Universidad Internacional San Isidro Labrador

Escuela de Ingeniería en Sistemas

Análisis sobre las implicaciones de la promulgación de tecnologías e innovación web como parte del desarrollo progresivo del E-Government bajo el marco jurídico y caso Costarricense con énfasis en aprendizajes y hallazgos en el periodo de crisis sanitaria del COVID-19.

Gustavo Villanueva Sandi. Carné: 1-1642-0797

Seminario de graduación para optar por el grado de Licenciatura en Ingeniería en Sistemas.

San Isidro del General, Pérez Zeledón, 2024

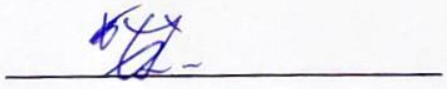
Declaración Jurada

Por este medio yo, Gustavo Villanueva Sandi portador de cédula de identidad número 1-1642-0797, estudiante de la Universidad Internacional San Isidro Labrador de la carrera de Licenciatura de Ingeniería en Sistemas, declaro bajo fe de juramento y conscientes de las responsabilidades penales de este acto, que soy el autor intelectual del proyecto de graduación titulado:

Análisis sobre las implicaciones de la promulgación de tecnologías e innovación web como parte del desarrollo progresivo del E-Government bajo el marco jurídico y caso Costarricense con énfasis en aprendizajes y hallazgos en el periodo de crisis sanitaria del COVID-19.

Juro que este trabajo de tesis es original y que respeto las leyes de los derechos de autor, por lo que declaro a la Universidad Internacional San Isidro Labrador, libre de cualquier responsabilidad en caso de que mi declaración sea falsa.

Brindada en San Isidro, Pérez Zeledón, San José, Costa Rica el día 10 de noviembre del año 2024.



Ing. Gustavo Villanueva Sandi

Céd 1-1642-0797

Tribunal Examinador

Seminario de graduación de Licenciatura en Ingeniería de Sistemas, presentado en diciembre del 2024, en la Universidad Internacional San Isidro Labrador ante el siguiente tribunal examinador.

Lic. Rudy Rodríguez Acuña

Director de La Escuela de Ingeniería en Sistemas

Lic. Eric Corella Solís

Profesor Tutor

MSc. Michael Corrales Oviedo

Profesor Lector

Contenidos

1. **Introducción**

En la actualidad, la transformación digital se ha convertido en un eje fundamental para el desarrollo de procesos de eficiencia administrativa y la mejora continua en la prestación de servicios públicos. Entiéndase por E-Government no solo como el proceso de digitalización de trámites, sino como la implementación de un entorno que facilite la interoperabilidad en tramitología y procesos burocráticos, garantizando la eficiencia, legalidad, seguridad y accesibilidad por la vía digital de ventanilla de servicios. Dentro de este concepto la Firma Digital juega un papel clave como columna vertebral en los todos los requerimientos técnicos de seguridad necesarios para blindar los sistemas involucrados ante amenazas maliciosas, y de esta manera cumplir con las diferentes normativas y estándares internacionales.

Este proyecto propone un análisis comparativo entre Costa Rica y Estonia, dos países que han implementado tecnologías de Firma Digital con enfoques y resultados diferentes, pero que comparten similitudes técnicas significativas.

Dicho análisis pretende enfocar la atención del estudio en las circunstancias vividas durante y después de la crisis sanitaria del COVID-19, un periodo de significativa importancia debido al papel que jugaron las iniciativas de E-Government en la correcta toma de decisiones y el óptimo manejo de la crisis sanitaria, dicha importancia se ve reflejada por la cantidad de información disponible y la transparencia de los datos institucionales durante dicho periodo, particularidad clave para favorecer la tarea del estudio comparativo.

De dicho análisis derivan 2 preguntas que deben ser abordadas en pro de cumplir con los objetivos de la investigación y este proyecto:

¿Se puede determinar mediante un análisis comparativo si existen o no limitantes meramente técnicas que hayan influido en las particularidades del modelo costarricense frente a su contraparte del modelo estonio?

¿Inspirándose en el modelo estonio, qué propuestas técnicas podrían dar cabida a convertirse en un aporte significativo sobre el esfuerzo conjunto en la implementación de tecnologías de E-Government en Costa Rica?

Este enfoque permitiría buscar la manera de plantear soluciones para fortalecer el marco tecnológico y normativo de Costa Rica, contribuyendo un grano más de arena en el progreso del país hacia un modelo de E-Government más eficiente y accesible.

1.1 Justificación

La implementación de herramientas web estandarizadas y de código abierto juega un papel clave en adopción de la Firma Digital como método de transformación digitalizadora de servicios y demás aspectos fundamentales en el desarrollo del E-Government. Basándonos en casos exitosos de E-Government como el de Estonia; se pueden identificar varias recomendaciones a considerar a la hora de evaluar las esfuerzos que se ha venido llevando a cabo en Costa Rica para mejorar los índices de adopción y cobertura de dichas tecnologías de E-Government.

La digitalización de servicios mediante el E-Government no solo tiene beneficios para los ciudadanos y la administración pública, sino también para la industria de servicios, especialmente la industria de tecnologías de información.

Este análisis permitirá facilitar una mejor comprensión sobre el impacto económico y social en la implementación de soluciones de E-Government, usando como referencia el caso concreto de crisis social vivido durante la afectación del COVID-19 a la industria y sector servicios del país, eventos que llevaron a la administración pública a enfocar su atención en la digitalización de servicios; expertos y autoridades colaborando en la búsqueda de soluciones para poder salvaguardar el correcto funcionamiento de ciertos sectores económicos del sector público y privado mediante el uso de medios digitales resilientes a las estrictas restricciones sanitarias, así como restricciones de movilidad y presencialidad impuestas durante la pandemia.

Este trabajo busca hacer conciencia acerca de la importancia de dar prioridad al progreso tecnológico que permita construir una economía más resiliente y operativamente capaz de lidiar con eventuales momentos de crisis y restricciones que afecten la movilidad económica.

Por último, validar la viabilidad técnica de una implementación en código abierto de un middleware web estandarizado (que pueda ser compartido y masificado fácilmente) implementando el uso de Firma Digital como medio de autenticación, representa una oportunidad para incentivar el desarrollo de un entorno de trabajo capaz de ampliar los márgenes de cooperatividad y mejora continua, en vista de fortalecer los índices de adopción y cobertura de dichas tecnologías de E-Government, para esto es esencial la implementación de código abierto, capaz de permitirle a pequeñas entidades y agentes

económicos los medios para acceder de forma flexible y transparente al desarrollo e innovación sobre dichas plataformas digitales. Utilizar tecnología estandarizada permite facilitar muchos de los requerimientos más básicos y genéricos del mercado en una única solución integral, un enfoque más orientado a la eficiencia operativa, reutilización de recursos y a ampliar índices de adopción. Sin este tipo de iniciativas toda pyme y pequeña empresa se vería en la necesidad de contratar a agentes especializados para desarrollar una solución entera desde cero, con una arquitectura hecha a la medida, algo que no necesariamente está al alcance de las organizaciones más pequeñas y limitadas de recursos. El objetivo final siempre es facilitar la ruta de implementación de las tecnologías de E-Government a la vez que se reducen riesgos y se facilita la aceptación con del usuario final mediante la reutilización de componentes de software con las cuales se van a terminar familiarizando el usuario final.

Validando cada uno de los puntos anteriores, podríamos llegar a identificar márgenes de mejora, recomendaciones y demás valor agregado que este proyecto pueda generar, buscando poder realizar un aporte positivo que sume al impacto esperado de este y demás proyectos recurrentes que se preocupan por los mejorar el proceso de expansión del E-Government.

1.2 Objetivos:

1.2.1 Objetivo general:

Determinar la viabilidad e importancia de promulgar tecnologías web estándar para el desarrollo de servicios digitales basado en la jurisdicción de E-Government del estado de Costa Rica acorde al contexto de adopción y cobertura de la Firma Digital como principal tecnología de E-Government durante el periodo de restricción social del COVID-19 (2019-2021).

1.2.2 Objetivos específicos:

- Determinar el estado de avance actual en la adopción de la Firma Digital como principal tecnología de E-Government y digitalización de servicios públicos en Costa Rica.
- Investigar acerca del contexto de adopción y uso de la Firma Digital como tecnología de E-Government en Estonia con énfasis en los antecedentes sobre la implementación de Firma Digital y tecnologías Web.
- Analizar de forma comparativa el comportamiento de adopción y cobertura de la Firma Digital durante y después del periodo de COVID-19 (2019~2021) para los diferentes escenarios de Costa Rica y Estonia.
- Identificar tecnologías web estándar ya existentes que cumplan como proveedores de servicios de autenticación y que puedan integrarse con la Firma Digital apegándose a las necesidades de la jurisdicción de Costa Rica.

- Explorar la viabilidad técnica de una implementación de código abierto; de un middleware web estandarizado de autenticación mediante el uso de Firma Digital según los requerimientos de la legislación Costarricense.

2. Marco Metodológico

En esa sección vamos determinar y esclarecer como va a estar compuesto el documento en torno al cumplimiento de los objetivos propuestos.

2.1 Enfoque metodológico

El proyecto se divide en dos fases:

Análisis de datos e investigación comparativa: Esta fase empleará un enfoque mixto que combinará métodos cualitativos y cuantitativos para la recolección y análisis. La investigación será de carácter comparativa, utilizando el caso de Costa Rica y el ejemplo de Estonia, un país con alto nivel de madurez en la implementación de Firma Digital, el objetivo será obtener información contextual sobre la adopción de tecnologías de E-Government para ambos casos y compararlos. La expectativa de esta primera fase reside en demostrar positivamente la importancia de cumplir con el ultimo objetivo de este proyecto académico que es el de demostrar la viabilidad técnica de una solución de software que se adopte a las especificaciones de dicho objetivo.

Desarrollo Exploratorio: En esta fase, se realizará un desarrollo experimental, una Prueba de Concepto que aporte el conocimiento necesario para avanzar en el diseño de un prototipo de software que cumpla con los requerimientos técnicos del último objetivo de este proyecto. Esto permitirá explorar la viabilidad técnica de un middleware de autenticación que integre la cohesión entre tecnologías web estándar y Firma Digital.

2.2 Diseño de la investigación

La primera fase es la principal investigación del proyecto académico y esta conlleva una investigación comparativa de datos a partir de 2 casos de estudio de escenarios bien diferenciados (Costa Rica y Estonia).

Las diferencias encontradas deben ser estudiadas y analizadas con el objetivo de poder concluir el impacto de dichas diferencias así como discrepancias en términos de políticas públicas que contribuyeron de forma directa o indirecta al resultado de dichas diferencias.

La fase de desarrollo exploratorio implica también una investigación de tipo exploratoria que permitirá identificar y analizar las diferentes tecnologías que se ven involucradas en el funcionamiento de la Firma Digital y como estas entran en cohesión con las tecnologías de autenticación Web Estándar ampliamente utilizadas en internet, analizando y probando de las diferentes opciones disponibles aquellas tecnologías que puedan cumplir con los requerimientos técnicos necesarios para cumplir con una implementación formal de Firma Digital que cumpla con la normativa costarricense.

2.2.1 Justificación del Diseño

Este diseño responde a la necesidad de recopilar datos que permitan realizar un análisis exhaustivo sobre la adopción y evolución de la Firma Digital en Costa Rica y compararlo al caso Estonio. El objetivo es poder determinar el grado de importancia en la diferencias del enfoque en términos de políticas públicas para el caso de los 2 países en estudio.

Además, la investigación exploratoria de tecnologías Web estándar permitirá determinar la viabilidad practica de optar por un enfoque más activo de políticas públicas, optando

por un modelo de expansión más agresivo y similar al Estonio. Pudiendo esclarecer así que la ausencia de este enfoque en jurisdicción costarricense no se debe necesariamente a un tema de limitaciones técnicas o faltantes técnicos.

2.3 Técnicas de recolección de datos

La principal técnica de recolección de datos aplicada a lo largo de este proyecto es la Revisión Documental, la cual para este caso se enfocara en el entendimiento de los manuales técnicos, así como la investigación, análisis e interpretación de los datos circunstanciales del contexto socioeconómico que influyan de forma directa en las conclusiones y resoluciones de los objetivos de este documento.

2.3.1 Alcance de la investigación

La investigación abarca principalmente a las Instituciones Públicas y el sector público de las jurisdicciones de Costa Rica y Estonia, datos oficiales de autoridades pertinentes, así como información relevante de otros estudios académicos realizados y debidamente referenciados. En caso de existir los datos suficientes, se podría evaluar información sobre la relación con otros agentes jurídicos y económicos que interactúen con las instituciones y el entorno de E-Government de ambas jurisdicciones (Autoridades certificadoras).

La muestra se enfocara especialmente en datos encontrados dentro del periodo de aislamiento social por la crisis del COVID19 dentro del periodo 2019-2021.

2.3.2 Fuentes de información

Las fuentes primarias de la investigación son principalmente autoridades pertinentes del ámbito de la tecnología informática (especialmente aquellas que estén involucradas en el desarrollo e implementación en tecnologías de Firma Digital), así como instituciones públicas y reguladores de los gobiernos de Estonia y Costa Rica que puedan proveer información veraz acerca de los datos de cobertura y alcance de Firma Digital y así como contexto de selección de herramientas de E-Government (tecnologías) para cada una de las jurisdicciones correspondientes.

2.4 Técnicas de análisis de datos.

Análisis Cuantitativo: Los datos recolectados a través de la investigación y demás estadísticas se analizarán mediante herramientas de análisis descriptivo (frecuencias, porcentajes) y análisis de tendencia para observar cambios en la adopción de la Firma Digital antes, durante y después del periodo de COVID-19 para cada uno de los escenarios en investigación.

Análisis Comparativo: Se hará una comparación del caso costarricense con el caso estonio para identificar factores comunes y diferenciadores que puedan determinar la importancia de adoptar un enfoque similar al estonio así como justificar la preocupación de este proyecto por comprobar la viabilidad de implementar nuevas tecnologías web de vanguardia a la arquitectura de E-Government en Costa Rica.

2.5 Diseño del desarrollo practico.

Con el objetivo de determinar viabilidad técnica en la implementación de tecnologías Web de código abierto como parte del marco de trabajo de la Firma Digital en Costa Rica, se

realizara una propuesta técnica de diseño que cumpla con los estándares requeridos y que determine su funcionalidad basados en antecedentes técnicos de implementaciones homologas o en otras jurisdicciones.

2.5.1 Justificación de la propuesta experimental.

Poder determinar la viabilidad de desarrollar software basado en tecnologías web estándar de código abierto como medio de autenticación implementando el uso de Firma Digital. El desarrollo de una propuesta formal permite determinar si existen limitaciones para las tecnologías de E-Government a nivel de normativa administrativa, o si existen limitaciones técnicas que impidan el avance incremental de dichas tecnologías en pro de mejorar su adopción y cobertura en la jurisdicción costarricense.

2.6 Análisis de resultados

El análisis de resultados de la investigación debe ser determinista en su capacidad de comprobar si las diferencias en la adopción de tecnologías web estándar, software libre y Firma Digital entre Costa Rica y Estonia responden concretamente a factores técnicos o factores administrativos específicos del contexto en madurez de políticas de E-Government. Es así como; destacar las diferencias existentes entre el escenario estonio y costarricense y su impacto en la efectividad y cobertura de los servicios E-Government es un tema crucial y concerniente a los objetivos de este proyecto. Los resultados concluyentes deben valorar la importancia de considerar tanto las especificaciones técnicas como las condiciones regulatorias y de gobernanza digital promovidas por el estado Costarricense para poder proporcionar recomendaciones claras y de valor.

3. Marco teórico

Antes de proceder con el avance de la investigación realizada en este proyecto académico, es importante comprender el contexto de ciertos términos técnicos en los cuales vamos a hacer énfasis a lo largo de análisis y desarrollo de los objetivos de la investigación incluida en este documento.

3.1 E-Government

Se refiere a las tendencias en el uso de tecnologías de la información para optimizar los procesos de burocracia administrativa, agilizar la gobernanza y la participación ciudadana, aumentar la cobertura y accesibilidad de las ventanillas digitales de servicios, facilitar la participación ciudadana en la económica digital, promover la transparencia institucional y promover la cooperación público-privada en pro de la mejora en la calidad de la digitalización de servicios.

En términos generales, el E-Government es impulsado por factores principales que son determinantes para poder definir el grado de éxito y avance en términos de adopción y funcionabilidad, podemos mencionar algunos como:

- Infraestructura Tecnológica: Esto se refiere no solo a la infraestructura física, ni a la potencia de cómputo instalada, sino también a los esfuerzos conjuntos para lograr un mejor desempeño de los sistemas y servicios digitales públicos existentes. Hablamos de términos como la Interoperabilidad de los sistemas, accesibilidad tecnológica, simplificación de procesos, etc.
- Participación Ciudadana: Para que los ciudadanos y empleados públicos puedan aprovechar al máximo las herramientas y servicios de E-Government, es

fundamental centrarse en campañas y programas de alfabetización digital que busquen involucrar a los ciudadanos en los procesos de adopción, innovación, fiscalización y participación de los nuevos canales digitales de servicios.

- Seguridad y Privacidad de la Información: El aumento de la digitalización implica la gestión de grandes cantidades de datos personales y sensibles, por lo cual es crucial garantizar un entorno seguro con sus debidas medidas de ciberseguridad que implemente políticas de protección de datos, requerimientos técnicos de encriptación, auditorias de seguridad, concientización ciudadana, entre otros.

La promoción de los factores mencionados del E-Governance implican una mejora en la interacción de los ciudadanos y las empresas con el gobierno, induciendo mejoras en temas de transparencia, participación y eficiencia en el manejo de políticas y servicios públicos. El impacto consecuente en la económica es más perceptible en algunas industrias y sectores de la económica muy concretos, especialmente en aquellos que son fuertemente regulados por políticas públicas como: La industria financiera y bancaria, aseguradoras, sector salud, servicios públicos, telecomunicaciones, servicios en la nube, sector educación, sector transporte, entre otros. Además de mencionar la oportunidad de mejorar las capacidades técnicas y accesibilidad de los servicios de fiscalización tributaria, lo cual tendría un impacto indirecto en la competitividad de toda la economía afectando a empresas, pymes y contribuyentes autónomos.

3.2 Software y tecnologías de firma y autenticación segura.

3.2.1 Firma Digital

La Firma Digital son un conjunto de mecanismos criptográficos que permiten firmar documentos electrónicos de manera segura, garantizando la autenticidad, integridad y el no repudio de la información. Estas firmas digitales son legalmente equivalentes a las firmas manuscritas en aquellos países que reconozcan dichas tecnologías digitales en su jurisdicción legal, lo que las convierte en una herramienta clave para la validación de contratos, transacciones electrónicas y comunicaciones oficiales.

A diferencia de las firmas electrónicas simples que se utilizan en otros sectores o industrias donde la principal función es la de salvaguardar la integridad de la información en tránsito, las Firmas Digitales de uso legal se especializan en asegurar y salvaguardar el no repudio de la información.

Uno de los mayores beneficios de la Firma Digital es la capacidad de garantizar el no repudio, es decir, el firmante no puede negar haber firmado el documento digital. Esto se debe a la seguridad proporcionada por la encriptación asimétrica y el vínculo legal establecido entre el certificado digital utilizado con la identidad del firmante.

Para esto; la tecnología usada se basa en algoritmos criptográficos avanzados que utilizan un sistema de cifrado de clave pública (PKI) para proteger y validar la identidad del firmante y la integridad del documento. La Firma Digital no solo confirma que el firmante es quien dice ser, sino que también asegura que el documento no ha sido alterado después de haber sido firmado.

3.2.2 Encriptación Asimétrica

Es un método de cifrado que utiliza un par de claves: una clave pública y una clave privada. A diferencia de la encriptación simétrica (donde se utiliza una sola clave para cifrar y descifrar los datos) en la encriptación asimétrica se usan estas dos claves para realizar procesos de cómputo inversos (una simplemente puede encriptar y la otra desencriptar datos), estas claves están matemáticamente relacionadas pero son íntegramente distintas entre sí (haciendo prácticamente imposible poder relacionar una con la otra a simple vista o usando algún método básico de comparación), su única relación matemática está basada en cálculos de números complejos, los cuales están diseñados para suponer un reto técnico a nivel de capacidades de cómputo, haciendo poco práctico e inviable intentar derivar o calcular una clave a partir de la otra haciendo uso de métodos de “fuerza bruta” de cómputo.

La encriptación asimétrica presenta características que la hacen ideal para ciertas tareas y aplicaciones muy concretas, si bien a nivel de seguridad es una solución altamente confiable, presenta problemas técnicos a la hora de intentar procesar grandes cantidades de datos en sus algoritmos de encriptación, haciendo que sea poco viable su uso en comunicación intensiva con grandes volúmenes de datos (costos de cómputo y energéticos).

Debido a estas limitaciones técnicas, los usos más comunes de la encriptación asimétrica se pueden generalizar en 2 grandes categorías:

- Encriptación de secretos: Usualmente para salvaguardar la privacidad de contraseñas, huellas de autenticación, o para transmitir otros tipos de llaves secretas (usadas en otros

algoritmos de encriptación más eficientes o especializados) creando canales de comunicación privados y seguros para este fin. El objetivo acá siempre es intentar aprovechar la confiabilidad de la encriptación asimétrica sin comprometer la eficiencia y las capacidades de cómputo de los sistemas involucrados.

- Firma digital: El otro uso recurrente es la firma de documentos, usado para garantizar la integridad y la autenticidad de la información enviada entre un agente emisor y un agente receptor. En este caso la flexibilidad de la encriptación asimétrica es clave, ya que la firma digital requiere de que la llave publica del ente emisor sea de conocimiento público, de manera que cualquiera pueda validar la autenticidad de la información sin necesidad de conocer completamente el proceso utilizado y sin acceso a la llave privada utilizada para firmar inicialmente el documento. De esta forma cualquier persona con la clave pública puede verificar la autenticidad de la firma, pero no puede generar una firma válida sin la clave privada.

3.2.3 Encriptación RSA

Desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, es uno de los sistemas de cifrado asimétrico más conocidos y ampliamente utilizados. Se basa en la dificultad matemática de factorizar números enteros grandes, lo suficientemente grandes para suponer un reto técnico de realizar mediante los métodos de cómputo actuales, esta complejidad proporciona la base de su seguridad. El algoritmo RSA se utiliza tanto para el cifrado de datos como para la Firma Digital.

Sus características particulares lo han convertido en el algoritmo de uso común en muchas implementaciones y protocolos de comunicación ampliamente utilizados. Debido

a su alta confiabilidad y aceptación, RSA ha pasado a formar parte esencial de la columna vertebral de internet, siendo implementado en los protocolos TLS (Transport Layer Security) y en los sistemas de certificados de seguridad X.509.

Una forma simplificada de comprender el funcionamiento del algoritmo RSA se puede resumir como “buscar una versión matemáticamente simplificada para representar un cálculo complejo de números primos de gran magnitud”. Los números primos, por definición, suponen un reto técnico de computación en funciones aritméticas, ya que, conforme aumentan la cantidad de dígitos de un numero natural es más difícil poder validar si realmente ese número es (o no es) un numero primo, ya que la permutabilidad de posibles divisores también aumenta, lo que hace que el proceso de verificación sea exponencialmente complejo (y costoso) conforme aumenta la magnitud del número que se está validando.

El algoritmo RSA se aprovecha de estas características para poder generar pares de llaves criptográficas con factores matemáticamente inversos. La llave privada contiene un par de números primos previamente calculados así como un conjunto de variables calculadas a partir de dichos números primos (“factores de encriptación” utilizados en el proceso de criptografía) llamados “modulo” y “exponente”, mientras tanto la llave publica contiene únicamente su versión inversa de “modulo” y “exponente” (diferentes a los valores de la llave privada, aunque matemáticamente relacionados). Esto permite que la llave publica cumpla su función sin tener que llegar a conocer realmente cuales fueron los números primos que dieron origen al par de llaves asimétricas desde un principio. Para intentar calcular nuevamente la llave privada habría que conocer que números primos se utilizaron en el proceso de generación y dichos números únicamente existen

como parte del “secreto” de la llave privada. La complejidad de calculo que supone buscar (de entre un universo de permutaciones posibles) aquellos números primos iniciales (usados en el proceso de generación de las llaves asimétricas) es lo que mantiene al algoritmo RSA seguro y previene que atacantes insistan en la idea de romper la seguridad del algoritmo debido a la inviabilidad provocada por las limitaciones de cómputo de la actual generación tecnológica, sumado a los altos costos implicados en intentarlo.

3.2.4 Certificados X.509 y PKI

La seguridad digital de la era moderna de la computación y las redes sin fronteras (Internet) se basan principalmente en la Infraestructura de Clave Publica (Public Key Infraestructure ó PKI). PKI no es necesariamente un manual técnico, sino más bien un modelo de arquitectura donde se definen los roles y responsabilidades de todos los sujetos y sistemas involucrados en el proceso de creación, gestión, distribución y revocación de certificados digitales, certificados que posteriormente son utilizados para proporcionar un entorno seguro y resiliente para la autenticación y cifrado de datos dentro redes de comunicación descentralizadas.

X.509 es un estándar de arquitectura PKI cuyo objetivo era la autenticación, integridad y confidencialidad en redes de telecomunicaciones. Publicado inicialmente por el ITU-T (International Telecommunication Union) en 1988, X.509 define una serie de pautas y protocolos en la generación, composición y utilización de certificados digitales, generando así un entorno robusto de seguridad digital basado en el concepto de “cadena de confianza” (Chain of trust). Estas cualidades llevaron a X.509 a formar parte de TLS

(Transport Layer Security), el cual es el protocolo de encriptación más ampliamente utilizado en la seguridad de internet de actual generación.

Un certificado X.509 es un archivo digital que contiene información que permite verificar la identidad de una entidad en una red. Incluye una serie de campos de datos, entre los que destacan:

- Versión: Especifica la versión del certificado, permitiendo interoperabilidad.
- Número de Serie: Número único asignado por la Autoridad Certificadora (CA) para identificar el certificado.
- Algoritmo de Firma: Indica el algoritmo de Firma Digital utilizado para el certificado.
- Emisor (Issuer): ID o nombre de la Autoridad Certificadora que emitió el certificado.
- Validez: Define un período de tiempo en el que el certificado es válido, con una fecha de inicio y de fin.
- Sujeto (Subject): Nombre de la entidad a la cual pertenece el certificado (persona, dispositivo o dominio).
- Clave Pública del Sujeto: La clave pública de la llave asimétrica, utilizada para la autenticación y el cifrado.
- Extensiones de uso: Palabras clave utilizadas para definir las capacidades y limitaciones del certificado en cuestión.
- Firma Digital: Una firma generada por la Autoridad Certificadora, la cual garantiza la integridad y autenticidad del certificado.

La seguridad de los certificados X.509 depende de la confianza depositada en la Autoridad Certificadora (CA) que los emite. Si la clave privada de una CA es

comprometida, se podría comprometer la seguridad de cualquier certificado emitido por esta autoridad.

Debido a dichos riesgos de seguridad, el estándar X.509 define ciertas tareas y responsabilidades que deben cumplir cada una de las partes involucradas en la utilización de los certificados:

- Autoridad Certificadora (CA): Es la entidad encargada de firmar los nuevos certificados. La CA debe verificar la identidad de los solicitantes antes de emitir nuevos certificado así como salvaguardar la autenticidad de su cadena de confianza subsecuente. Deben recurrir a auditorías externas para validar la seguridad y confidencialidad de los certificados bajo su custodia.
- Autoridad de Registro (RA): Actúa como intermediaria entre los usuarios y la CA. La RA se encarga de recolectar y proveer los datos necesarios para validar la identidad de los usuarios y además funciona como una interfaz segura por la cual solicitar y distribuir los certificados con sus usuarios. Además es la entidad encargada de validar los procesos de revocación de certificados de forma oportuna para no comprometer la cadena de confianza.
- Sujeto: Es el usuario, la entidad (persona, organización o dispositivo) que solicita y posee el certificado y la clave privada incluida en él. El sujeto utiliza el certificado para identificarse y para encriptar o firmar datos bajo su nombre y autoría.
- Parte Confiante: Es la persona o sistema que confía en la Autoridad Certificadora y utiliza la clave pública de los certificados X.509 para verificar la autenticidad del sujeto o los sujetos con el cual se está comunicando.

Cuando una parte confinante necesita verificar la identidad del sujeto, solicita su certificado X.509 y verifica la Firma Digital de la CA utilizando la clave pública del certificado para realizar 2 validaciones:

- Autenticidad: Verifica que la Firma Digital de la CA sea válida, asegurándose de que el certificado fue emitido por una autoridad confiable.
- Revocación: Consulta una Lista de Revocación de Certificados (CRL) o un Protocolo de Estado de Certificado en Línea (OCSP) para confirmar que el certificado aún es confiable y no ha sido revocado.

Mediante las disposiciones de operación dadas por X.509, se puede generar un entorno donde las CA y RA tienen un alto grado de control (y responsabilidad) sobre la cadena de confianza que estas custodian, de forma que la Parte Confiante se puede desentender de muchas responsabilidades técnicas y pasar a adoptar un rol más pasivo, una posición muy conveniente para la adopción masiva del sistema de seguridad propuesto por X.509.

3.2.5 Firma Digital en Costa Rica, Certificado Raíz

La Firma Digital en Costa Rica utiliza una infraestructura de certificados de seguridad PKI basados en el estándar X.509, el cual es un estándar ampliamente adoptado internacionalmente gracias a sus cualidades que permiten asegurar la autenticidad y validez de las firmas digitales mediante un esquema jerárquico y robusto de verificación descentralizada.

X.509 se ajusta al formato requerido (para el caso de uso costarricense) ya que permite que las propias autoridades gubernamentales sean las encargadas de salvaguardar la cadena de confianza (Autoridades de Certificación), mientras que la parte Confiante

(instituciones) puedan trabajar con los certificados existentes bajo un marco de confianza promulgado por mero proteccionismo gubernamental y política pública. Todo esto, operando de forma descentralizada y funcionando bajo una arquitectura fuera de línea, donde el ente Confiante únicamente necesita conocer cuál es la cadena de confianza (de la Autoridad Certificadora) para poder validar la autenticidad de cualquier certificado de Firma Digital con el cual necesite relacionarse.

En este caso la Autoridad Certificadora se denomina como “CA SINPE - Persona Física” o “CA SINPE - Persona Jurídica”, la cual es operada por el BCCR (Banco Central de Costa Rica), siendo este el organismo responsable de resguardar y gestionar los certificados de la Autoridad de Certificación (certificado raíz y certificados intermedios) convirtiéndose en el responsable directo sobre la cadena de confianza del sistema, proveyendo una robustez institucionalizada, necesaria para poder operar el sistema de Firma Digital a nivel nacional de forma confiable y segura.

Por su parte el MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica) es el ente encargado de supervisar la implementación de las políticas y los correctos estándares en los servicios tecnológicos de orden público. En este caso el DCFD (Dirección de Certificadores de Firma Digital del MICITT) es la unidad encargada de supervisar directamente la gestión y operatividad de la infraestructura de Firma Digital en Costa Rica, asegurando el cumplimiento de los estándares y regulaciones establecidos para la emisión de certificados.

Además podemos destacar que actualmente la Firma Digital de Costa Rica está optando por el uso de una combinación de los algoritmos SHA-512 y RSA para el proceso de

Firma Digital. Además de que actualmente los certificados de Firma Digital cuentan con una llave RSA de 2048 bits de longitud.

Actualmente el sistema de Firma Digital de Costa Rica sigue todos estos estándares modernos de seguridad criptográfica. Concluyendo con la descripción técnica del funcionamiento de la Firma Digital en Costa Rica, se podría describir el procedimiento de uso común de la Firma Digital de la siguiente manera

0. El firmante cuenta con los insumos para el proceso de Firma Digital, estos serían; el documento que se quiere firmar así como un certificado de Firma Digital emitido (a nombre y titular del firmante) por la Autoridad Certificadora competente.
1. El firmante genera un hash del documento mediante el algoritmo criptográfico SHA-512 (Secure Hash Algorithm), este hash es único y permite realizar una validación matemática bit por bit de que el contenido del documento no ha sido alterado ni modificado posterior al momento de la firma.
2. El hash generado se cifra usando la llave privada del firmante, (usando factores matemáticos que forman parte del secreto de la llave privada), generando así una Firma Digital segura, un mensaje encriptado imposible de replicar sin tener acceso a la llave privada del certificado del firmante.
3. El documento, junto con la Firma Digital y otros valores adjuntos (copias o referencias al certificado utilizado en el proceso de firmado, por ejemplo) se agrupan en un solo mensaje y se envía al destinatario.
4. El destinatario utiliza la clave pública del certificado del firmante, para descifrar la firma y recuperar el hash original del mensaje (generado por el firmante) durante el proceso de firmado.

5. El destinatario genera un nuevo hash del documento recibido y lo compara con el hash descifrado de la firma. Si ambos coinciden se puede deducir entonces que la firma es vigente y el documento no ha sido modificado.
6. Por último, el destinatario realiza una validación de la cadena de confianza del certificado digital del firmante, permitiendo validar si el certificado es legítimo y si proviene de una cadena de confianza segura, autenticando así la identidad del firmante y propietario del certificado.

3.3 Requerimientos y limitaciones legales de la jurisdicción Costarricense.

Es esta sección vamos a revisar las 3 principales normativas de orden legal y administrativo que tiene injerencia directa en el ejercicio propuesto de evaluar la viabilidad técnica en el desarrollo e implementación de nuevas tecnologías sobre la arquitectura tradicional de Firma Digital del país.

Estas 3 normativas son:

La Ley de Certificados, Firmas y Documentos Electrónicos, la cual es la primera Ley promulgada con el objetivo de expandir el uso de medios digitales en el procedimiento burocrático costarricense.

Además de un par de reglamentos administrativos y estándares de uso, el primero emitido por el MICITT como ente regulador de la operación de Firma Digital, mientras

que el otro fue emitido por el Banco Central de Costa Rica, como principal ente certificador del país.

3.3.1 Ley de Certificados, Firmas Digitales y Documentos Electrónicos

La "Ley de Certificados, Firmas Digitales y Documentos Electrónicos" de Costa Rica regula el uso de tecnologías para autenticar documentos digitales y establecer equivalencias entre la legalidad de los documentos físicos y sus homólogos digitales. Promulgada en agosto del 2005, la Ley N.º 8454 tiene el objetivo de fortalecer el amparo legal para la utilización segura y regulada de documentos digitales y transacciones electrónicas como parte de procedimientos jurídicos y administrativos. Esto quiere decir que, a través de esta nueva ley, la normativa reconoce la figura legal detrás de la Firma Digital y establece el marco para los criterios de operación de la misma dentro del órgano institucional-administrativo del estado.

Principales aspectos referenciados en la Ley N.º 8454:

- Ámbito de Aplicación: La ley se aplica a transacciones y actos jurídicos en los sectores público y privado, siempre que sean compatibles con el uso de certificados y firmas digitales (medios digitales).
- Alcance del certificado: La ley determina lo que se puede considerar como “Certificados Digitales válidos”. Define al certificados como una herramienta digital capaz de garantizar: la autenticidad, integridad y vinculación jurídica (entre firmante y firma) de un documento electrónico firmado.
- Equivalencia Funcional: Los documentos electrónicos tienen la misma validez que los documentos físicos. Además, se reconoce la fuerza probatoria de estos

documentos, otorgándoles el mismo peso legal que a los documentos tradicionales.

- Roles y responsabilidades: La ley establece un marco para la implementación de firmas digitales mediante la asignación de roles y responsabilidades durante el proceso de emisión y operación de los certificados digitales. Se definen las figuras de Autoridades de Certificación y Autoridades Reguladoras. Las responsabilidades de estas figuras van dirigidas a dar soporta y salvaguardar la autenticidad e integridad de la Firma Digital durante su ciclo de operación. Además, se nombra al MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones) como el órgano regulador superior encargado de supervisar todo el sistema de Firma Digital.
- Suspensión y Revocación de Certificados: Los certificados digitales pueden suspenderse o revocarse en casos específicos, como solicitud del usuario, compromisos de seguridad, orden judicial o incumplimiento de políticas o normativas.
- Sanciones y penalizaciones: La ley establece un marco de operación para poder ejecutar sanciones y penalizaciones a aquellos sujetos que incumplan con sus responsabilidades legales o que realicen un uso fraudulento del sistema durante el cumplimiento de sus funciones. La gravedad de las sanciones pueden ir desde amonestaciones económicas hasta la completa revocatoria de la inscripción de un Ente Certificador en “La Dirección de Certificadores de Firma Digital” a nivel nacional, lo cual implica un cese inmediato de sus funciones.

3.3.2 Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos

Esta es una normativa promulgada con carácter de decreto ejecutivo que busca establecer las disposiciones para la implementación y uso de firmas digitales, reglamentando aspectos técnicos y administrativos vitales para garantizar la efectividad, seguridad y legalidad de esta nueva implementación tecnológica, apegándose a lo estipulado en la Ley N.º 8454.

Principales Disposiciones del Reglamento

1. **Propósito y Alcance (Capítulo I)**:

El reglamento tiene como objetivo reglamentar la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley N.º 8454), proporcionando un marco de normas para el uso de firmas digitales en transacciones electrónicas.

Define términos importantes, como **Autenticación** (verificación de la identidad), **Autenticación Mutua** (cuando dos entidades verifican su identidad entre sí), y **Certificado Digital** (documento que vincula una clave pública con una identidad), Certificados Validos y Certificados Inválidos, entre otros.

2. **Certificados Digitales (Capítulo II)**:

Esta sección detalla los lineamientos para el proceso de emisión, suspensión y revocación de los certificados digitales.

Se establece que es responsabilidad de La Dirección de Certificadores de Firma Digital poder determinar de manera delimitada cuales son los tipos de certificados que

pueden emitirse, asegurando la interoperabilidad entre sistemas y el cumplimiento de normas internacionales.

En este apartado se detalla por ejemplo la exigencia del uso de Módulos Seguros de Creación de Firma (MSCF) que cumplen con estándares de seguridad como FIPS 140-1 (Federal Information Processing Standard, National Institute of Standards and Technology, Estados Unidos de América) nivel 2 o superior, del cual de manera breve podemos mencionar que el estándar FIPS 140-1 detalla estándares de seguridad informáticos para la confidencialidad de datos sensibles y se basa en un modelo de seguridad por capas el cual se subcategoriza en niveles, el nivel 2 hace mención a requerimientos de seguridad tanto físicos, ambientales y de software, para más detalle se puede consultar la referencia a dicho documento.

3. **Certificadores Registrados (Capítulo III)**:

Acá se reitera nuevamente que solo los certificados emitidos por Certificadores Registrados ante la Dirección de Certificadores de Firma Digital (DCFD) tendrán validez legal.

Los certificadores deben cumplir con requisitos técnicos y administrativos definidos en el anexo del documento, y deben someterse a auditorias por parte del Ente Costarricense de Acreditación (ECA) para garantizar su idoneidad.

Además de referenciar lineamientos técnicos, acá también se profundiza sobre los roles y responsabilidades de los entes certificadores. Se menciona entre otras cosas que:

- Tienen la responsabilidad de llevar registros detallados de sus suscriptores y mantener un Repositorio Electrónico en línea para consulta pública.

- Deberá mantener actualizada la documentación que los acredita como Certificadores subscritos a la DCFD, dentro de la cual se encuentran datos como razón social, información de contacto de la entidad, información de contacto de los trabajadores involucrados, entre otros.
- Expedir certificados digitales siguiendo las pautas de seguridad y confidencialidad mencionadas en los lineamientos técnicos del reglamento.
- Bajo ninguna circunstancia, el Certificador podrá copiar o conservar información relativa a la clave privada de los certificados emitidos bajo el nombre o titular de algunos de sus usuarios, clientes o suscritos.

4. **Funciones de la Dirección de Certificadores de Firma Digital (Capítulo IV)**:

La DCFD (parte del Ministerio de Ciencia y Tecnología) es responsable de la supervisión del sistema nacional de certificación digital y actúa como Certificador Raíz. Como Certificador Raíz, la DCFD no tiene contacto directo con ningún usuario del sistema, pero, al formar parte de la cadena de confianza de la arquitectura PKI que compromete toda la seguridad criptográfica del sistema de Firma Digital, la propia DCFD tiene que apegarse a sus propios lineamientos técnicos emitidos, así como deben seguir las mismas pautas, políticas y estándares internacionales impuestos a las demás autoridades certificadoras vigentes, incluyendo el requerimiento de someterse a auditoria constante por parte del Ente Costarricense de Acreditación (ECA).

La DCFD tiene además la labor de actualizar y emitir nuevas políticas y procedimientos para la gestión planificada de la seguridad del sistema de certificados digitales. Así también debe asegurarse de mantener un registro controlado de los certificados emitidos

a nivel nacional y monitorear la seguridad criptográfica del sistema de certificados vigente.

La DCFD también tiene entre sus responsabilidades mantener canales abiertos de comunicación, disposición a colaborar con organismos externos e instituciones internacionales, así como ofrecer capacitaciones y campañas de concientización acerca del correcto uso y cuidados de seguridad al respecto del uso del sistema de Firma Digital.

5. **Sanciones y Responsabilidad (Capítulo V)**:

Establece sanciones para los certificadores que incumplen el reglamento, incluyendo multas, suspensión de operaciones y revocación de registro.

Define procedimientos para la resolución de conflictos y establece la posibilidad de imponer medidas disciplinarias y multas administrativas en caso de incumplimiento de las normas.

6. **Lineamientos Técnicos (Anexos)**

Define los requerimientos técnicos necesarios para poder emitir y operar certificados en la cadena de confianza del sistema nacional de certificación digital en Costa Rica.

- Disposiciones generales de la administración de políticas de seguridad:

Acá se definen las figuras de Entidad de Gestión de Políticas (EGP), Política de Certificado (PC) y Declaración de Prácticas de Certificación (DPC).

La Entidad de Gestión de Políticas (EGP) es responsable de definir las políticas y requerimientos para el uso de certificados digitales, estos serán especificados en la Política de Certificado (PC) y se regulara su cumplimiento estricto en la Declaración de

Prácticas de Certificación (DPC) acordados entre el EGP y el ente certificador. Estas políticas aseguran que los procesos administrativos y de seguridad cumplan con los requerimientos específicos de cada tipo de certificado.

Se exige un control ambiental estricto, que incluye auditorías periódicas y una revisión continua de las prácticas de certificación. Esto ayuda a garantizar que los controles implementados en la DPC puedan soportar los requerimientos planificados a futuro de la PC.

- Administración de Seguridad de la Información:

Los certificadores deben implementar políticas de seguridad de información aprobadas por la gerencia del ente certificador. Estas políticas deben cubrir aspectos críticos como la seguridad física de las instalaciones, controles de acceso para empleados y terceros, protección contra programas maliciosos, planes de resiliencia ante amenazas a la cadena de suministro, administración de activos, políticas de seguridad sobre el personal, seguridad de equipos electrónicos, entre otros.

Menciona la necesidad de un proceso formal de reporte y creación de incidentes y establece que los planes de continuidad de negocio son obligatorios, y deben incluir estrategias de recuperación ante desastres, almacenamiento seguro de material criptográfico y una disponibilidad adecuada de sitios de respaldo y recuperación.

- Seguridad Física y Ambiental:

Los certificadores deben proteger sus instalaciones mediante un perímetro de seguridad restringido, control de accesos físicos y un sistema de detección de intrusos.

Las instalaciones donde se generan y almacenan certificados requieren de un ambiente seguro contra amenazas ambientales y riesgos físicos, como incendios o intrusiones. Se exige también el uso de sistemas de detección de radiación electromagnética para evitar fugas de información.

- Control de Acceso al Sistema y a la Red:

La administración de acceso incluye el uso de identificadores únicos para cada usuario, control de acceso basado en roles y permisos, conexiones remotas al sistema a través de autenticación mutua, acceso restringido a las terminales locales, políticas mínimo privilegio y restricciones de tiempo para tareas de alto riesgo.

Los sistemas deben estar protegidos por firewalls y otros dispositivos de seguridad de red, y deben emplearse controles de enrutamiento para la segmentación de la red y el monitoreo de la circulación de la información de acuerdo con las políticas del certificador.

Obligatoriamente se solicita que lo sistemas críticos como el sistema de Certificador Raíz (PKI) deben aislarse dentro de un ambiente informático dedicado.

- Módulos Seguros de Creación de Firma (MSCF):

Los MSCF deben cumplir con estándares como ISO 15408, o FIPS 140-1 nivel 2 o superior. Estos dispositivos criptográficos resguardan las claves y aseguran que la generación de firmas digitales se realice de forma segura y protegida contra accesos no autorizados.

Los MSCF deben contar con mecanismos de sello de garantía que detecten intentos de manipulación, y ofrecer capacidades de generación de claves y protección contra falsificación.

- Protocolo de Estado de Certificado en Línea (OCSP) y Lista de Revocación de Certificados (LRC):

El OCSP permite verificar en tiempo real el estado de los certificados, ofreciendo una alternativa a la Lista de Revocación de Certificados (LRC). Este protocolo es esencial para casos en los que la disponibilidad inmediata del estado de validez del certificado es crítica.

Las LRC proporcionan una lista periódica de certificados revocados, la cual es utilizada principalmente cuando no se dispone de acceso en tiempo real.

- Manejo y Seguridad de los Medios de Almacenamiento:

Los medios de almacenamiento que contengan datos sensibles deben ser destruidos o sobrescritos de forma segura antes de su eliminación.

Los controles deben asegurar que la información almacenada se maneje y proteja adecuadamente, con autorización y trazabilidad en todos los procesos de remoción de medios de almacenamiento de la organización.

- Cumplimiento de los Requisitos Legales y Contractuales:

Los certificadores deben cumplir con todas las leyes y regulaciones relevantes en materia de criptografía y protección de datos. Las políticas de seguridad deben definir claramente la confidencialidad y el acceso a la información.

Los registros críticos deben protegerse contra la falsificación, pérdida o destrucción.

- Administración, desarrollo y mantenimiento de Sistemas:

Se deben seguir procedimientos de control de cambios para el hardware, software y configuraciones de red, incluyendo una revisión completa de los sistemas operativos tras cualquier actualización.

Los programas fuente deben estar bajo control estricto, y el software utilizado debe cumplir con el estándar ISO 15408 para asegurar su autenticidad y confiabilidad.

- Planes de Continuidad de Negocio y Recuperación ante Desastres:

Los planes de continuidad de negocio deben contemplar procedimientos detallados para la restauración de operaciones críticas. El almacenamiento de dispositivos criptográficos y datos críticos en sitios alternos es obligatorio para permitir la recuperación en caso de desastres en el sitio primario.

Estos planes incluyen pruebas regulares para asegurar que están actualizados y son efectivos, con objetivos de tiempo de recuperación claramente definidos (RTO).

Finalmente cabe comprender que este reglamento no está basado únicamente en el criterio de las autoridades locales, sino que está ligado a estándares internacionales y buenas prácticas, permitiendo fortalece la confianza en la Firma Digital y fomentando una transformación digital más segura y transparente para Costa Rica.

3.3.3 Estándar Electrónico; firmador validador y autenticador

Esta es una guía detallada proporcionada por el Banco Central de Costa Rica (BCCR) para el procesamiento en tiempo real de firmas digitales, validación de certificados y autenticación de suscriptores mediante el uso de la plataforma GAUDI dentro del contexto de servicios financieros (SINPE) brindados por el Banco Central en su plataforma en línea “Central Directo”. Su propósito es asegurar que las entidades participantes puedan implementar y consumir los servicios de firma y autenticación digital bajo un único marco o estándar nacional, facilitando procesos seguros de expansión y adopción de servicios de firma y autenticación digital en diferentes servicios y entornos de la economía financiera.

A nivel técnico, la plataforma descrita por el este documento, se puede resumir como una serie de servicios web que facilitan la implementación de los principales casos de uso de Firma Digital, abstrayendo la complejidad técnica de la implementación de certificados digitales a nivel de sistema operativo o hardware, y ofreciendo una alternativa más amigable para entornos de ejecución web, mediante el cual muchos sistemas modernos basados en arquitecturas web podrían acceder de forma simplificada, estandarizada y segura a servicios de Firma Digital sin tener que lidiar con la dificultad de incompatibilidades de hardware, sistema operativo o plugin/webkits del navegador o entorno web donde se estén ejecutando dichos aplicativos.

El documento hace siempre un amplio énfasis en su principal objetivo son todos aquellos servicios financieros en línea que podrían verse directamente implicados en las iniciativas de expansión y renovación tecnológica del sistema financiero nacional de Costa Rica. Aun así, se reconoce que las utilidades de estas herramientas van más allá

del ámbito financiero o banca en línea (e-banking) y que otros sectores de la burocracia administrativa gubernamental también se pueden ver ampliamente beneficiados por este tipo de iniciativas.

Dentro de toda la información mencionada en este documento, podemos destacar los requerimientos técnicos más relevantes definidos por norma, como lo son:

1. **Servicios para Firmar Documentos y Autenticar Suscriptores**:

El documento menciona que los 2 primeros casos de uso que son tomados en cuenta en esta normativa son:

- **Proceso de Firma Digital**: Proceso mediante el cual una entidad puede invocar métodos para procesar solicitudes de firma y autenticación de usuarios. El documento define diferentes tipos de métodos que pueden ser invocados dependiendo de los requerimientos técnicos puntuales y particulares de dicha implementación y dicha entidad (métodos como RecibaLaSolicitudDeFirmaXmlEnvelopedCoFirma y RecibaLaSolicitudDeFirmaPdf) para distintos tipos de documentos (XML, MS Office, ODF, PDF) y escenarios con diferentes tipos de firma (cofirma y contrafirma).
- **Autenticación del Suscriptor**: Proceso mediante el cual una entidad invoca una solicitud de Firma Digital dirigida exclusivamente como medio de autenticación digital para validar la autenticidad del usuario portador del certificado. Se definen métodos para facilitar y cumplir esta función, por ejemplo el método RecibaLaSolicitudDeAutenticacion se encarga de

verificar la identidad del suscriptor antes de proceder con otras solicitudes de firmas digitales de documentos o transacciones electrónicas.

2. **Web Service y WCF Firmador**:

Se describe el uso de tecnologías como Web Service y Windows Communication Foundation (WCF) para la transmisión segura de solicitudes de firma. Estos servicios están protegidos con TLS 1.2 o superior y certificados digitales específicos de persona jurídica, garantizando la integridad y confidencialidad de los datos.

3. **Servicios de Validación de Certificados y Documentos**:

Estos son servicios que forman parte de la misma plataforma GAUDI, pero en este caso los métodos involucrados están estrictamente dirigidos a fortalecer las capacidades para que las propias entidades puedan proceder con monitorear o detectar escenarios de errores en la validación de la autenticidad de certificados digitales como hasta incluso detectar posibles intentos de estafa o fraude mediante el intento de utilización de certificados inválidos. Los principales métodos a mencionar son:

- **Validación de Certificados**: Las entidades pueden validar la autenticidad y vigencia de los certificados de Firma Digital. Los métodos permiten verificar si el certificado pertenece a la jerarquía nacional y si está activo y en buen estado.
- **Validación de Documentos Firmados**: A través de métodos como ValideElDocumentoXmlEnvelopedCoFirma, las entidades pueden comprobar la integridad y autenticidad de documentos ya firmados digitalmente, asegurando que no han sido modificados.

4. **Servicios para Sellar Documentos**:

Como parte del conjunto de herramientas proporcionadas por el BCCR, están ofrecen otros tipos de servicios relacionados como los métodos para aplicar un sello electrónico a los documentos. Este sello utiliza un certificado digital custodiado por el BCCR, garantizando así la autenticidad y trazabilidad de los documentos. Los formatos soportados incluyen XML, MS Office, ODF y PDF.

5. **Control de Accesibilidad, Notificación y configuración de GAUDI**:

Como parte de las capacidades de la plataforma GAUDI, el BCCR también se compromete a ofrecer otros tipos de servicios relacionados al comportamiento de la plataforma de cara al usuario, métodos los cuales permiten consultar información extra acerca de la configuración y customización de un usuario concreto, mediante el cual se puede determinar eventualidades ocurridas durante el proceso de Firma Digital. Los métodos más destacados de esta sección de la documentación son:

   - **Notificación por Accesibilidad**: Permite que el sistema ajuste la presentación y notificación de solicitudes según las necesidades de accesibilidad del usuario acorde a la configuración local o personalizada de la plataforma GAUDI de cada del usuario (por ejemplo, habilitando opciones para personas con capacidades especiales).

6. **Convenciones en Tecnologías de Normas**:

Existen diferentes tecnologías particulares que son reconocidas oficialmente por la norma para poder involucrarse en el proceso de Firma Digital facilitada por la plataforma GAUDI, dentro de las cuales se puede destacar:

- **Documento electrónico**: Se define como documento electrónico únicamente una serie de formatos electrónicos como XML, ODF, Microsoft Office o PDFs, además de que se describe al formato de encriptación Base 64 como método de codificado y decodificado para la transferencia de archivos binarios entre los diferentes servicios web de la plataforma GAUDI.
- **TLS 1.2 y Certificados Digitales**: Los servicios están asegurados mediante el uso de TLS 1.2 o superior y certificados digitales, lo cual es esencial para proteger las transacciones y mantener la privacidad de los datos.

3.4 Implementación de la Firma Digital en Estonia.

La implementación de e-Government y Firma Digital en Estonia es un ejemplo destacado a nivel mundial de cómo un país puede transformar digitalmente sus servicios gubernamentales para beneficiar a la sociedad. Esta transformación comenzó en la década de 1990, después de que Estonia obtuviera su independencia de la Unión Soviética en 1991. En lugar de reconstruir una infraestructura gubernamental tradicional, Estonia optó por invertir en tecnología digital para modernizar sus servicios públicos y fomentar la transparencia y accesibilidad.

3.4.1 Reseña histórica Firma Digital en Estonia

A mediados de los años 90, el gobierno Estonio enfrentó grandes desafíos económicos, incluyendo recursos limitados y una falta de infraestructura moderna. Posterior a la caída

de la Unión Soviética, Estonia se encontró en la situación de ser unos de las regiones más desfavorecidas en términos de infraestructura estratégica de entre todas las repúblicas ex soviéticas. Debido a esto el gobierno Estonio se tuvo que concentrar en atacar y resolver 2 grandes desafíos inmediatos que eran aparentemente claves para la planificación económica de la (recién independiente) joven república báltica. Estonia necesitaba cimentar una “competitividad productiva” inexistente para una fecha en la cual el país se veía obligada a abrir sus fronteras comerciales con el resto del bloque occidente capitalista. Además, Estonia se enfrentaba ante una problemática de identidad civil, lo cual representaba un problema mayúsculo al ser una de las regiones menos pobladas del ex bloque soviético, haciendo que la joven república democrática estuviera expuesta a escenarios de alta inestabilidad política generada por las dinámicas migratorias en la región báltica para dicha época.

Debido a esto y sumado a la falta de recursos económicos que la nueva república tenía para invertir en nueva infraestructura, el gobierno Estonio lanzó varias iniciativas tecnológicas para sentar las bases de una administración digital. En 1997, se introdujo el programa "Tigrihüpe" (Salto del Tigre), cuyo objetivo era mejorar la alfabetización digital y el acceso a internet en todo el país, preparando a los ciudadanos para una sociedad digital mientras esperaba con altas expectativas que todas estas nuevas inversiones sociales se convirtieran a mediano y largo plazo en una ventaja competitiva única que diferenciara a Estonia del resto de países de la región.

En 2000, Estonia adoptó la Ley de Firma Digital, una de las primeras leyes en el mundo que otorgó a las firmas digitales el mismo valor legal que a las firmas manuscritas. Esta ley fue fundamental para la digitalización del gobierno, ya que estableció las bases para

una infraestructura de clave pública (PKI), permitiendo que los ciudadanos firmaran documentos electrónicos con total validez legal.

En 2002, el gobierno lanzó la tarjeta de identidad electrónica (e-ID), que se convirtió en el principal medio de autenticación para acceder a servicios en línea. La e-ID permite a los ciudadanos autenticarse en portales del gobierno y realizar firmas digitales con su tarjeta. La tarjeta e-ID se complementó posteriormente con Mobile-ID (autenticación y Firma Digital desde dispositivos móviles) y Smart-ID (una alternativa en la nube), aumentando la accesibilidad.

El sistema X-Road, introducido en 2001, permitió la interoperabilidad entre diferentes bases de datos y sistemas gubernamentales, posibilitando que las instituciones compartan información de forma segura y rápida. X-Road es la columna vertebral de los servicios de e- Government en Estonia, ya que permite que los ciudadanos, empresas y el gobierno realicen transacciones electrónicas sin duplicar información y con total seguridad, además de que permite ofrecer a la ciudadanía una plataforma uniformes de servicios en línea basados en la misma arquitectura compartida entre instituciones gubernamentales así como el uso de Firma Digital como principal medio de autenticación y control de acceso unificado entre los diferentes subsistemas de orden público del estado estonio.

3.4.2 Situación actual de E-Government en Estonia

Hoy en día, los ciudadanos estonios pueden acceder a la mayoría de los servicios públicos en línea, desde votar electrónicamente hasta consultar sus historiales médicos

y se ha convertido en una columna vertebral de la idiosincrasia popular del pueblo estonio.

Actualmente el uso de certificados digitales es mandatorio para toda la población económicamente activa en Estonia, esto mediante la implementación de la “Tarjeta de Identificación Digital” como principal y único documento de identificación establecido por ley. Aproximadamente 1.1 millones de estonios (datos del 2024) poseen un certificado digital valido y participan activamente de la plataforma digital de gobierno para cumplir sus responsabilidades civiles. Esta tarjeta cumple una doble función como certificado digital valido para acceder servicios en línea, así como documento comprobatorio físico, incluyendo algunas características comunes como una foto legal del propietario, nombre completo y otros datos comprobatorios como fechas de emisión y de vencimiento, números de identificación únicos, entre otros.

La implementación de la Firma Digital y el E-Government ha convertido a Estonia en un referente global, permitiéndole ahorrarse históricamente millones de horas de trabajo burocrático y establecer una plataforma de gobierno más transparente, segura y flexible.

La apuesta de Estonia por la digitalización, respaldada por una infraestructura digital robusta y un marco legal avanzado, ha impulsado el desarrollo de una sociedad digital que representa a día de hoy un modelo a seguir para otros países interesados en modernizar sus administraciones públicas.

3.4.3 Open-eID

Open-eID es una plataforma de software de código abierto directamente administrada por una autoridad gubernamental denominada Autoridad del Sistema de Información de

Estonia (RIA), la cual se encarga de la gestión, desarrollo y mantenimiento del software de eID que soporta el sistema de Firma Digital de Estonia, además de colaborar con el sector privado para garantizar la interoperabilidad y eficacia de los servicios de eID en el país. Para esto, se diseñó una seria de servicios en una plataforma de código abierto para facilitar y estandarizar el uso de la Firma Digital en la jurisdicción nacional, otorgando total libertad tanto a los ciudadanos estonios como a otras entidades privadas el poder participar activamente del desarrollo de servicios y sistemas complementarios basados de la plataforma de Certificados Digitales eID. Esto dando como objetivo el promulgar la innovación en el desarrollo de una amplia gama de servicios digitales diseñados para ciudadanos estonios y residentes. **Open-eID** constituye una parte esencial de la infraestructura de e-Government en Estonia y es una herramienta clave para la implementación de servicios de gobierno digital, tanto en el ámbito público como en el privado.

Open-eID ha logrado cambios significativos en la divulgación, adopción, uso y cobertura de los servicios digitales basados en Firma Digital, todo esto mediante el desarrollo colaborativo de herramientas y tecnologías de código abierto promulgados y administrador por la autoridad gubernamental competente.

Dentro de las iniciativas involucradas como parte de la plataforma Open-eID podemos mencionar:

1. **DigiDoc**: Es el núcleo del sistema Open-eID y consta de aplicaciones y bibliotecas que permiten la creación, verificación y manipulación de firmas digitales en documentos electrónicos. DigiDoc proporciona:

- **DigiDoc4 Client**: Una aplicación de escritorio que permite a los usuarios firmar y verificar documentos digitalmente, revisar la validez de certificados y realizar autenticaciones.
- **LibDigiDoc**: Una biblioteca de código abierto que permite a los desarrolladores integrar funcionalidades de Firma Digital en sus propias aplicaciones.
- **DigiDocService**: Un servicio en línea que proporciona una API para que terceros puedan incorporar capacidades de autenticación y Firma Digital en sus plataformas.

2. **Mobile-ID y Smart-ID**: Estos servicios no son necesariamente del todo de código abierto, pero su concepción y desarrollo giraron en torno a la infraestructura y a las herramientas ofrecidas por Open-eID. Esto son servicios orientados a ofrecer autenticación y Firma Digital desde dispositivos y sistemas no convencionales, sin necesidad de una tarjeta de identidad o certificado físico.
   - **Mobile-ID**: Permite a los usuarios utilizar sus teléfonos móviles como una herramienta de autenticación y Firma Digital. Este sistema ha sido especialmente popular porque elimina la necesidad de lectores de tarjetas y es más accesible para los usuarios en movimiento.
   - **Smart-ID**: Es una solución tipo SaaS (software a as a service) que permite operar servicios de Firma Digital (eID) con los más altos estándares de seguridad y sin la particularidad de verse limitado por las capacidades de hardware o limitaciones en el sistema cliente del usuario, esto se traduce

como una solución nativa en la nube, la cual, aunque no sea en si misma de código abierto, esta si depende en gran medida de las herramientas y tecnologías desarrolladas en Open-eID para funcionar.

3. **Integración con X-Road**: Open-eID desarrolla varias tecnologías y herramientas que forman parte clave de la arquitectura X-Road que utiliza el gobierno de Estonia para la interoperabilidad de sistemas institucionales. Open-eID permite que esta integración de X-Road se extienda aún más allá, permitiendo la participación de entes privados como parte de la plataforma de información compartida. Esta integración permite que la Firma Digital (eID) funcione de manera fluida entre todos los servicios públicos y privados integrados en la plataforma.

Gracias a estas iniciativas de apertura y desarrollo colaborativo de tecnologías es que Estonia se ha consolidado como líder en innovación de gobierno digital y como un modelo para otros países en este aspecto.

3.4.4 X-Road

X-Road es un sistema de interconexión segura de servicios de datos y su funcionamiento es muy similar a un Service Mesh en cuanto a que ambos proporcionan una capa de comunicación segura, estandarizada y centralmente gestionada para conectar diferentes sistemas o servicios. Ambos modelos garantizan características esenciales como el cifrado de las comunicaciones, la autenticación y autorización de las solicitudes, y la trazabilidad de las transacciones mediante registros auditables. Además, de manera muy similar a un servicio de Service Mesh tradicional se emplean lineamientos específicos a

la hora de registrar servicios de datos X-Road, como por ejemplo, correcta implementación de protocolos de comunicación estandarizados como SOAP (Simple Object Access Protocol) o REST (Representational State Transfer), así como definición clara y estandarizada de los servicios publicados (OpenAPI Specification).

Sin embargo, X-Road va más allá de ser solo un Service Mesh de intercomunicación, ya que está diseñado específicamente para entornos gubernamentales y de intercambio de datos entre organizaciones públicas y privadas, para esto, X-Road debe adaptar lo que en un principio sería una arquitectura descentralizada para imponer políticas y reglas de seguridad centralizadas usando el sistema autorizado de Firma Digital para otorgas validez legal a las transacciones realizadas dentro de la red X-Road. Mientras que una solución simple y estándar de Service Mesh suele tener entornos de redes limitadas donde interactúan una cantidad muy restringida de organizaciones o entidades jurídicas, X-Road es una solución orientada a la interoperabilidad entre sistemas autónomos y heterogéneos, a menudo de diferentes jurisdicciones y entidades legales.

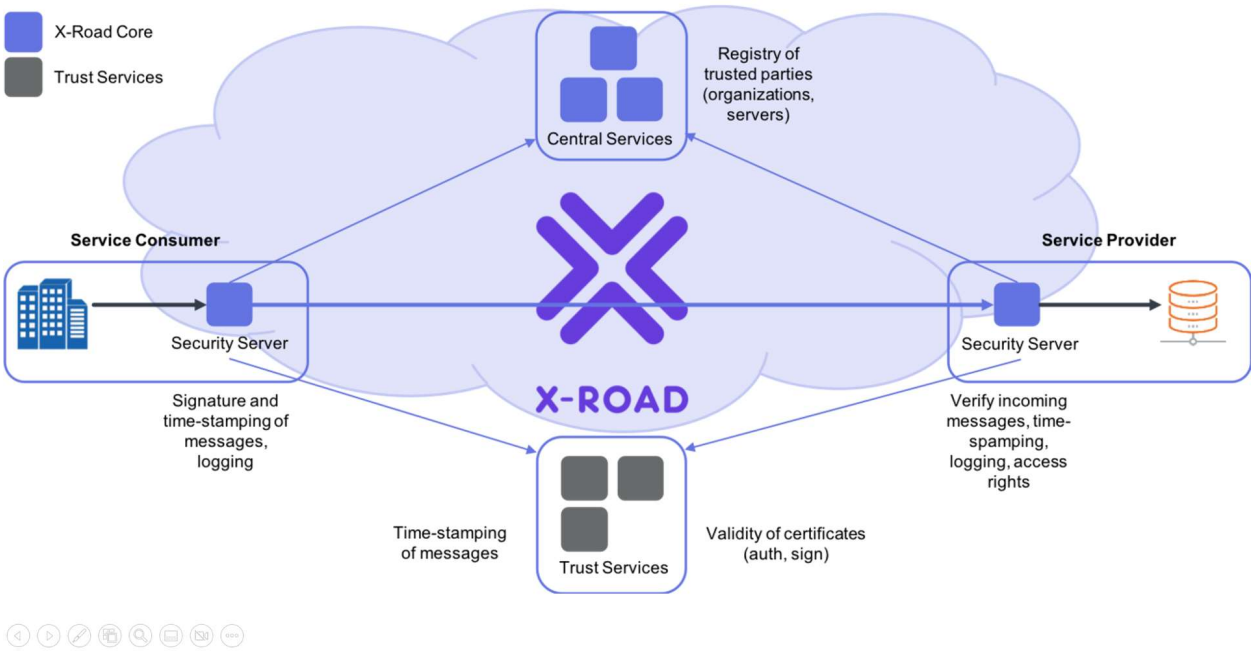


Figura 1. Arquitectura general de X-Road (Nordic Institute for Interoperability Solutions, niis.org)

X-Road opera como una capa de integración distribuida que conecta diferentes sistemas de información, permitiendo el intercambio de datos de manera estandarizada y segura. Sus componentes principales incluyen:

- Servidores de Seguridad: Actúan como intermediarios entre los sistemas de información y la red X-Road, es la unidad de seguridad encargada de validar las reglas y políticas de autorización y autenticación implantadas en cada institución, funcionan como servidores proxy seguros, encargándose de firmar y cifrar las comunicaciones de la red garantizando la autenticidad, integridad y confidencialidad de los datos. Funcionan también como principal control de acceso autorizado para los servicios publicados en cada entidad de datos, de forma que cada entidad externa debe formar parte de un grupo autorizado (Global

Group) que le permita acceder a las APIs (Application Programming Interface) y datos subsecuentes para cada entidad particular.

- Autoridad certificadora: Mantiene un registro de todos los miembros de X-Road, encargado de gestionar los certificados digitales y salvaguardar la cadena de confianza de la red PKI, asegurando que solo entidades autorizadas participen en el intercambio de datos.
- Servicios Centrales: Proporcionan funcionalidades esenciales en términos de monitoreo, auditoria, control de la red, coordinación con los servicios complementarios de X-Road, entre otros.
- Operadores de Datos Personales: Es uno de los principales servicios complementario de la red X-Road, son entidades que brindan el servicio de monitoreo de tráfico de datos personales en X-Road y permite llevar un control auditable de los datos de cada ciudadano que se transmiten por la red X-Road.

Toda transacción de datos que transcurra en X-Road debe tener como mínimo 2 Firmas Digitales autorizadas para que la red permita que la transacción se procese correctamente:

- Autorización del usuario: Debe existir en alguna de las Operadores de Datos Personales de la red X-Road una autorización firmada digitalmente por el individuo particular en cuestión; autorizando a X-Road a transmitir sus datos personales y describiendo el alcance de confidencialidad y las entidades involucradas que están autorizadas.
- Firma autenticadora de la entidad solicitante: La transacción debe ir firmada usando la Firma Digital del ente que este solicitando los datos. Esta firma se

realiza de forma segura por el Servidor de Seguridad (proxy) del ente solicitante, de forma que, cualquier comunicación subsecuente dentro de la red X-Road es segura y está aislada de cualquier interferencia que pueda surgir desde la red organizacional o institución solicitante.

3.5 Tecnologías Web como proveedores de autenticación.

3.5.1 OAuth 2.0

OAuth 2.0 es un protocolo de autorización abierto y estándar que permite a las aplicaciones y servicios de terceros acceder a recursos protegidos en nombre de un usuario, sin necesidad de compartir las credenciales (como contraseñas) del usuario. Este protocolo proporciona una manera segura de delegar permisos para que una aplicación pueda actuar en nombre de otra, mediante un sistema de tokens.

OAuth 2.0 trabaja mediante el uso de tokens de acceso (access tokens), que son permisos temporales que autorizan a una aplicación a acceder a recursos específicos en nombre de un usuario. Cuando un usuario quiere permitir a una aplicación el acceso a sus datos en un recurso protegido, sigue el siguiente flujo general:

- Solicitud de Autorización: La aplicación solicita permiso al usuario para acceder a sus datos.
- Autenticación del Usuario: El usuario se autentica en el servidor de autorización, generalmente en una pantalla de inicio de sesión proporcionada por el servidor.
- Consentimiento del Usuario: El usuario revisa los permisos solicitados y da su consentimiento.

- Emisión del Token de Acceso: Si el usuario concede el acceso, el servidor de autorización emite un token de acceso a la aplicación, que actúa como "clave" para acceder a los recursos.
- Acceso al Recurso: La aplicación utiliza el token de acceso para interactuar con los recursos protegidos en el servidor de recursos.

OAuth 2.0 permite a una aplicación de terceros autenticar a un usuario mediante el uso de un servidor de autorización. Esto es útil para aplicaciones web y móviles que desean integrar servicios externos sin manejar directamente las credenciales ni la logística de protocolos de autenticación más sofisticados como PKI o doble factor de autenticación.

3.5.2. OpenID Connect (OIDC)

OpenID Connect es un protocolo de autenticación que se construye sobre el estándar de autorización OAuth 2.0. Este funciona como una extensión, añadiendo una capa de autenticación capaz de ofrecer las herramientas necesarias para identificar de manera segura al usuario que está dando esos permisos. Esto significa que, OpenID Connect funciona sobre OAuth 2.0, y utiliza su flujo de autorización, pero añade componentes y parámetros adicionales para que el servidor de autorización pueda autenticar al usuario y devolver información sobre su identidad.

Al igual que OAuth 2.0, este tiene un flujo de datos y comunicación muy similar, el cual podemos describir como:

- Solicitud de Autorización: La aplicación cliente (que quiere autenticar al usuario) redirige al usuario al servidor de autorización de OpenID Connect.

- Autenticación del Usuario: El usuario se autentica en el servidor de autorización usando sus credenciales.
- Emisión del ID Token: Una vez autenticado, el servidor de autorización emite un ID Token junto con el token de acceso. El ID Token contiene información sobre el usuario y permite a la aplicación cliente verificar su identidad.
- Verificación del Token: La aplicación cliente recibe y verifica el ID Token para confirmar que el usuario ha sido autenticado de manera segura.

Se puede entender el ID Token como un mensaje cifrado que contiene todos los componentes necesarios para identificar un usuario y validar la autenticidad de la sesión del mismo. En la práctica la implementación técnica de esto se traduce como un **JSON Web Token (JWT)** firmado digitalmente por el proveedor de OIDC, el cual contiene toda la información del usuario autenticado.

3.5.3. Client Certificate Authentication (CCA)

Es un método de autenticación que utiliza certificados digitales para verificar la identidad de un cliente (como un usuario o un dispositivo) que intenta acceder a un sistema o aplicación. Este método se basa en la infraestructura de clave pública (PKI), donde cada cliente posee un par de claves (pública y privada) y un certificado digital emitido por una autoridad de certificación (CA) que vincula su identidad con su clave pública.

Esta tecnología se diferencia de las demás debido a que no necesita un de un servicio centralizado de autorización ni autenticación, sino que, a través de la cadena de confianza generada por la arquitectura PKI, permite que usuarios clientes y servidores

se comuniquen de forma segura únicamente usando la criptografía de los certificados y sin necesidad de intermediarios.

El proceso de autenticación usando CCA se puede resumir como:

- Solicitud de Conexión: Cuando un servidor detecta un cliente intentando comunicarse, este le responde al cliente enviando su propio certificado público firmado, además de otros parámetros adjuntos pseudoaleatorios necesario para el handshake TLS (Transport Layer Security).
- El cliente recibe el certificado del servidor y procede a realizar las validaciones del certificado recibido, valida la integridad del mensaje firmado para asegurar no haya sido alterado, posteriormente valida algunas otras cosas como la fecha de caducidad el certificado o la firma del ente emisor que autoriza la cadena de confianza.
- Si la validación por parte del cliente es exitosa, este continua el proceso enviando al servidor su propio certificado publico firmado además de otros parámetros requeridos para el hadshake TLS.
- El servidor realiza las validaciones requeridas del certificado del cliente y se asegura que la cadena de confianza a la cual pertenece dicho certificado este debidamente autorizada para acceder a los servicios sistemas allí alojados.
- Por último, tanto cliente como servidor intercambian un último mensaje de "Finished” con el cual validan toda la cadena de mensajes previos (mediante el uso de Hashes) finalizado el proceso de validación, este último mensaje también sirve para que ambas partes acuerden una llave simétrica que será utilizada para

encriptar el canal de comunicación de allí en adelante. Finalizando así el proceso del Handshake y autenticación.

Si bien Client Certificate Authentication es una de las soluciones de autenticación más robustas al ser basada y compatible con las tecnologías de certificados digitales PKI, sus requisitos de implementación son igualmente superiores a otras alternativas; usualmente para poder implementar dicha tecnología en los dispositivos clientes se vuelve necesario tener que realizar modificaciones o adaptaciones incluso a nivel de Sistema Operativo o Hardware dependiendo del dispositivo del que estemos hablando. Esto ha provocado que Client Certificate Authentication sea mayormente rezagado al mundo empresarial o sistemas corporativos, entornos donde es más fácil tener control de que tipos de dispositivos se utilizan dentro de la red.

3.5.4 FIDO2

FIDO2 es un conjunto de estándares de autenticación que permiten la autenticación en sitios web y aplicaciones sin el uso de contraseñas. FIDO2 se compone de dos componentes principales; WebAuthn y CTAP (Client to Authenticator Protocol).

Estos estándares fueron desarrollados por la FIDO Alliance (Fast Identity Online Alliance) y están respaldados por grandes empresas tecnológicas como Google, Microsoft, Apple, y Mozilla, así como por el World Wide Web Consortium (W3C).

La idea principal detrás de FIDO2 es la de facilitar alternativas que permitan a los usuarios autenticarse utilizando dispositivos de seguridad (como llaves físicas, teléfonos inteligentes, o incluso lectores biométricos integrados) en lugar de depender de contraseñas tradicionales. Esto con el objetivo de generar entornos Web más seguros y

libres de riesgos de phishing, suplantación de la identidad u otras prácticas fraudulentas. Para esto se necesita atacar 2 problemáticas técnicas muy independientes entre sí, pero que en su conjunto forman parte de la logística principal detrás del objetivo de FIDO2 que es definir métodos seguros de autenticación:

WebAuthn (Web Authentication): Este es un API desarrollado por W3C (World Wide Web Consortium) encargado de definir los métodos, funciones y en general toda la interacción en la comunicación llevada a cabo entre el cliente y el servidor durante el proceso de autenticación del usuario. Para eso, el API se debe implementar a nivel de Navegador Web y viene acompañado con una serie de librerías Web que deben ser implementadas dentro de cada uno de los sitios web que quieran incorporar la herramienta.

WebAuth es a final del día un API web (Application Programming Interface) encargado de dar soporte y disponer los canales de acceso para que los diferentes sitios y aplicativos web puedan acceder las diferentes herramientas que vienen soportadas con el paquete FIDO2.

El API de WebAuth tiene sus traducciones y versiones para cada una de las plataformas y lenguajes web más utilizados; Javascript, TypeScript, .NET, Python, entre otros. Y su soporte se extiende por los principales navegadores web como Google Chrome, Mozilla Firefox, Apple Safari o Microsoft Edge.

CTAP2 (Client to Authenticator Protocol): Este es la otra parte complementaria a WebAuth para el funcionamiento de FIDO2. CTAP2 es un protocolo estándar que define las interfaces necesarias que deben existir para la comunicación entre los Navegadores

Web y los diferentes Dispositivos Autenticadores (dispositivos electrónicos orientados a la autenticación segura de doble factor) que sean compatibles con FIDO2.

CTAP2 soporta múltiples métodos de conexión de Dispositivos Autenticadores como USB, NFC o Bluetooth. Además define la forma segura en la que dichos dispositivos deben comunicarse ya que en CTAP2 los autenticadores (como llaves de seguridad, teléfonos, o dispositivos biométricos) son los encargados de almacenar las llaves privada y publicas que se utilizan en el proceso de autenticación por criptografía asimétrica y CTAP2 se encarga de definir un entorno donde la llave privada este segura en el Dispositivo Autenticador y esta nunca se vea comprometida. Cuando el usuario intenta autenticarse, el Dispositivo Autenticador utiliza la clave privada para firmar un desafío que el servidor puede verificar utilizando la clave pública correspondiente.

FIDO2 es un estándar de autenticación que se pensó inicialmente como una alternativa de doble factor de autenticación, uno que fuese estándar y que no dependiese de las particularidades técnicas de una u otra compañía, un estándar simplificado capaz de ajustarse únicamente a las necesidad de la Web Estándar, y por tanto, su funcionamiento es completamente descentralizado. Esta descentralización es por otra parte, una de las principales limitaciones técnicas del estándar FIDO2, pues esto impide tener un control o registro centralizado de las llaves que se utilizan para la autenticación, haciendo inviable uso en requerimientos de autenticación complejos donde se necesite más información más allá de la comprobación de un par de llaves asimétricas.

4. Desarrollo

4.1 Contexto sociocultural, comparativa caso Costa Rica y caso Estonia.

Para poder realizar un análisis comparativo entre los escenarios planteado para cada una de las jurisdicciones objetivo, es necesario comprender diferencias en otros tipos de ámbitos sociales y políticos que nos permita realizar una comparación amplia, pasando por un análisis cuantitativo de los datos e informes de adopción gradual de la Firma Digital, así como también conocer y poder comparar datos cualitativos en torno a la percepción de los usuario y ciudadanos de cada país durante la época temporal en la cual se enfoca este estudio (COVID-19), así también como diferencias en términos de política pública y normativa institucional que hayan afectado la percepción de los usuarios en torno al uso de Firma Digital.

¿Porque Estonia?

Haciendo un sondeo entre los diferentes candidatos posibles para el caso de estudio, Estonia sobresale por presentar un modelo de trabajo de las tecnologías de Firma Digital muy diferentes al caso de Costa Rica, pero, manteniendo similitudes técnicas importantes en cuanto a tecnologías utilizadas y especificaciones técnicas.

Estonia y Costa Rica desarrollaron exactamente la misma arquitectura con muy ligeras diferencias, pero Estonia tomo un enfoque administrativo muy distinto y continuo expandiendo sus servicios y sistemas subyacentes de forma centralizada y controlada.

Otro factor importante para realizar este análisis comparativo con Estonia es la facilidad de información pública y oficial que maneja el gobierno estonio, permitiendo acceso a mucha documentación detallada sobre sus procesos, tecnologías y normativas. Esta transparencia facilita el estudio técnico y el análisis de los modelos administrativos implementados en cada país.

Por último, alineándonos a los objetivos de este proyecto de investigación, debemos reconocer que Estonia es ampliamente mencionada como un líder global en E-Government y digitalización así como un caso de éxito en cuanto al manejo de la pandemia del COVID-19, esto lo convierte en un referente ideal para poder evaluar ambos modelos de manera comparativa y así atacar en paralelo los 2 puntos clave detrás del objetivo general de este proyecto; poder definir viabilidad técnica a partir de la resolución de un análisis comparativo y también poder determinar cuál es la importancia real (en afectación social) detrás de proponer adoptar soluciones del modelo estonio que sean compatibles para adaptarlas al contexto de Costa Rica.

4.1.1 Contexto Histórico y Evolución del E-Government

En esta sección se realizara una reseña histórica de la evolución en la adopción de la Firma Digital para cada uno de los países en cuestión, además de que se realizara un pequeño análisis de los datos recopilatorios históricos obtenidos que sean relevantes al periodo de crisis sanitaria del COVID-19.

Evolución de la Firma Digital en Costa Rica

El auge por la modernización tecnológica y la digitalización en Costa Rica comenzó en la década de los 90, cuando se empezaron a organizar diferentes comunidades

académica y técnicas para predicar e influenciar en las esferas del poder político del país acerca de la importancia de estas nuevas herramientas digitales. Dichos esfuerzos conjuntos dieron como resultado el apoyo público a ciertas iniciativas concretas como la primera conexión internacional a internet que iba orientada a universidades públicas del país, además de planes de inversión en educación y alfabetización digital, entre otras.

En el año 2002, Costa Rica lanzó su primera campaña publica de adopción digital, el Programa Nacional de Tecnologías de Información y Comunicación fue implementado por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y marcó los primeros pasos hacia la consolidación de una estrategia de digitalización burocrática mediante una seria de campañas de capacitación.

Un avance crucial fue la implementación de la Firma Digital en Costa Rica mediante la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley N° 8454) en el año 2005. Esta ley otorgó a las firmas digitales el mismo valor legal que a las firmas manuscritas en documentos físicos, permitiendo el uso de la Firma Digital para autenticar documentos y transacciones electrónicas en el ámbito tanto público como privado. Con esta legislación, Costa Rica sentó las bases para el funcionamiento de una infraestructura de clave pública (PKI).

Con el marco legal establecido, el siguiente paso fue la implementación de la infraestructura de clave pública (PKI) en el país. Para lo cual el MICITT trabajo en la redacción de la primera normativa administrativa, con la cual definía al Banco Central de Costa Rica (BCCR) como entidad certificadora, y determinaba las pautas de operación con las cuales se iba a administrar la PKI de Firma Digital del país.

No fue sino hasta el año 2009 que el BCCR implementó la infraestructura tecnológica necesaria para poder emitir certificados para el uso del público general.

Durante la década de 2010, Costa Rica experimentó un aumento en la adopción de la Firma Digital, especialmente en el sector público. A través del Sistema Nacional de Pagos Electrónicos (SINPE) del Banco Central, la firma digital comenzó a integrarse en diversos servicios de banca en línea, pagos electrónicos y transacciones financieras.

A pesar de los avances aún persiste una fuerte desconexión de la población general, muchos ciudadanos aún perciben la Firma Digital como una herramienta burocrática complicada, lo que afecta la adopción en sectores amplios de la población.

La pandemia de COVID-19 aceleró significativamente el uso de E-Government y la Firma Digital en Costa Rica. Las restricciones de movilidad y la necesidad de mantener la distancia física llevaron al gobierno y a las instituciones a digitalizar una mayor cantidad de trámites, permitiendo que los ciudadanos realizaran gestiones en línea sin tener que desplazarse a oficinas físicas. Muchas de las ventanillas de servicios más críticas y ampliamente utilizadas fueron presionadas a migrarse a la digitalización, contribuyendo así a la digitalización forzosa y apresurada que se observó durante la crisis sanitaria del COVID-19.

Aun en pleno 2024, son frecuentes los casos de resistencia al cambio tecnológico, uno de los últimos casos fue cuando los usuarios de la Junta de Protección Social (JPS) manifestaron su preocupación y descontento por la implementación de la Firma Digital para la compra de lotería en línea. La inquietud surgió luego de que se anunciara la posibilidad de utilizar la Firma Digital como un método de autenticación en el sistema de

compra en línea de la JPS, a lo cual las autoridades de dicha entidad tuvieron que salir a esclarecer las dudas de los usuarios y a asegurar que la institución no pensaba integrar el uso de Firma Digital como una obligatoriedad burocrática.

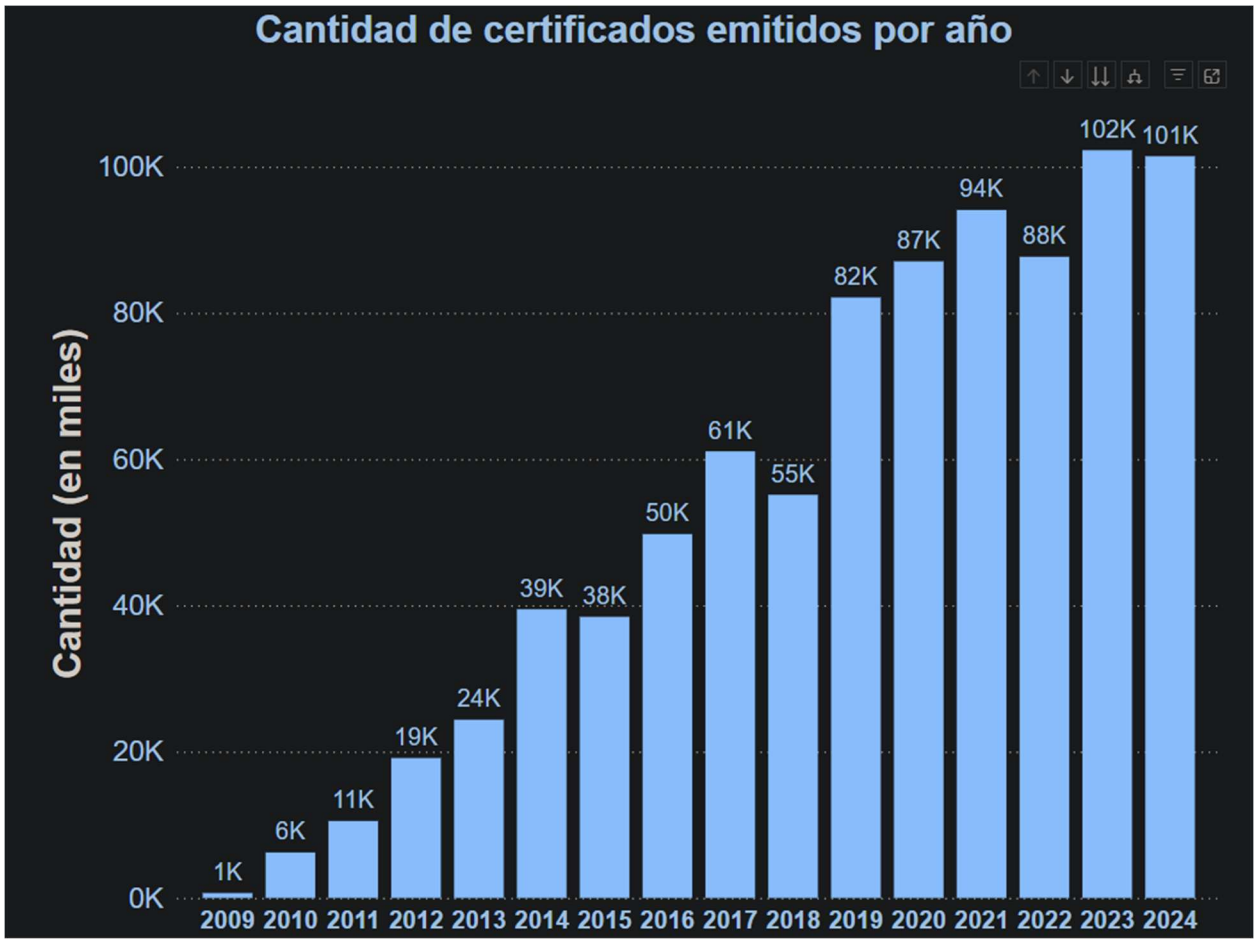


Gráfico 1. Estadísticas de emisión de certificados (Banco Central de Costa Rica)

El gráfico muestra el número de certificados de Firma Digital emitidos anualmente en Costa Rica desde 2009 hasta 2024. La tendencia general refleja un crecimiento significativo año con año, pero también se destaca que el progreso no ha sido necesariamente lineal durante todo el histograma, y se pueden rescatar ciertas épocas temporales aisladas que presentan características diferenciadoras:

Primeros Años (2009-2013): época muy proxima a la implementación inicial de la Firma Digital en Costa Rica, esta fase inicial indica un período de introducción, en el que el sistema de Firma Digital estaba en proceso de adopción y donde realmente era muy poco el potencial practico de la herramienta para dicha época.

Crecimiento Moderado (2014-2018): Acá se observa un aumento inconsistente a lo largo de los años, con periodos de estancamiento seguidos por periodos de aceleración. Tomando en cuenta que para la época la infraestructura de Firma Digital estaba en constante desarrollo y crecimiento, lo normal hubiese sido un aumento en la adopción lineal que fuese a la par con el crecimiento general de la infraestructura, lo que sugiere como posibilidad la existencia de factores temporales que generaban desincentivos en el proceso de adopción. Uno de los principales alicientes de esta tecnología que podamos destacar es el precio estándar de las comisiones cobradas por la emisión del certificado, comisiones que además traen adjunto el costo de los adaptadores y demás periféricos de hardware necesarios para poder hacer uso practico de dichas tecnologías. Podemos tomar por ejemplo el caso del costo por parte del BCR (Banco de Costa Rica) que era uno de los intermediarios autorizados en la emisión de certificados, según los datos históricos recolectados de su propio sitio web, el costo estándar del certificados más periféricos de hardware asociados (Periférico adaptador para computadoras personales) ascendía a los 65$ dólares americanos por unidad para el año 2016, esto quiere decir que simplemente ajustándonos a la inflación de la moneda estadunidense el costo de acceso a dicha tecnología se ha convertido aproximadamente un 30% más económico desde ese entonces.

Impacto del COVID-19 y aceleración histórica (2019-2022): En 2021, se emitieron 94,000 certificados, un aumento significativo desde el 2018 marcando un crecimiento de aproximadamente el 70% en un periodo menor de 4 años, un crecimiento histórico posiblemente motivado por la pandemia de COVID-19, que generó una necesidad de realizar trámites de manera remota. En 2022 el crecimiento volvió a un periodo de estancamiento para posteriormente volver a repuntar un crecimiento moderado en 2023 con 103,000 certificados emitidos.

En la actualidad, datos oficiales del Banco Central de Costa Rica revelados por medio de varios medios de prensa y periódicos nacionales como La Nación o La Extra, revelan que para mayo del 2024 en Costa Rica había una cifra estimada ligeramente superior a 500,000 certificados válidos y activos en circulación, distribuidos entre personas físicas y jurídicas que han solicitado el servicio de Firma Digital.

Esto contrastado con comunicados oficiales del MICCIT distribuidos en sus redes sociales oficiales, donde confirman que para una muestra tomada en octubre del 2024 confirmaban la existencia de un total de 398,028 certificados validos en circulación bajo la figura legal de “Personas Físicas”, esto quiere decir que del total de certificados validos en circulación a la fecha de publicación de dicha información, y tomando en cuenta información oficial de la ONU en su programa de proyección poblacional (Revision of World Population Prospects) donde se estima que para octubre del 2024 la población aproximada de Costa Rica es de 5,138,539, podemos concluir que el dato más actualizado que podríamos estimar para el grado de cobertura del servicio de Firma Digital, a fecha de octubre del 2024, es de aproximadamente un 7.74% del total de la población de Costa Rica.

Figura 2. Certificados Digitales de Persona Físicas (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones)

Además, a través de los datos recolectados publicados por medios de prensa nacionales, una entrevista publicada por el medio El Financiero realizada a Carlos Melegatti (Director de la división de sistemas de pagos del Banco Central de Costa Rica), confirma que no fue sino hasta periodo Q1 del 2023 que se puso a disposición de los usuarios el nuevo beneficio de “Firma Digital para móviles”, el cual facilita la accesibilidad a la plataforma digital de certificación mediante recortes significativos en el costo del hardware implementado. Lo cual funciona como un incentivo positivo que fomenta el auge en el crecimiento del ritmo de emisión de certificados, situación que se alinea con el auge mostrado por los datos del Banco Central de Costa Rica donde para los 2023 y 2024 se está empezando a retomar un crecimiento lineal en el ritmo de emisión de nuevos certificados anuales según lo mostrado en el grafico 1.

Cabe destacar que el nuevo beneficio de “Firma Digital para móviles” no fue lanzado sino hasta después del periodo de exclusión social y crisis sanitaria provocada por el COVID19, lo cual nos indica que este no funciono como un incentivo sistemático durante el periodo de pandemia.

Incentivos gubernamentales durante periodo de Pandemia: Revisando documentación oficial, comunicados y directrices promulgadas por el MICCIT y el BCCR, encontramos que durante el periodo de pandemia de COVID-19 los incentivos públicos promulgados en búsqueda de maximizar la adopción de la Firma Digital se limitan principalmente a dos principales iniciativas encaminadas a promover el buen uso de la herramienta: Las 2 iniciativas podrían mencionarse de forma simple como:

- Proyecto de desarrollo e implementación de la solución integral de firmador FVA (Firmador Validador y Autenticador)
- Programas de capacitaciones ampliadas para trabajadores del sector público.

El proyecto FVA desarrollado por el Banco Central de Costa Rica, es una plataforma electrónica compuesta de diferentes soluciones de software que ofrecen un servicio web capas de permitir a entidades de terceros poder realizar operaciones digitales seguras, implementando el uso de la Firma Digital, sin la necesidad de tener que preocuparse por los requerimientos puntuales o las limitaciones técnicas de hardware para cada uno de los usuarios objetivo de los servicios de autenticación. La plataforma está integrada dentro del Sistema Nacional de Pagos Electrónicos (SINPE) y permite realizar procesos de validación de certificados digitales y la autenticación de usuarios en tiempo real.

Como parte de los avances logrados del proyecto FVA durante el tiempo de pandemia se puede destacar el despliegue de la herramienta GAUDI que facilita el acceso viniendo a resolver problemas de compatibilidad de cara al usuario, sino que también se publican distintas guías técnicas para favorecer el uso e incorporación en las nuevas herramientas como el “Estándar Electrónico Firmador Validador y Autenticador” el cual funciona como una guía de uso normativo y regulatorio de la plataforma y cuyas primeras versiones publicas datan del año 2019.

Además, en lo que respecta a los planes de capacitaciones promulgadas por el MICCIT, podemos destacar el dato de que según su “Informe Final de Evaluación Física y Financiera de la Ejecución del Presupuesto 2020" se detalla que se realizaron procesos de capacitación y evaluación con resultados positivos en un 8.73% del total de empleados de trabajadores públicos del estado para el año 2020.

Según los estudios realizados como parte del proyecto de graduación llamado “Análisis de la implementación de Firma Digital en servicios públicos: los casos de las municipalidades de Santa Ana, Heredia y San José para el año 2019” (Facultad de Ciencias Económicas, UCR), podríamos tomar la situación de las Municipalidad de San José y Heredia como una muestra con tendencias positivas del uso e implementación de las herramientas de Firma Digital en Costa Rica. Importante destacar la mención acerca de “tendencias positivas”, esto debido a que estas 2 municipalidad son de las más desarrolladas y metropolitanas del país, por lo que no pueden ser consideradas como una muestra justa o promedio en la situación del total de municipalidades del país, el mismo documento hace mención que del total de 81 municipalidades locales únicamente 7 prestaban servicios públicos usando la herramienta de Firma Digital previo a la llegada

del COVID-19. El mismo documento continua mencionando que San José y Heredia muy a pesar de ser de las municipalidades que más avanzadas están en temas de digitalización de servicios a nivel nacional, el estudio arroja hallazgos, situaciones y deficiencias destacables que fueron detectadas justamente previo y durante el periodo de pandemia provocada por el COVID-19, dentro de las deficiencias encontradas podemos destacar:

- En el caso de la Municipalidad de Heredia, se destaca que aunque cuenta con una gran cantidad de servicios digitalizados, algunos usuarios reportaron dificultades para navegar en los sistemas digitales, lo que indica la necesidad de interfaces más intuitivas así como guías y manuales claros de uso, se visibiliza una importante brecha digital que limita la adopción de la Firma Digital, especialmente en poblaciones con carencias y grandes factores de resistencia al cambio como lo son adultos mayores, población con baja alfabetización, entre otros. Se documenta que el personal encargado en el municipio ha reportado que si bien el esfuerzo institucional es mayúsculo en abogar por la digitalización de servicios, dificultades en torno al servicio de Firma Digital han provocado que los resultados estén muy por debajo de la meta esperada, mencionando que solo un 4% de la población han utilizado la Firma Digital como parte de sus trámites o demás interacciones con la institución, y que de este subconjunto de la población, solo el 50% ha reportado que la calidad del servicio sea satisfactoria.
- En el caso de la Municipalidad de San José, se documenta que la situación es aún más confusa, ya que aun para el año 2019 la municipalidad no llevaba ningún registro consultable o estadísticas ni información de dominio público acerca del

proceso de adopción de las nuevas herramientas digitales incluyendo a la Firma Digital. Se documenta que a la hora de querer consultar con las autoridades municipales estas respondieron alegando que dicha información era de índole e interés privado y no podía ser compartida. Se destaca el hecho de que la ventanilla de servicios digitales era extrañamente limitada para el año 2019, limitándose únicamente a los tramites más críticos del servicio municipal como lo son pagos tributarios, solicitudes de patentes o permisos de construcción. Funcionarios municipales si reportaron que el uso de la Firma Digital en tramitología interna de la institución estaba muy ampliamente extendida muy a pesar de la negatoria de la alcaldía por aprobar una directriz que promulgara la transición obligatoria hacia la digitalización en la tramitología interna de la institución.

Concluyendo con el análisis realizado usando a los datos recopilados como muestra representativa sobre el uso y adopción de la Firma Digital en Costa Rica durante y posterior al periodo de crisis sanitario del COVID-19, podemos destacar una amplia situación de rezago técnico y cultural en torno al correcto uso de la herramienta durante el periodo de la pandemia. Una combinación de factores que van desde claro y documentado desinterés cultural, fortalecido por el vació de poder dejado por la falta de claridad en el liderazgo institucional adjunto a la incertidumbre percibida sobre los beneficios e incentivos reales sobre la economía y calidad de vida del segmento popular de la población. Algo que también quedo documentado en el estudio mencionado anteriormente (Facultad de Ciencias Económicas, UCR) donde las encuestas informan que una mayoría generalizada de los usuarios no consideran que la digitalización de los tramites hayan simplificado realmente los procesos administrativos, aunque también

debemos considerar otros factores que alteren la percepción popular, factores que giren en torno a otras situaciones negativas de la administración pública que no necesariamente estén ligadas al uso de la tecnología o medios digitales (burocracia normativa, tiempos de respuesta, etc.).

También tenemos indicios que a partir de los datos revelado por el MICITT en recientes comunicados oficiales de este año que el proceso de adopción retorno a un ritmo favorable a partir del periodo de crisis sanitaria, que se han doblado los esfuerzos institucionales según los informes de una docena de instituciones públicas y de que estamos encaminados en vías hacia un futuro estado de madures tecnológica que permita un mejor uso y explotación de las herramientas de certificados y Firma Digitales actuales.

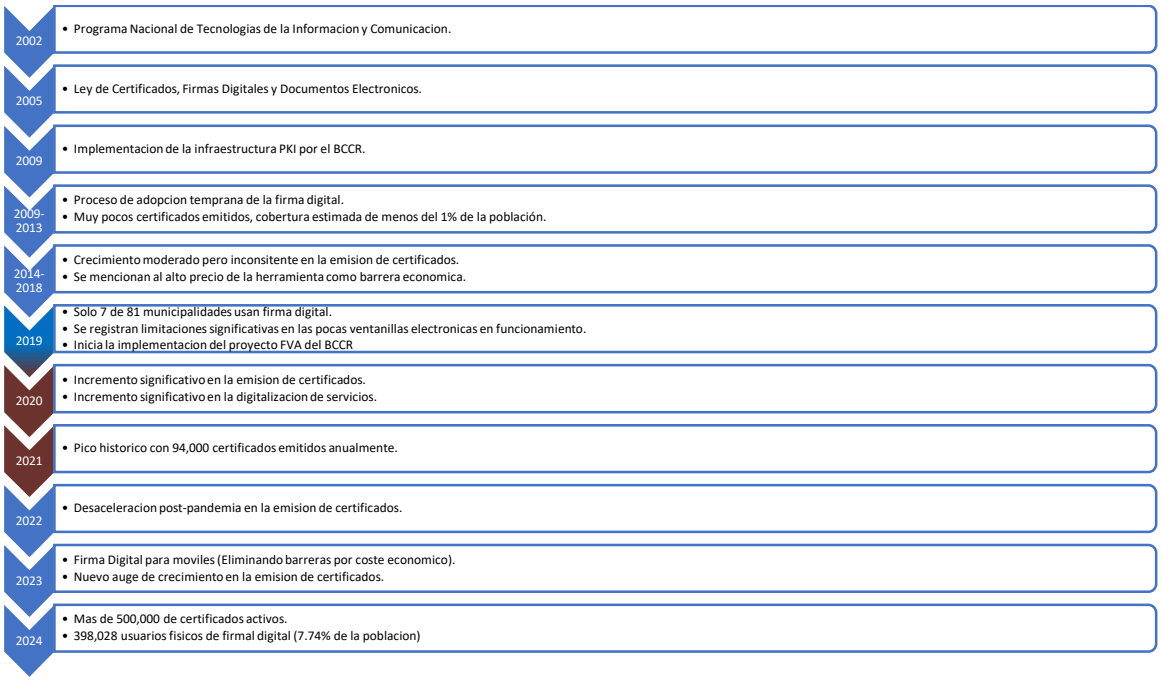


Figura 3. Línea de tiempo de tiempo de Firma Digital en Costa Rica (Elaboración propia)

Desarrollo de la Firma Digital en Estonia

Estonia comenzó su transformación digital en los años noventa, después de independizarse de la Unión Soviética en 1991, y en lugar de seguir el camino tradicional de reconstrucción de grandes obras de infraestructura pública optó por un modelo que se apegara más a sus necesidades estratégicas, lo cual lo llevo a centrarse en la infraestructura tecnológica como el centro de su estrategia de políticas públicas.

Tras su independencia en 1991, Estonia enfrentó importantes desafíos económicos y sociales, un periodo de escasez donde no se contaba con los recursos locales ni las materias primas para invertir en grandes obras de infraestructura en el país, iniciando así una búsqueda intensa de un modelo alternativo de competitividad, llevando a Estonia a lanzar en 1997 el programa "Tigrihüpe" (Salto del Tigre), una iniciativa de alfabetización digital que otorgaba recursos e incentivaba a los ciudadanos a conectarse y participar en la nueva sociedad digital.

Uno de los hitos más significativos fue la promulgación de la Ley de Firma Digital en el año 2000, una de las primeras leyes en el mundo que otorgó el mismo valor legal a las firmas digitales que a las firmas manuscritas. Esto estableció la base para la implementación de la infraestructura de clave pública (PKI), la cual facilitaba el uso de la Firma Digital en documentos y transacciones electrónicas de manera segura y con validez jurídica.

En 2001, Estonia lanzó el sistema X-Road, una plataforma de intercambio de datos que permite la interoperabilidad entre diversas bases de datos y sistemas gubernamentales. X-Road es la columna vertebral del E-Government en Estonia, permitiendo que las

instituciones públicas y privadas intercambien información de manera segura y ofreciendo servicios más eficientes a sus ciudadanos.

Para facilitar el acceso a los nuevos servicios de E-Government, en 2002 Estonia lanzó la tarjeta de identificación electrónica (e-ID), una tarjeta que sirve tanto como documento de identidad física como medio de autenticación digital. Cada ciudadano y residente legal en Estonia tiene una tarjeta e-ID, que funciona con un sistema PKI y contiene las claves privadas que permiten a los ciudadanos firmar documentos electrónicamente y acceder a los servicios del gobierno en línea y realizar transacciones bancarias y comerciales de manera segura.

En 2005, Estonia se convirtió en uno de los primeros países del mundo en ofrecer votación en línea para sus ciudadanos. Este sistema de votación llamado i-Voting, permite a los ciudadanos votar desde cualquier lugar del mundo utilizando su e-ID, una innovación que ha aumentado significativamente la participación electoral.

Para el año 2006 se había logrado el hito de un total de 1,000,000 de certificados validos en circulación, lo que equivale a que un aproximado al 90% de la población económicamente activa contaba con un certificado valido de Firma Digital.

El año 2007 se vio marcado con la salida del servicio Mobile ID, el cual permitía a los ciudadanos utilizar sus propios dispositivos móviles como dispositivo de Firma Digital, esto utilizando las capacidades de un chip SIM especializado que permitía a los ciudadanos el poder portar de forma segura las llaves criptográficas de su Firma Digital consigo y en todo momento.

Durante el año 2007 Estonia se enfrentó a sus primeros casos significativos de ciberataques de escala nacional. Aunque Estonia había avanzado significativamente en la digitalización de su gobierno, este ataque masivo reveló vulnerabilidades críticas en su infraestructura digital, generando dudas sobre la confianza pública en las instituciones gubernamentales responsables. A raíz de dichos acontecimientos el gobierno de Estonia decidió redoblar esfuerzos a partir de 3 ejes claves de toma de decisiones:

- Inversión en Resiliencia Digital; Encadenado con un cambio significativo en las normativas y regulaciones legales, se lanzaron grandes proyectos de protección y resiliencia de datos para las instituciones más importantes del estado. El resultado de este esfuerzo es una red de centros de datos conocidos como “embajadas de datos” a lo largo y amplio de la Unión Europea, de manera que la arquitectura critica del sistema gubernamental siempre contase con respaldos y puntos de contingencia en caso de ataques que comprometieran la continuidad de los servicios locales.
- Inversión en educación y capacitación; Parte importante del presupuesto educativo se utilizó para crear programas de formación en ciberseguridad tanto para funcionarios públicos como para ciudadanos y estudiantes, se fortalecieron los estudios técnicos y superiores en el ámbito de la ciberseguridad y se firmaron convenios con algunas de las principales instituciones académicas de Europa y Norte América.
- Atracción de inversión extranjera; Estonia lideró la iniciativa para establecer el Centro de Excelencia de Ciberdefensa de la OTAN (CCDCOE) bajo suelo y jurisdicción estonio, inaugurado en 2008 en la ciudad capital (Tallin), la OTAN se

encargó de reunir expertos internacionales para desarrollar políticas, estrategias y capacidades de ciberdefensa. Esto consolidó a Estonia como un líder global en ciberseguridad y como un socio estratégico de la OTAN.

A partir del 2011 el gobierno de Estonia se encamino en un proyecto de escala nacional para digitalizar e integrar a la industria médica y farmacéutica del país al proyecto de datos compartidos del estado X-Road. Permitiendo así la integración de los principales sistemas médicos a una unica plataformas de E-Government que estaba a disposición de los ciudadanos 24/7. Esto jugo un papel significativo e importante en lo que fueron posteriormente todos los planes de mitigación y manejo de la crisis sanitaria del COVID-19 en Estonia.

Para el año 2016 se llegaba a un acuerdo extrafronterizo con el resto de la Unión Europea para que sus certificados de Firma Digital pudieran ser oficialmente reconocidos por instituciones públicas de otros estados miembros, lo que al mismo tiempo abría la ruta legal para que residentes Europeos pudieran homologar sus certificados domésticos en el sistema e-Residency de Estonia.

Con una infraestructura digital robusta y políticas innovadoras, para el año 2019 Estonia informa haber logrado que más del 99% de los servicios públicos estén disponibles en línea y el 100% de sus ciudadanos laboralmente activos cuenten con una e-ID valida. Esto provoco que Estonia destacara favorablemente durante el período del COVID-19, donde el uso de la Firma Digital (como principal medio de autenticación segura y jurídicamente reconocida) permitía que la ciudadanía resolviera sus trámites y

necesidades administrativas sin interrupciones aun durante los tiempos de crisis sanitaria.

Para el año 2019 Estonia introduce de forma masiva su nuevo sistema Smart-ID, el cual es un servicio en la nube que permite a los ciudadanos acceder a servicios de firma y autenticación digital aun cuando estos no cuenten con los dispositivos o el soporte de hardware físico requerido. Si bien el servicio se encontraba activo desde el año 2017 como una API consumible, no fue hasta el 2019 que se dispuso de una aplicación móvil que funcionaba como ventana de acceso al servicio Web y que habilitaba un medio de acceso más seguro y controlado para con la información confidencial del usuario. La propia aplicación cuenta con sus controles internos de seguridad como métodos de doble factor de autenticación obligatorios, pensados para asegurarse que los usuarios estén protegidos ante intentos de ataques tipo phishing o ingeniería social.

Desde marzo de 2020, el gobierno estonio procede a declarar el estado de emergencia y cerrar sus fronteras, pero su alto nivel de digitalización de las plataformas de servicios públicos permitieron al país dar un manejo bastante particular a la situación de la crisis sanitaria. Algunos ejemplos son:

- Continuidad de los servicios; Durante el confinamiento, el 99% de todos los trámites gubernamentales se podían realizar en línea, además de que el 100% de la ciudadanía económicamente activa contaba con medios de Firma Digital. Esto permitió de forma paradójica que las ventanillas de servicios físicas pudieran permanecer abiertas en aras de proteger la inclusión social y la protección de la población más vulnerable en tiempos de crisis social y económica. Datos oficiales derivan que un total del 95% de la población activa realizaban sus trámites

gubernamentales de forma digital, dato que se ha mantenido hasta la fecha y que no ha sufrido deterioro aún después del periodo de crisis del COVID-19.

- Automatización en la atención de incidentes: Se asigno personal competente en los diferentes centros de salud e instituciones públicas para que, en casos de situaciones burocracias que requerían atención y seguimiento por parte de los ciudadanos, estos pudieran despreocuparse de la tramitología y concentrarse en la atención de su salud personal y la de sus seres queridos. Algunos ejemplos de esto son; la activación automática del trámite de incapacidad laboral por salud, activación automática de beneficios sociales por riesgo socioeconómico, automatización en procesos de seguimiento médico y él envió de recetas médicas, activación automática de seguros de salud complementarios, notificación y recalendarización automática de citas médicas y audiencias administrativas, entre otros.
- Educación Digital; el 87% de las instituciones educativas pudieron realizar una transición casi inmediata y transparente a la educación en línea gracias al alto nivel de digitalización y a la amplia cobertura de herramientas como la Firma Digital en la población. En este caso es importante destacar la importancia de la respuesta temprana de las autoridades competentes, quienes se encargaron de habilitar masivamente las plataformas de forma planificada incluso semanas antes de haber llegado al punto más crítico de declaratoria de emergencia y aislamiento social provocado por la crisis sanitaria.
- Participación ciudadana; Gracias a las plataformas de E-Government se facilitó enormemente el desarrollo e implementación de soluciones inteligentes en

términos de logística, respuesta a crisis y ayuda comunitaria. El mismo gobierno se encargó de llevar a cabo campañas de innovación "Hack the Crisis" con el cual buscaban concentrar esfuerzos colaborativos para sacar provecho utilizando las plataformas digitales instaladas, con el objetivo de resolver y aliviar problemáticas provocadas por la misma crisis sanitaria.

En 2020 el informe anual de la autoridad reguladora de Información y Sistemas (Information System Authority Yearbook 2020) revelo algunos datos relevantes de dicho periodo anual, de los cuales podemos mencionar:

- El 99% de las prescripciones medicas fueron digitales.
- Se disponen de más de 5000 servicios público-privados donde el usuario se puede identificarse con su e-ID.
- El 98% de las declaraciones y pagos de impuestos fueron a través de las plataformas digitales.

Factores sociopolíticos y económicos que influyeron en ambos países

En el ámbito socioeconómico podemos destacar algunas situaciones que ocurrieron en paralelo a la situación de crisis sanitaria del COVID19 para uno de ambos países bajo estudio:

Crecimiento económico: Primero que todo, hay que destacar que las economías de Costa Rica y Estonia no son comparables, ni tampoco es el objetivó de este estudio el realizar una comparación macroeconómica directa entre ambos países.

El caso de Estonia es muy diferente y presenta un crecimiento significativamente más acelerado en su PIB per cápita. Mientras que Costa Rica y Estonia tenían economías

comparables para el año 2000 (donde el PIB per cápita de Costa Rica era de 3,941 USD y el de Estonia de 4,084 USD), actualmente ya para el año 2024 se proyecta que la diferencia se haya maximizado al punto de que Estonia ya doble a Costa Rica en términos de PIB per cápita, con proyecciones de 31,530 USD y 17,860 USD respectivamente. Este contraste refleja diferencias importantes en las estrategias de desarrollo y diversificación económica adoptadas por cada país, provocando así que realizar una comparación cuantitativa de sus números netos sea inviable de realizar sin una exhaustiva investigación macroeconómica que acompañe dicho análisis. Por tanto, nos vamos a enfocar en otros dato derivado que nos puede ayudar a comprender de mejor manera la situación socioeconómica suscitada en ambos países durante y después del periodo del COVID-19.

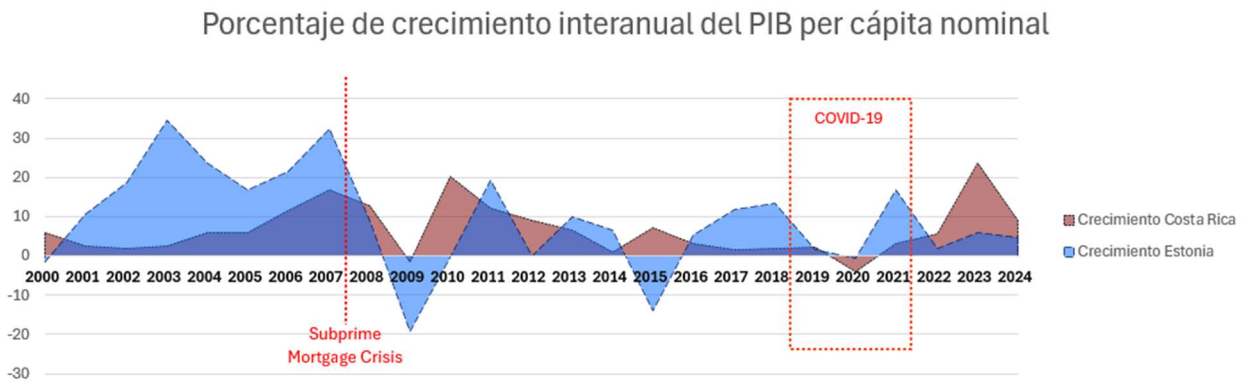


Gráfico 2. Comparativa de crecimiento económico de Estonia y Costa Rica periodo 2000-2024 (Fondo Monetario Internacional)

Durante el periodo inicial del nuevo milenio (2000-2007) Costa Rica experimentó un crecimiento económico moderado pero consistente, el país consolidó su posición como un destino turístico clave y reforzó sectores como la agricultura, el turismo sostenible y la exportación de productos electrónicos (Intel estableció su planta en 1997). Mientras

tanto Estonia mostró un crecimiento más acelerado, con datos de crecimiento interanuales que rondaban normalmente por encima del 20% interanual, periodo que fue marcado en Estonia por su acelerada digitalización e integración en la Unión Europea, lo que atrajo consigo grandes capitales de inversión extranjera.

Todo este auge de crecimiento se vio frenado por la Crisis Financiera del 2007, y queda demostrado en las estadísticas de ambos países, el siguiente fue un periodo de inestabilidad donde el crecimiento del PIB per cápita deja de ser un tema de previsible y pasa a ser un valor inestable y cambiante, dando paso a resultados más modestos y tendencias que no siempre apuntaban al alza.

Ya para la llegada del COVID-19 las económicas de ambos países eran muy distante, mientras Estonia tenía desempeños propios de un país del bloque occidental de la Unión Europea, Costa Rica aún se encontraba dando pequeños pasos en términos de avance económico, destacando severos problemas de crecimiento que sufría el país desde el año 2016.

Durante la pandemia el PIB per cápita de Costa Rica cayó de 12,669 USD a 12,163 USD para el 2020 debido al impacto del COVID-19, con demarcada afectación a actividades económicas clave como el turismo (un pilar de la economía costarricense).

Por su parte, Estonia mostró una resiliencia notable durante la pandemia. Aunque su PIB per cápita disminuyó ligeramente de 24,023 USD a 23,911 USD en 2020, creció rápidamente a 27,966 USD en 2021 y 28,469 USD en 2022.

Cabe resaltar la rápida y acelerada recuperación de la economía de Estonia tras momentos de crisis global, durante la pandemia de COVID-19 Estonia mostró una

resiliencia notable, no solo evitando que el país entrara en un periodo de recesión y decrecimiento mayor (como si fue el caso de Costa Rica y otros países), el gobierno estonio pudo contener dicha recesión apenas meses después de haber pasado el pico pandémico de la primera ola de COVID-19 (primera mitad del 2020), apenas meses después de haber publicado su declaratorio de emergencia, ya para finales del 2020 e inicios del 2021 el gobierno estonio estaba implementando planes efectivos de recuperación económica. Planes de política público-privada como el impulso de plataformas digitales seguras en tiempos de pandemia fueron clave para una recuperación temprana de la capacidad productiva del país, un ejemplo de esto fueron las campañas “Close the Digital Divides”, con el cual el gobierno de Estonia buscaba liderar la iniciativa de interconectar sistemas públicos entre diferentes estados miembros de la Unión Europea con el fin de facilitar la implementación de soluciones inteligentes de logística de transporte comercial y recursos médicos a lo largo de la Unión Europea.

Este tipo de iniciativas, sumadas a incentivos fiscales y a un muy positivo manejo de la crisis fitosanitaria (promovido en gran medida por las plataformas digitales de servicios) es lo que permitió que Estonia en menos de un año volviera nuevamente a tendencias de crecimiento económico y a volver a repuntar para el año 2021 como una de las economías desarrolladas con mayor auge de crecimiento económico y avance tecnológico.

Manejo epidemiológico de las crisis sanitaria

El manejo efectivo de la crisis del COVID-19 en Estonia se atribuye a varios factores claves en cuanto a la aplicación de políticas públicas y al buen uso e implementación de la infraestructura digital promovida por el estado.

El gobierno estonio implementó medidas rápidas y decisivas, como la declaración de estado de emergencia y restricciones de movilidad, lo que permitió una respuesta oportuna a la propagación del virus. Decisiones que fueron tomadas en el contexto de confianza que existía sobre la infraestructura digital publica instalada, lo que llevo de forma casi inmediata a las autoridades públicas a iniciar campañas de migración masiva a entornos de trabajo remoto, plataformas virtuales de servicios y comercio electrónico.

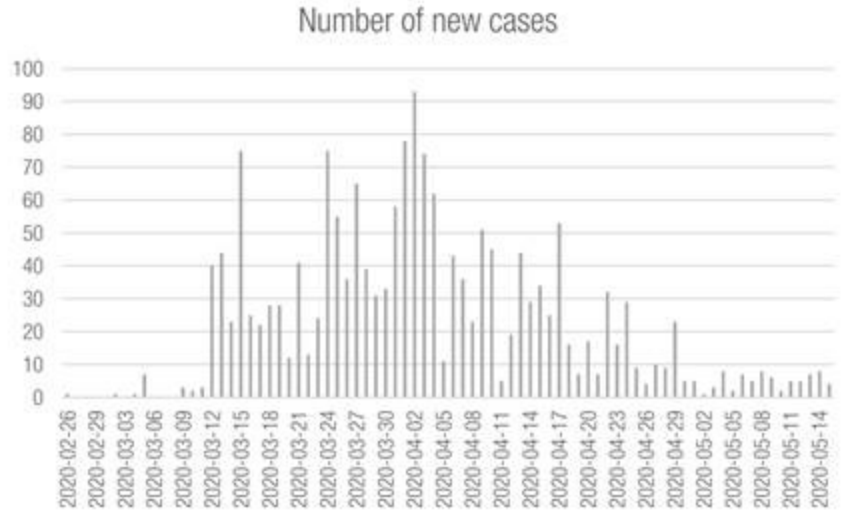


Gráfico 3. Numero diario de casos nuevos de COVID19 en Estonia (Tallinn University of Technology, Estonia)

El resultado de todos estos esfuerzos se puede ver revelado en los datos en torno al manejo de la crisis sanitaria, donde Estonia destaca por haber tenido una de las afectaciones más leves y controladas de toda la Unión Europea. Por ejemplo, la ventana de tiempo de las restricciones sanitarias de Estonia fue la más baja de entre los países bálticos, declarando emergencia sanitaria dentro del periodo comprendido entre el 13 de marzo al 17 de mayo del año 2020, con un total de únicamente 1,870 casos registrados al momento de finalización del estado de emergencia, lo cual representa alrededor de un

0.14% de la población. A fecha de julio del 2022 Estonia registraba un total de 582,867 casos confirmados, lo que suponen un aproximado al 43.1% de la población del país, un crecimiento sustancial desde los años previos de crisis sanitaria, con la salvedad de que las autoridades estonias abogaban que dicho crecimiento estaba estrictamente ligado a la apertura fronteriza de libre tránsito con la Unión Europea. Por su contraparte, Costa Rica tuvo que manejar un control de la pandemia que se vio atropellado debido a las necesidades económicas inminentes que debía atender el país entorno a la productividad del sector turismo, el cual era una de las industrias más importantes del país y que a su vez es una de las industrias que representan un riesgo mayor de contagio y propagación pandémico, así fue como Costa Rica en un entorno de presión social e intereses enfrentados entre las organizaciones de salud pública y cámaras y asociaciones comerciales, se tuvo que extender el estado de emergencia y medidas sanitarias desde el 16 de marzo del 2020 hasta el 10 de agosto del 2022, manteniendo restricciones sanitarias por un periodo aproximado de 2 años y 5 meses. Estas medidas prolongadas permitieron mantener la crisis sanitaria bajo el control de las capacidades operativas del sistema de salud pública, reportando a fecha de mayo del 2022 un total de 904.934 casos confirmados, lo que representa un aproximado al 17.9% de la población.

Y si bien Costa Rica tuvo un manejo positivo de la pandemia en términos de salud pública y seguridad social, el efecto sobre la económica que tuvieron esos 2 años y 5 meses de restricciones sanitarias se pueden ver reflejados en los datos, donde no fue sino hasta el año 2022 que se pudo observar un proceso de recuperación económica significativo que permitiera compensar el rezago de los años anteriores, eso, sin mencionar otras áreas

que igualmente se vieron severamente afectadas como; el rezago educativo, déficit fiscal, aumento en la brecha de desigualdad económica, entre otros.

4.1.2 Infraestructura y Políticas de Firma Digital

Estonia ha desarrollado una arquitectura PKI más robusta, interoperable y ampliamente interconectada, lo que les permite liderar a nivel global en digitalización y ciberseguridad. Costa Rica, aunque cuenta con una base sólida, necesita abordar desafíos relacionados con la accesibilidad, interoperabilidad y percepción pública para aprovechar plenamente su infraestructura PKI y expandir el uso de las herramientas de Firmas y Certificados Digitales para así poder explotar al máximo la tecnología instalada y percibir realmente beneficios cuantificables de todo el esfuerzo técnico y político realizado hasta la fecha.

El análisis a nivel de sistema y E-Government se va a realizar en 7 diferentes ejes, 4 de ellos enfocándose en el apartado técnico de la Infraestructura y los 3 enfocándose en el apartado político y normativo.

- Interoperabilidad; Estonia supera significativamente a Costa Rica en interoperabilidad, integrando su PKI en el sistema X-Road, lo que permite el intercambio seguro de datos entre instituciones y países de la UE. Además, el sistema es completamente transparente e interoperable para cada una de sus diferentes soluciones tecnológicas de cara al usuario, con las adiciones de Mobile-ID y Smart-ID Estonia se asegura un nivel de accesibilidad y facilidad de uso muy superior al entorno actual de otros países como el caso de Costa Rica.
- Seguridad y actualización; Ambos países utilizan estándares criptográficos internacionales (X.509 y RSA), por lo cual no se encuentra necesariamente

diferencias relevantes en términos de seguridad técnica de las herramientas implementadas. Además, se implementan los mismos estándares de seguridad de datos impulsados por el NIST (The National Institute of Standards and Technology es una agencia federal de Estados Unidos de América). En términos de capacidades regulatorias Estonia si cuenta con una ventaja significativa sobre Costa Rica y es la integración de normas y estándares con la Unión Europea, lo cual no solo genera un marco regulatorio más robusto, sino que facilita la integración practica y mayor potencial subsecuente en cuanto al uso transfronterizo de la herramienta.

- Accesibilidad: A partir del año 2019 se introduce de forma masiva el servicio de Smart-ID como plataforma homologa al servicio tradicional de Firma Digital. Este es un cambio revolucionario porque permite a todos los ciudadanos la posibilidad de acceder a las funciones de Firma Digital como un servicio SaaS en la nube (Software as a service), una plataforma que funciona independientemente de las cualidades del dispositivo del usuario y que implementa los más altos estándares de seguridad digital para proteger a sus usuarios de ataques cibernéticos. El punto más revolucionarios de esta herramienta es su capacidad de permitir que los ciudadanos accedan dicho servicio aun fuera de las fronteras del país, permitiendo por ejemplo que un ciudadano estonio realice tramites claves como el registro o la renovación de su certificado sin la necesidad de presentarse físicamente en una oficina o embajada para hacerlo. A nivel de arquitectura esto es una ventaja enorme con la cual no se cuenta en la jurisdicción costarricense, y si bien, no necesariamente es un factor que haya jugado un papel importante en el éxito de

adopción histórica del e-ID en Estonia, si será un factor importante para en un futuro próximo se amplíen aún mas las brechas y diferencias en términos de expansión y capacidad tecnológica en comparación a otro países como la actual arquitectura costarricense.

- Falta de control de especificaciones técnicas en el proceso de emisión: Mientras que en Estonia la operación de emisión de certificados esta subcontratada a empresas privadas, cada contratación cuenta con una delimitación de especificaciones técnicas que deben acatar además de las regulaciones técnicas impuestas por el ente regulador (Estonian Information System Authority), esto permite en Estonia tener un control estricto, centralizado y más granular de las especificaciones técnicas y cualidades de cada certificado, ayudando a facilitar el soporte y planificaciones en temas de homologación de hardware y temas de manejo de la incompatibilidad tecnológica. En Costa Rica por su contraparte, si bien el MICITT y el BCCR define especificaciones que deben seguir cada uno de los certificados emitidos, estos no tienen un control granular de las especificaciones de hardware puntuales que se utilizan en cada certificado, permitiendo que ocurran situaciones reportadas por los usuarios tales como; certificados emitidos sin la inclusión de todos sus respectivos certificados intermedios, así como la circulación de lectores y tarjetas de Firma Digital incompatibles entre sí por utilizar formatos reducidos del estándar ISO/IEC 7816 (Estándar establecido por el MICITT).

Análisis de las políticas públicas y su impacto en el proceso de adopción

- Inversión en soporte; Estonia ha integrado su PKI con una variedad de servicios, liderando proyecto como votaciones en línea hasta recetas electrónicas, mostrando una implementación ágil en términos de liderazgo institucional. Además la propuesta del modelo regulatorio de Estonia difiere en gran medida por su alto nivel de subcontratación y terciarización sobre el soporte de las tecnologías y servicios que forman parte de la plataforma de E-Government del país (E-Service), en el caso de la Firma Digital, por ejemplo, la principal empresa privada detrás del soporte de las herramientas es “SK ID Solutions”, además de que el gobierno estonio obliga de forma regulatoria a sus subcontratantes a trabajar en herramientas de código abierto y liberar documentación técnica para todo aquellos casos que no involucren la confidencialidad y seguridad de los sistemas implementados, regulación que dio origen a iniciativas como “Open eID”, donde las autoridades públicas, empresas subcontratadas y terceros pueden colaborar en el desarrollo de herramientas técnicas que favorezcan la adopción y uso libre de las herramientas. Esta estrategia enfocada en inversión pública en innovación y colaboración abierta con herramientas de software libre han sido claves para el avance del modelo digital estonio, un país que, según declaraciones de sus lideres parlamentarios; era un pionero en su área y por ende debía tomar la iniciativa técnica de liderazgo en sus propias manos.
- Planificación y adopción; Estonia alcanzó una adopción masiva gracias a su enfoque temprano y alto grado de inversión económico y recursos jurídicos en estrategias clave como la tarjeta e-ID obligatoria, Open-eID, programas de

interoperabilidad de datos, subcontratación de terceros expertos e inversión en alfabetización digital y concientización en Ciberseguridad. Por contraparte las autoridades costarricenses no han podido mantener el ritmo en agilidad de implementación o interés de financiación, y si bien los primeros esfuerzos en política y normativa costarricense llegaron lo suficientemente temprano, lo cierto es que la poca capacidad de reacción administrativa para aplicar dicha normativa y así poner a disposición las nuevas herramientas tecnológicas ha venido generando rezagos, esto ha sido un problema constante a lo largo de la línea de tiempo histórica desde la primera etapa de implementación por allá del año 2008, demarcando faltas graves en términos de inversión económica e impacto por parte del liderazgo institucional.

Otro de los ejemplos en los cuales se puede representar la falta de liderazgo institucional costarricense es la falta de iniciativas para tomar medidas con el objetivo de homologar el sistema de Firma Digital actual con otros documentos oficiales del estado. Mas concretamente, falta de iniciativas para homologar el sistema de Firma Digital con el sistema de Cedulas de Identidad que es administrado por el TSE (Tribunal Supremo de Elecciones), una iniciativa que podría otorgar a los 2 documentos el mismo valor y reconocimiento jurídico, en el cual, por una cuestión de tecnicismos administrativos hasta la fecha no ha podido ser llevado a cabo. En un reporte publicado por el medio de comunicación Delfino.cr se informaba que el costo de producción de una Cedula de Identidad ascendía a $7.29 dólares americanos (2022, Denfino.cr), mientras que el costo de emisión de una tarjeta electrónica de Firma Digital es de $32 dólares americanos

(costo de producción + costos administrativos y comisiones), una iniciativa de homologación podría crear una nueva alternativa donde los ciudadanos podrían adquirir el documento de Firma Digital sin pagar o pagando únicamente el sobrecoste determinado de dicha operación, con el beneficio de que el nuevo documento podría cumplir una doble función. Otro ejemplo sería el de una iniciativa que permitiese liberar a los servicios de emisión de Firmas Digitales del pago de gravámenes tributarios como el IVA, así como otros beneficios tributarios que permitan hacer a la herramienta más atractiva de cara al usuario.

- Incumplimiento sistemático de la normativa legal:

  Desde el año 2006 y según la publicación del Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Nº 33018) existen las herramientas administrativas para incentivar el uso de la Firma Digital como método de personificación jurídica durante tramites y procesos administrativos, según determina dicho reglamento en su capítulo primero artículo 4 donde dice “el Estado y todas las dependencias públicas incentivarán el uso de documentos electrónicos, certificados y firmas digitales para la prestación directa de servicios a los administrados…”, esto, junto con la resolución ejecutiva del MICITT publicada en 2014 bajo serie N° 067-MICITT-H-MEIC define los pasos necesarios que debería seguir a administración pública para la correcta adopción de la Firma Digital en sus operaciones y tramitología. Esto en resumen se podría interpretar de la siguiente forma; que el sector público costarricense y sus dependencias deben acatar la normativa existente, y por ende, se encuentran en la obligación de considerar la validez legal de la Firma Digital (toda firma que cumpla con la

normativa vigente), y en caso de no poder dar trámite conforme a la ley, se deben tomar medidas acorde a la resolución N° 067-MICITT-H-MEIC, siempre que esto se ajuste a sus capacidades presupuestarias. La resolución del MICITT incluso va más allá y determina que cualquier nuevo desarrollo en materia de Sistemas de Información presupuestado por cualquiera de las dependencias del estado debe obligatoriamente contemplar la inclusión de la Firma Digital como medio de autenticación. Todo lo anterior mencionado ha sido fuente de polémica en torno a la situación jurídica de la administración pública, al menos desde la fecha límite de la resolución del MICITT establecida en 2016, esto debido a que dicha normativa ha sido (hasta la fecha) sistemáticamente ignorada, puesto que no existen métodos ni procesos de evaluación o control de calidad que permitan dar seguimiento al cumplimiento de la norma, tal y como lo menciona el proyecto de ley “Adición de un artículo 9 bis a la Ley de Protección al Ciudadano del Excelso de Requisitos y Trámites Administrativos N°8220, para la implementación de Sede Digital en el sector público”, expediente N°20.089 del año 2016, proyecto el cual además argumenta que debido a dichas falencias de control y seguimiento es difícil poder determinar si la capacidad instalada del sistema de Firma Digital esta subutilizada o incluso poder llegar a determinar un grado cuantificable de subutilización de la misma.

4.1.3 Cobertura y Adopción de Tecnologías de Firma Digital

Mientras que Estonia se ha consolidado como un referente global en la adopción y uso de la Firma Digital, Costa Rica muestra un rezago significativo en términos de expansión y adopción. Las diferencias radican principalmente en la visión estratégica, la

infraestructura tecnológica y la aceptación cultural. Para cerrar esta brecha, Costa Rica debe enfocarse en soluciones más accesibles, interoperabilidad y campañas educativas que muestren los beneficios de la Firma Digital.

Aspecto	Costa Rica	Estonia
Cobertura de la Población (2024)	Un 7.74% de la población cuenta con certificados activos (398,028 certificados para personas físicas).	Más del 98% de los ciudadanos utilizan regularmente la e-ID para interactuar con servicios digitales.
Factores Técnicos	- Requiere hardware específico (lectores de tarjetas).	- No presenta barreras significativas en infraestructura.
Uso Popular	Limitado principalmente a trabajadores públicos y profesionales en actividades formales.	Usado por prácticamente todos los ciudadanos en actividades diarias (banca, salud, votaciones).
Resistencia Cultural	Alta: la Firma Digital es percibida como una herramienta burocrática y compleja.	Baja: adoptada ampliamente gracias a una cultura tecnológica, control centralizado de sistemas y campañas efectivas de alfabetización digital.
Crisis del COVID-19	Aceleró la adopción en servicios críticos, pero la expansión fue limitada por la falta de soluciones accesibles como la Firma Digital Móvil.	La infraestructura digital avanzada permitió continuidad permanente de servicios, impulsando aún más su adopción, especialmente en su uso transfronterizo.

Adopción de la Firma Digital en cooperación público-privado de ambos países

Estonia lidera ampliamente las métricas en cuanto a adopción de la Firma Digital, con una integración efectiva entre los sectores público y privado, impulsada por una infraestructura sólida, soluciones accesibles y una cultura digital avanzada. Costa Rica, aunque ha progresado, enfrenta desafíos significativos en términos de accesibilidad, percepción cultural y ecosistema colaborativo.

El sistema X-Road de Estonia es una ventaja competitiva significativa en términos de integración y el nivel de interoperabilidad y transparencia que existe en dicha arquitectura es clave para la integración de agentes privados.

4.1.4 Hallazgos del análisis comparativo

En términos técnicos el análisis comparativo de los 2 casos de estudio se pueden resumir de la siguiente manera:

Aspecto Técnico	Costa Rica	Estonia
Base legal	Ley de certificados en 2005. Implementación de la norma en 2008.	Ley de certificados en 2000. Implementación de la norma en 2002.
Infraestructura de Clave Pública (PKI)	Basada en estándares X.509 y RSA	Basada en estándares X.509 y RSA
Certificados Emitidos	Emitidos para personas físicas, jurídicas y servicios gubernamentales	Emitidos para personas físicas, jurídicas y servicios interoperables a través de e-ID
Compatibilidad	Utiliza hardware (lectores de tarjetas y tokens USB) para firmar digitalmente	Amplia interoperabilidad con Mobile-ID, Smart-ID (en la nube) y e-ID basado en tarjetas
Seguridad Criptográfica	Utiliza algoritmos RSA de 2048 bits y SHA-512	Algoritmos avanzados RSA de 2048 bits, con actualización periódica según estándares de la UE
Validación de Certificados	A través del servicio FVA (Firmador, Validador y Autenticador) del BCCR	Integrada en el sistema X-Road
Interoperabilidad	Limitada a sistemas locales e instituciones del gobierno	Totalmente integrada en servicios transfronterizos de la UE (Reglamento eIDAS) X-Road para el uso compartido de datos.
Usabilidad	Requiere hardware específico y es menos flexible en dispositivos móviles	Soluciones más accesibles con Mobile-ID y Smart-ID, sin necesidad de hardware adicional
Tiempos de Implementación	Inicialmente limitada (2009) y con adopción moderada hasta 2020	Implementación masiva desde principios de la década de 2000
Impacto Social y Alcance	Uso aún limitado, con cobertura estimada en un 7.74% de la población (2024)	Amplia adopción con más del 98% de los ciudadanos utilizando servicios de e-ID
Estrategia administrativa	Regulación centralizada. Desarrollo e implementación descentralizados.	Regulación centralizada. Implementación centralizada. Desarrollo colaborativo.

Finalizando con la parte de análisis comparativo, podemos determinar a través de una interpretación de los datos recolectados, menciones y referencias, una seria de puntos resolutorios que nos pueden ayudar a esclarecer preocupaciones clave de los objetivos de este proyecto, por ejemplo:

- Se identifica en Costa Rica un avance muy limitado en el proceso de adopción de Firma Digital, y si profundizamos y ahondamos en detalles normativos podemos encontrar que la situación actual del país se ve reflejada en las preocupaciones de legisladores y demás autoridades y expertos técnicos que destacan la incapacidad administrativa derivada de la carencia de métodos de control y seguimiento en cuanto al cumplimiento normativo en el proceso de adopción del servicio de Firma Digital.
- El proceso de gestión de Firma Digital en Estonia esta demarcado por una fuerte tendencia en apostar por modelos de desarrollo colaborativo, uso de herramientas de código abierto, control estricto y centralizado del proceso de implementación tecnológica, así como fuertes incentivos políticos y fiscales a la hora de impulsar la adopción masiva de los servicios digitales provistos y liderados por el estado.
- Que a pesar de que Estonia presenta un modelo de adopción más agresivo, y que la efectividad de dicho modelo se ve reflejada en términos de escala y cobertura frente al caso Costarricense, es necesario resaltar el hecho de que ambas arquitecturas están basadas en el mismo conjunto de tecnologías y que ambas arquitecturas comparten la gran mayoría de especificaciones de software entre sí, lo cual nos puede indicar que, con una inversión de esfuerzos enfocados principalmente a solventar cualquier problema remanente de incompatibilidad,

sería viable evaluar replicar soluciones independientes de la arquitectura de software de Estonia dentro del sistema costarricense de Firma Digital.

- Por último, que si bien la pandemia tuvo consecuencias lamentables para todos los países del globo, es importante resaltar como una robusta implementación de E-Government puede significar una diferencia sustancial en el grado de libertad de toma de decisiones, especialmente a la hora de tener que implementar medidas o políticas restrictivas en momentos de crisis. En este caso se puede interpretar que Estonia contaba con libertades, oportunidades y alternativas de software con las cuales Costa Rica no contaba.

4.2 Validación técnica del prototipo de Middleware de Autenticación.

Para determinar la viabilidad de un middleware funcional es necesario comprender los paralelismo técnicos de algunas de las soluciones implementadas en el modelo de arquitectura de firma de Costa Rica y Estonia.

Uno de los paralelismos clave se encuentra entre la solución SmartID de Estonia y el sistema de “Firmador Validador Autenticador” (FVA) del Banco Central de Costa Rica (BCCR). Ambas soluciones buscan garantizar la autenticidad, integridad y no repudio de las transacciones electrónicas mediante el uso de firmas digitales, así como también ambas soluciones disponen de APIs (Application Programming Interfaces) que permiten a aplicaciones de terceros acceder a las funciones de la Firma Digital como método de autenticación. Esto abre la posibilidad de desarrollar “middleware” o adaptadores de software que permitan traducir y codificar dichas interfaces de comunicación dentro de

protocolos de autenticación que sean más populares, con mayor potencial de adopción para maximizar la cuota de mercado objetivo, abriendo así un nuevo marco de posibilidades donde aplicaciones existentes podría incorporar las funciones del “Firmador Validador Autenticador” realizando cambios mínimos a su arquitectura y por ende implicando menos riesgos de implementación.

4.2.1 Diseño del Prototipo de Middleware de Autenticación

Lo importante del diseño de un prototipo funcional es validar la existencia de soluciones previas o software estandarizado que sea aprovechable debido a sus antecedentes en términos de adopción y éxito.

Un ejemplo destacado de esto es la implementación exitosa de los estándares IETF 6750 y IETF 6749 en Estonia, específicamente en el proyecto Authentigate, desarrollado por la empresa subcontratada SK ID Solutions.

El proyecto Authentigate, implementa las funcionalidades de SmartID y sirve como medio para transformar y ofrecer las funciones y beneficios de SmartID como parte de los protocolos de autenticación OAuth 2.0 y OpenID.

La experiencia de Authentigate es un ejemplo claro de cómo puede ser implementado middleware con el fin de incorporar estándares y protocolos ampliamente utilizados en el mercado, mejorando el proceso de adopción de nuevas herramientas.

El diseño aquí propuesto tiene como objetivo principal buscar facilitar el acceso abierto a las capacidades de software necesarias para impulsar la tecnología de Firma Digital hacia un proceso acelerado de adopción, resolviendo limitaciones técnicas y facilitando

soluciones a temas de compatibilidad e interoperabilidad entre distintas tecnologías de Internet.

Validación de las tecnologías disponibles para su uso en el prototipo.

Los estándares IETF 6749 y IETF 6750 son los fundamentos técnicos que permiten la gestión segura de autenticación y autorización en aplicaciones modernas en internet.

IETF 6749 (OAuth 2.0): Orientado en proporcionar un marco flexible para delegar permisos mediante la generación de tokens de acceso.

IETF 6750 (Bearer Token Usage): Especifica cómo los tokens de acceso deben ser utilizados y transmitidos a través de interfaces HTTP.

El uso de estas tecnologías ha facilitado la adopción masiva de estándares de autenticación como OpenID Connect (OIDC). Hoy en día, plataformas web y servicios Cloud líderes como Google Cloud, AWS, Microsoft Azure, y aplicaciones como Facebook, LinkedIn, y Spotify, utilizan OIDC como parte de sus sistemas de inicio de sesión federado.

También existe el Proveedor de OIDC, que es una entidad o servicio que implementa el protocolo OpenID Connect (OIDC) para facilitar la autenticación de usuarios y la distribución de información sobre su identidad mediante tokens seguros. Este proveedor actúa como intermediario confiable entre una autoridad de gestión de identidades y otras aplicaciones cliente (de terceros), facilitando los medios para usar dicho servicios para identificar y autorizar a sus usuarios, para esto, OIDC emplea un estándar de comunicación cliente-servidor mediante el uso de Json Web Tokens.

Por otros lado tenemos a Authlib, esta una biblioteca de código abierto desarrollada en Python que proporciona herramientas completas para implementar el protocolo OAuth 2.0 y OpenID Connect (OIDC). Está diseñada para facilitar la construcción de sistemas de autenticación y autorización seguros, escalables y compatibles con estándares internacionales. Aunque no es un proveedor OIDC por sí mismo, permite crear y configurar uno, cumpliendo con todas las responsabilidades técnicas necesarias (en cuanto a estándares de seguridad) para desempeñar esta función de forma segura.

Authlib puede ser utilizado para desarrollar un módulo especializado que sirva como un puente entre el servicio Firmador Validador Autenticador (FVA) del BCCR y otras aplicaciones web de terceros que requieran interfaces o servicios OAuth y OIDC. Al ser una biblioteca modular, Authlib acelera el desarrollo de la solución, reduciendo los costos y el esfuerzos en código redundante, además de que es flexible como para desarrollar flujos de autenticación personalizados, algo clave para su funcionamiento como intermediador del FVA bajo la normativa legal.

Requerimientos del prototipo

Se presentan a continuación los principales requerimientos técnicos que forman parte de la propuesta de software de código abierto “middleware”, con el cual se busca satisfacer las preocupaciones e inquietudes plasmadas como parte del objetivo de este proyecto de investigación:

Propuesta: Servicio OIDC estandarizado para la implementación masiva de métodos de autenticación por medio de Firma Digital Costa Rica (SOIDCFDCR).

ID	REQ-001
Nombre	Integración de los conceptos formales de “Cloud Native”
Descripción	La arquitectura y diseño de la solución deben ajustarse a la definición oficial de "Cloud Native" documentada por Microsoft, que implica adoptar principios como serverless, containerization, DevOps, y desarrollo orientado a servicios.
Justificación	Maximizar la resiliencia y portabilidad de la solución, apuntando a procesos de implementación minimalistas y transparentes en entornos de computación en la nube. Facilitar el cumplimiento normativo de estándares internacionales de seguridad valiéndose del soporte experto disponible en plataformas Cloud.
Referencia	Documentación oficial “Microsoft Cloud Native Documentation”
Criterios de Aceptación	1. Arquitectura basada en microservicios.
	2. Uso de contenedores para implementación.
	3. Código compatible con la implementación de DevOps.

ID	REQ-002
Nombre	Implementación de cliente para el API FVA del BCCR
Descripción	El sistema debe implementar la implementación de WCF (Windows Communication Foundation) para el "Firmador Validador Autenticador" siguiendo las especificaciones técnicas del BCCR documentadas en el estándar "Firmador Validador y Autenticador".
Justificación	Cumplir con la normativa nacional en el uso de firmas digitales y servicios asociados.
Referencia	Documento del BCCR: "Estándar Electrónico Firmador Validador y Autenticador".
Criterios de Aceptación	1. Conformidad técnica con las guías del BCCR.
	2. Capacidad de acceder a los servicios para firmar, validar y autenticar documentos conforme al estándar mencionado.

ID	REQ-003
Nombre	Método de autorización RSA para Firma Digital
Descripción	Implementar un método de autorización para validar archivos firmados utilizando la criptografía RSA apuntando a la utilización de los certificados emitidos por la cadena de confianza oficial de la autoridad certificadora del BCCR.
Justificación	Garantiza y facilita la seguridad y autenticidad en el proceso de inicio de sesión web con el correcto manejo y uso de documentos firmados con Firma Digital.
Referencia	Documento del BCCR: "Estándar Electrónico Firmador Validador y Autenticador".
Criterios de Aceptación	1. Validación criptográfica RSA implementada.
	2. Compatibilidad con los certificados de la autoridad certificadora del BCCR.

ID	REQ-004
Nombre	Servicio Web OIDC integrando Authlib
Descripción	Utilizar el proyecto de código abierto Authlib para implementar un servicio web que cumpla como servidor proveedor de OpenID Connect (OIDC), cumpliendo con los estándares de OAuth 2.0 y OpenID 1.0 definidos por la OpenID Foundation.
Justificación	Proveer un mecanismo estándar y seguro de autenticación federada usando tecnologías existentes y ampliamente adoptadas en la Web. Authlib ofrece como parte de su documentación técnica los datos de las referencias de todas las certificaciones implementadas en la herramienta para el cumplimiento de los estándares internacionales entorno a los protocolos OAuth 2.0 y OpenID 1.0.
Referencia	Documentación técnica de OpenID Foundation.
Criterios de Aceptación	1. Servidor web funcional con capacidad OIDC.
	2. Cumplimiento de los estándares de OAuth 2.0 y OpenID 1.0.

ID	REQ-005
Nombre	Manejo de archivos confidenciales con Apache Libcloud
Descripción	Implementar el proyecto Apache Libcloud para la gestión de archivos firmados, autorizaciones digitales, datos de sesión y datos de usuarios, utilizando los estándares de seguridad recomendados por los proveedores de almacenamiento en la nube.
Justificación	Asegurar el manejo seguro y eficiente de información sensible en entornos Cloud.

	Apache Libcloud es muy transparente en aspectos de seguridad y ofrece como parte de su documentación oficial los detalles relacionados al debido cumplimiento de las normativas de los principales proveedores de almacenamiento en la nube.
Referencia	Documentación oficial de Apache Libcloud.
Criterios de Aceptación	1. Integración funcional con los principales proveedores de almacenamiento en la nube (Amazon Web Services y Microsoft Azure).

ID	**REQ-006**
Nombre	Implementacion de JWT con Claims Personalizados
Descripción	Definir e implementar un token JWT (Json Web Token) acorde a los estándares del IANA para OpenID 1.0, incluyendo los claims personalizados para identificación de usuarios y sesión; un identificador único (GUID) del archivo firmado que autoriza la sesión de usuario, así como la huella digital SHA256 de dicho archivo en formato hexadecimal.
Justificación	Garantizar integridad y trazabilidad de los archivos firmados.
Referencia	Especificaciones de JWT en OpenID 1.0.
Criterios de Aceptación	1. JWT con claims personalizados implementados.
	2. Generación de hashes validos SHA256 de archivos firmados.
	3. Generación de GUID único.

Selección de tecnologías de autenticación.

La selección de tecnologías para este proyecto se fundamenta en criterios de transparencia, interoperabilidad, escalabilidad y cumplimiento de estándares de seguridad. A continuación, se justifica cada tecnología seleccionada:

- Apache Libcloud; Apache Libcloud destaca por su documentación detallada, lo que permite a los desarrolladores entender claramente cómo se manejan y protegen los datos sensibles durante las interacciones con los proveedores de servicios Cloud. Además de que ofrece una API unificada para múltiples servicios Cloud, simplificando la gestión de archivos en entornos distribuidos donde

múltiples proveedores de almacenamiento en la nube pueden funcionar de forma intercambiable. Se procura siempre el interés del usuario al no limitar las opciones funcionales de la solución a un único proveedor privado de servicios como una dependencia limitante.

- Authlib; El principal factor para esta selección es la importancia en la libertad creativa y colaborativa del producto final, Authlib al estar bajo una licencia BSD, permite su uso y modificación sin restricciones significativas, lo que lo hace ideal para integrarse en soluciones comerciales y de código abierto. Además, claramente están las condiciones de compatibilidad con estándares conocidos y ampliamente utilizados: En este caso el objetivo son los protocolos OAuth 2.0 y OpenID 1.0.
- OAuth 2.0 y OpenID 1.0; Estas tecnologías son estándares de facto para autenticación y autorización en sistemas web de la actual generación de internet, utilizadas por proveedores como Google, Microsoft, y Amazon. La gran comunidad de desarrolladores garantiza soporte continuo y amplia variedad de recursos de documentación sobre la cual se pueden desarrollar soluciones derivadas. El conjunto de estos 2 protocolos permite desarrollar flujos de autenticación personalizados incluyendo capacidades de gestión de identidad de usuarios. La inspiración original viene de una solución similar implementada en Estonia llamada Authentigate.
- Adopción de tecnologías Cloud Native; En vista de la falta de iniciativa pública y esfuerzos centralizados por parte de las autoridades competentes, surge la necesidad de buscar una alternativa de software que cumpla con objetivos básicos

de accesibilidad, cumplimiento de estándares y separación de responsabilidades, en pro de maximizar las probabilidades de adopción masiva de la solución asegurando entornos seguros. “Masificación” es la clave para justificar sostenibilidad en cuanto al esfuerzo invertido en desarrollar y mantener software de código abierto (entre más de use la herramienta, más provechosa es la inversión del esfuerzo realizado). El uso de servicios Cloud-native, nos permite además desarrollar las funciones meramente operativas y algorítmicas de software suponiendo de antemano una base sólida de soporte en estándares internacionales, directamente proveídos por los principales proveedores de infraestructura y servicios en la nube. Esto reduce riesgos asociados al manejo directo de infraestructura, como errores de configuración que podrían comprometer la seguridad de la solución, factores que de alguna u otra manera suman a la facilidad de adopción por parte de terceros.

Descripción de la arquitectura propuesta.

La base de la arquitectura del sistema es “Cloud Native”. Esto implica que a nivel de software se tiene que contemplar una clara independencia de responsabilidades orientándose al desarrollo de microservicios.

La estructuración interna de las diferentes capas de software deben seguir una clara separación estricta entre componentes, mediante el uso de definición de interfaces que faciliten la comunicación horizontal entre cada uno de los componentes que conformen la totalidad del sistema.

No se contempla la necesidad de implementar una base de datos en la solución para que esta pueda cumplir exitosamente con las descripciones contempladas en los criterios de aceptación definidos en los requerimientos técnicos. Es más, debido a que la solución propuesta tenga como objetivo principal buscar maximizar el proceso de adopción de la Firma Digital, implementar una base de datos sin una justificante considerable podría simplemente entorpecer el objetivo principal de la herramienta, creando barreras de implementación por temas de aumento en costes y complejidad técnica.

Debido a que el sistema de Firma Digital no cuenta como un sistema de categorización y que todos los certificados de un mismo nivel de la cadena de confianza cuentan con el mismo peso en términos de capacidad jurídica, un sistema resultante de autenticación de usuarios partiría entonces de una base de privilegios plana, donde todos los usuarios debidamente autenticados tengan el mismo nivel de privilegios en su estado inicial, esta particularidad del sistema podría trasladarse al funcionamiento de la solución propuesta, en pro de simplificar la solución y optar por un minimalismo técnico que facilite el proceso de adopción, de esta forma, se reduce la complejidad de la solución, relegando a cada una de las aplicaciones clientes a realizar su manejo individual de roles y permisos.

De esta forma, la configuración y demás necesidades básicas de persistencia de datos podría ser cubierta por los mismo servicios de almacenamiento en la nube, en un sistema básico de almacenamiento de datos en objetos JSON (JavaScript Object Notation).

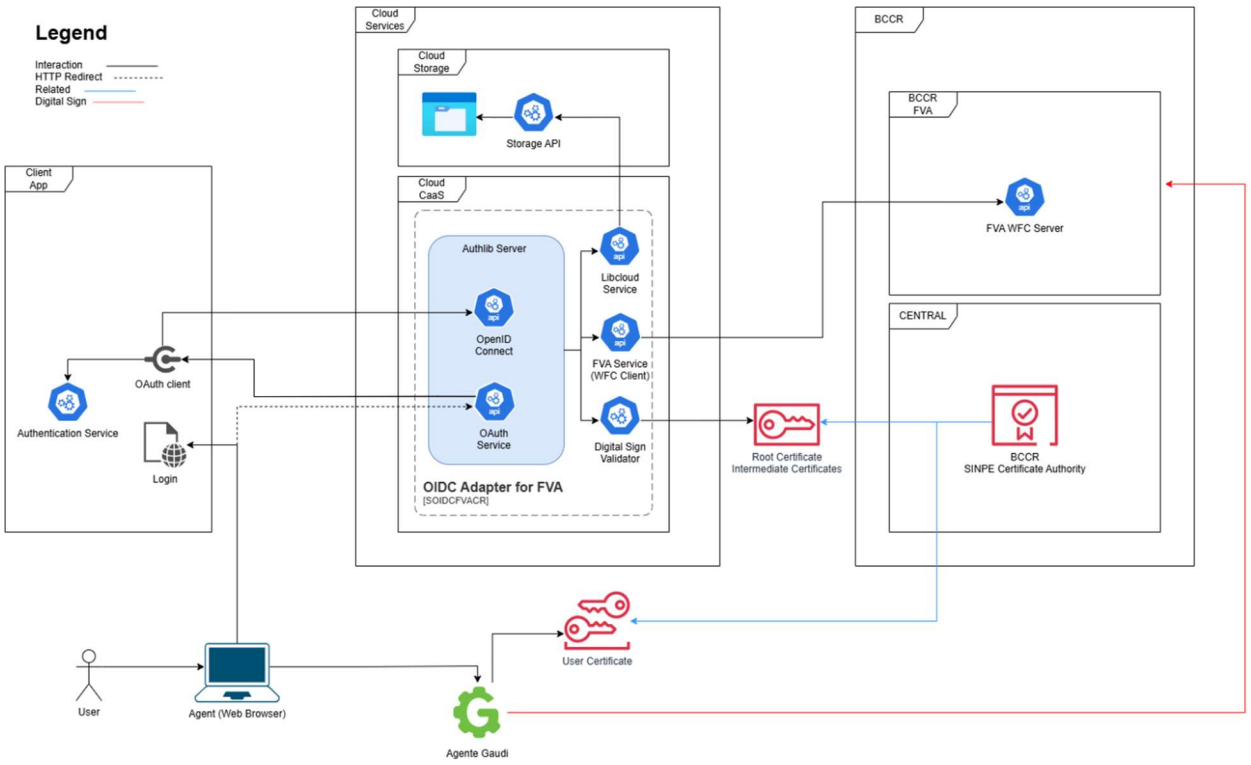


Figura 4. Diagrama de arquitectura de la propuesta SOIDCFDCR (Autoría propia)

A continuación una explicación detallada del diagrama de arquitectura propuesto.

- OIDC Adapter for FVA: Es el nombre informal de la solución propuesta en este documento, también conocida como SOIDCFDCR.
- Cloud CaaS: “Containerization as a Service” se refiere a la plataforma de servicios Cloud Native que se utilizan para desplegar aplicaciones en contenedores.
- Cloud Services: Plataforma de servicios Cloud, usualmente representan una red virtualizada (VLAN) donde se ejecutan y despliegan los diferentes servicios que el usuario solicite, dichas VLAN son generalmente aisladas y entornos seguros para la interconexión local de servicios.
- WFC: Es el protocolo de comunicación utilizado en el API definido por el sistema de Firmador Validador y Autenticador del BCCR.

- Agente GAUDI, es el nombre del paquete de software y drivers utilizados para la correcta utilización de los certificados físicos de Firma Digital dentro del sistema FVA del BCCR.

El funcionamiento de la solución se da gracias a la interacción de diferentes sistemas y servicios externos necesarios para poder hacer llegar los datos necesarios de identidad de los usuarios hasta los aplicativos clientes de terceros.

El proceso genérico de caso de uso de este modelo se puede resumir de la siguiente forma:

- El usuario accede a través de su dispositivo a la página de Login del aplicativo cliente al cual quiere ingresar. Dicha página de Login lo redirecciona al servicio OAuth 2.0 que es parte de los servicios de SOIDCFDCR y el navegador despliega la interfaz gráfica de dicho servicio.
- La interfaz gráfica de OAuth 2.0 solicita al usuario su número de identidad nacional (número de cedula), para así activar el proceso de FVA.
- A través del cliente de FVA integrado en SOIDCFDCR, se invocan los servicios del FVA del BCCR y se envía una solicitud de Firma Digital sobre un documento de autorización XML con los datos respectivos de autorización de la sesión (Ajustándose a los lineamientos y estándares de uso de FVA de acuerdo a la documentación del BCCR)
- El FVA habilita el proceso de Firma Digital a través del cual el usuario firma y certifica con su documento XML de autorización (debidamente firmado) que SOIDCFDCR queda autorizado para generar los Access Tokens para el aplicativo

cliente y además le permite compartir la información personal del usuario contenida en el certificado público del usuario.

- SOIDCFDCR procede a generar un hash SHA256 del archivo firmado y procede a guardar el documento en el Cloud Storage a través de Apache Libcloud, generando en el proceso un Identificador Único (GUID) con el cual identificar el archivo en el repositorio de almacenamiento.
- SOIDCFDCR Genera un JWT con los datos del usuario autenticado y siguiendo los estándares definidos en los estándares de OAuth y los requerimientos técnicos de este proyecto. Genera un Access Token temporal y se lo envía al cliente OAuth del aplicativo cliente.
- El aplicativo cliente, siguiendo los lineamientos de OAuth, puede utilizar el Access Token temporal compartido por SOIDCFDCR para consultar el API OpenID Connect para obtener el JWT con los datos de autenticación del usuario. Dicho JWT contiene toda la información necesaria para que el proceso de autenticación y autorización continue por parte del aplicativo cliente de terceros.

Las ventajas de esta arquitectura general es que permite que aquellos agentes y terceros interesados en realizar el proceso de implementación, pueden seleccionar las soluciones en la nube de su interés para realizar el proceso, además de que también le permite cumplir con las regulaciones normativas impuestas por el MICITT y el BCCR sin la necesidad de realizar cambios significativos en sus aplicativos, ya que la complejidad de del manejo de los archivos firmados y los procesos de validación de la Firma Digital se encuentra encapsulado en SOIDCFDCR y no en el aplicativo cliente. El cual, para cumplir del todo con los requisitos normativos únicamente tiene que salvaguardar de manera

persistente y auditable el Identificador Único que le permita consultar el archivo firmado que autoriza al proceso de autenticación (XML firmado que autoriza la sesión), así como el Hash que garantiza la integridad de dicho archivo.

Descripción de los módulos del prototipo.

Authlib Server: Componente principal de la solución, modulo encargado de implementar y configurar de manera correcta las herramientas Authlib, así como desarrollar los flujos de autenticación personalizados requeridos para integrar la funcionalidades de los demás módulos de la solución como parte del proceso de autenticación del servicio OIDC.

Libcloud Service: Modulo tipo API encargado de abstraer la complejidad de uso y comunicación con las diferentes plataformas de servicio de almacenamiento en la nube.

FVA Service: Modulo encargado de implementar el cliente WCF para el consumo de los servicios del sistema FVA del BCCR. Además de ser el módulo encargado de abstraer la complejidad de la comunicación en cumplimiento con las normativas del BCCR en su documentación de Estándar Electrónico; firmador validador y autenticador.

Digital Sign Validator: Componente encargado de abstraer y encapsular toda la complejidad de las librerías y algoritmos necesarios para realizar el debido proceso de validación de autenticidad de los archivos firmados, así como realizar el proceso de validación de integridad de los archivos almacenados en el Almacenamiento en la Nube.

4.2.2 Casos de uso de implementación del Middleware propuesto

El principal caso de uso de implementación de esta herramienta sería en aquellos escenarios particulares donde las organizaciones pequeñas, ya sea por limitaciones

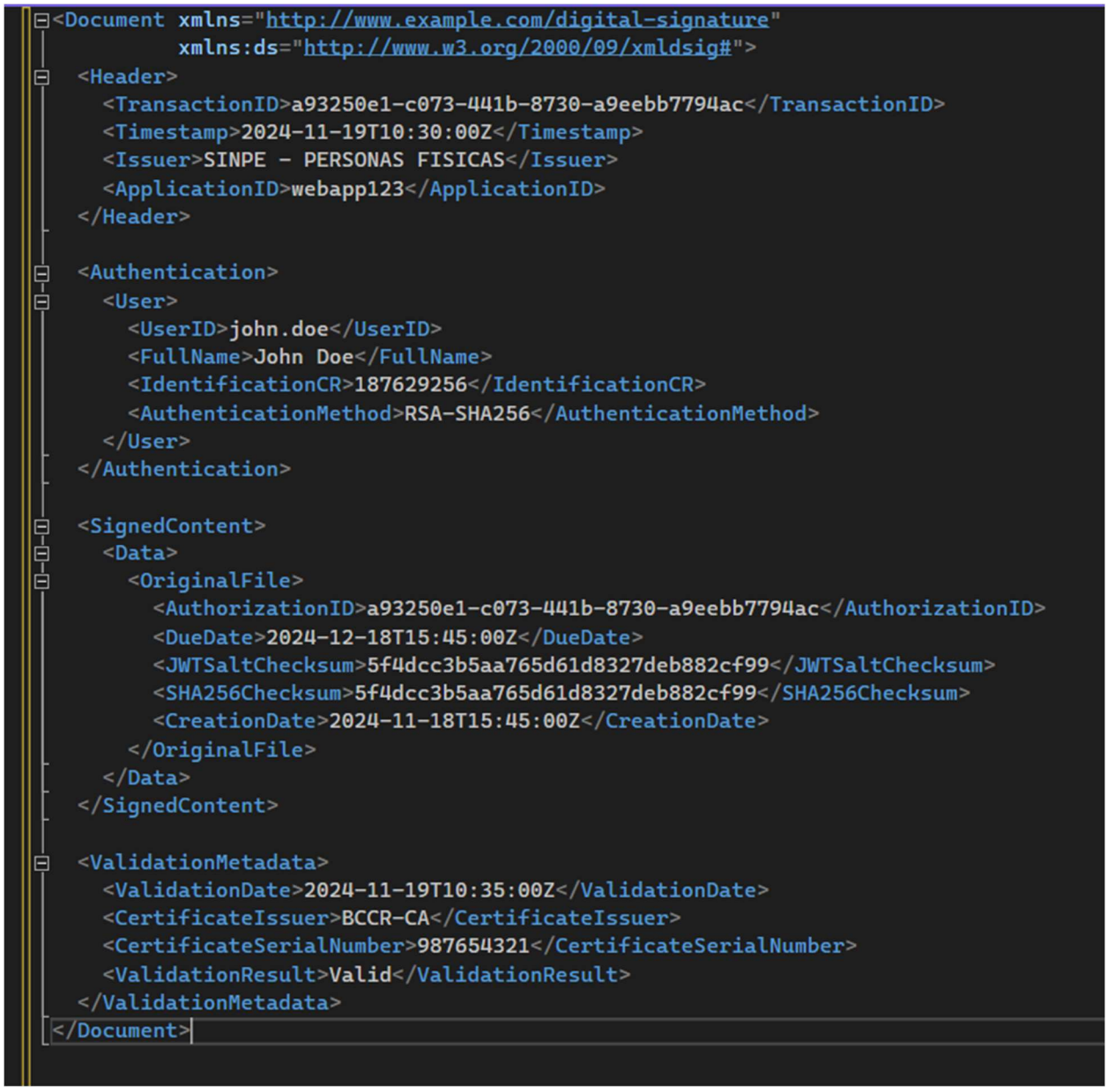
presupuestarias o técnicas, no tienen los recursos para desarrollar desde cero una solución propia de autenticación y Firma Digital, pero necesitan implementar una herramienta confiable y alineada con los estándares internacionales. Estas organizaciones deben contar eso sí; con condiciones técnicas mínimas, como conocimiento básico de uso de servicios en la Nube, un aplicativo con soporte para protocolos OIDC (OpenID Connect), y al menos los recursos iniciales necesarios para contratar servicios los servicios Clousd que faciliten el despliegue y la escalabilidad de la herramienta (dando por entendido de que dichas organizaciones deben cumplir todos los requisitos administrativos del BCCR para el uso del FVA).

Además, otra idea fundamental de este proyecto es fomentar el desarrollo colaborativo de código abierto, permitiendo que una comunidad diversa contribuya con mejoras y nuevas funcionalidades. Este enfoque no solo reduce los costos de desarrollo y mantenimiento, sino que también mejora y amplía la capacidad de innovación del mercado, al facilitar que múltiples actores aprovechen y adapten la herramienta a sus necesidades particulares. Asimismo, al tratarse de un proyecto de código abierto, se impulsa un proceso de adopción basado en transparencia y confianza, elementos clave para promover su adopción en sectores sensibles como el financiero, gubernamental y empresarial.

Finalmente, esta herramienta tendría el potencial de democratizar el acceso a soluciones avanzadas de autenticación y Firma Digital, incluso siendo utilizado en entornos académicos o educativos como en compañas de alfabetización.

Integración con Firma Digital en Costa Rica

El sistema de autenticación OIDC puede tener una integración lógica e interrelacionar de los datos entre los datos utilizados para la autenticación web del usuario y la validación de la Firma Digital, por ejemplo, SOIDCFDCR permitiría agregar una validación del JWT generado para la autenticación del usuario, esto quiere decir que, se puede aprovechar una sección fija del JWT de sesión, para que, en conjunto de una referencia bidireccional se permita generar un hash de validación de la integridad de un subconjunto de valores clave del JWT, para así agregar dicho hash generado en una sección especializada del documento XML Digitalmente Firmado, de manera que, pueda existir una validación de integridad mutua y bidireccional entre la Firma Digital generada (XML firmado) y el JWT de autenticación generado.



```xml
<Document xmlns="http://www.example.com/digital-signature"
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <Header>
    <TransactionID>a93250e1-c073-441b-8730-a9eebb7794ac</TransactionID>
    <Timestamp>2024-11-19T10:30:00Z</Timestamp>
    <Issuer>SINPE - PERSONAS FISICAS</Issuer>
    <ApplicationID>webapp123</ApplicationID>
  </Header>

  <Authentication>
    <User>
      <UserID>john.doe</UserID>
      <FullName>John Doe</FullName>
      <IdentificationCR>187629256</IdentificationCR>
      <AuthenticationMethod>RSA-SHA256</AuthenticationMethod>
    </User>
  </Authentication>

  <SignedContent>
    <Data>
      <OriginalFile>
        <AuthorizationID>a93250e1-c073-441b-8730-a9eebb7794ac</AuthorizationID>
        <DueDate>2024-12-18T15:45:00Z</DueDate>
        <JWTSaltChecksum>5f4dcc3b5aa765d61d8327deb882cf99</JWTSaltChecksum>
        <SHA256Checksum>5f4dcc3b5aa765d61d8327deb882cf99</SHA256Checksum>
        <CreationDate>2024-11-18T15:45:00Z</CreationDate>
      </OriginalFile>
    </Data>
  </SignedContent>

  <ValidationMetadata>
    <ValidationDate>2024-11-19T10:35:00Z</ValidationDate>
    <CertificateIssuer>BCCR-CA</CertificateIssuer>
    <CertificateSerialNumber>987654321</CertificateSerialNumber>
    <ValidationResult>Valid</ValidationResult>
  </ValidationMetadata>
</Document>
```

(Grafico 1) Ejemplo de XML firmado (elaboración propia)

La posibilidad de personalizar la plantilla de documento XML digitalmente firmado es prácticamente infinita, en este caso por ejemplo podríamos agregar un valor conocido como JWTSaltChecksum el cual contenga el hash de validación de atributos clave del JWT que estemos utilizando.

(Grafico 1) Ejemplo de JWT valido (elaboración propia)

Mientras tanto, el JWT generado por el OIDC puede contener los parámetros necesarios para poder realizar un seguimiento auditable de los archivos firmados que se utilizaron para autorizar el proceso de autenticación web. En este ejemplo los valores SignedFileGUID y SignedXMLChecksum permiten hacer un análisis auditable de los archivos firmados, manteniendo una referencia única que permita localizar el archivo (SignedFileGUID), así como comparando un hash SHA256 para la validación de la integridad de dicho archivo firmado. Además, se agrega un TrasactionID que también funciona como referencia bidireccional entre ambos documentos, donde el TrasactionID simplemente significa un valor único aleatorio predefinido y acordado previo al proceso de creación de cada uno de los 2 documentos en cuestión, un valor de referencia que permite crear una conexión mutua e inmutable entre ambos documentos (debido a los proceso de validación de Hashes).

Adaptaciones para conformidad con normativa costarricense

Realizando un análisis a la documentación proporcionada por el BCCR y el MICITT se determina que la propuesta de arquitectura y modelo de desarrollo de software involucrada en este proyecto (SOIDCFDCR) permite cumplir con efectividad las normativas técnicas establecidas en el Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, así como a las disposiciones dadas en el Estándar Electrónico; Firmador Validador y Autenticador del BCCR, simplemente con facilitar las secciones especializadas en la interfaz del usuario para cumplir con este fin.

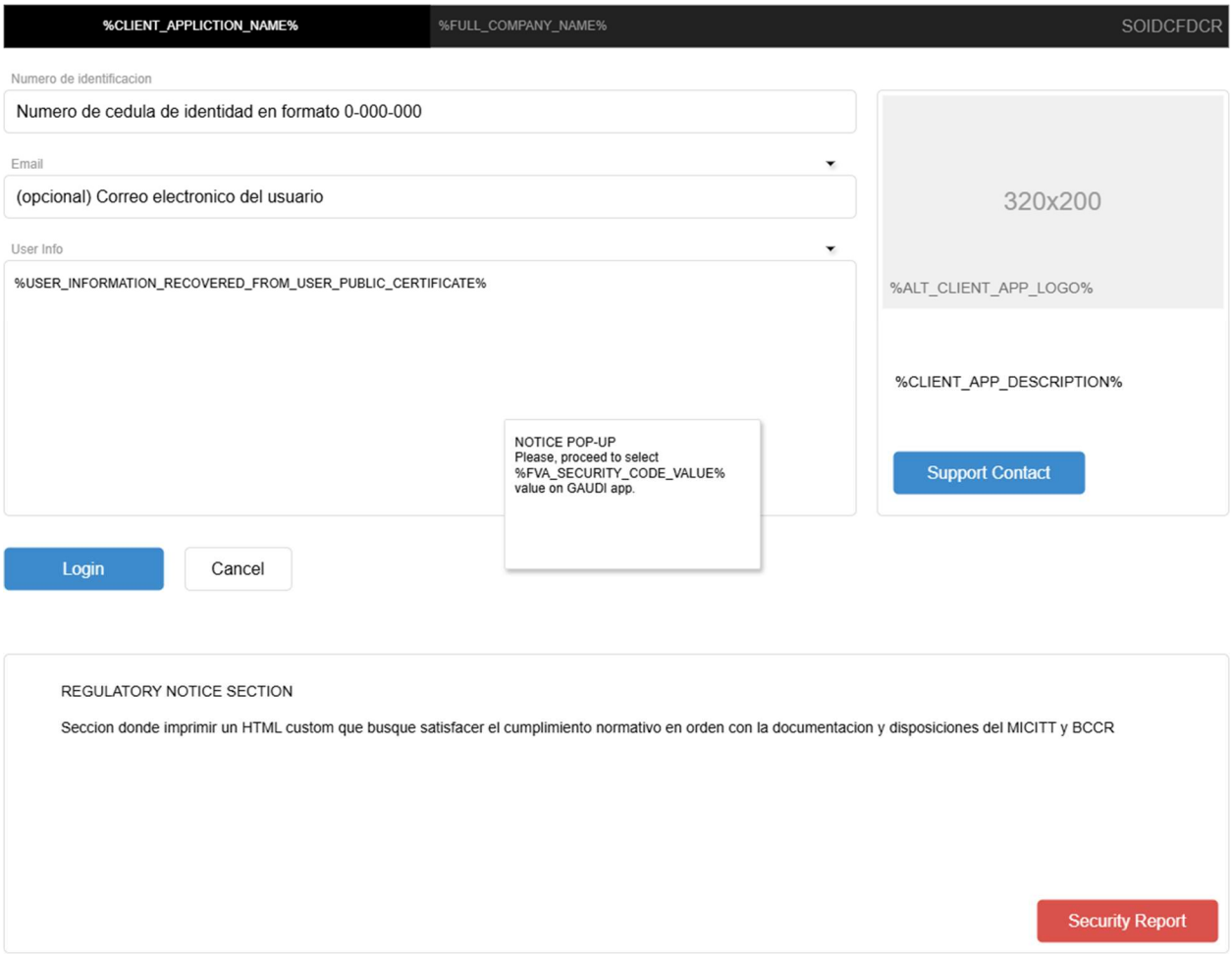


Figura 5. Esquema de propuesta de interfaz gráfica para SOIDCFDCR (Elaboración propia)

Además, acorde a las necesidades de adaptarse a requerimientos y normativas cambiantes para poder cumplir con una correcta implementación flexible (que facilite los cambios necesario), se propone una estructura de interfaz gráfica que permite a los administradores de SOIDCFDCR modificar de manera fácil y rápida una sección dinamica de la interfaz directamente orientada al contenido o mensajes regulatorios que sean definido por los entes reguladores competentes (MICITT y BCCR).

4.2.3 Análisis de Viabilidad Técnica y Normativa

SOIDCFDCR presenta una viabilidad técnica y normativa sólida. Su implementación no solo está alineada con los marcos regulatorios nacionales, sino también toma y adopta los mismo principios que su homólogo en Estonia. Demas también aprovecha los estándares internacionales y prácticas tecnológicas modernas que puedan ofrecer la arquitectura Cloud Native, ofreciendo una solución escalable, segura y accesible. Eso sin mencionar que existen otros antecedente de implementación de soluciones homologas con especificaciones muy similares al nuestro, como es el caso de Estonia y su sistema Authentigate.

Por último, haciendo un análisis de la Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027, se comprende la preocupación detrás de las autoridades del país a la hora de implementar tecnologías en infraestructuras críticas que puedan comprometer la ciberseguridad del país y sus instituciones, por tanto, hay que contemplar que si bien el modelo propuesto cumple correctamente con los requerimientos normativos, en un caso

de implementación real en infraestructuras criticas requeriría de esfuerzos exhaustivos en el cumplimiento técnico y estricto de estándares de control de calidad y medidas de evaluación de seguridad informática. Procedimientos que deben ser auditados durante todo el ciclo de vida de un producto para así asegurar que el software final no se vea comprometido durante su tiempo de vida útil. Estas son consideraciones que no están evaluadas y no forman parte de la iniciativa de este proyecto, pero cabe recalcar que sobrellevar dichas limitaciones requeriría de un esfuerzo organizacional e institucional, lo que actualmente no ocurre en Costa Rica, soluciones que tengan como objetivo ser integradas en arquitecturas institucionales o criticas requieren obligatoriamente de seguimiento institucional, y por ende, asignación de fondos y financiamiento.

Limitaciones y consideraciones de implementación real en ambientes productivos.

Acá es donde la propuesta del proyecto se torna negativa y se afronta limitaciones e impedimentos, más concretamente aquellos relacionados al entorno de desarrollo de tecnologías públicas en Costa Rica y su uso en entornos productivos.

La propuesta SOIDCFDCR tiene un problema enorme en torno a cumplir sus objetivos ideales planteados en el documento (impulsar la masificación de tecnologías de Firma Digital), existen problemas y limitaciones de distintas indoles, pero la gran mayoría coinciden en un único punto clave de desventaja competitiva a nivel país; La falta de seguimiento institucional a propuestas populares de tecnología e innovación en software de interés público.

Por tanto podemos resumir y finalizar el análisis concluyendo que si bien la solución y modelo SOIDCFDCR tiene el potencial para convertirse en una herramienta que impacte realmente los índices de adopción de la Firma Digital en Costa Rica, lo cierto del caso es que no podemos recomendar la utilización de este modelo en entornos productivos de sistemas críticos (o en grande instituciones) BAJO NINGUNGA CIRCUNSTANCIA donde no se cumplan o implementen las debidas medidas de control de calidad y seguridad de desarrollo de software, con su debido financiamiento para procesos estrictos y auditables.

Al final del día, en términos de limitaciones a este tipo de iniciativas de innovación; la debilidad más grande de Costa Rica frente a otros modelos como el estonio, es que en Estonia es el propio estado y sus autoridades competentes los que adoptan y lideran proyecto de innovación tecnológica (software de código abierto) que terminan siendo parte del capital de software que generan valor añadido a sus propias instituciones.

5. Conclusiones

1. En torno al estado de avance actual en la adopción de Firma Digital en Costa Rica, podemos destacar 2 principales hallazgos:
    - El ritmo del proceso de adopción de la Firma Digital ha sido inconsistente a lo largo de los años desde la apertura popular del servicio en 2008, los datos determinan que el avance no ha sido progresivo y difiere mucho de una progresión lineal, a 14 años del lanzamiento del servicio solo una pequeña minoría del total cuenta con el beneficio. Se determina entonces que el

comportamiento actual de adopción imposibilita un escenario real de adopción masiva de la herramienta.

- Estudios arrojan que para el año 2019 solo 7 de 81 municipalidades utilizaban siquiera la tecnología de Firma Digital, un dato alarmante que se suma a la preocupación de autoridades legislativas que mencionan como la falta de mecanismo administrativos de seguimiento y control del uso de la herramienta han provocado una situación de default técnico donde es imposible determinar el correcto cumplimiento normativo en el sector publico, induciendo a la propia administración pública a un estado constante de incumplimiento y subversión administrativa.

2. En el caso de Estonia se puede determinar que el éxito de su modelo de E-Government y Firma Digital radica en iniciativas de subsidios tributarios y en que la capacidad de la administración pública por adoptar y liderar iniciativas de desarrollo de software que busquen sacarle provecho a su inversión tecnológica. Cabe destacar que gran parte de las soluciones de software implementadas se basan en proyectos de código abierto liderados por el mismo gobierno mediante la subcontratación de empresas especializadas.
3. Los datos arrojan que durante el periodo de pandemia y crisis sanitaria, el manejo de la pandemia por parte de ambos países eran similares en cuanto a la efectividad real de las medidas y restricciones tomadas y su impacto en el sistema sanitario. En lo que si difieren los datos es en el impacto económico reflejado durante la época de pandemia, donde Costa Rica tardo aproximadamente 2 años más que su contraparte en mostrar mejoras que pudieran verse reflejadas en los

datos interanuales de crecimiento económico. Se refleja además en comunicados oficiales que para el año 2019 Estonia ya contaba con niveles de adopción de Firma Digital cercanas al 99%, esto fue un factor clave que permitió al gobierno imponer medidas sanitarias de forma más expedita y con un mayor margen de toma de decisiones.

4. Se confirma mediante análisis técnicos la posibilidad de implementar exitosamente tecnologías Web y software de código abierto, adaptando otros estándares existentes a la implementación de la Firma Digital, en este caso mediante el proyecto Firmador Autenticador y Validador del Banco Central de Costa Rica. La investigación también arrojo antecedentes de proyectos similares implementados en Estonia basados concretamente en los protocolos OAuth 2.0 y OpenID Connect.
5. Se confirma mediante el ejercicio de estudio y la propuesta experimental del diseño prototipo, que no existen limitaciones técnicas en cuanto a la correcta implementación de tecnologías web de código abierto al actual entorno de trabajo de la Firma Digital en Costa Rica, conclusión soportada también por antecedentes técnicos encontrados en el caso Estonio (jurisdicción con regulaciones tencias más estrictas a la nuestra debido a su integración con la Unión Europea).

6. Recomendaciones

1. Evaluar la posibilidad de que mediante control político u otros mecanismos de participación ciudadana se pueda abordar la situación de falta de medios de

control y evaluación sobre el debido cumplimiento de las normativa administrativa de Firma Digital. Incluso se podría argumentar la posibilidad de utilizar la vía judicial como medio para imponer acciones remediales en el órgano ejecutivo del estado.

2. Se podrían contemplar iniciativas populares lideradas por instituciones académicas, organizaciones gremiales, colegios profesionales (u otro tipo de organizaciones), que busquen orientar esfuerzos conjuntos al desarrollo de alianzas público-privadas que involucren a las autoridades de la administración pública en actividades de control y seguimiento en proyectos de desarrollo de software libre de interés público. Con los correctos canales de comunicación y la intervención de autoridades públicas competentes se podría hacer un mejor uso de los recursos académicos al redirigir esfuerzos y concentrarlos en temas de interés nacional.
3. Viendo los resultados de los análisis comparativos y los hallazgos encontrados en los demás estudios académicos referenciados en este proyecto, es claro poder diferenciar que el principal problema y el más inmediato que debemos abordar en Costa Rica es el problema de alfabetización digital. Este tema es clave si queremos realmente cambiar la percepción popular y la forma con la cual queremos abordar en un futuro la problemática que conlleva el rezago tecnológico en temas de eficiencia administrativa, burocracia y accesibilidad a servicios. Si Costa Rica se visualiza realmente como un futuro país digitalizado al estilo Estonia, es imperante incorporar a la academia e instituciones educativas a impartir campañas de alfabetización digital. De lo contrario, Costa Rica seguiría

estando en una situación vulnerable frente a escenarios de crisis como el del COVID-19.

4. En cuanto a las iniciativas de innovación en torno a la implementación de nuevos estándares y tecnologías al entorno de trabajo actual de E-Government, lo cierto es que lo ideal sería que estas iniciativas sean lideradas de forma centralizada por las propias autoridades públicas competentes, ya sea de forma directa o a través de subcontrataciones de servicios. Otra alternativa más realista y adaptada al contexto actual de Costa Rica, es que sean las propias universidades e instituciones académicas las que tomen la batuta de organizar y redirigir iniciativas estudiantiles hacia una red interinstitucional de proyectos de software libre de interés público, así también como iniciativas que promuevan incluir en los planes educativos actividades relacionadas el aporte colaborativo de dichos proyectos de software libres. A su vez, por contraparte, no es recomendable invertir recursos en proyectos que no cuenten con un seguimiento ni soporte institucional detrás, esto debido a la vulnerabilidad operativa y financiera que enfrentan los proyectos sin patrocinio a la hora de querer certificar sus productos o acceder a servicios de auditoria especializada.
5. Se deberían de concentrar más esfuerzos en tropicalización de soluciones de software implementadas en jurisdicciones que cuenten con plataformas de E-Government homologas a la nuestra. En este caso por ejemplo, Estonia que presenta un sistema de Firma Digital homologo al nuestro y que también presenta avances notables en términos de Software implementado, podría funcionar como

una fuente importante de avances técnicos que podríamos implementar de forma local con un alto grado transparencia y factibilidad.

7. Referencias

Asamblea Legislativa de la Republica de Costa Rica. (2005). **Ley de Certificados, firmas digitales y Documentos Electrónicos**. La Gaceta. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=102972

Ministro de Ciencia, Tecnología y Telecomunicaciones. (2006). Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=56884&nValor3=103000&strTipM=TC

Ministro de Ciencia, Tecnología y Telecomunicaciones. (2014). Masificación de la implementación y el uso de la firma digital en el sector público costarricense. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=77067&nValor3=96446&strTipM=TC

Ministro de Ciencia, Tecnología y Telecomunicaciones. (2018). Mejoras en la eficacia del gasto público mediante el uso adecuado de tecnologías digitales en el sector público costarricense. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=87498&nValor3=114021&strTipM=TC

Banco Central de Costa Rica. (2024). **Estándar Electronico Firmador Validador y Autenticador Serie de Normas y Procedimientos**. https://www.bccr.fi.cr/firma-digital/DocFirmaDigital/EE_Firmador_Validador_Autenticador.pdf

Banco Central de Costa Rica. (2023).. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=56884&nValor3=103000&strTipM=TC

SK ID Solutions. (2024). **Authentigate Documentation**. https://github.com/SK-EID/authentigate-documentation

OpenID Foundation. (2024). **How OpenID Connect Works**. https://openid.net/developers/how-connect-works/

M. Jones, D. Hardt. (2012). **The OAuth 2.0 Authorization Framework: Bearer Token Usage** (RFC 6750). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc6750

D. Hardt. (2012). **The OAuth 2.0 Authorization Framework** (RFC 6749). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc6749

SK ID Solutions. (2024). **Smart-ID Documentation**. https://github.com/SK-EID/smart-id-documentation

H. Yang. (2024). Authlib: Python Authentication. https://docs.authlib.org/en/v1.3.2/

ISO/IEC 27001:2022. (2022). ISO. https://www.iso.org/standard/27001

Microsoft. (2023) What is Cloud Native?. https://github.com/dotnet/docs/blob/main/docs/architecture/cloud-native/definition.md

The Apache Software Foundation. (2023). Apache Libcloud's documentation. https://libcloud.readthedocs.io/en/v3.8.0/index.html

Internet Assigned Numbers Authority. (2024). JSON Web Token (JWT). https://www.iana.org/assignments/jwt/jwt.xhtml

D.Shin. (2024) Python Domain-Driven-Design(DDD) Example. https://github.com/qu3vipon/python-ddd

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). Estrategia Nacional de Ciberseguridad, Costa Rica 2023-2027. https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

Nordic Institute for Interoperability Solutions. (2018). X-Road as a Platform to Exchange MyData. https://www.niis.org/blog/2019/10/30/x-road-as-a-platform-to-exchange-mydata

R.Raudla. (2020). Estonian response to COVID-19 pandemic: learning, cooperation, and the advantages of being a small country. Tallinn University of Technology. https://www.redalyc.org/journal/2410/241066211008/html/

Estonia Ministry of Foreign Affairs. (2020). Estonia and Singapore call for support for global digitalization. https://vm.ee/en/news/estonia-and-singapore-call-support-global-digitalisation

L.Madrigal. (2022). Congreso autoriza en definitiva al TSE a cobrar por reposición de cédulas de identidad. Delfino. https://delfino.cr/2022/04/congreso-autoriza-en-definitiva-al-tse-a-cobrar-por-reposicion-de-cedulas-de-identidad

Banco Central de Costa Rica. (2024). Certificados de Personas Físicas, Emisores y costos. https://www.bccr.fi.cr/firma-digital/certificados-de-personas-f%C3%ADsicas/emisores-y-costos

O.Guevara, J.Cambronero. (2016) Proyecto de Ley, Adición de un articulo 9 Bis a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, N° 8220, para implementacion de Sede Digital en el sector público. Asamblea Legislativa de la Republica de Costa Rica. https://proyectos.conare.ac.cr/asamblea/20089.pdf

Ministro de Ciencia, Tecnología y Telecomunicaciones. (2024). Webinar: Firma Digital Certificada: Casos de Éxito y otros avances año 2024. https://www.youtube.com/watch?v=kAOLapZSr6A

Ministro de Ciencia, Tecnología y Telecomunicaciones. (2021). Informe Final de la Evaluación Física y Financiera de la Ejecución del Presupuesto 2020. https://www.micitt.go.cr/sites/default/files/presupuestos/Informe-de-Evaluacion-Anual-2020-MICITT.pdf

M.Gutierrez, M.Mejia, M.Solano. (2019). Análisis de la implementación de Firma Digital en servicios públicos: Los casos de las municipalidades de Santa Ana, Heredia y San José para el año 2019. Escuela de Administración Pública, Universidad de Costa Rica. https://repositorio.sibdi.ucr.ac.cr/server/api/core/bitstreams/fc17c9a6-1931-456f-9a21-db12e581e78d/content

Estonian Business and Innovation Agency. (2024). ID-card. https://e-estonia.com/solutions/estonian-e-identity/id-card/

Estonian Business and Innovation Agency. (2024). Smart ID. https://e-estonia.com/solutions/estonian-e-identity/smart-id/

M.Van de Poll. (2020). The History of Digital Identity in Estonia. CYBERNETICA. https://cyber.ee/resources/news/the-history-of-digital-identity-in-estonia/

R.Bartels, A.Mora, R.Villalon-Fonseca, G.Marin. (2020). Triple Helix PKI:Desarrollo de la firma digital en Costa Rica con lacooperaci´on Universidad-Industria-Gobierno. Universidad de Costa Rica. https://revistas.tec.ac.cr/index.php/memorias/article/view/4534/4104

United Nations. (2024). 2024 Revision of World Population Prospects. https://population.un.org/wpp/

L.Zarate. (2022). Cliente para conectar instituciones con BCCR FVA. https://github.com/Solvosoft/pyfva

I.Basile. (2020). Estonia's Digital Solutions to COVID-19. Foreign Policy Research Institute. https://www.fpri.org/article/2020/08/estonias-digital-solutions-to-covid-19/

Estonia Ministry of Foreign Affairs. (2020). Close the Digital Divides: the Digital Response to COVID-19. https://vm.ee/en/close-digital-divides-digital-response-covid-19

World Economic Forum. (2020). Estonia built one of the world's most advanced digital societies. During COVID-19, that became a lifeline. https://www.weforum.org/stories/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/

M.Cerdas. (2023). Así se puede solicitar la firma digital para móviles. El Financiero. https://www.elfinancierocr.com/finanzas/asi-puede-solicitar-la-firma-digital-para-moviles/CMLU6YJUHZAM3MEOEC53CO7FTY/story/

J.Herrera. (2024). JPS aclara que firma digital no será obligatoria para comprar lotería en línea. Teletica. https://www.teletica.com/nacional/jps-aclara-que-firma-digital-no-sera-obligatoria-para-comprar-loteria-en-linea_358494

Unión Europea. (2016). **Reglamento eIDAS (Reglamento UE N.º 910/2014)**. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910