidad básica con el objetivo de que permitiera implementar en ella firma digital para así poder evaluar la *Guía de implementación*. Como consecuencia, para que la aplicación pueda ser utilizada dentro del SNCD como una autoridad registradora de OID, requiere extender su funcionalidad, así como la generación de pruebas de funcionalidad y de seguridad, entre otros.

El módulo de DSS tiene una funcionalidad para validación de los certificados dentro de un *Trusted Lists*. Que es una lista centralizada donde se puede localizar toda la jerarquía de certificados de los países. Sin embargo, dentro del SNCD aún no se cuenta con una lista como esta. Para solucionar este requerimiento en las guías que se proveen por el MICITT, se recomienda que se instale el certificado del usuario en la máquina local, para poder realizar esta validación en la jerarquía del certificado CA-Raíz, certificados de CA-Políticas y certificados de CA-SINPE. Por consiguiente, la Política que se enuncia como "Se debe validar que el certificado digital que se utilizará en el proceso de firma pertenece a la jerarquía nacional de certificadores registrados", no puede ser validada utilizando la funcionalidad de *Trusted List*. Como consecuencia, se recomienda que se disponga de un servicio de "Listas de Confianza" a nivel nacional.

Otro aspecto para trabajo futuro son las políticas que hacen referencia a "Se debe validar que el documento electrónico cuyo formato se va a verificar/convertir, no contiene código oculto (por ejemplo, macros) o malicioso". Este tema no es trivial, por lo que requerirá un desarrollo de un módulo de antivirus para poder verificar que los documentos que ingresan en el sistema están libres de virus, *malware* o código malicioso, u obtener un servicio o software de antivirus para realizar el escaneo de estos documentos y hacer cumplir dicha política.

Finalmente, la guía que se utilizó durante esta investigación para validar la aplicación prototipo, es la primera versión del TFIA de Alejandro Mora. Sin embargo, la guía actualmente esta siendo modificada para corregir algunos detalles, esta nueva versión aún no esta lista, por lo que no se utilizó para efectos de esta investigación. En consecuencia, queda para trabajo futuro realizar la evaluación de la aplicación con la versión final de la guía.

8. Bibliografía

[1] MICITT, «Entidades que utilizan Firma Digital,» [En línea]. Available: http://www.mifirmadigital.go.cr/fdigital/pdf/fd-instituciones.pdf. [Último acceso: Abril 2019].

[2] Gobierno de Costa Rica, Masificación de la implementación y el uso de la firma digital en el sector público costarricense, Diario Oficial La Gaceta, 25 de Abril de 2014.

[3] A. Mora, «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 Sistema Nacional de Certificación Digital. Universidad de Costa Rica,» 2017.

[4] A. Mora, «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. Universidad de Costa Rica,» 2017.

[5] Gobierno de Costa Rica, Ley de certificados, firmas digitales y documentos electrónicos No. 8454, Diario Oficial La Gaceta, 2005.

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

[7] M. Bishop, Computer Security: Art and Science, Addison Wesley, 2002.

[8] R. Shirey, Security Architecture for Internet Protocols: A Guide for Protocol Designs and Standards, Internet Engineering Task Force, 1994.

[9] J. A. Buchman, E. Karatsiolis y A. Wiesmaier, Introduction to Public Key Infrastructures, Springer, 2013.

[10] ISO/IEC, Information technology — Security techniques — Information security risk management, 2008.

[11] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley y W. Polk, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,»

Mayo 2008. [En línea]. Available: https://tools.ietf.org/html/rfc5280. [Último acceso: Abril 2019].

[12] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin y C. Adams, «X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,» Junio 2013. [En línea]. Available: https://tools.ietf.org/html/rfc6960. [Último acceso: Abril 2019].

[13] C. Adams, P. Cain, D. Pinkas y R. Zuccherato, «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP),» Agosto 2001. [En línea]. Available: https://tools.ietf.org/html/rfc3161. [Último acceso: Abril 2019].

[14] European Parliament and Council, Directive 1999/93/EC of the European Parliament and of the Council, Dec 1999.

[15] M. Mazzeo, «Digital Signatures and European Laws,» Enero 2004. [En línea]. Available: https://www.symantec.com/connect/articles/digital-signatures-and-european-laws. [Último acceso: Abril 2019].

[16] Recommendation ITU-T X.660, Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree, Recommendation ITU-T X.660, 2011.

[17] Recommendation ITU-T X.680, Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation, Recommendation ITU-T X.680, 2015.

[18] T. Howes, S. Kille, W. Yeon y C. Robbins, «The String Representation of Standard Attribute Syntaxes,» Marzo 1995. [En línea]. Available: https://www.ietf.org/rfc/rfc1778.txt. [Último acceso: Abril 2019].

[19] Orange SA, «OID Repository,» Orange SA, [En línea]. Available: http://www.oid-info.com/cgi-bin/display?tree=1.2. [Último acceso: Abril 2019].

[20] OWASP, «OWASP Top 10 - 2017. Los diez riesgos más críticos en Aplicaciones Web,» 2017. [En línea]. Available: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf. [Último acceso: Abril 2019].

[21] Nowina Solutions, «Nowina Solutions,» [En línea]. Available: http://nowina.lu/. [Último acceso: Abril 2019].

[22] European Commission, «CEF Digital Connecting Europe,» [En línea]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS. [Último acceso: Abril 2019].

[23] Gobierno de Costa Rica, Política de certificados para la jerarquía nacional de certificadores registrados, Dirección de Certificadores de Firma Digital Ministerio de Ciencia y Tecnología, 04 de Setiembre de 2008.

[24] H. Tipton, Official (ISC)2 Guide to the CISSP CBK, Second Edition, Auerbach Publications; 2 edition, 2009.

9. Apéndices

9.1. Apéndice 1

En esta sección se describen con detalle cada uno de los requerimientos establecidos para la aplicación "Autoridad de Registro OID" desarrollada para esta investigación. En la primera sección se definen los requerimientos funcionales y en la segunda sección los requerimientos de seguridad.

9.1.1. OID: Requerimientos funcionales

A continuación, se describen cada uno de los requerimientos funcionales:

Tabla 10. *Requerimiento funcional: RFOID01 – Crear OID*

RFOID01 – Crear OID			
Un usuario debe poder solicitar la inclusión de un nuevo OID hijo o hermano a partir de uno ya existente.			
	Origen	**Afectados**	**Tipo**
	Investigación	Usuario final	Funcional
Fundamento	Una de las funciones básicas de una Autoridad de Registro es poder crear un nuevo OID en el Sistema, almacenarlo correctamente y proveerlo al usuario final para el uso que requiera.		
Comentarios	Esta Autoridad de Registro tendrá la función técnica, no solo asignará nombres inequívocos, si no, también registrará en el Sistema la		

	definición de los objetos y verificará que estén en conformidad con las recomendaciones de la ITU-T norma internacional.
Campos requeridos	**Designación del OID** ● ID Padre. *(Requerido)* Número identificador. Mayor o igual a 0. No puede ser utilizado antes en el mismo nivel del árbol. *(Requerido)* ● Identificador. Cadena de caracteres. Inicia con minúscula. Puede tener '-' pero no '_'. *(Opcional)* ● Otros identificadores. Utilizado cuando la descripción del OID es actualizada. *(Opcional)* **Descripción del OID** ● Descripción del OID. Explica para que esta siendo identificado por el OID. Texto largo. *(Requerido)* ● Información. Pueden ser URLs, referencias a documentos, reglas de como los hijos del OID serán registrados. *(Opcional)* **Información del remitente** ● Nombre *(Requerido)* ● Apellido *(Requerido)* ● Correo Electrónico *(Requerido)* **Actual Autoridad de Registro** Es la RA compañía o persona a cargo de almacenar arcos y su-barcos e información general del OID que se desea generar. Si ya existe la RA, esta sección sirve para notificar por correo cada vez que alguien quiere registrar un OID en el OID actual o cualquier hijo. ● Nombre ● Apellido ● Dirección ● País ● Correo Electrónico

	● Teléfono ● Fecha de modificación. Es la fecha de cuando la primera RA es oficialmente reemplazada por el registro actual. **Primer Autoridad de Registro** Es la primera persona responsable de manejar este OID. Cuando las responsabilidades son transferidas a alguien más, se debe llenar la información de "Actual Autoridad de registro" y esa información es guardada para propósitos históricos. ● Nombre. ● Apellido. ● Dirección. ● País. ● Correo Electrónico. ● Teléfono. ● Fecha de creación. Aceptar términos y condiciones.

***Tabla 11**. Requerimiento funcional: RFOID02 – Modificar OID*

<table>
<tr><th colspan="4">RFOID02 – Modificar OID</th></tr>
<tr><td colspan="4">Un usuario debe poder solicitar la actualización de un OID existente.</td></tr>
<tr><td></td><td>Origen</td><td>Afectados</td><td>Tipo</td></tr>
<tr><td></td><td>Investigación</td><td>Usuario final</td><td>Funcional</td></tr>
<tr><td>Fundamento</td><td colspan="3">Una de las funciones básicas de una Autoridad de Registro es poder modificar OID existentes en el Sistema, almacenar la nueva información correctamente y informar al usuario la modificación.</td></tr>
<tr><td>Comentarios</td><td colspan="3">Esta Autoridad de Registro tendrá la función técnica, no solo asignará nombres inequívocos, si no, también registrará en el Sistema la definición de los objetos y verificará que estén en conformidad con las recomendaciones de la ITU-T norma internacional.</td></tr>
<tr><td>Campos requeridos</td><td colspan="3">Designación del OID
● Identificador. Cadena de caracteres. Inicia con minúscula. Puede tener ‘-’ pero no ‘_’. (Opcional)
● Otros identificadores. Utilizado cuando la descripción del OID es actualizada. (Opcional)
Descripción del OID
● Descripción del OID. Explica para que esta siendo identificado por el OID. Texto largo. (Requerido)
● Información. Pueden ser URLs, referencias a documentos, reglas de como los hijos del OID serán registrados. (Opcional)
Información del remitente
● Nombre (Requerido)</td></tr>
</table>

	● Apellido *(Requerido)* ● Correo Electrónico *(Requerido)* **Actual Autoridad de Registro** Es la RA compañía o persona a cargo de almacenar arcos y su-barcos e información general del OID que se desea generar. Si ya existe la RA, esta sección sirve para notificar por correo cada vez que alguien quiere registrar un OID en el OID actual o cualquier hijo. ● Nombre ● Apellido ● Dirección ● País ● Correo Electrónico ● Teléfono ● Fecha de modificación. Es la fecha de cuando la primera RA es oficialmente reemplazada por el registro actual. **Primer Autoridad de Registro** Es la primera persona responsable de manejar este OID. Cuando las responsabilidades son transferidas a alguien más, se debe llenar la información de "Actual Autoridad de registro" y esa información es guardada para propósitos históricos. ● Nombre. ● Apellido. ● Dirección. ● País. ● Correo Electrónico. ● Teléfono. ● Fecha de creación. **Notas al Administrador del Repositorio** Explicación para el administrar del repositorio de OID. Por ejemplo, explicar porque quiere actualizar o remover el OID del repositorio. Esta información es confidencial solo el administrador la puede ver.

Tabla 12. *Requerimiento funcional: RFOID03 – Notificación de solicitud*

RFOID03 – Notificación de solicitud			
A partir de la creación o modificación de un OID el sistema deberá crear una notificación al administrador de la autoridad de registros de OID para que sea informado de dicha solicitud.			
	Origen	**Afectados**	**Tipo**
	Investigación	Administrador de la Autoridad de Registro de OID	Funcional
Fundamento	El administrador de la autoridad de registros de OID recibirá una notificación para revisión de un OID.		
Comentarios	Esta notificación se hará por medio de correo electrónico.		
Campos requeridos	Número de gestión. Correo electrónico.		

Tabla 13. *Requerimiento funcional: RFOID04 – Aprobación de solicitud*

RFOID04 – Aprobación de solicitud			
El usuario administrador del sistema, una vez conforme con la solicitud de creación/modificación de OID podrá aprobar la solicitud realizada.			
	Origen	**Afectados**	**Tipo**
	Investigación	Administrador de la Autoridad de Registro de OID	Funcional
Fundamento	El administrador de la autoridad de registros de OID necesita tener un medio para aprobar una solicitud de creación o modificación de OID.		
Comentarios	Esto generara oficialmente el OID. Además, genera una notificación al remitente del OID. Para informar del estado de aprobación de su solicitud.		
Campos requeridos	Número de gestión. Correo electrónico de solicitante.		

Tabla 14. *Requerimiento funcional: RFOID05 – Rechazo de solicitud*

RFOID05 – Rechazo de solicitud			
El usuario administrador del sistema si está inconforme o ve algún problema con la información solicitada, puede rechazar la solicitud.			
	Origen	**Afectados**	**Tipo**
	Investigación	Administrador de la Autoridad de Registro de OID	Funcional
Fundamento	El administrador de la autoridad de registros de OID necesita tener un medio para rechazar una solicitud de creación o modificación de OID, si esta no cumple con los requisitos.		
Comentarios	Esto, genera una notificación al remitente del OID. Para informar del estado de su solicitud.		
Campos requeridos	Número de gestión. Correo electrónico del solicitante.		

Tabla 15. *Requerimiento funcional: RFOID06 – Autenticación*

RFOID06 – Autenticación			
Los usuarios se deben autenticar en el sistema para poder ingresar en el mismo.			
	Origen	**Afectados**	**Tipo**
	Investigación	• Administrador de la Autoridad de Registro de OID • Usuario final	Funcional
Fundamento	Un usuario debe poder autenticarse en el sistema para poder ingresar y hace uso de este.		
Comentarios	La autenticación se llevará a cabo por medio de firma digital.		
Campos requeridos	Dispositivo de firma digital.		

Tabla 16. *Requerimiento funcional: RFOID07 – Generación de un documento comprobante firmado*

RFOID07 – Generación de un documento comprobante firmado			
El sistema debe generar un documento oficial comprobante de la solicitud, firmado digitalmente con la información del nuevo OID			
	Origen	**Afectados**	**Tipo**
	Investigación	• Administrador de la Autoridad de Registro de OID • Usuario final	Funcional
Fundamento	Se necesita generar un documento legal y firmado digitalmente que sirva como comprobante de la creación del nuevo OID.		
Comentarios			
Campos requeridos			

9.1.2. OID: Requerimientos de seguridad

A continuación, se describen cada uno de los requerimientos de seguridad:

Tabla 17. *Requerimiento de seguridad: A1 - Inyección*

Riesgo	**A1:2017 Inyección**
Definición	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
Como se mitigó	Desde el módulo de manejo de datos se utilizan objetos de tipo `SQLParameters` del *framework* de .NET para todas las consultas realizadas a la base de datos. Dichos objetos no permiten enviar código ejecutable al motor de base de datos.

Tabla 18. *Requerimiento de seguridad: A2 - Pérdida de Autenticación*

Riesgo	**A2:2017 Pérdida de Autenticación**
Definición	Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, *token* de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
Como se mitigó	Para la autenticación de usuarios en este caso se hace por medio de firma digital, por lo que el usuario y contraseña son únicos y es información que esta custodiada solo por el cliente. Así mismo, la administración de la sesión del usuario en la aplicación web es manejada por el servidor por lo que se encuentra encriptada y además se genera un ID de sesión aleatorio para cada inicio de sesión.

Tabla 19. *Requerimiento de seguridad: A3 - Exposición de datos sensibles*

Riesgo	**A3:2017 Exposición de datos sensibles**
Definición	Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.
Como se mitigó	Para mitigar este problema en: **Datos almacenados:** No se almacenan datos sensibles en ningún servidor ni dentro de la aplicación. **Datos en tránsito:** Se deben configurar las aplicaciones para que sean accedidas o envíen datos únicamente por HTTPS. Este punto no es parte del alcance de este proyecto, ya que se enfoca sólo en la etapa de desarrollo. Esto debe tomarse en cuenta al momento de implementar la aplicación. **Datos procesados:** Se utilizan algoritmos de cifrado fuertes que proveen los *framework* de los lenguajes de programación, no se utilizan algoritmos propios.

Tabla 20. *Requerimiento de seguridad: A4 - Entidades Externas XML (XXE)*

Riesgo	**A4:2017 Entidades Externas XML (XXE)**
Definición	Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear

	puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).
Como se mitigó	La aplicación no acepta XML de ninguna entidad externa. La única conexión que tiene es con los servicios REST de DSS y dicha conexión se realiza por medio del formato JSO. Sin embargo, acepta archivos XML subidos por el del cliente, la aplicación valida que su formato sea correcto, y además utiliza `XMLResolver` para validar que no existan recursos externos desconocidos.

Tabla 21. *Requerimiento de seguridad: A5 - Pérdida de Control de Acceso*

Riesgo	**A5:2017 Pérdida de Control de Acceso**
Definición	Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.
Como se mitigó	Este riesgo se dispone para realizar a trabajo futuro por no ser parte de los objetivos principales del este proyecto de investigación.

Tabla 22. *Requerimiento de seguridad: A6 - Configuración de Seguridad Incorrecta*

Riesgo	**A6:2017 Configuración de Seguridad Incorrecta**
Definición	La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, *frameworks*, dependencias y componentes desactualizados, etc.

Como se mitigó	Este riesgo se dispone para realizar a trabajo futuro por no ser parte de los objetivos principales del este proyecto de investigación.

Tabla 23. *Requerimiento de seguridad: A7 - Secuencia de Comandos en Sitios Cruzados (XSS)*

Riesgo	**A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)**
Definición	Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (*defacement*) los sitios web, o redireccionar al usuario hacia un sitio malicioso.
Como se mitigó	Los formularios de entrada de datos en la aplicación web de OID están creados utilizado el *framework* de MVC.NET los cuales ya contienen mecanismos de encripción para validar este tipo de riesgos. Se implementa la función de `ValidateAntiForgeryToken` que evita que una entidad externa realice llamadas al formulario de la aplicación sin autorización. Adicionalmente el sitio en MVC contiene controles de seguridad como `HttpRequestValidation`, el cual verifica que no vaya ningún código ejecutable o malicioso dentro de la solicitud.

Tabla 24. *Requerimiento de seguridad: A8 - Deserialización Insegura*

Riesgo	**A8:2017 Deserialización Insegura**
Definición	Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

Como se mitigó	La aplicación OID no acepta objetos serializados de fuentes no confiables, ni tampoco utiliza medios de serialización que sólo permitan tipos de datos primitivos. Por lo tanto, dada la arquitectura que tiene la aplicación este riesgo es mitigado.

Tabla 25. *Requerimiento de seguridad: A9 - Componentes con vulnerabilidades conocidas*

Riesgo	**A9:2017 Componentes con vulnerabilidades conocidas**
Definición	Los componentes como bibliotecas, *frameworks* y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.
Como se mitigó	Para la aplicación desarrollada, no se utilizan componentes de terceros no confiables. Solo utilizan librerías oficiales.

Tabla 26. *Requerimiento de seguridad: A10 - Registro y Monitoreo Insuficientes*

Riesgo	**A10:2017 Registro y Monitoreo Insuficientes**
Definición	El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos.
Como se mitigó	Este riesgo se dispone para realizar a trabajo futuro por no ser parte de los objetivos principales del este proyecto de investigación.

9.2. Apéndice 2

Las siguientes tablas presentan las políticas de seguridad de la información a ser evaluadas.

9.2.1. Creación de firma digital y sello electrónico

Tabla 27. *Políticas de Seguridad: Creación de firma digital y sello electrónico*

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				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	x			1
2	I	Se debe validar que el documento electrónico que se va a firmar no contiene código oculto o malicioso.	1	x			2
3	I	Se debe validar que los documentos electrónicos resultantes, firmados en formato simple, puedan convertirse posteriormente a formatos avanzados válidos.	2	x			3

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
4	I	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.	3			x	4
5	I	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.	3			x	4
6	I	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.	3			x	4
7	I	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.	3			x	4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
8	I	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.	4			x	5
9	I	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.	4			x	5
10	I	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.	4			x	5
11	I	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5			x	6

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
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	x			7
13	A	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de firma es válido.	7	x			8
14	A	Se debe validar que el certificado digital que se utilizará en el proceso de firma pertenece a la jerarquía nacional de certificadores registrados.	8			x	20
15	A	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.	9	x			18
16	A	Se debe validar que el certificado digital que se utilizará en el proceso de firma se encuentra almacenado en un dispositivo criptográfico seguro.	10	x			9
17	A	Se debe validar el uso correcto del certificado que se utilizará en el proceso de firma.	11	x			10

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
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	x			11
19	C	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no puedan ser obtenidas utilizando mecanismos de fuerza bruta.	14	x			
20	C	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.	15, 20	x			
21	C	Se debe validar que el documento electrónico firmado resultante no se entregue a usuarios no autorizados.	16	x			12

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
22	C	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.	17			x	4
23	C	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.	20			x	5
24	C	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.	18			x	13
25	C	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19			x	13
26	NR	El resumen del documento electrónico que se va a firmar debe calcularse utilizando algoritmos *hash* seguros.	21	x			14

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
27	NR	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.	22	x			15
28	NR	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.	23	x			
29	NR	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.	24	x			

9.2.2. Verificación de firma digital y sello electrónico

***Tabla 28**. Políticas de Seguridad: Verificación de firma digital y sello electrónico*

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				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		x		18
31	I	Se debe validar que el documento electrónico cuyas firmas se van a verificar, no contiene código oculto (por ejemplo, macros) o malicioso.	1		x		19
32	I	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.	3			x	4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
33	I	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.	3			x	4
34	I	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.	3			x	4
35	I	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.	3			x	4
36	I	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.	3			x	4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
37	I	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.	4			x	5
38	I	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.	4			x	5
39	I	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.	4			x	5
40	I	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.	4			x	5

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
41	I	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5			x	6
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			x	20
43	A	Se debe validar el uso correcto de los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar.	11	x			10
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			x	4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
45	C	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.	20			x	5
46	C	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.	18			x	13
47	C	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19			x	13
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	x			16
49	NR	El resumen del documento electrónico cuyas firmas se van a verificar debe calcularse utilizando algoritmos *hash* seguros.	21	x			14

9.2.3. Conversión de una firma digital en formato simple a formato avanzado

***Tabla 29**. Políticas de Seguridad: Conversión de una firma digital en formato simple a formato avanzad*

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				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	x			3
51	I	Se debe validar que el documento electrónico cuyo formato se convertirá, no contiene código oculto (por ejemplo, macros) o malicioso.	1		x		19
52	I	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.	3		x		17

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
53	I	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.	3		x		17
54	I	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.	3		x		17
55	I	Se debe proteger los *tokens* de estampado de tiempo, mientras se transmiten por red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	3		x		17
56	I	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.	~~3~~	x			

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
57	I	Se debe proteger el documento electrónico cuyo formato se convertirá, así como sus representaciones intermedias (documento electrónico firmado en formato avanzado), mientras se transmite por una red, de manera que no pueda ser modificado por usuarios no autorizados.	3			x	4
58	I	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.	3			x	4
59	I	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.	3			x	4
60	I	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.	3			x	4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
61	I	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.	4			x	5
62	I	Se debe proteger los atributos obtenidos para la creación del documento electrónico en formato avanzado, mientras transita por la memoria local, de manera que no puedan ser modificados por usuarios no autorizados.	4			x	5
63	I	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5			x	6
64	A	La ruta 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	x			

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
65	A	La ruta 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.	12	x			
66	A	Las rutas 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.	12	x			
67	A	La ruta requerida para obtener los *tokens* de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.	12			x	21
68	C	Se debe validar que el documento electrónico resultante, firmado en formato avanzado, no se entregue a usuarios no autorizados.	16	x			12

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
69	C	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.	17			x	4
70	C	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.	18			x	13
71	C	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19			x	13
72	NR	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	25	x			22
73	NR	Se debe validar que las respuestas OCSP no sean reutilizables.	26	x			23

9.2.4. Autenticación de usuarios mediante certificados digitales

Tabla 30. *Políticas de Seguridad: Autenticación de usuarios mediante certificados digitale*

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				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		x		17
75	I	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.	3		x		17
76	I	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.	3		x		17

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
77	I	Se debe proteger los *tokens* de estampado de tiempo, mientras se transmiten por una red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	3		x		17
78	I	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.	3			x	4
79	I	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.	3			x	4
80	I	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.	3			x	4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
81	I	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.	4			x	4
82	I	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.	4			x	5
83	I	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.	4			x	5
84	I	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5			x	6

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
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	x			7
86	A	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de autenticación es válido.	7	x			8
87	A	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación pertenece a la jerarquía nacional de certificadores registrados.	8			x	20
88	A	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación se encuentra almacenado en un dispositivo criptográfico seguro.	10	x			9
89	A	Se debe validar el uso correcto del certificado que se utilizará en el proceso de autenticación.	11	x			10

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
90	A	La ruta 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	x			
91	A	La ruta 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.	12	x			
92	A	Las rutas 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.	12	x			
93	A	La ruta requerida para obtener los *tokens* de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.	12			x	21

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
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	x			11
95	C	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no puedan ser obtenidas utilizando mecanismos de fuerza bruta.	14	x			
96	C	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no sean almacenadas en caché para su uso posterior.	15, 20	x			
97	C	Se debe proteger los datos generados aleatoriamente para el proceso de autenticación, así como sus representaciones derivadas (resumen de los datos aleatorios y resumen cifrado de los datos aleatorios), mientras se transmiten por una red, de manera que no sean revelados a usuarios no autorizados.	17			x	4
98	C	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.	18			x	13

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
99	C	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19			x	13
100	NR	El resumen de los datos de autenticación que se van a firmar debe calcularse utilizando algoritmos *hash* seguros.	21	x			14
101	NR	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación se encuentra vigente.	22	x			15
102	NR	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	25	x			22
103	NR	Se debe verificar que las respuestas OCSP no sean reutilizables.	26	x			23

9.2.5. Lista de Objetivos de Control Para Evaluar el Cumplimiento de las Políticas de Seguridad de la Información

La siguiente tabla 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 definidas.

Tabla 31. *Objetivos de Control*

No.	Servicio de seguridad	Objetivo de Control	Políticas
1	I	Se deben validar los datos que el usuario introduce en el sistema, verificando que cada entrada cumple al menos con los siguientes requisitos: *Cuando la entrada es texto* • Los caracteres introducidos deben ser válidos, según el conjunto de caracteres permitido correspondiente. • La longitud de los caracteres introducidos debe estar dentro de los límites mínimo y máximos correspondientes. • Si la entrada requiere un formato específico (como una fecha, una dirección de correo electrónico, un número telefónico, etcétera), los caracteres introducidos deben cumplir con ese formato.	Hace cumplir políticas: 1, 2, 30, 31, 50, 51

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• Si la entrada se utiliza como argumento en una operación de creación, lectura, actualización o borrado de registros en una base de datos, se debe hacer a través de sentencias parametrizadas (*prepared statements*), y no mediante la concatenación de hileras de caracteres. • Si la entrada debe mostrarse al usuario posteriormente, durante su interacción con el sistema, deben aplicarse las reglas de escape correspondientes según el o los lenguajes utilizados. *Cuando la entrada es un archivo* • El archivo debe tener un formato permitido. • El formato del archivo debe ser correcto. • El tamaño del archivo no debe exceder un tamaño máximo permitido. • El archivo no debe almacenar contenido malicioso, como virus, *malware*, etcétera. • Si el archivo se almacenará en el sistema de archivos de un servidor, su nombre o ubicación no debe ser igual al de algún archivo de configuración según el tipo de servidor. Por ejemplo, *.htaccess* en Apache, o *Web.conf* en IIS, entre otros.	

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.	Hace cumplir políticas: 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.	Hace cumplir 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
4	I	Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, *malware* y cualquier otro tipo de *software* malicioso que facilite la modificación no autorizada de datos, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final*	Hace cumplir políticas: 8, 9, 10, 37, 38, 39, 40, 61, 62, 81, 82, 83

No.	Servicio de seguridad	Objetivo de Control	Políticas
		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: • 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. *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final* Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique: • 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.	

No.	Servicio de seguridad	Objetivo de Control	Políticas
5	I	Se debe validar que el *software* complementario, requerido para ejecutar la aplicación, se encuentra actualizado en la máquina donde se ejecuta, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final* Se debe validar la existencia un procedimiento periódico, ejecutado como máximo cada 7 días naturales, para comprobar que al menos el sistema operativo, los navegadores de Internet, los *frameworks*, los *plug-ins* y los *drivers* 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: • 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). *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final*	Hace cumplir políticas: 11, 41, 63, 84

No.	Servicio de seguridad	Objetivo de Control	Políticas
		Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique: • Recomendaciones para mantener el *software* complementario actualizado en la máquina. • La importancia que tiene el mantener dicho *software* actualizado, en lo que respecta al no repudio de la información.	
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.	Hace cumplir políticas: 12, 85
7	A	Se debe validar que el perfil del certificado digital cumple con los requisitos establecidos en la sección 7.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013).	Hace cumplir políticas: 13, 86
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).	Hace cumplir políticas: 14, 42, 87
9	A	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.	Hace cumplir política 15

No.	Servicio de seguridad	Objetivo de Control	Políticas
10	A	Se debe garantizar que los certificados digitales utilizados se cargan desde los dispositivos criptográficos seguros conectados.	Hace cumplir políticas: 16, 88
11	A	Se debe validar que el uso del certificado digital cumple con los requisitos establecidos en la sección 1.4.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013).	Hace cumplir políticas: 17, 43, 89
12	A	Las rutas 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: • CRL*:* el valor está contenido en el certificado, y dado por el campo *Punto de distribución del CRL*, como lo indica la sección 7.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013). • OCSP*:* el valor está contenido en el certificado, y dado por la primera posición del campo *Acceso a la información de a la autoridad*, como lo indica la sección 7.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013).	Hace cumplir políticas: 64, 65, 66, 67, 90, 91, 92, 93

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• Certificado de la CA emisora*:* el valor está contenido en el certificado, y dado por la segunda posición del campo *Acceso a la información de la autoridad*, como lo indica la sección 7.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* (Gobierno de Costa Rica, 2013). • Servicio de estampado de tiempo*:* el valor está definido en la sección 6.1 del *Estándar electrónico – Servicios Firma Digital en Internet* (SINPE, 2016).	
13	C	La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro debe cumplir al menos con los siguientes requisitos: • Cuando las credenciales deban ser introducidas por el usuario, el campo de texto destinado para ese fin debe enmascarar todos los caracteres, sustituyéndolos por algún otro símbolo, por ejemplo, un asterisco (*). • Las credenciales no deben, bajo ninguna circunstancia, ser almacenadas en bitácoras, ni mostradas al usuario durante su interacción con la aplicación.	Hace cumplir políticas: 18, 94
14	C	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:	Hace cumplir políticas: 19, 95

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• 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.	
15	C	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: *Cuando el almacenamiento en caché está prohibido* • La aplicación debe implementarse de manera tal que las credenciales no sean almacenadas en cualquier tipo de memoria caché. • Cuando aplique, se debe desactivar el almacenamiento en caché de las credenciales a nivel de navegador de Internet. • Cuando aplique, se debe desactivar el almacenamiento en caché de las credenciales a nivel de sistema operativo. *Cuando el almacenamiento en caché es requerido*	Hace cumplir políticas: 20, 96

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• 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: ▪ 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: ▪ 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. • Las bitácoras generadas deben almacenarse como se indica a continuación: ▪ 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.	

No.	Servicio de seguridad	Objetivo de Control	Políticas
		▪ 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: ▪ 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.	

No.	Servicio de seguridad	Objetivo de Control	Políticas
16	C	Para que la entrega del documento electrónico firmado sea posible, se debe satisfacer al menos un control de autorización.	Hace cumplir políticas: 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.	Hace cumplir políticas: 22, 44, 69, 97
18	C	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.	Hace cumplir políticas: 24, 46, 70, 98
19	C	La prevención del despliegue de datos que revelan detalles acerca de la configuración e implementación del sistema debe cumplir al menos con los siguientes requisitos: • Ningún tipo de información sensible debe mostrarse a través de mensajes de error, incluyendo, pero no limitándose a: detalles del sistema, identificadores e información de cuentas. • Se debe usar manejadores de errores que no despliegan información de depuración, ni *stack traces*.	Hace cumplir políticas: 25, 47, 71, 99

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• 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.	
20		Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, *malware* y cualquier otro tipo de *software* malicioso que facilite la divulgación no autorizada de datos, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final* Se debe validar la existencia de un procedimiento periódico, 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: • Nombre del responsable de ejecutar el procedimiento. • Fecha y hora en la que se ejecuta el procedimiento.	Hace cumplir políticas: ~~18~~, 20, 23, 45, 94, 96

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• Identificador de la máquina. • Herramienta utilizada para ejecutar el procedimiento. • Lista de archivos analizados. • Resultado del análisis. *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final* Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique: • 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.	
21	NR	Se debe validar que los algoritmos de *hash* utilizados son seguros, y tienen una efectividad igual o superior a SHA-2, y rechazar los demás.	Hace cumplir políticas: 26, 49, 100
22	NR	La validación de la vigencia del certificado debe cumplir con los siguientes requisitos: • Se debe verificar que el certificado se encuentra activo, es decir, que no ha expirado ni ha sido revocado o suspendido.	Hace cumplir políticas: 27, 48, 101

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• 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.	
23	NR	La visualización del documento electrónico debe utilizar un método que cumpla con el principio WYSIWYS.	Hace cumplir política 28
24	NR	La captura de la manifestación de la voluntad del usuario debe cumplir con los siguientes requisitos: • 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.	Hace cumplir política 29
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 *Siguiente actualización*.	Hace cumplir políticas: 72, 102

No.	Servicio de seguridad	Objetivo de Control	Políticas
26	NR	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.	Hace cumplir políticas: 73, 103

9.2.6. Lista de observaciones de la evaluación

La siguiente tabla contiene las observaciones relevantes identificadas durante el proceso de evaluación de la aplicación con la *Guía de implementación*.

Tabla 32. *Lista de observaciones de la evaluación*

No.	Observaciones
1	Validaciones implementadas: *Cuando la entrada es texto* • Se validan las entradas de texto que deben tener formatos específicos. Por ejemplo, el identificador de OID debe contener sólo caracteres alfabéticos y el caracter '-'. Esta validación se realiza en la capa de negocios de la aplicación prototipo. • Longitud de datos es restringida desde la capa de datos. Esta validación se ejecuta al momento de realizar una solicitud de OID, por lo tanto, el documento que se va a firmar de la solicitud realizada, por defecto ya contendrá los datos validados. • Formatos de fecha y correos electrónicos o valores numéricos, tienen doble validación, primero desde la capa de presentación de la aplicación, y seguidamente en la capa de negocios.

	• Todas las entradas ingresadas por el usuario que van a la base de datos son validadas en formato y, además, son enviadas a través de sentencias parametrizadas (*prepared statements*), y no mediante la concatenación de hileras de caracteres. *Cuando la entrada es un archivo* • Se valida que el archivo tenga un formato permitido. Validando su extensión y contenido. La aplicación prototipo únicamente acepta archivos de tipo XML. • Se valida que el formato del XML se correcto, antes de procesarlo. • El tamaño que archivo no exceda de los 20MB. Variable podría ser cambiada en el código de la aplicación según sea necesario. • Validar que el archivo no contenga, código malicioso, virus o *malware*: ▪ Creación de firma digital y sello electrónico: para este caso el archivo a firmar es generado por la misma aplicación con datos ya validados, por lo tanto, no contendrá código malicioso, virus, *malware*, etc.
2	El archivo que se va a firmar es generado por la misma aplicación con datos ya validados, por lo tanto, no contendrá código malicioso, virus, *malware*, etc.

3	El formato del documento firmado en formato simple corresponde a **XMLDsig**. Dicho formato es manejado por el servicio `getDataToSign` de DSS. Ejemplo del documento resultado que provee el servicio:
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">`

	<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" /> <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /> <ds:Reference Id="r-id-1" Type="http://www.w3.org/2000/09/xmldsig#Object" URI="#o-id-1"> <ds:Transforms> <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#base64" /> </ds:Transforms> <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /> <ds:DigestValue>UsEX/yTsRdojX/esreNbf1LZOx79RxJuupTSMCpC14I=</ds:DigestValue> </ds:Reference> <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-id-2243c802fbeba3536823cafa272c5f5b"> <ds:Transforms> <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" /> </ds:Transforms> <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /> <ds:DigestValue>idVjIgRXNmgcNIiiG4WGcM1Zbz6S0q8Enc53cf5WQ9s=</ds:DigestValue> </ds:Reference> </ds:SignedInfo>
4	La política no aplica para el contexto de desarrollo de la aplicación. Sin embargo, debe ser considerada al momento de su implementación en un servidor tanto para la aplicación OID como para los servicios REST de DSS. Para la transmisión de datos, se debe utilizar algún protocolo que proporcione cifrado de datos, con una efectividad igual o superior a la ofrecida por TLS 1.0. Por ejemplo, HTTPS.
5	La política no aplica para el contexto de desarrollo de la aplicación. Sin embargo, debe ser considerada al momento de su implementación en un servidor tanto para la aplicación OID como para los servicios REST de DSS. Se deben de cumplir los objetivos de control número **4** en la sección **9.2.5**.

6	Esta política aplica parcialmente. Para el caso de las librerías a terceros, la aplicación desarrollada efectivamente utiliza las últimas versiones. Sin embargo, para el resto de criterios mencionados para la validación del software complementario no aplican en el contexto de desarrollo de la aplicación prototipo, pero deben ser consideradas al momento de su implementación en un servidor.
7	Esta política si se cumple porque ya existe el mecanismo de autenticación en el dispositivo criptográfico para las tarjetas inteligentes que se utilizan dentro de SNCD. Las cuales utiliza el mecanismo de autenticación de PIN el cual es generado y debe ser resguardado únicamente por la persona dueña de la firma.
8	Los certificados digitales generados por SNCD ya cumplen con los requisitos establecidos en la sección 7.1 de la *"Política de certificados para la jerarquía nacional de certificadores registrados"*. Adicionalmente el módulo de DSS también valida dichos formatos.
9	Los certificados digitales siempre son extraídos por la aplicación de los dispositivos criptográficos seguros conectados.
10	El uso del certificado digital dentro de la aplicación prototipo está en acuerdo con los requisitos establecidos en la sección 1.4.1 de la "Política de certificados para la jerarquía nacional de certificadores registrados".
11	Para el objetivo de control número 13: La protección de la confidencialidad de las credenciales de autenticación en el dispositivo criptográfico seguro cumplen con los siguientes requisitos:

	• Cuando las credenciales son introducidas por el usuario, el campo de texto destinado para ese fin enmascara todos los caracteres, sustituyéndolos por un asterisco (*). • Las credenciales no son, bajo ninguna circunstancia almacenadas en bitácoras, ni mostradas al usuario durante su interacción con la aplicación. Para el objetivo de control número 20: Para la aplicación desarrollada en esta investigación, el componente que se conecta con el dispositivo lector de tarjetas se encuentra instalado en la máquina del usuario final, por lo tanto: Se agrega documentación, entregada por el proveedor del software al usuario final, en la que indica: • 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.
12	El documento firmado es entregado solamente a la persona que firma y está autenticada en ese momento en la aplicación.
13	Esta política no aplica en el contexto de la aplicación prototipo desarrollada. Sin embargo, este control debe ser considerado al momento de su implementación en un servidor.

14	El componente encargado de la criptografía es el módulo de DSS, el cual soporta múltiples algoritmos de encripción. Sin embargo, para la aplicación desarrollada se selecciona el uso de SHA256.
15	El componente encargado de cumplir con esta política es el módulo de DSS, el cual tiene el parámetro `signWithExpiredCertificate` para activar estas validaciones, las cuales son ejecutadas por medio de CRLs y OCSP según el estándar europeo. La aplicación prototipo utiliza este parámetro activado, para que garantice que la firma se realice solo con certificados que no han expirado.
16	La validación de los certificados digitales utilizados para firmar documentos forma parte del estándar europeo que implementa el módulo de DSS. Por lo consiguiente, se cumple con esta política en el módulo DSS que hace uso de CRLs y OCSP.
17	Los servicios de CRLs, OCSP y estampa de tiempo que se encontraron dentro de los certificados utilizan el protocolo HTTP, el cual no es seguro. Por lo tanto, la información viaja en texto plano y no se encontró durante esta investigación ningún servicio proveído con HTTPS. Esto es un riesgo que se da por un tercero y esta fuera del alcance de este proyecto de investigación.
18	Al momento de autenticar al usuario en la aplicación, se guarda en la sesión encriptada del servidor información del certificado del usuario autenticado, para luego utilizarlos como validación cuando el usuario solicite realizar una firma digital dentro del sitio web.

19	Para hacer cumplir esta política requerirá el desarrollo de un módulo de antivirus para poder verificar que los documentos que ingresan en el sistema están libres de virus, *malware* o código malicioso, u obtener un servicio o software de antivirus para realizar el escaneo de estos documentos, dicho módulo queda para trabajo futuro de esta investigación.
20	El módulo e DSS cuenta con la funcionalidad para validación de los certificados dentro de un *Trusted Lists*. Sin embargo, dentro del SNCD aún no se cuenta con una lista como esta. Por lo que en la documentación del gobierno se recomienda instalar los certificados de la jerarquía en la máquina local. Por lo tanto, para poder realizar esta validación, se desarrolló dentro de la librería de DSS un módulo que realiza dicha validación desde el almacén de certificados de la máquina local.
21	El objetivo de seguridad correspondiente indica que se debe obtener la dirección de la TSA desde un recurso que ya no esta disponible, por esta razón no se pudo cumplir con la política.
22	El módulo de DSS realiza la función de verificar que la CRL este vigente revisando el campo llamado *Siguiente actualización*.
23	El módulo de DSS no almacena en caché información de consultas de OCSP anteriores. Siempre realiza al proveedor del servicio OCSP solicitudes frescas cada vez necesita verificar la vigencia de un certificado.

9.3. Apéndice 3

9.3.1. Lista de políticas con la misma redacción

A continuación, se muestra la lista de políticas encontradas en la *Guía de implementación* con la misma redacción:

Tabla 33. *Lista de políticas con la misma redacción*

No. Políticas	Política
72, 102	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.
12, 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.
11, 41, 63, 84	El software complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, frameworks, plug-ins y drivers, debe tener instaladas las actualizaciones de seguridad más recientes.
64, 90	La ruta 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.
93, 67	La ruta requerida para obtener los tokens de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.

No. Políticas	Política
66, 92	Las rutas 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.
25, 47, 71, 99	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.
19, 95	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no puedan ser obtenidas utilizando mecanismos de fuerza bruta.
54, 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.
24, 46, 70, 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.

9.4. Apéndice 4

9.4.1. Lista de políticas agrupadas por redacción y contexto similar

A continuación, se muestra la lista de políticas encontradas en la *Guía de implementación* con la misma redacción y con contexto similar que podrían ser reformuladas para ser compactadas y finalmente reducir el tamaño final de la guía:

Tabla 34. *Lista de políticas agrupadas por redacción y contexto similar*

Nuevo No. Política	No. Política	Política	Objetivo de control
1	51	Se debe validar que el documento electrónico cuyo formato se convertirá, no contiene código oculto (por ejemplo, macros) o malicioso.	1
	2	Se debe validar que el documento electrónico que se va a firmar no contiene código oculto o malicioso.	1
	31	Se debe validar que el documento electrónico cuyas firmas se van a verificar, no contiene código oculto (por ejemplo, macros) o malicioso.	1
2	100	El resumen de los datos de autenticación que se van a firmar debe calcularse utilizando algoritmos *hash* seguros.	21
	49	El resumen del documento electrónico cuyas firmas se van a verificar debe calcularse utilizando algoritmos *hash* seguros.	21

Nuevo No. Política	No. Política	Política	Objetivo de control
	26	El resumen del documento electrónico que se va a firmar debe calcularse utilizando algoritmos *hash* seguros.	21
3	73	Se debe validar que las respuestas OCSP no sean reutilizables.	26
	103	Se debe verificar que las respuestas OCSP no sean reutilizables.	26
4	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.	15, 20
	96	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no sean almacenadas en caché para su uso posterior.	15, 20
	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.	13, 20
	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.	13, 20
5	43	Se debe validar el uso correcto de los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar.	11

Nuevo No. Política	No. Política	Política	Objetivo de control
	89	Se debe validar el uso correcto del certificado que se utilizará en el proceso de autenticación.	11
	17	Se debe validar el uso correcto del certificado que se utilizará en el proceso de firma.	11
6	88	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación se encuentra almacenado en un dispositivo criptográfico seguro.	10
	16	Se debe validar que el certificado digital que se utilizará en el proceso de firma se encuentra almacenado en un dispositivo criptográfico seguro.	10
7	21	Se debe validar que el documento electrónico firmado resultante no se entregue a usuarios no autorizados.	16
	68	Se debe validar que el documento electrónico resultante, firmado en formato avanzado, no se entregue a usuarios no autorizados.	16
8	101	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación se encuentra vigente.	22
	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.	22
	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.	22

Nuevo No. Política	No. Política	Política	Objetivo de control
9	86	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de autenticación es válido.	7
	13	Se debe verificar que el perfil del certificado digital que se utilizará en el proceso de firma es válido.	7
10	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.	1
	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.	1
11	87	Se debe validar que el certificado digital que se utilizará en el proceso de autenticación pertenece a la jerarquía nacional de certificadores registrados.	8
	14	Se debe validar que el certificado digital que se utilizará en el proceso de firma pertenece a la jerarquía nacional de certificadores registrados.	8
	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.	8
12	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.	2

Nuevo No. Política	No. Política	Política	Objetivo de control
13	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.	1, 2
14	3	Se debe validar que los documentos electrónicos resultantes, firmados en formato simple, puedan convertirse posteriormente a formatos avanzados válidos.	2
15	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.	9
16	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.	24
17	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.	23
18	72	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	25
	102	Antes de utilizar una CRL, se debe validar que ésta se encuentra vigente.	25
19	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.	6

Nuevo No. Política	No. Política	Política	Objetivo de control
	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.	6
20	11	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5
	41	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5
	63	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5
	84	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5
21	64	La ruta 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

Nuevo No. Política	No. Política	Política	Objetivo de control
	90	La ruta 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
22	65	La ruta 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.	12
	91	La ruta 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.	12
23	93	La ruta requerida para obtener los *tokens* de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.	12
	67	La ruta requerida para obtener los *tokens* de estampado de tiempo debe ser almacenada por la aplicación, y su valor debe ser el indicado por la CA correspondiente.	12
24	66	Las rutas 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.	12

Nuevo No. Política	No. Política	Política	Objetivo de control
	92	Las rutas 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.	12
25	25	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19
	47	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19
	71	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19
	99	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19
26	19	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no puedan ser obtenidas utilizando mecanismos de fuerza bruta.	14
	95	Se debe proteger las credenciales de autenticación del dispositivo criptográfico seguro, de manera que no puedan ser obtenidas utilizando mecanismos de fuerza bruta.	14
27	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.	3

Nuevo No. Política	No. Política	Política	Objetivo de control
	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.	3
28	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.	18
	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.	18
	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.	18
	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.	18
29	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.	3
	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.	3
	44	Se debe proteger el documento electrónico cuyas firmas se van a verificar, así como sus representaciones derivadas (resúmenes cifrados extraídos, documento electrónico original,	17

Nuevo No. Política	No. Política	Política	Objetivo de control
		resumen del documento electrónico original, resúmenes descifrados), mientras se transmiten por red, de manera que no puedan ser revelados a usuarios no autorizados.	
	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.	3
	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.	3
	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.	17
	57	Se debe proteger el documento electrónico cuyo formato se convertirá, así como sus representaciones intermedias (documento electrónico firmado en formato avanzado), mientras se transmite por una red, de manera que no pueda ser modificado por usuarios no autorizados.	3

Nuevo No. Política	No. Política	Política	Objetivo de control
	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.	17
	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.	3
	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.	3
	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.	3

Nuevo No. Política	No. Política	Política	Objetivo de control
	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.	3
	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.	3
	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.	3
	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.	3
	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.	3
	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.	3

Nuevo No. Política	No. Política	Política	Objetivo de control
	55	Se debe proteger los *tokens* de estampado de tiempo, mientras se transmiten por red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	3
	77	Se debe proteger los *tokens* de estampado de tiempo, mientras se transmiten por una red hacia la aplicación, de manera que no puedan ser modificados por usuarios no autorizados.	3
	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.	3
	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.	3
	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.	3
	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.	3

Nuevo No. Política	No. Política	Política	Objetivo de control
	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.	3
	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.	3
	97	Se debe proteger los datos generados aleatoriamente para el proceso de autenticación, así como sus representaciones derivadas (resumen de los datos aleatorios y resumen cifrado de los datos aleatorios), mientras se transmiten por una red, de manera que no sean revelados a usuarios no autorizados.	17
	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.	3
	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.	3

Nuevo No. Política	No. Política	Política	Objetivo de control
30	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.	4
	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.	4
	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.	20
	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.	4
	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.	4
	62	Se debe proteger los atributos obtenidos para la creación del documento electrónico en formato avanzado, mientras transita por la memoria local, de manera que no puedan ser modificados por usuarios no autorizados.	4
	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.	4

Nuevo No. Política	No. Política	Política	Objetivo de control
	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.	20
	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.	4
	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.	4
	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.	4
	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.	4